

Guide de fonctionnement et
d'administration des systèmes

**Fujitsu SPARC M12 et
Fujitsu M10/SPARC M10**



Code du manuel: C120-E679-24FR
Mars 2018

Copyright © 2007, 2018, Fujitsu Limited. Tous droits réservés.

Oracle et/ou ses affiliés ont fourni et vérifié des données techniques de certaines parties de ce composant.

Oracle et/ou ses affiliés et Fujitsu Limited détiennent et contrôlent chacun des droits de propriété intellectuelle relatifs aux produits et technologies décrits dans ce document. De même, ces produits, technologies et ce document sont protégés par des lois sur le droit d'auteur, des brevets, et d'autres lois sur la propriété intellectuelle et des traités internationaux.

Ce document, le produit et les technologies afférents sont exclusivement distribués avec des licences qui en restreignent l'utilisation, la copie, la distribution et la décompilation. Aucune partie de ce produit, de ces technologies ou de ce document ne peut être reproduite sous quelque forme que ce soit, par quelque moyen que ce soit, sans l'autorisation écrite préalable d'Oracle et/ou ses affiliés et de Fujitsu Limited, et de leurs éventuels concédants de licence. Ce document, bien qu'il vous ait été fourni, ne vous confère aucun droit et aucune licence, exprès ou tacites, concernant le produit ou la technologie auxquels il se rapporte. Par ailleurs, il ne contient ni ne représente aucun engagement, de quelque type que ce soit, de la part d'Oracle ou de Fujitsu Limited, ou des sociétés affiliées de l'une ou l'autre entité.

Ce document, ainsi que les produits et technologies qu'il décrit, peuvent inclure des droits de propriété intellectuelle de parties tierces protégés par le droit d'auteur et/ou cédés sous licence par des fournisseurs à Oracle et/ou ses sociétés affiliées et Fujitsu Limited, y compris des logiciels et des technologies relatives aux polices de caractères.

Conformément aux conditions de la licence GPL ou LGPL, une copie du code source régi par la licence GPL ou LGPL, selon le cas, est disponible sur demande par l'Utilisateur Final. Veuillez contacter Oracle et/ou ses affiliés ou Fujitsu Limited. Cette distribution peut comprendre des composants développés par des parties tierces. Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie.

UNIX est une marque déposée de The OpenGroup.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés.

Fujitsu et le logo Fujitsu sont des marques déposées de Fujitsu Limited.

SPARC Enterprise, SPARC64, le logo SPARC64 et toutes les marques SPARC sont utilisées sous licence et sont des marques déposées de SPARC International, Inc., aux Etats-Unis et dans d'autres pays.

Tout autre nom mentionné peut correspondre à des marques appartenant à leurs propriétaires respectifs.

Si ce logiciel, ou la documentation qui l'accompagne, est concédé sous licence au Gouvernement des Etats-Unis, ou à toute entité qui délivre la licence de ce logiciel ou l'utilise pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique :

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Avis de non-responsabilité : les seules garanties octroyées par Oracle et Fujitsu Limited et/ou toute société affiliée de l'une ou l'autre entité en rapport avec ce document ou tout produit ou toute technologie décrits dans les présentes correspondent aux garanties expressément stipulées dans le contrat de licence régissant le produit ou la technologie fournis.

SAUF MENTION CONTRAIRE EXPRESSEMENT STIPULEE AU DIT CONTRAT, ORACLE OU FUJITSU LIMITED ET/OU LES SOCIETES AFFILIEES A L'UNE OU L'AUTRE ENTITE DECLINENT TOUT ENGAGEMENT OU GARANTIE, QUELLE QU'EN SOIT LA NATURE (EXPRESSE OU IMPLICITE) CONCERNANT CE PRODUIT, CETTE TECHNOLOGIE OU CE DOCUMENT, LESQUELS SONT FOURNIS EN L'ETAT. EN OUTRE, TOUTES LES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFACON, SONT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE. Sauf mention contraire expressément stipulée dans ce contrat, dans la mesure autorisée par la loi applicable, en aucun cas Oracle ou Fujitsu Limited et/ou l'une ou l'autre de leurs sociétés affiliées ne sauraient être tenues responsables envers une quelconque partie tierce, sous quelque théorie juridique que ce soit, de tout manque à gagner ou de perte de profit, de problèmes d'utilisation ou de perte de données, ou d'interruptions d'activités, ou de tout dommage indirect, spécial, secondaire ou consécutif, même si ces entités ont été préalablement informées d'une telle éventualité.

LA DOCUMENTATION EST FOURNIE "EN L'ETAT" ET TOUTE AUTRE CONDITION, DECLARATION ET GARANTIE, EXPRESSE OU TACITE, EST FORMELLEMENT EXCLUE, DANS LA MESURE AUTORISEE PAR LA LOI EN VIGUEUR, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFACON.

Table des matières

Préface xxix

Chapitre 1 Comprendre la présentation du SPARC M12/M10 1

- 1.1 Principes de base du SPARC M12/M10 1
- 1.2 Bases du microprogramme XSCF 5
 - 1.2.1 Présentation de XSCF 5
 - 1.2.2 Fonctionnalités de XSCF 5
 - 1.2.3 Fonctions de XSCF 10
 - 1.2.4 Mécanisme XSCF maître/de veille/esclave 14
 - 1.2.5 Différences entre les configurations XSCF par modèle 15
- 1.3 Configuration réseau 17
 - 1.3.1 Présentation des connexions réseau 17
 - 1.3.2 Numéros et fonctions des ports XSCF-LAN et pare-feu 23
- 1.4 Bases du microprogramme superviseur 25
- 1.5 Bases d'Oracle VM Server pour SPARC 25
- 1.6 Bases d'OpenBoot PROM 26

Chapitre 2 Connexion à / Déconnexion de XSCF 29

- 2.1 Connexion du terminal de gestion du système 29
 - 2.1.1 Connexion avec le port série 30
 - 2.1.2 Fonctions disponibles pour les terminaux de la connexion série 33
 - 2.1.3 Connexion avec un port XSCF-LAN 34

2.1.4	Fonctions disponibles pour les terminaux de la connexion XSCF-LAN	37
2.2	Connexion au Shell XSCF	38
2.2.1	Comment se connecter au shell XSCF avec une connexion série	39
2.2.2	Comment se connecter au shell XSCF avec une connexion SSH via XSCF-LAN	41
2.2.3	Comment se connecter au shell XSCF avec une connexion Telnet via XSCF-LAN	42
2.3	Déconnexion du shell XSCF	43
2.4	Connexion à XSCF Web	43
2.4.1	Éléments devant être définis à l'avance	44
2.4.2	Navigateurs pris en charge	44
2.4.3	Fonctions devant être activées dans le navigateur Web	44
2.4.4	Comment se connecter avec XSCF Web	45
2.5	Déconnexion de XSCF Web	46
2.6	Nombre d'utilisateurs pouvant se connecter	47
Chapitre 3 Configuration du système		49
3.1	Tâches préparatoires pour la configuration de XSCF	49
3.1.1	Tâches initiales avant configuration	49
3.1.2	Informations complémentaires	50
3.1.3	Interface utilisateur pour la configuration et méthode d'accès	50
3.1.4	Configuration de manière fluide	51
3.2	Comprendre le contenu des paramètres du microprogramme XSCF	52
3.2.1	Éléments de réglage destinés à l'utilisation du XSCF	52
3.2.2	Vérification du XSCF maître	53
3.2.3	Fonctions exécutables sur le XSCF de veille	55
3.2.4	Vérification détaillée des options de commande sur les pages de manuel	55

3.3	Configuration depuis le shell XSCF	56
3.4	Configuration depuis le XSCF Web	61
3.5	Création/gestion des utilisateurs XSCF	62
3.5.1	Comptes d'utilisateur XSCF	63
3.5.2	Mots de passe et stratégie de mot de passe	63
3.5.3	Types de privilège d'utilisateur	65
3.5.4	Vérification des éléments de réglage et des commandes liées aux comptes d'utilisateur XSCF	67
3.5.5	Procédure d'enregistrement d'un compte d'utilisateur XSCF	68
3.5.6	Vérification des utilisateurs enregistrés	69
3.5.7	Vérification/Modification de la stratégie de mot de passe	70
3.5.8	Ajout d'un compte d'utilisateur XSCF et réglage d'un mot de passe	72
3.5.9	Réglage d'un privilège d'utilisateur	74
3.5.10	Activation/Désactivation d'un compte d'utilisateur	74
3.5.11	Activation/Désactivation de la fonction de verrouillage d'identification	75
3.5.12	Gestion de comptes d'utilisateur XSCF à l'aide de LDAP	76
3.5.13	Gestion de comptes d'utilisateur XSCF à l'aide d'Active Directory	83
3.5.14	Gestion de comptes d'utilisateur XSCF à l'aide de LDAP sur SSL	101
3.6	Réglage de l'heure/date du XSCF	120
3.6.1	Compréhension de la relation entre l'heure du XSCF et l'heure des partitions physiques	121
3.6.2	Stratégie de gestion du temps d'un domaine logique	121
3.6.3	Vérification des éléments de réglage et commandes liés à l'heure	122
3.6.4	Réglage du fuseau horaire	122
3.6.5	Réglage de l'heure d'été	124
3.6.6	Réglage de l'heure du système	125

3.6.7	Synchronisation des heures du domaine de commande et du XSCF	126
3.6.8	Spécification du XSCF comme serveur NTP	127
3.6.9	Spécification du XSCF comme client NTP	128
3.6.10	Configuration des serveurs NTP utilisés par le XSCF	129
3.6.11	Configuration du tourniquet DNS du serveur NTP	131
3.6.12	Spécification/annulation de la préférence pour un serveur NTP	132
3.6.13	Réglage de la valeur de couche du XSCF	133
3.6.14	Modification de l'adresse de l'horloge locale du XSCF	134
3.7	Configuration du service SSH/Telnet pour la connexion à XSCF	136
3.7.1	Vérification des éléments de réglage et des commandes liés à SSH et Telnet	137
3.7.2	Activation/Désactivation des services SSH et Telnet	138
3.7.3	Réglage d'une clé d'hôte du service SSH	139
3.7.4	Enregistrement/Suppression d'une clé publique d'utilisateur pour le service SSH	140
3.7.5	Réglage du délai d'expiration des services SSH/Telnet	141
3.8	Configuration du service HTTPS pour la connexion à XSCF	142
3.8.1	Flux pour l'utilisation d'une autorité de certification externe ou sur l'intranet	143
3.8.2	Flux d'utilisation de l'autorité de certification autonome	143
3.8.3	Vérification des éléments de réglage et commandes liés à HTTPS	144
3.8.4	Activation/Désactivation du service HTTPS	144
3.8.5	Importation d'un certificat de serveur web à l'aide d'une autorité de certification sur l'intranet ou externe	145
3.8.6	Configuration d'une autorité de certification autonome et création d'un certificat de serveur web	147
3.9	Configuration du réseau XSCF	148
3.9.1	Utilisation de services via le réseau XSCF	148

3.9.2	Compréhension des interfaces du réseau XSCF	149
3.9.3	Configuration de l'interface réseau XSCF	150
3.9.4	Compréhension des sous-réseaux des groupes de réseaux	153
3.9.5	Compréhension des adresses IP définies avec SSCP	154
3.9.6	Vérification des éléments de réglage et des commandes liés au réseau XSCF	156
3.9.7	Flux de configuration du réseau XSCF	157
3.9.8	Activation/Désactivation du réseau XSCF et réglage des adresses IP de XSCF-LAN et des masques de réseau	159
3.9.9	Réglage de l'adresse IP de reprise	161
3.9.10	Définition d'une adresse IP de SSCP	162
3.9.11	Définition d'un nom d'hôte et d'un nom de domaine XSCF	165
3.9.12	Réglage de l'acheminement du XSCF	166
3.9.13	Paramétrage de DNS pour le XSCF	169
3.9.14	Réglage des règles de filtrage des paquets IP pour le réseau XSCF	171
3.9.15	Diffusion des réglages de réseau XSCF	172
3.9.16	Vérification de l'état de connexion au réseau XSCF	175
3.10	Configuration de l'audit pour renforcer la sécurité de XSCF	176
3.10.1	Mener un audit	176
3.10.2	Compréhension des termes liés à l'audit	177
3.10.3	Gestion des audits	177
3.10.4	Vérification des éléments de réglage et commandes liés à l'audit	179
3.10.5	Flux d'un audit	181
3.10.6	Affichage/Réglage de la stratégie d'audit	183
3.10.7	Activation/Désactivation de l'audit	185
3.10.8	Suppression des données de journal d'audit	185
3.10.9	Référencement d'un journal d'audit	187
3.10.10	Gestion du journal d'audit du XSCF de veille	187
Chapitre 4 Configuration du système selon le type d'utilisation		189

4.1	Paramétrage / vérification de l'altitude du système	189
4.1.1	Paramétrage de l'altitude du système	190
4.1.2	Vérification des réglages de l'altitude du système	190
4.2	Contrôle de démarrage du système	191
4.2.1	Réglage/Vérification du délai de préchauffage	191
4.2.2	Réglage/Vérification du temps d'attente au démarrage	193
4.3	Activation / désactivation de la double alimentation électrique	194
4.3.1	Activation de la double alimentation électrique	195
4.3.2	Désactivation de la double alimentation électrique	195
4.3.3	Vérification du réglage de la double alimentation électrique	196
4.4	Diminution de la consommation électrique	197
4.4.1	Réglage de la valeur de limite supérieure de la consommation électrique	197
4.4.2	Gestion en cas d'anomalie au niveau de la température/d'une charge due à une alimentation anormale	200
4.4.3	Diminution de la consommation électrique du matériel inutilisé ou peu utilisé	200
4.5	Connexion d'un lecteur de DVD	205
4.5.1	Utilisation d'un lecteur DVD externe	205
4.5.2	Utilisation d'un lecteur DVD externe pour installer Oracle Solaris	208
4.6	Utilisation du stockage à distance	212
4.6.1	Qu'est-ce que le stockage à distance ?	213
4.6.2	Configuration réseau du stockage à distance	214
4.6.3	Moyens d'utilisation du stockage à distance	221
4.6.4	Configuration d'exploitation requise des terminaux et des navigateurs	223
4.6.5	Réglages d'Oracle Solaris	226
4.6.6	Versions logicielles du stockage à distance	226
4.6.7	Chemins d'accès et alias des dispositifs de stockage à distance	227

- 4.6.8 Remarques sur le stockage à distance 227
- 4.6.9 Flux pour l'utilisation du stockage à distance 229
- 4.6.10 Configuration du XSCF-LAN utilisé avec le stockage à distance 231
- 4.6.11 Statut du serveur de stockage à distance XSCF 232
- 4.6.12 Connexion aux supports en utilisant le stockage à distance 234
- 4.6.13 Utilisation du stockage à distance depuis Oracle Solaris 240
- 4.6.14 Déconnexion du support/Fin du stockage à distance 243
- 4.6.15 Autres points à noter et opérations 247

Chapitre 5 Activation de processeur 251

- 5.1 Concepts de base d'une activation de processeur 251
- 5.2 Clé d'activation de processeur 253
- 5.3 Ajout des ressources du cœur du processeur 254
 - 5.3.1 Processus jusqu'à l'ajout d'un cœur de processeur à une partition physique et un domaine logique 255
 - 5.3.2 Achat d'activation de processeur supplémentaire 255
 - 5.3.3 Vérification de la clé d'activation du processeur 256
 - 5.3.4 Enregistrement d'une clé d'activation du processeur 256
 - 5.3.5 Attribution de ressources de cœur de processeur à une partition physique 257
 - 5.3.6 Ajout de cœurs de processeurs à un domaine logique 260
 - 5.3.7 Enregistrement des informations de configuration du domaine logique 261
- 5.4 Suppression des ressources du cœur du processeur 261
 - 5.4.1 Processus de suppression d'une activation de processeur 261
 - 5.4.2 Suppression des cœurs de processeurs de domaines logiques 262
 - 5.4.3 Déconnexion de ressources de cœur du processeur d'une partition physique 262
 - 5.4.4 Vérification de la clé d'activation de processeur à supprimer 263

5.4.5	Suppression des clés d'activation de processeur	263
5.5	Déplacement des ressources du cœur du processeur	264
5.5.1	Processus de déplacement d'une activation de processeur	264
5.5.2	Vérification de la clé d'activation de processeur à déplacer	265
5.6	Affichage des informations d'activation de processeur	266
5.6.1	Vérification des informations de réglage et d'enregistrement de l'activation du processeur	266
5.6.2	Consultation du journal de COD	267
5.6.3	Affichage des informations de la clé d'activation de processeur	267
5.6.4	Affichage de l'utilisation des ressources de cœur de processeur activées	269
5.7	Sauvegarde/restauration des clés d'activation de processeur	270
5.7.1	Sauvegarde des clés d'activation de processeur	270
5.7.2	Restauration des clés d'activation de processeur	271
5.8	Dépannage des erreurs d'activation de processeur	271
5.8.1	Le nombre de cœurs de processeurs dépasse le nombre de cœurs de processeurs activés	271
5.8.2	Le nombre de cœurs de processeurs en fonctionnement passe sous la barre du nombre d'activations de processeur en raison d'un échec	272
5.9	Remarques importantes au sujet de l'activation de processeur	272
Chapitre 6 Démarrage/Arrêt du système		275
6.1	Démarrage du système	275
6.1.1	Étapes à suivre depuis la mise sous tension jusqu'au démarrage du système	275
6.1.2	Utilisation du commutateur ALIMENTATION	276
6.1.3	Utilisation de la commande poweron	279
6.2	Arrêt du système	280
6.2.1	Étapes à suivre depuis l'arrêt du système jusqu'à la mise hors tension	280

6.2.2	Sauvegarde des informations de configuration du domaine logique avant l'arrêt du système	281
6.2.3	Arrêt du système complet	281
6.3	Redémarrage du système	283
6.4	Empêcher le démarrage d'Oracle Solaris lors de la mise sous tension	283
Chapitre 7 Contrôle des partitions physiques		285
7.1	Configuration d'une partition physique	285
7.2	Réglage des modes de fonctionnement de la partition physique	286
7.2.1	Processeur installé sur une partition physique et mode de fonctionnement du processeur	286
7.2.2	Vérification du fonctionnement de l'alimentation lors du rétablissement du courant/définition de la mise sous tension automatique	293
7.3	Mise sous tension de la partition physique	296
7.4	Mise hors tension de la partition physique	297
7.5	Modification de la configuration d'une partition physique	298
Chapitre 8 Contrôle des domaines logiques		301
8.1	Configuration d'un domaine logique	301
8.2	Configuration de la zone noyau d'Oracle Solaris	302
8.2.1	Conditions matérielles et logicielles des zones noyau d'Oracle Solaris	302
8.2.2	Gestion du processeur dans les zones noyau d'Oracle Solaris	303
8.2.3	Notes sur les zones noyau d'Oracle Solaris	303
8.3	Passage à la console du domaine de commande depuis le shell XSCF	304
8.3.1	Passage du shell XSCF à la console du domaine de commande	304
8.3.2	Connexion à la console du domaine de commande dans des circonstances appropriées	305

8.4	Retour au shell XSCF depuis la console du domaine de commande	305
8.4.1	Passage de la console du domaine de commande au shell XSCF	305
8.4.2	Déconnexion de la console du domaine de commande	306
8.5	Démarrage d'un domaine logique	306
8.6	Arrêt d'un domaine logique	307
8.7	Arrêt commandé des domaines logiques	308
8.7.1	Tableau des domaines (IdomTable)	309
8.7.2	Ressources d'informations sur le domaine (Idom_info)	310
8.8	Vérification des informations d'activation de processeur	311
8.9	Réglage des variables d'environnement d'OpenBoot PROM du domaine de commande	312
8.9.1	Variables d'environnement OpenBoot PROM pouvant être réglées avec le microprogramme XSCF	312
8.9.2	Réglage des variables d'environnement d'OpenBoot PROM pour le domaine de commande	314
8.9.3	Affichage des variables d'environnement d'OpenBoot PROM définies du domaine de commande	315
8.9.4	Initialisation des variables d'environnement d'OpenBoot PROM définies du domaine de commande	316
8.10	Fonction de connexion de la console du domaine	317
8.10.1	Méthode de désactivation de la fonction de connexion de la console	317
8.10.2	Méthode de d'activation de la fonction de connexion de la console	318
8.10.3	Exigences pour le domaine de service	318
8.10.4	Tableau de groupe de la console virtuelle (IdomVconsTable)	318
8.10.5	Ressources de la console	319
8.11	Modification de la configuration d'un domaine logique	320

8.12	Réglage de l'heure des domaines logiques	320
8.13	Collecte d'un fichier de vidage du superviseur	321
8.13.1	Bases du vidage du superviseur	321
8.13.2	Commandes utilisées pour la fonction de vidage du superviseur	321
8.13.3	Points à noter sur l'utilisation de la fonction de vidage du superviseur	324
8.14	Gestion des ressources des domaines logiques associées aux sockets de processeur	325
8.14.1	Vue d'ensemble des contraintes des sockets de processeur	325
8.14.2	Exigences matérielles et logicielles des contraintes des sockets de processeur	327
8.14.3	Restrictions des contraintes des sockets de processeur	327
8.14.4	Création d'un domaine logique extrêmement fiable à l'aide des contraintes des sockets de processeur	327
8.14.5	Configuration de la mise en miroir de la mémoire vers la puce de processeur	328
8.14.6	Retrait des ressources associées au socket de processeur depuis le domaine de commande	330
8.14.7	Configuration des contraintes des socket de processeur par rapport à la configuration du domaine logique	332
8.15	Réglage de la stratégie de reconfiguration dynamique de la partition physique	334
8.15.1	Stratégie de reconfiguration dynamique de la partition physique	334
8.15.2	Détails sur la stratégie de réduction des ressources	335
8.15.3	Comment modifier la stratégie PPAR DR	338
8.16	Configuration de la taille de page maximale d'un domaine logique	339
8.16.1	Taille de page maximale d'un domaine logique	339
8.16.2	Avantages d'une taille de page maximale plus grande	339

8.16.3	Inconvénients d'une taille de page maximale plus grande	339
8.16.4	Définition et modification de la taille de page maximale d'un domaine logique	341
8.16.5	Vérification de la taille de page maximale d'un domaine logique	343
Chapitre 9 Gestion quotidienne des systèmes 345		
Chapitre 10 Se préparer et prendre des mesures en cas de pannes 347		
10.1	Familiarisation avec les procédures de dépannage et les fonctions connexes	348
10.2	Réception de notifications par e-mail lorsqu'une panne se produit	349
10.2.1	Caractéristiques de la fonction de notification par e-mail	349
10.2.2	Détails des notifications de panne	350
10.2.3	Vérification des éléments de réglage et des commandes liés aux notifications par e-mail	351
10.2.4	Procédures de réglage pour configurer une notification par e-mail	352
10.2.5	Réglage du nom d'hôte, du numéro de port, de l'adresse e-mail des réponses et de la méthode d'authentification du serveur SMTP	352
10.2.6	Réglage de l'adresse e-mail de destination pour la notification et activation/désactivation de la fonction de notification par e-mail	353
10.3	Surveillance/Gestion de l'état du système avec l'agent SNMP	354
10.3.1	Bases de SNMP	354
10.3.2	Termes liés à SNMP	355
10.3.3	Bases d'un fichier de définition de la MIB	356
10.3.4	Traps	357
10.3.5	Vérification des éléments de réglage et des commandes liés à l'agent SNMP	359
10.3.6	Procédures de réglage de l'agent SNMP	361

10.3.7	Réglage des informations de gestion du système sur l'agent SNMP et activation/désactivation de l'agent SNMP	364
10.3.8	Configuration des traps SNMPv3	365
10.3.9	Désactivation des traps à l'hôte cible pour SNMPv3	366
10.3.10	Activation/Désactivation de la communication SNMPv1 et SNMPv2c	366
10.3.11	Configuration des traps SNMPv1 et SNMPv2c	367
10.3.12	Désactivation des traps à l'hôte cible pour SNMPv1 et SNMPv2c	368
10.3.13	Restauration des valeurs par défaut pour les paramètres SNMP	368
10.3.14	Réglage des informations de gestion d'USM	369
10.3.15	Réglage des informations de gestion de VACM	370
10.4	Surveillance du système	372
10.4.1	Compréhension du mécanisme de la fonction Host watchdog / de vérification d'activité	372
10.4.2	Contrôle de la surveillance et du fonctionnement du serveur	373
10.5	Comprendre le mécanisme de détérioration suite à une panne	374
10.6	Vérification des ressources matérielles en panne	375
10.6.1	Vérification d'une mémoire ou de processeurs en panne avec la commande list-domain	375
10.6.2	Vérification d'une mémoire ou de processeurs en panne avec la commande list-device	375
10.7	Configuration d'une substitution automatique de cœurs du processeur en panne	376
10.7.1	Conditions requises pour la substitution automatique d'un cœur de processeur	376
10.7.2	Méthode de modification de la politique de substitution automatique	379

10.7.3	Méthodes de modification du nombre de tentatives maximum et intervalle entre les tentatives	380
10.8	Configuration du mode de récupération	380
10.9	Configuration de composants redondants	381
10.10	Sauvegarde/restauration des informations des réglages de XSCF	381
10.10.1	Compréhension de la sauvegarde/restauration des informations des réglages de XSCF	381
10.10.2	Sauvegarde des informations des réglages de XSCF	383
10.10.3	Restauration des informations des réglages de XSCF	384
10.11	Sauvegarde / restauration des informations de configuration du domaine logique dans le XSCF	385
10.11.1	Sauvegarde/Affichage des informations de réglage du domaine logique	386
10.11.2	Restauration des informations de configuration du domaine logique	387
10.12	Sauvegarde / restauration des informations de configuration du domaine logique dans un fichier XML	390
10.12.1	Sauvegarde/Vérification des informations de configuration du domaine logique	390
10.12.2	Restauration des informations de configuration du domaine logique	391
10.13	Enregistrement/Restauration des variables d'environnement d'OpenBoot PROM	393
10.13.1	Sauvegarde des variables d'environnement d'OpenBoot PROM	393
10.13.2	Restauration des variables d'environnement d'OpenBoot PROM	395
10.14	Sauvegarde / Restauration du contenu d'un disque dur	397
10.15	Réinitialisation d'un domaine logique	397
10.16	Génération d'une panique dans un domaine logique	398
10.16.1	Génération d'une panique dans un domaine invité	399

10.16.2	Génération d'une panique dans un domaine de commande	399
10.17	Reconfiguration d'une partition physique	400
10.18	Restauration de l'état du serveur aux valeurs par défaut en vigueur à l'expédition	402
10.18.1	Compréhension des commandes d'initialisation	402
10.18.2	Initialisation du serveur	402
10.19	Récupération d'un fichier de vidage d'incident à l'aide du vidage différé	404
Chapitre 11	Vérifier l'état du système	405
11.1	Vérifier la configuration et l'état du système	405
11.1.1	Vérification des éléments et des commandes liés à la configuration et à l'état du système	405
11.1.2	Vérification des composants montés dans le système	406
11.1.3	Vérification de l'environnement du système	411
11.1.4	Vérification des composants en panne/détériorés	415
11.1.5	Affichage de l'état de l'unité d'extension PCI	416
11.2	Vérification d'une partition physique	419
11.2.1	Vérification des éléments et des commandes liés à la configuration/à l'état des partitions physiques et des domaines logiques	419
11.2.2	Vérification de la configuration de la partition physique	420
11.2.3	Vérification de l'état de fonctionnement de la partition physique	424
11.2.4	Vérification des réglages du mode de mise en miroir de la mémoire	425
11.2.5	Vérification de l'état de la PSB	426
11.2.6	Vérification de l'état du domaine logique	427
Chapitre 12	Consultation des journaux et des messages	429
12.1	Consultation d'un journal enregistré par le XSCF	429

12.1.1	Vérification des types de journaux et commandes de référence	429
12.1.2	Comment afficher le journal	433
12.1.3	Consultation du journal d'erreur	434
12.1.4	Consultation du journal des messages de surveillance	436
12.1.5	Consultation du journal d'alimentation	437
12.1.6	Consultation du journal des événements	439
12.1.7	Consultation du journal de console	439
12.1.8	Consultation du journal de panique	440
12.1.9	Consultation du journal IPL	441
12.1.10	Consultation du journal d'audit	441
12.1.11	Consultation du journal de COD	443
12.1.12	Consultation des journaux Active Directory	444
12.1.13	Consultation des journaux LDAP sur SSL	444
12.1.14	Consultation du journal d'historique de la température	445
12.1.15	Sauvegarde d'un journal dans un fichier avec snapshot	445
12.1.16	Sauvegarde d'un journal sur un périphérique USB local	446
12.1.17	Sauvegarde du journal par le réseau sur les terminaux utilisant XSCF Web	447
12.1.18	Sauvegarde du journal par le réseau, sur les serveurs spécifiés avec snapshot	448
12.2	Consultation des messages d'avertissement et de notification	448
12.2.1	Consultation des types de messages et des méthodes de référence	448
12.2.2	Action à mener pour les messages de notification	451
Chapitre 13 Passer en mode Verrouillé / Service		455
13.1	Compréhension des différences entre le mode Verrouillé et le mode Service	455
13.2	Changer le mode de fonctionnement	456
Chapitre 14 Configuration d'un système hautement fiable		461
14.1	Configuration de la mise en miroir de la mémoire	461

14.1.1	Présentation de la mise en miroir de la mémoire	461
14.1.2	Configuration de la mise en miroir de la mémoire	462
14.2	Configuration du RAID matériel	463
14.2.1	Base du RAID matériel	464
14.2.2	Commandes de l'utilitaire FCode	468
14.2.3	Précautions relatives au RAID matériel	468
14.2.4	Préparation avant utilisation du RAID matériel	471
14.2.5	Création d'un volume RAID matériel	473
14.2.6	Suppression d'un volume RAID matériel	477
14.2.7	Gestion d'un composant de rechange à chaud d'un volume RAID matériel	479
14.2.8	Vérification du statut d'un volume RAID matériel et d'un lecteur de disque	479
14.2.9	Vérification d'un lecteur de disque défaillant	482
14.2.10	Remplacement d'un lecteur de disque défaillant	484
14.2.11	Réactivation d'un volume RAID matériel	485
14.2.12	Spécification d'un volume RAID de matériel en tant que périphérique de démarrage	487
14.3	Utilisation du service LDAP	488
14.4	Utilisation du démarrage SAN	488
14.5	Utilisation d' iSCSI	488
14.6	Gestion de l'alimentation à distance pour le SPARC M12/M10 et les périphériques d'E/S	489
14.6.1	Fonction de gestion de l'alimentation à distance pour SPARC M12/M10	489
14.6.2	Compréhension des formes de connexion pour la gestion de l'alimentation à distance	490
14.6.3	Structure de la gestion de l'alimentation à distance	493
14.6.4	Avant de régler la gestion de l'alimentation à distance	495
14.6.5	Flux pour régler la gestion de l'alimentation à distance	495

14.6.6	Vérification du réglage de la gestion de l'alimentation à distance	497
14.6.7	Initialisation du réglage de la gestion de l'alimentation à distance	497
14.6.8	Activation/Désactivation de la fonction de gestion de l'alimentation à distance	498
14.6.9	Création d'un fichier de gestion	498
14.6.10	Activation/Désactivation du service IPMI utilisé par la fonction de gestion de l'alimentation à distance du XSCF	500
14.6.11	Acquisition d'informations de réglage du groupe de gestion de l'alimentation à distance	500
14.6.12	Réglage d'un groupe de gestion de l'alimentation à distance	501
14.7	Utilisation de l'alimentation sans interruption	501
14.8	Utilisation du démarrage vérifié	501
14.8.1	Bases du démarrage vérifié	501
14.8.2	Mécanisme de vérification du démarrage par le démarrage vérifié	502
14.8.3	Certificats de clé publique X.509 pour le démarrage vérifié	503
14.8.4	Stratégies de démarrage vérifié	504
14.8.5	Versions d'Oracle Solaris et XCP qui prennent en charge le démarrage vérifié	506
14.8.6	Liste de prise en charge du démarrage vérifié	506
14.8.7	Remarques et restrictions	507
14.8.8	Vérification des réglages et des commandes liés au démarrage vérifié	508
14.8.9	Procédures de réglage du démarrage vérifié	509
14.8.10	Enregistrement d'un certificat de clé publique X.509	510
14.8.11	Activation/Désactivation d'un certificat de clé publique X.509	513

14.8.12	Suppression d'un certificat de clé publique X.509 enregistré	516
14.8.13	Affichage d'un certificat de clé publique X.509 enregistré	518
14.8.14	Réglage des stratégies de démarrage vérifié	519
14.8.15	Affichage des stratégies de démarrage vérifié	520
Chapitre 15 Extension de la configuration du système 521		
15.1	Modification de la configuration des processeurs virtuels	521
15.2	Modification de la configuration de la mémoire	523
15.3	Fonction de reconfiguration dynamique pour les périphériques de destination PCIe	525
15.3.1	Ajout d'un périphérique physique d'E/S à un domaine d'E/S	527
15.3.2	Retrait d'un périphérique physique d'E/S d'un domaine d'E/S	528
15.4	Utilisation de l'unité d'extension PCI	529
15.4.1	Vérification de l'unité d'extension PCI	529
15.4.2	Contrôle de l'alimentation de l'unité d'extension PCI	530
15.4.3	Remarques sur la configuration dans laquelle le système est connecté à une unité d'extension PCI	530
15.5	Extension de SPARC M12-2S/M10-4S	534
Chapitre 16 Mise à jour du microprogramme XCP 535		
16.1	Bases de la mise à jour du microprogramme	535
16.1.1	Types de microprogrammes à mettre à jour	535
16.1.2	Fonctionnalités de la mise à jour du microprogramme	536
16.1.3	Mécanisme de la mise à jour du microprogramme	536
16.1.4	Correspondance des versions	538
16.1.5	Mise à jour en utilisant plusieurs XSCF	538
16.2	Avant de mettre à jour le microprogramme	539
16.2.1	Remarques sur la mise à jour	539
16.2.2	Méthode et format de la distribution du fichier de mise à jour	540

16.2.3	Méthode de vérification de la version du microprogramme	540
16.2.4	Méthodes de mise à jour et durées des tâches	542
16.3	Procédure de mise à jour	543
16.4	Préparation d'un fichier image XCP	544
16.5	Mise à jour du microprogramme	544
16.5.1	Mise à jour de XCP sur un système avec un XSCF	544
16.5.2	Mise à jour de XCP dans un système de configuration de bloc de construction avec plusieurs XSCF	550
16.6	Mettre à jour le microprogramme depuis XSCF Web	559
16.7	Correspondance de la version du microprogramme avec le remplacement d'éléments	565
16.7.1	Correspondance de la version du microprogramme pour l'ajout/remplacement avec l'alimentation sous tension	566
16.7.2	Correspondance de la version du microprogramme pour l'ajout/remplacement avec l'alimentation hors tension	567
16.8	Problème lors de la mise à jour du microprogramme	570
16.9	FAQ concernant la mise à jour du microprogramme	570
Chapitre 17	Mise à jour d'Oracle Solaris et d'Oracle VM Server pour SPARC	573
Chapitre 18	Dépannage	575
18.1	Dépannage du XSCF	575
18.2	Précautions relatives à l'utilisation du commutateur RESET	579
18.3	Foire aux questions/FAQ	580
18.4	Dépannage du système avec le XSCF	581
Annexe A	Listes des chemins d'accès de périphériques des systèmes SPARC M12/M10	583
A.1	Chemins d'accès de périphériques SPARC M12-1	583
A.2	Chemins d'accès de périphériques SPARC M12-2	586
A.2.1	Pour une configuration à 1 processeur au moment de l'installation initiale	587

A.2.2	Pour une configuration à 2 processeurs au moment de l'installation initiale	590
A.3	Chemins d'accès de périphériques SPARC M12-2S	593
A.3.1	Pour une configuration à 1 processeur au moment de l'installation initiale	593
A.3.2	Pour une configuration à 2 processeurs au moment de l'installation initiale	599
A.4	Chemins d'accès de périphériques SPARC M10-1	605
A.5	Chemins d'accès de périphériques SPARC M10-4	608
A.5.1	Pour une configuration à 2 processeurs au moment de l'installation initiale	609
A.5.2	Pour une configuration à 4 processeur au moment de l'installation initiale	612
A.6	Chemins d'accès de périphériques SPARC M10-4S	615
A.6.1	Pour une configuration à 2 processeurs au moment de l'installation initiale	615
A.6.2	Pour une configuration à 4 processeur au moment de l'installation initiale	621
Annexe B	Identifier un périphérique SAS2 en fonction de WWN	629
B.1	Syntaxe World Wide Name (WWN)	629
B.2	Présentation du résultat de la commande probe-scsi-all	630
B.3	Identification de l'emplacement d'un disque à l'aide de la commande probe-scsi-all	630
B.3.1	Exemple d'identification de l'emplacement d'un disque à l'aide de la commande probe-scsi-all (SPARC M12-1/M12-2/M12-2S/M10-1/M10-4/M10-4S)	631
B.4	Identification de l'emplacement d'un disque	633
B.4.1	Utilisation de la commande de formatage (Oracle Solaris 11)	634
B.4.2	Utilisation de la commande diskinfo (Oracle Solaris 11)	636
B.4.3	Utilisation de la commande diskinfo (Oracle Solaris 10)	638

Annexe C Liste des pages de XSCF Web 639

- C.1 Aperçu des pages 639
- C.2 Comprendre la configuration du menu 642
- C.3 Pages disponibles 645
 - C.3.1 Pages indiquant l'état du système, les partitions physiques et les domaines logiques 645
 - C.3.2 Pages permettant d'utiliser une partition physique 647
 - C.3.3 Pages permettant de configurer le serveur 651
 - C.3.4 Pages relatives à la maintenance du serveur 664
 - C.3.5 Pages d'affichage des journaux 667

Annexe D Informations sur la MIB de XSCF 669

- D.1 Identification d'objet MIB 669
- D.2 MIB standard 671
- D.3 MIB étendue 671
 - D.3.1 Objets de la MIB étendue de XSCF 672
- D.4 Traps 673

Annexe E Fonctions spécifiques du système SPARC M12/M10 pour Oracle VM Server pour SPARC 675

- E.1 Arrêt commandé des domaines logiques 675
- E.2 Prise en charge de l'activation du processeur 675
- E.3 Vérification des ressources en panne 676
 - E.3.1 Confirmation de panne ou d'absence de panne de la mémoire ou du processeur en utilisant la commande list-domain sub 676
 - E.3.2 Affichage de panne ou d'absence de panne de la mémoire ou du processeur en utilisant la commande list-device sub 676
- E.4 Remplacement automatique du réglage des processeurs en erreur 676
- E.5 Vidage du superviseur 677
- E.6 Fonction de connexion de la console du domaine 677
- E.7 Restrictions du socket du processeur 677

Annexe F Exemples d'affichage de la commande d'utilitaire SAS2IRCU 679

- F.1 Affichage d'une liste des contrôleurs SAS reconnus par sas2ircu 679

F.2	Affichage des informations d'un volume RAID matériel	680
F.3	Ajout d'un volume RAID matériel	684
F.4	Affichage de l'état de configuration d'un volume RAID matériel	686
F.5	Création d'un composant de rechange à chaud d'un volume RAID matériel	687
F.6	Suppression d'un composant de rechange à chaud d'un volume RAID matériel	689
F.7	Suppression d'un volume RAID matériel	690
F.8	Identification du lecteur de disque défaillant d'un volume RAID matériel	692
Annexe G Fonction de mode de démarrage du XSCF SPARC M12-1/M10-1		
		697
G.1	Présentation de la fonction	697
G.1.1	Qu'est-ce que la fonction de mode de démarrage du XSCF ?	697
G.1.2	Conditions d'utilisation	698
G.2	Restrictions et remarques	699
G.2.1	Restrictions et remarques au moment de l'installation du système	699
G.2.2	Restrictions et remarques pendant le fonctionnement du système	700
G.2.3	Restrictions lors de la maintenance	700
G.3	Procédure de configuration	701
Annexe H Variables d'environnement et commandes d'OpenBoot PROM		
		705
H.1	Affichage des périphériques SCSI	705
H.2	Variables d'environnement d'OpenBoot PROM non prises en charge	705
H.3	Commandes d'OpenBoot PROM non prises en charge	706
H.4	Comportement avec le mode de sécurité activé	707
Annexe I Comment spécifier le périphérique de démarrage		
		709

- I.1 Chemin d'accès de périphérique du stockage interne 709
- I.2 Méthode de spécification avec un numéro PHY 710
- I.3 Méthode de spécification avec un ID cible 711
- I.4 Méthode de spécification avec une adresse SAS 713
- I.5 Méthode de spécification avec un nom de périphérique de volume 714

Annexe J Listes des alias des lecteurs DVD 717

- J.1 Alias des lecteurs DVD externes 717
 - J.1.1 Alias des lecteurs DVD externes SPARC M12-1 717
 - J.1.2 Alias des lecteurs DVD externes SPARC M12-2 718
 - J.1.3 Alias des lecteurs DVD externes SPARC M12-2S 718
 - J.1.4 Alias des lecteurs DVD externes SPARC M10-1 721
 - J.1.5 Alias des lecteurs DVD externes SPARC M10-4 721
 - J.1.6 Alias des lecteurs DVD externes SPARC M10-4S 721
- J.2 Alias des lecteurs DVD de stockage à distance 723
 - J.2.1 Alias des lecteurs DVD de stockage à distance SPARC M12-1 723
 - J.2.2 Alias des lecteurs DVD de stockage à distance SPARC M12-2 723
 - J.2.3 Alias des lecteurs DVD de stockage à distance SPARC M12-2S 724
 - J.2.4 Alias des lecteurs DVD de stockage à distance SPARC M10-1 724
 - J.2.5 Alias des lecteurs DVD de stockage à distance SPARC M10-4 725
 - J.2.6 Alias des lecteurs DVD de stockage à distance SPARC M10-4S 725

Annexe K Permis temporaire d'activation de processeur 727

- K.1 Qu'est-ce que le permis temporaire d'activation de processeur ? 727
- K.2 Conditions d'utilisation du permis temporaire d'activation de processeur et précautions 728

K.3	Commandes liées	729
K.3.1	Commandes pour l'utilisation d'un permis temporaire d'activation de processeur	729
K.3.2	Commandes liées à l'utilisation d'un permis temporaire d'activation de processeur	730
K.4	Étapes et procédures d'utilisation d'un permis temporaire d'activation de processeur	730
K.4.1	Flux et procédures pour XCP 2330 et version ultérieure	731
K.4.2	Flux et procédures pour XCP 232x	743
K.4.3	Cas dans lequel la fonction a expiré ou a été désactivée	750
K.5	Notification d'événement d'un permis temporaire d'activation de processeur	755
K.5.1	Types de notification	755
K.5.2	Exemples de notifications	756
K.6	Autres notes importantes	758
K.6.1	PPAR DR et permis temporaire d'activation de processeur	758
K.6.2	Lors de la tentative d'utiliser le permis temporaire d'activation de processeur (pour XCP 232x uniquement)	758
K.6.3	Déplacement des clés d'activation de processeur (suppression/déplacement)	759
K.6.4	Résultat de la commande ldm	760
Index		761

Préface

Ce document décrit les méthodes de paramétrage et de gestion à suivre après l'installation de systèmes SPARC M12/M10 d'Oracle ou de Fujitsu. Lisez les passages requis pour l'utilisation de tout système SPARC M12/M10.

Nous vous recommandons de lire le *Guide rapide Fujitsu SPARC M12* ou *Guide rapide des systèmes Fujitsu M10/SPARC M10* avant de lire ce document.

Au Japon, Fujitsu SPARC M12 est vendu sous le nom de SPARC M12 par Fujitsu. Fujitsu SPARC M12 et SPARC M12 sont des produits identiques.

Au Japon, Fujitsu M10 est vendu sous le nom de SPARC M10 par Fujitsu. Le M10 de Fujitsu et le SPARC M10 sont identiques.

Public visé

Ce document est destiné aux administrateurs système ayant des connaissances avancées des réseaux informatiques et d'Oracle Solaris.

Documentation connexe

Tous les documents concernant votre serveur sont disponibles en ligne, sur les sites suivants.

- Documents concernant les logiciels de Sun Oracle (Oracle Solaris, etc.)
<http://docs.oracle.com/en/>
- Documents Fujitsu
Site global
<http://www.fujitsu.com/global/products/computing/servers/unix/sparc/downloads/manuals/>
Site japonais

Pour un système utilisant le SPARC M12, consultez les manuels listés dans
« [Documentation liée au SPARC M12](#) ».

Pour un système utilisant le SPARC M10, consultez les manuels listés dans
« [Documentation liée au SPARC M10](#) ».

Documentation liée au SPARC M12

Noms des manuels (*1)

Notes de produit Fujitsu SPARC M12

Guide rapide Fujitsu SPARC M12

*Guide de démarrage Fujitsu SPARC M12 (*2)*

*Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Important Legal and Safety Information (*2)*

Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Safety and Compliance Guide

Software License Conditions for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10

Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Security Guide

Fujitsu SPARC Servers/SPARC Enterprise/PRIMEQUEST Common Installation Planning Manual

Guide d'installation Fujitsu SPARC M12-1

Guide d'installation Fujitsu SPARC M12-2

Guide d'installation Fujitsu SPARC M12-2S

Fujitsu SPARC M12 PCI Card Installation Guide

Guide de fonctionnement et d'administration des systèmes Fujitsu SPARC M12 et Fujitsu M10/SPARC M10

Guide de configuration du domaine Fujitsu SPARC M12 et Fujitsu M10/SPARCM10

*Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 RCIL User Guide (*3)*

Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual

Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF MIB and Trap Lists

Fujitsu SPARC M12-1 Service Manual

Fujitsu SPARC M12-2/M12-2S Service Manual

Crossbar Box for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Service Manual

PCI Expansion Unit for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Service Manual

Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Glossary

External USB-DVD Drive user guide

*1 Les manuels faisant l'objet de la liste peuvent être modifiés sans préavis.

*2 Les manuels imprimés sont fournis avec le produit.

*3 Ce document s'applique de manière spécifique au SPARC M12/M10 et au système de stockage sur disque FUJITSU ETERNUS.

Noms des manuels (*1)

Notes de produit des systèmes Fujitsu M10/SPARC M10

Guide rapide des systèmes Fujitsu M10/SPARC M10

*Guide de démarrage des systèmes Fujitsu M10/SPARC M10 (*2)*

*Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Important Legal and Safety Information (*2)*

Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Safety and Compliance Guide

Software License Conditions for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10

Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Security Guide

Fujitsu SPARC Servers/SPARC Enterprise/PRIMEQUEST Common Installation Planning Manual

Guide d'installation Fujitsu M10-1/SPARC M10-1

Guide d'installation Fujitsu M10-4/SPARC M10-4

Guide d'installation Fujitsu M10-4S/SPARC M10-4S

Fujitsu M10/SPARC M10 Systems PCI Card Installation Guide

Guide de fonctionnement et d'administration des systèmes Fujitsu SPARC M12 et Fujitsu M10/SPARC M10

Guide de configuration du domaine Fujitsu SPARC M12 et Fujitsu M10/SPARCM10

*Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 RCIL User Guide (*3)*

Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual

Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF MIB and Trap Lists

Fujitsu M10-1/SPARC M10-1 Service Manual

Fujitsu M10-4/Fujitsu M10-4S/SPARC M10-4/SPARC M10-4S Service Manual

Crossbar Box for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Service Manual

PCI Expansion Unit for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Service Manual

Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Glossary

External USB-DVD Drive user guide

*1 Les manuels faisant l'objet de la liste peuvent être modifiés sans préavis.

*2 Les manuels imprimés sont fournis avec le produit.

*3 Ce document s'applique de manière spécifique au SPARC M12/M10 et au système de stockage sur disque FUJITSU ETERNUS.

Remarques sur la sécurité

Consultez les documents suivants en détail avant d'utiliser ou de manipuler un SPARC M12/M10.

- *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Important Legal and Safety Information*

Conventions de mise en forme du texte

Ce manuel utilise les polices de caractère et les symboles suivants pour exprimer certains types d'information.

Police / symbole	Signification	Exemple
AaBbCc123	Ce qui est saisi par opposition à ce qui s'affiche à l'écran. Cette police indique un exemple de saisie de commande.	XSCF> adduser jsmith
AaBbCc123	Noms de commandes, fichiers et répertoires affichés à l'écran. Cette police indique un exemple de résultat de commande dans le contexte concerné.	XSCF> showuser -P User Name: jsmith Privilèges : useradm auditadm
<i>Italique</i>	Indique le nom d'un manuel de référence.	Consultez le <i>Guide d'installation Fujitsu M10-1/SPARC M10-1</i> .
« »	Indique les noms de chapitres, sections, éléments, boutons ou menus.	Consultez le « Chapitre 2 Connexion au réseau ».

Syntaxe de commande dans le texte

Lorsque le numéro de section des commandes XSCF est (8) ou (1), celui-ci n'est pas indiqué dans le texte.

Pour de plus amples informations sur les commandes, consultez le document *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

Syntaxe de l'interface de ligne de commande (CLI)

La syntaxe de commande doit être conforme aux règles suivantes :

- Une variable nécessitant l'entrée d'une valeur doit être formatée en italique.
- Les éléments optionnels doivent être placés entre [].

- Un groupe d'options concernant un mot-clé optionnel doit être placé entre [] et délimité par |.

Commentaires sur la documentation

Pour tout commentaire ou demande concernant ce document, vous pouvez nous en faire part en précisant le code du manuel, son titre, la page concernée, et l'objet de votre demande sur l'un des sites suivants :

- Site global
<http://www.fujitsu.com/global/contact/>
- Site japonais
<http://www.fujitsu.com/jp/products/computing/servers/unix/sparc/contact/>

Chapitre 1

Comprendre la présentation du SPARC M12/M10

Ce chapitre donne un aperçu des systèmes SPARC M12/M10 et décrit le logiciel et le microprogramme utilisés avec eux.

- [Principes de base du SPARC M12/M10](#)
- [Bases du microprogramme XSCF](#)
- [Configuration réseau](#)
- [Bases du microprogramme superviseur](#)
- [Bases d'Oracle VM Server pour SPARC](#)
- [Bases d'OpenBoot PROM](#)

1.1 Principes de base du SPARC M12/M10

Cette section donne un aperçu des systèmes SPARC M12/M10.

Le SPARC M12/M10 est un système de serveur UNIX qui utilise le processeur SPARC et Oracle Solaris. L'activation de processeur permet d'étendre les ressources par unités d'un cœur, en phases. Le SPARC M12-2S/M10-4S utilise un système de bloc de construction pour que le système puisse être configuré comme nécessaire pour l'usage prévu par l'entreprise et la taille de cette dernière. Les serveurs peuvent être exploités de plusieurs manières telles que les serveurs de base de données qui sont plus indiqués pour les centres de données à l'heure de l'informatique de nuage et les serveurs web ou d'applications dont le débit élevé est sollicité.

Les modèles suivants ont été élaborés afin de satisfaire aux différentes utilisations.

- **SPARC M12-1**
Ce modèle compact à 1 processeur de six cœurs maximum est conçu à des fins d'économie d'espace et de haute performance.
- **SPARC M12-2**
Ce modèle comprend un maximum de deux processeurs, chacun possédant au

maximum 12 cœurs.

- SPARC M12-2S

Ce modèle comprend un maximum de deux processeurs, chacun possédant au maximum 12 cœurs. Avec le système de bloc de construction (BB), il est possible d'ajuster le nombre d'unités SPARC M12-2S connectées en fonction de la performance requise. Il est possible d'étendre une configuration jusqu'à quatre BB en connectant des unités SPARC M12-2S directement entre elles. De plus, l'utilisation de boîtiers à barre transversale peut prendre en charge une configuration allant jusqu'à 16 BB et admettre jusqu'à 32 processeurs (l'évolutivité est assurée).

- SPARC M10-1

Ce modèle compact à 1 processeur de 16 cœurs maximum est conçu à des fins d'économie d'espace et de haute performance.

- SPARC M10-4

Ce modèle comprend un maximum de quatre processeurs, chacun possédant au maximum 16 cœurs.

- SPARC M10-4S

Ce modèle comprend un maximum de quatre processeurs, chacun possédant au maximum 16 cœurs. Avec le système de bloc de construction (BB), il est possible d'ajuster le nombre d'unités SPARC M10-4S connectées en fonction de la performance requise. Il est possible d'étendre une configuration jusqu'à quatre BB en connectant des unités SPARC M10-4S directement entre elles. De plus, l'utilisation de boîtiers à barre transversale peut prendre en charge une configuration allant jusqu'à 16 BB et admettre jusqu'à 64 processeurs (l'évolutivité est assurée).

Remarque : si le système de bloc de construction est utilisé, le SPARC M12-2S et le SPARC M10-4S ne peuvent pas être mélangés dans la même configuration.

Configuration du système

Cette section décrit la configuration du système.

[Figure 1-1](#) montre un exemple de configuration du système dans laquelle plusieurs SPARC M12-2S ou plusieurs SPARC M10-4S sont connectés grâce au système de bloc de construction. Une seule unité SPARC M12-2S/M10-4S pouvant avoir une configuration de bloc de construction correspond à un bloc de construction. Une partition physique (PPAR) est configurée en combinant un ou plusieurs blocs de construction.

[Figure 1-2](#) montre un exemple de configuration de système de SPARC M12-1/M12-2/M10-1/M10-4. Une seule unité SPARC M12-1/M12-2/M10-1/M10-4 ne peut pas disposer d'une configuration de bloc de construction, mais est parfois appelée une partition physique. Notez que le SPARC M12-2S et le SPARC M10-4S dans une configuration d'unité simple est parfois appelée une partition physique.

Figure 1-1 Exemple de configuration de système SPARC M12-2S/M10-4S

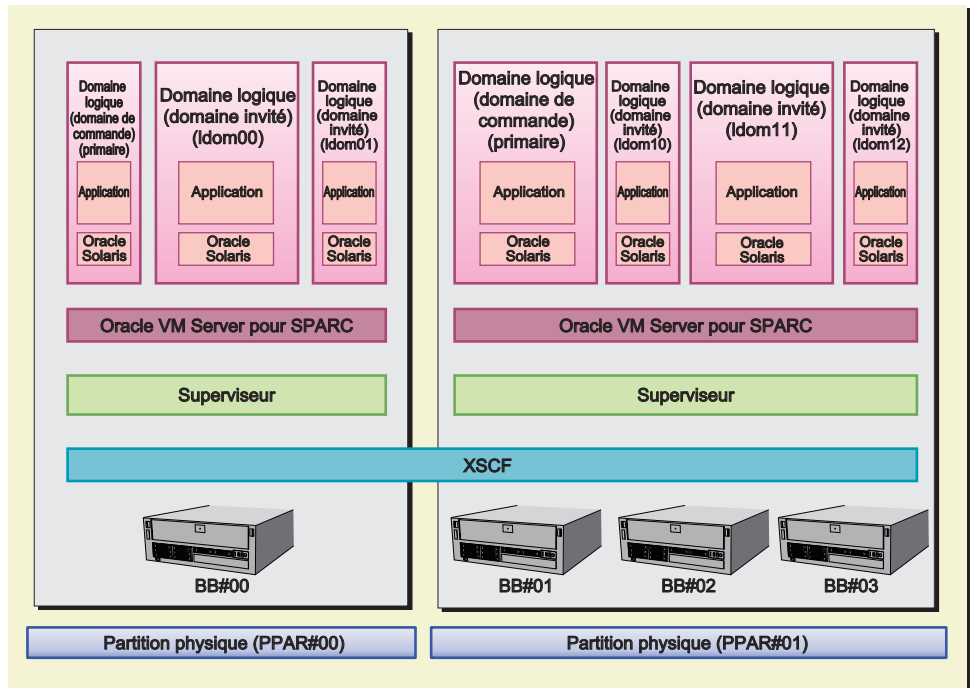
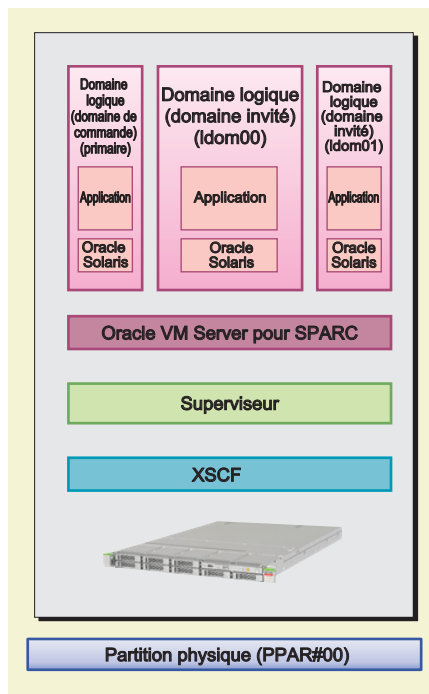


Figure 1-2 Exemple de configuration de système SPARC M12-1/M12-2/M10-1/M10-4



Les sections suivantes décrivent les « partitions physiques » et les « domaines logiques », qui sont des éléments majeurs de la configuration des systèmes.

Configuration de partitions physiques

Pour configurer un système SPARC M12-2S ou SPARC M10-4S, configurez une partition physique (PPAR) en combinant un ou plusieurs blocs de construction du même modèle. La configuration des partitions physiques s'appelle partitionnement, et l'objet configuré qui en résulte s'appelle partition physique (PPAR). Les partitions physiques sont configurées à l'aide du microprogramme XSCF, qui est le microprogramme de gestion du système.

Dans l'exemple indiqué dans [Figure 1-1](#), PPAR#00 est un des blocs de construction (BB) et BB#00 est configuré comme la partition physique PPAR#00. De manière similaire, la partition physique PPAR#01 est configurée à partir de BB#01, BB#02 et BB#03.

Une fois qu'une partition physique est configurée, les ressources matérielles se trouvant sur la partition physique sont assignées aux domaines logiques.

Notez que le système SPARC M12-1/M12-2/M10-1/M10-4 est un modèle constitué d'une seule unité, qui peut être configuré à l'aide d'une seule partition physique.

Configuration de domaines logiques

Dans une partition physique, les CPU, la mémoire, les dispositifs E/S et d'autres ressources matérielles doivent être assignés aux domaines logiques. Un domaine logique est configuré à l'aide du logiciel Oracle VM Server pour SPARC.

Un domaine logique configuré est géré comme un système UNIX du point de vue logiciel. L'application Oracle Solaris et les autres applications peuvent être installées dans les domaines logiques et appliquées aux tâches séparément. Dans l'exemple indiqué dans [Figure 1-1](#), les domaines logiques primary, ldom00 et ldom01 sont configurés avec l'attribution de ressources matérielles de la partition physique PPAR#00.

De même, les domaines logiques primary, ldom10, ldom11, et ldom12 sont configurés avec la partition physique PPAR#01.

L'un des domaines logiques auquel les ressources de la partition physique sont assignées sert de domaine de commande de tous les domaines logiques. Il s'agit du domaine de commande. Le domaine de commande, qui est le contrôleur des domaines logiques, sert également à traiter la communication entre la partition physique et les domaines logiques.

Microprogramme/Logiciel requis pour les systèmes

Les partitions physiques sont implémentées avec le microprogramme XSCF et le domaine logique, Oracle VM Server pour SPARC. Même pour une configuration du domaine de commande uniquement, Oracle VM Server pour SPARC est requis. La communication entre le microprogramme XSCF et Oracle VM Server pour SPARC, destinée à contrôler et à gérer tout le système, est gérée à l'intérieur du système. Cela ne concerne pas l'utilisateur.

Dans les systèmes SPARC M12/M10, l'interface entre le microprogramme XSCF et

Oracle VM Server pour SPARC est implémentée par le microprogramme appelé superviseur.

« 1.2 Bases du microprogramme XSCF » et les sections suivantes décrivent le microprogramme et le logiciel utilisés dans les systèmes.

1.2 Bases du microprogramme XSCF

Cette section résume le microprogramme XSCF ainsi que ses fonctions.

1.2.1 Présentation de XSCF

Le microprogramme XSCF est le dispositif intégré standard de contrôle du système, utilisé par les systèmes SPARC M12/M10. Le microprogramme XSCF est exécuté sur un processeur (processeur de service) dédié, indépendamment des processeurs de serveur. Le châssis de chaque système SPARC M12/M10 comporte un package complet du microprogramme XSCF pour la communication avec les domaines logiques et la gestion de tout le système. Lorsque plusieurs serveurs sont associés à l'aide d'un système de bloc de construction (BB), le serveur est interconnecté à d'autres serveurs à l'aide de boîtiers à barre transversale (XBBOX). Chacun de ces boîtiers à barre transversale comporte un processeur de service permettant d'exécuter le microprogramme XSCF.

Le microprogramme XSCF est exécutée et assure constamment le fonctionnement correct du serveur aussi longtemps que le serveur est alimenté, même si le domaine logique n'est pas en cours d'exécution ou que la partition physique n'est pas alimentée. Cela modifie également la configuration du serveur et le met sous/hors tension selon le cas.

De plus, le microprogramme XSCF comprend une interface utilisateur fournissant des fonctions pour surveiller, gérer et contrôler le système.

Dans ce manuel, le microprogramme XSCF peut être appelé XSCF. La carte contenant le processeur de service sur lequel s'exécute le microprogramme XSCF peut être appelée l'unité XSCF.

1.2.2 Fonctionnalités de XSCF

Interface utilisateur utilisable pour le fonctionnement et la maintenance quotidiens du serveur

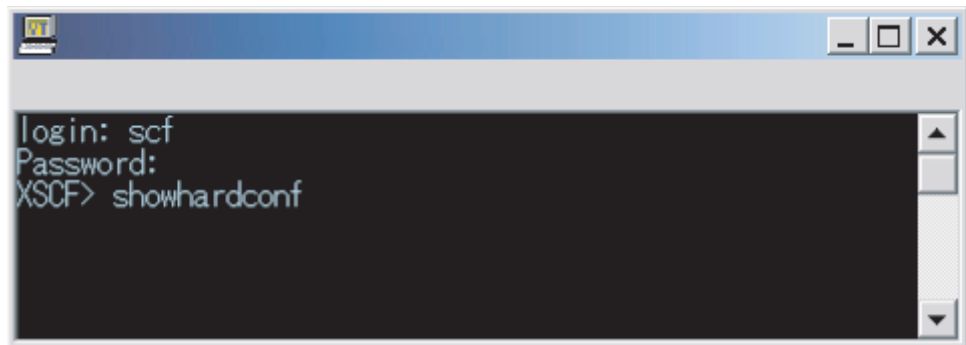
Vous pouvez avoir une idée de l'état du serveur, utiliser le serveur, et effectuer un travail d'entretien sur le serveur en accédant au XSCF à partir de la ligne de commande ou du navigateur Internet.

- **Shell XSCF (interface de ligne de commande)**

Vous pouvez connecter un PC d'utilisateur au serveur, directement à travers un câble série, ou connecter un câble Ethernet au LAN XSCF LAN, et effectuer des communications via le service SSH ou le service Telnet. Par conséquent, le PC peut être utilisé comme un terminal de shell XSCF, pouvant exécuter les commandes du shell XSCF. Sur le Shell XSCF, vous pouvez basculer sur la console vous permettant de faire fonctionner le domaine de commande (aussi appelée console du domaine de commande).

Figure 1-3 illustre un exemple de terminal du shell XSCF.

Figure 1-3 Exemple de terminal du Shell XSCF

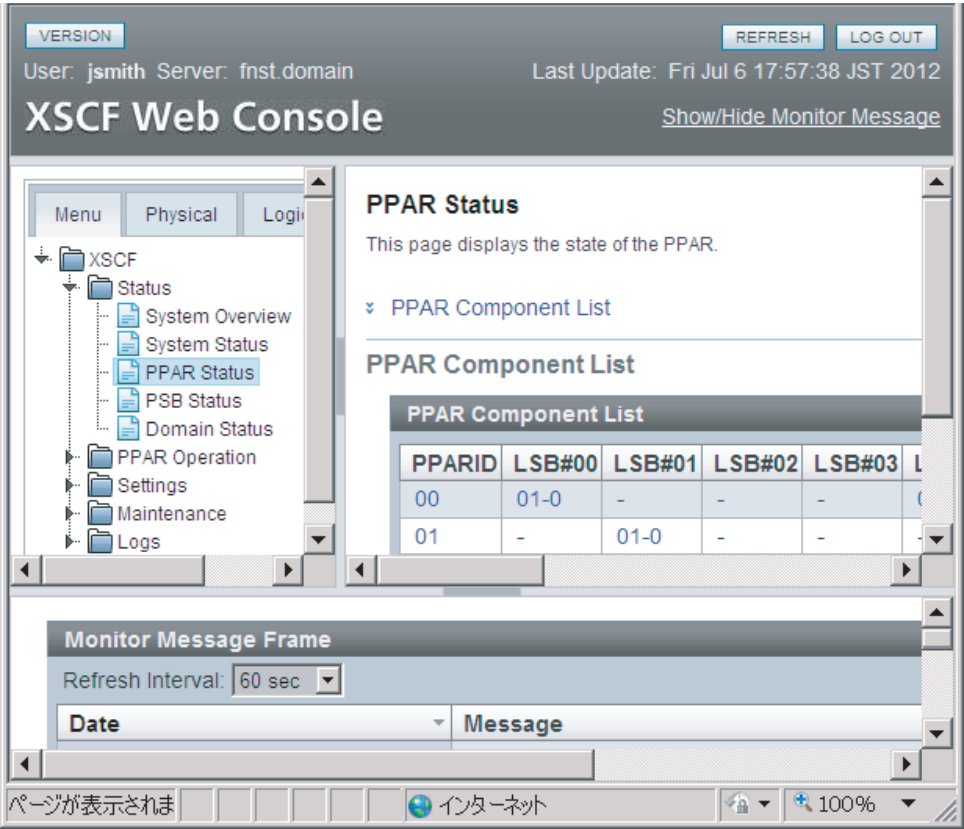


- **XSCF Web (interface utilisateur du navigateur)**

Cette interface vous permet de connecter le PC d'un utilisateur au LAN XSCF LAN via Ethernet et d'effectuer des communications à l'aide des protocoles HTTPS et SSL/TLS. Par conséquent, vous pouvez utiliser un navigateur Internet sur le PC pour utiliser la console XSCF Web. Avec le web XSCF, vous pouvez réduire la charge des opérations effectuées par les utilisateurs et réduire les coûts de gestion du serveur en affichant les composants de manière hiérarchique et en trouvant les opérations destinées à ces effets, à partir du menu.

Figure 1-4 illustre un exemple d'utilisation de la console Web XSCF.

Figure 1-4 Exemple de la console XSCF Web



XSCF dans la configuration de bloc de construction

Lorsque le système est configuré en utilisant le système de bloc de construction, le boîtier à barre transversale (XBBOX) contient également le XSCF. Le montage du XSCF dans le serveur et du XBBOX favorise une fiabilité élevée du système.

Remarque : si un système est configuré en utilisant le système de bloc de construction, les châssis SPARC M12-2S et SPARC M10-4S ne peuvent pas être mélangés dans la configuration.

Figure 1-5 illustre un exemple de système SPARC M12-2S ou SPARC M10-4S dans la configuration 4BB, avec des châssis directement interconnectés.

Figure 1-5 Exemple de configuration XSCF d'un système SPARC M12-2S/M10-4S (sans boîtier à barre transversale)

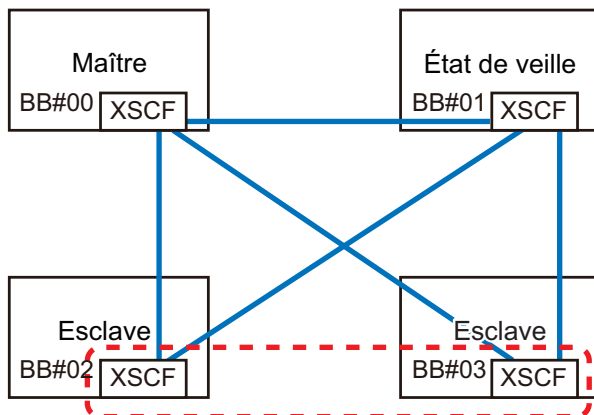
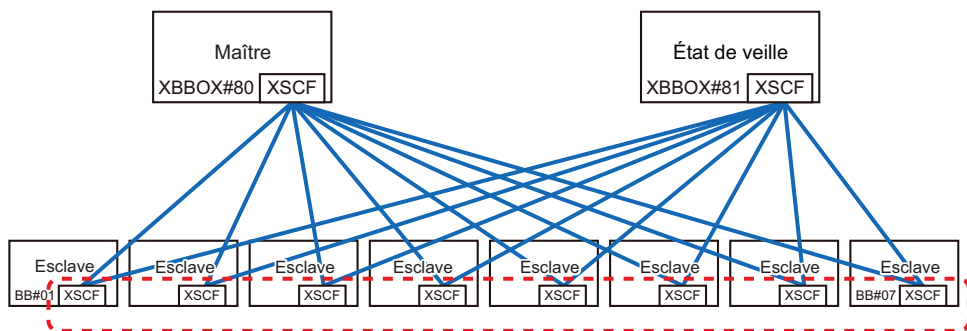


Figure 1-6 illustre un exemple de système SPARC M12-2S ou SPARC M10-4S dans la configuration 8BB avec un boîtier à barre transversale.

Figure 1-6 Exemple de configuration XSCF d'un système SPARC M12-2S/M10-4S (avec boîtier à barre transversale)



Les XSCF dans la configuration de bloc de construction sont classés en trois rôles : maître, de veille et esclave. Pour plus de détails, consultez « [1.2.4 Mécanisme XSCF maître/de veille/esclave](#) ».

Interfaces externes

Les châssis individuels et les boîtiers à barre transversale installés sur le SPARC M12/M10 possèdent les connecteurs XSCF (ports) et DEL suivants. Les utilisateurs, administrateurs système et ingénieurs de terrain peuvent contrôler et utiliser les serveurs grâce à ces interfaces et au microprogramme XSCF. Pour connaître l'emplacement de chaque interface et obtenir des détails sur chaque méthode de connexion, consultez l'un des éléments suivants.

- « Confirmer les caractéristiques du port d'interface externe » dans le *Guide d'installation* de votre serveur
- « Understanding the LED Indications » dans le *Service Manual* de votre serveur
- Port série

Le port série est utilisé avec le shell XSCF afin de configurer le serveur et afficher l'état du serveur. Le port série (RS-232C) utilise un connecteur RJ-45. La connexion entre le port série et l'ordinateur est effectuée via un câble série croisé RS-232C. Si vous effectuez la connexion avec un câble LAN, la connexion nécessite un câble de conversion RJ-45/RS-232C ou un connecteur de conversion.

- **Port XSCF-LAN (port Ethernet)**
Le port XSCF LAN est le port de connexion LAN, utilisé par l'administrateur du système afin d'utiliser le serveur via Ethernet. Le port XSCF-LAN permet à l'administrateur système de configurer le serveur et de consulter l'état du serveur en utilisant le Shell XSCF ou XSCF Web. Deux ports XSCF-LAN sont utilisés. Ces deux ports utilisent un connecteur RJ-45. Chaque port prend uniquement en charge la négociation automatique 10Base-T/100Base-TX/1000Base-T. La vitesse de connexion/le mode de connexion du XSCF-LAN ne peuvent pas être réglés.
- **Ports USB**
Le panneau avant possède un port USB (Type A) tandis que le panneau arrière possède deux ports USB pour les connexions avec les périphériques USB. Utilisez ces ports USB pour connecter un lecteur DVD afin d'installer Oracle Solaris par exemple. Le port USB dédié XSCF situé sur le panneau arrière prend en charge l'interface USB 1.1 ou USB 2.0. Utilisez-le pour enregistrer et restaurer les informations matérielles du XSCF et collecter les informations de journalisation.
- **DEL**
Les DEL suivantes concernent le XSCF et le XSCF-LAN.
 - **DEL PRÊT (vert)**
La DEL PRÊT s'allume en vert. La DEL PRÊT commence immédiatement à clignoter lorsque l'alimentation est activée. Lorsque la DEL clignote, cela indique que le XSCF est en train de s'activer et de s'initialiser. À la fin de l'initialisation, la DEL arrête de clignoter et reste allumée en continu.
 - **DEL DE CONTRÔLE (orange)**
La DEL DE CONTRÔLE s'allume en orange. La DEL DE CONTRÔLE s'allume immédiatement une fois l'alimentation du serveur activée. Cependant, la DEL DE CONTRÔLE reste éteinte lorsque le matériel fonctionne normalement. Elle s'allume lorsque le matériel a une défaillance.
 - **DEL MAÎTRE (verte, uniquement pour le système SPARC M12-2S/M10-4S)**
La DEL MAÎTRE s'allume en vert. La DEL MAÎTRE indique le châssis du SPARC M12-2S, le châssis du SPARC M10-4S ou le boîtier à barre transversale qui possède le XSCF maître, dans un système doté de plusieurs XSCF. Elle s'allume pour le XSCF maître et reste éteinte pour les XSCF de veille et esclave.
 - **VITESSE DE LIAISON (vert ou orange)**
Chaque port XSCF-LAN possède la DEL de vitesse de liaison, qui s'allume en vert ou orange. La DEL de vitesse de liaison s'allume en orange pour la connexion LAN 1 000 Mbit/s et en vert pour la connexion LAN 100 Mbit/s. Elle s'éteint avec une connexion LAN 10 Mbit/s.
 - **DEL ACT (vert)**
Chaque port XSCF-LAN possède une DEL ACT, qui s'allume en vert. Elle clignote en vert lorsque des données sont envoyées ou reçues. Elle s'éteint lorsqu'aucune donnée n'est envoyée ou reçue.
- **Protocole pour le port de communication SP à SP (port SSCP)**

Dans le système avec une configuration de bloc de construction et de plusieurs unités XSCF, les connecteurs (ports) suivants sont installés sur chaque châssis SPARC M12-2S ou SPARC M10-4S et sur les boîtiers à barre transversale, car les communications sont effectuées entre les processeurs de service. Pour la configuration des connexions entre XSCF, consultez « Chapitre 4 Réglage du SPARC M12-2S dans une configuration de bloc de construction » dans le *Guide d'installation Fujitsu SPARC M12-2S* ou « Chapitre 4 Configuration des connexions des blocs de construction » dans le *Guide d'installation Fujitsu M10-4S/SPARC M10-4S*.

- Côté SPARC M12-2S/M10-4S

Port de contrôle XSCF DUAL : 1 port. Ce port permet de connecter le XSCF maître et le XSCF de veille.

Port de contrôle XSCF BB : 3 ports. Ces ports connectent les XSCF maître et de veille aux XSCF esclaves.

- Côté boîtier à barre transversale

Port de contrôle XSCF DUAL : 1 port. Ce port permet de connecter le XSCF maître et le XSCF de veille.

Port de contrôle XSCF BB : 19 ports. Ces ports connectent les XSCF maître et de veille aux XSCF esclaves.

1.2.3 Fonctions de XSCF

Shell XSCF et XSCF Web

XSCF fournit le shell XSCF et le web XSCF, permettant aux utilisateurs d'afficher l'état du serveur, d'utiliser le serveur, d'afficher l'état de la partition physique, d'utiliser une partition physique, et d'afficher une console.

Initialisation du système et diagnostic initial

Le XSCF effectue lui-même un diagnostic initial au moment de l'alimentation ou du redémarrage du XSCF afin de détecter toute panne dans le XSCF et en informer l'utilisateur. Il définit également les paramètres initiaux du XSCF et initialise le matériel nécessaire au démarrage d'Oracle Solaris.

Reconnaissance de la configuration du système et gestion de la configuration des partitions physiques

Le XSCF gère les ressources de processeur, de mémoire et de système d'E/S depuis le châssis, affiche l'état de configuration du système et crée et modifie la configuration de partition physique.

Dans le SPARC M12-2S et le SPARC M10-4S, les utilisateurs peuvent configurer une partition physique en connectant plusieurs châssis à l'aide du système de bloc de construction avec un châssis (1BB) en tant qu'unité minimale. Les châssis (BB) et les unités de configuration de la partition physique sont gérés par les numéros logiques (numéros de LSB), qui sont reconnus par les domaines logiques.

De plus, grâce à une liaison avec le microprogramme superviseur, le microprogramme

XSCF surveille les ressources de mémoire, de processeur et d'E/S utilisées par les domaines logiques configurés à partir du logiciel Oracle VM Server pour SPARC.

Remarque : un système d'une unité SPARC M12/M10 est composé d'une seule partition physique.

Fonctions RAS et surveillance de panne

Le batch XSCF contrôle/surveille le serveur afin d'assurer la stabilité du fonctionnement du système. Lorsqu'il détecte une panne de système, il commence immédiatement à collecter les informations de journalisation du matériel, effectue une analyse, identifie le lieu de la panne, et détermine l'état de cette panne. Le XSCF indique l'état du serveur et effectue la détérioration des composants et de la partition physique et la réinitialisation du système au besoin, afin d'éviter une autre panne. Le XSCF assure une grande fiabilité, disponibilité et facilité de gestion (RAS) du système complet.

La cible de contrôle est la suivante.

- Gestion et contrôle de la configuration matérielle
- Contrôle de la configuration réseau
- Surveillance des unités de refroidissement, comme les ventilateurs, et de la température ambiante
- Contrôle de l'état de la partition physique et du domaine logique
- Contrôle des pannes de périphériques

Fonction de transmission des informations sur la panne à l'administrateur système

XSCF contrôle régulièrement le fonctionnement du système. Le XSCF offre les services suivants pour notifier l'administrateur du système des informations de la panne.

- Fonction de surveillance du serveur ne dépendant pas du fonctionnement d'Oracle Solaris
- Contrôle à distance du serveur depuis un site distant
- Notification par e-mail en cas de problème
- Notification de piège utilisant la fonction d'agent SNMP

Messages et journalisation

XSCF collecte et conserve les informations relatives à la panne du système. Les pannes et les emplacements où surviennent les pannes sont identifiés à partir des informations de panne matérielle, qui fournissent également des informations de prévision de pannes, ainsi que des informations correctes et facilement compréhensibles, aux utilisateurs, immédiatement après la manifestation de la panne. Pour plus de détails sur les messages d'erreur et les journaux, consultez « [Chapitre 12 Consultation des journaux et des messages](#) ».

Ci-après, les messages qui s'affichent.

- Message de diagnostic initial au démarrage du système
- Message affiché au même moment que le contrôle de la configuration réseau révèle une panne de configuration
- Message affiché au même moment que la panne d'une pièce est détectée
Grâce aux informations de suivi de l'état de l'unité d'alimentation, du ventilateur, de la carte système, la mémoire, CPU et d'autres composants, l'administrateur système peut rapidement déterminer la pièce à remplacer.
- Message affiché au même moment qu'une panne environnementale est détectée
Le contrôle de la température du serveur et du CPU peut éviter l'instabilité du système due à l'augmentation de température.

Ci-après, les journaux collectés.

- Journal d'erreur
- Journal des messages de surveillance
- Journal d'alimentation
- Journal des événements
- Journal de la console
- Journal de panique
- Journal IPL
- Journal d'audit
- Journal COD
- Journal de l'historique de la température
- Journal Active Directory
- Journal LDAP sur SSL

Gestion du compte d'utilisateur XSCF

Le XSCF permet de gérer les comptes d'utilisateur permettant d'utiliser le XSCF. Les types de privilèges de comptes d'utilisateur gérés par XSCF sont énumérés ci-après. Les opérations disponibles sur le shell XSCF et le web XSCF fournis dépendent du type de compte d'utilisateur (désigné privilège d'utilisateur).

- Administrateur système
- Administrateur de la partition physique
- Opérateur
- Technicien sur site

Sécurité

Le XSCF fournit des fonctions de chiffrement et d'audit par SSH et SSL/TLS. Les erreurs d'ordre opérationnel et les données d'accès invalide sont enregistrées dans les journaux pendant que le système fonctionne. L'administrateur système peut utiliser les journaux pour étudier les causes des pannes système ou des accès invalides.

Assistance dans le remplacement actif d'une pièce

Pendant le remplacement actif d'une pièce, XSCF participe aux travaux de maintenance à travers le shell XSCF. Lorsqu'une commande de maintenance est exécutée, le menu maintenance apparaît. L'utilisateur peut alors suivre les instructions du menu pour effectuer la maintenance.

Fonction de redirection de la console

Le XSCF offre des fonctions permettant d'effectuer une sortie vers la console OS (console du domaine de commande) d'Oracle Solaris dans chaque partition physique. En effectuant une connexion SSH (Secure Shell) ou Telnet vers le XSCF, celui-ci peut servir de console OS.

Fonction de gestion/enregistrement d'activation du processeur

L'enregistrement de la clé d'activation de processeur avec le XSCF permet l'utilisation permanente des ressources de processeur du serveur. Il importe d'acheter une ou plusieurs clés d'activation du CPU avant que le serveur ne commence à fonctionner.

Le XSCF effectue le travail d'ajout d'une clé d'activation de processeur lorsque des ressources de processeur supplémentaires deviennent nécessaires. Le XSCF effectue le travail de retrait d'une clé d'activation de processeur lorsque vous souhaitez diminuer les ressources de processeur.

Pour plus de détails sur l'utilisation de ressources de cœur de processeur, consultez « [Chapitre 5 Activation de processeur](#) ».

Fonction de mise à jour du microprogramme

En utilisant des commandes de XSCF Web et du Shell XSCF, un nouveau microprogramme (microprogramme XSCF, OpenBoot PROM, POST ou superviseur) est téléchargeable sans nécessiter la mise hors tension de la partition physique. De plus, les mises à jour du microprogramme sont applicables sans mettre les autres partitions physiques hors tension. Notez que si vous mettez à jour les microprogrammes OpenBoot PROM, POST ou superviseur lorsque la partition physique est démarrée, la mise à jour est appliquée lors du redémarrage de la partition physique. Pour plus de détails sur les mises à jour du microprogramme, consultez « [Chapitre 16 Mise à jour du microprogramme XCP](#) ».

Fonction d'informatique verte

Oracle Solaris, le superviseur et XSCF coupent l'alimentation des composants inutilisés pour réduire leur consommation électrique. De plus, le XSCF peut contrôler la limite supérieure autorisée de la consommation électrique pour réduire la consommation du système. Si la limite supérieure est dépassée, le XSCF détermine immédiatement les opérations électriques du système et effectue un arrêt ou une mise hors tension.

Contrôle de l'heure

Le SPARC M12/M10 règle l'horloge XSCF selon l'heure de référence du système. Les partitions physiques des systèmes SPARC M12/M10 synchronisent l'heure avec

l'horloge XSCF au démarrage de la partition physique. Le XSCF gère les différences d'heure à partir du domaine de commande en coopération avec le microprogramme superviseur.

Fonction de reconfiguration dynamique de la partition physique (PPAR DR)

Dans une configuration de bloc de construction, le XSCF prend en charge l'opération nécessaire à la modification dynamique de la configuration de la partition physique pendant que le système fonctionne. La reconfiguration dynamique de la partition physique (PPAR DR) vous permet d'ajouter ou supprimer un bloc de construction (SPARC M12-2S ou SPARC M10-4S) de la partition physique, pendant le fonctionnement de la partition physique. Pour plus de détails sur la fonction PPAR DR, consultez le *Guide de configuration du domaine Fujitsu SPARC M12 et Fujitsu M10/SPARCM10*.

Remarque : dans le SPARC M12-1/M12-2/M10-1/M10-4, la fonction PPAR DR ne peut pas être utilisée.

1.2.4 Mécanisme XSCF maître/de veille/esclave

Lorsque le SPARC M12-2S ou SPARC M10-4S est connecté par le système de bloc de construction, un XSCF est placé dans chaque châssis et boîtier à barre transversale SPARC M12-2S ou SPARC M10-4S. Les XSCF sont classés en trois types selon leurs rôles.

- XSCF maître
Le système ne comporte qu'un XSCF maître. En plus de surveiller et gérer le système complet, le XSCF maître gère également le SPARC M12-2S, SPARC M10-4S ou le boîtier à barre transversale sur lequel il est installé. Pour ce qui est de la duplication, un XSCF de veille fonctionne à titre de remplacement du XSCF maître.
- XSCF esclave
Le XSCF esclave est un XSCF autre que le XSCF maître. Le XSCF esclave surveille et gère uniquement le SPARC M12-2S, SPARC M10-4S ou le boîtier à barre transversale sur lequel il est installé.
- XSCF de veille
Ce XSCF fonctionne à titre de remplacement du XSCF maître. Il est également appelé XSCF de veille. Un XSCF de veille est inclus dans le XSCF esclave.

Le XSCF maître et le XSCF de veille se surveillent mutuellement. En cas de panne du XSCF maître, celui-ci peut devenir le XSCF de veille, afin d'assurer le fonctionnement et la gestion continus du système, sans interruption de l'activité.

Le XSCF maître est connecté aux XSCF esclaves via des câbles dédiés par le protocole dédié à XSCF appelé protocole de communication SP à SP (SSCP). Les paramètres configurés pour le XSCF maître sont appliqués sur les XSCF esclaves via SSCP. Les paramètres configurés pour une partition physique spécifique ne sont appliqués que sur les XSCF appartenant à la PPAR cible.

1.2.5 Différences entre les configurations XSCF par modèle

Cette section décrit comment les XSCF sont configurés et comment le système est surveillé et géré, pour les configurations respectives de SPARC M12/M10.

SPARC M12-1/M12-2/M10-1/M10-4, et SPARC M12-2S/M10-4S dans une configuration d'unité unique

Le SPARC M12-1/M12-2/M10-1/M10-4 et SPARC M12-2S/M10-4S dans une configuration d'unité unique n'emploient qu'un seul XSCF chacun. Aucun XSCF de veille ou XSCF esclave n'est disponible.

SPARC M12-2S/M10-4S dans une configuration de bloc de construction (sans boîtier à barre transversale)

Pour la configuration de bloc de construction sans boîtier à barre transversale, le système SPARC M12-2S/M10-4S est configuré avec quatre châssis SPARC M12-2S ou SPARC M10-4S maximum, donc quatre XSCF maximum sont configurés en conséquence. Dans ce cas, le XSCF se trouvant dans le châssis BB#00 ou BB#01 est le XSCF maître ou le XSCF de veille. Si une erreur se produit pour le XSCF maître, le XSCF de veille devient le XSCF maître. Les châssis BB#02 et BB#03 sont établis comme XSCF esclaves.

- Types de connexion

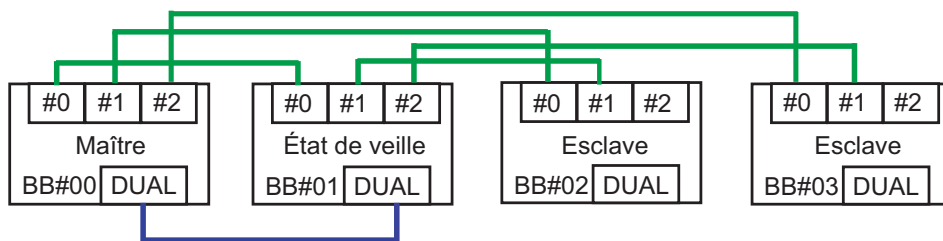
Le port de contrôle XSCF BB du XSCF maître (BB#00 se trouvant dans [Figure 1-7](#)) est connecté au port de contrôle XSCF BB dont l'ID de réseau est 0 (#0 port de BB#01 à BB#03 se trouvant dans [Figure 1-7](#)) sur chaque XSCF esclave.

Le port de contrôle XSCF BB du XSCF de veille (BB#01 se trouvant dans [Figure 1-7](#)) est connecté au port de contrôle XSCF BB dont l'ID de réseau est 1 (#1 port de BB#02 et BB#03 se trouvant dans [Figure 1-7](#)) sur chaque XSCF esclave. Le XSCF maître et le XSCF de veille sont connectés via des ports appelés DUAL. Le XSCF esclave n'est connecté qu'aux XSCF maître et de veille.

- Flux de contrôle XSCF

Le XSCF maître surveille et gère tous les XSCF. En principe, les différents paramètres du XSCF sont définis à partir du XSCF maître. Les paramètres configurés par le XSCF maître sont appliqués à tous les XSCF esclaves dont le XSCF de veille via le réseau SSCP. De même, les paramètres configurés par le XSCF maître d'un châssis SPARC M12-2S ou SPARC M10-4S donné sont également appliqués au XSCF de veille et esclave du châssis SPARC M12-2S ou SPARC M10-4S concerné.

Figure 1-7 Connexions XSCF (pour le SPARC M12-2S/M10-4S dans une configuration de bloc de construction (sans boîtier à barre transversale))



SPARC M12-2S/M10-4S dans une configuration de bloc de construction (avec boîtier à barre transversale)

Le SPARC M12-2S ou SPARC M10-4S en configuration de bloc de construction (avec boîtiers à barre transversale) est configuré avec 16 XSCF maximum ou les boîtiers à barre transversale avec quatre XSCF maximum. Dans ce cas, le XSCF se trouvant dans le boîtier à barre transversale XBBOX#80 ou XBBOX#81 est le XSCF maître ou de veille. Les XSCF des boîtiers à barre transversale XBBOX#82 et XBBOX#83 et de tous les châssis SPARC M12-2S ou SPARC M10-4S sont établis comme XSCF esclaves.

■ Types de connexion

- Connexion aux boîtiers à barre transversale

Le XSCF maître (XBBOX#80) est connecté au port de contrôle BB XSCF avec l'ID réseau 16 (port #16 de XBBOX#81 à XBBOX#83 dans [Figure 1-8](#)) sur chaque XSCF esclave. Le XSCF de veille (XBBOX#81) est connecté au port de contrôle BB XSCF avec l'ID réseau 17 (port #17 de XBBOX#82 et XBBOX#83 dans [Figure 1-8](#)) sur chaque XSCF esclave. Le XSCF maître et le XSCF de veille sont connectés via des ports appelés DUAL. Le XSCF esclave n'est connecté à aucun autre XSCF que le XSCF maître et le XSCF de veille.

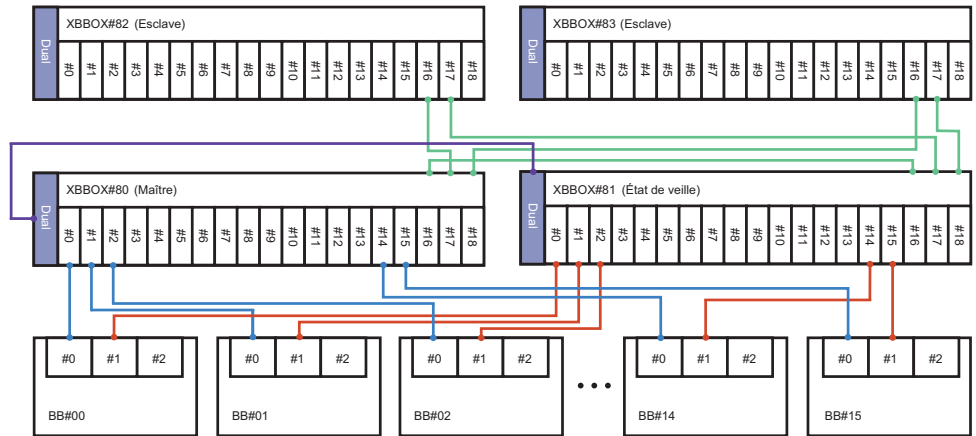
- Connexions au SPARC M12-2S/M10-4S

Le XSCF maître (XBBOX#80) est connecté au port de contrôle BB XSCF avec l'ID réseau 0 (port #0 de BB#00 à BB#15 dans [Figure 1-8](#)) sur chaque XSCF esclave. Le XSCF de veille (XBBOX#81) est connecté au port de contrôle BB XSCF avec l'ID réseau 1 (port #1 de BB#00 et BB#15 dans [Figure 1-8](#)) sur chaque XSCF esclave. Les XSCF fixés au XSCF esclave (BB#00 à BB#15) ne sont connectés qu'aux XSCF maître et de veille.

■ Flux de contrôle XSCF

Le XSCF maître surveille et gère tous les XSCF. En principe, les différents paramètres du XSCF sont définis à partir du XSCF maître. Les paramètres configurés par le XSCF maître sont appliqués à tous les XSCF esclaves dont le XSCF de veille via le réseau SSCP. De même, les paramètres configurés par le XSCF maître d'un châssis SPARC M12-2S ou SPARC M10-4S donné sont également appliqués au XSCF de veille et esclave du châssis SPARC M12-2S ou SPARC M10-4S concerné.

Figure 1-8 Connexions XSCF (pour le SPARC M12-2S/M10-4S dans une configuration de bloc de construction (avec boîtier à barre transversale))



1.3 Configuration réseau

1.3.1 Présentation des connexions réseau

Cette section présente les connexions réseau nécessaires au fonctionnement du système.

Le système est composé de deux réseaux principaux. L'un est le réseau utilisateur et l'autre un réseau de contrôle du système.

- Réseau utilisateur

Le réseau utilisateur est utilisé pour appliquer un système configuré pour l'activité. Le réseau utilisateur est connecté à d'autres serveurs, PC et périphériques requis pour les tâches, et configuré correctement.

L'environnement réseau utilisateur est sécurisé par l'installation d'un pare-feu et par d'autres mesures de sécurité, selon la nécessité lorsque le réseau peut être connecté à Internet de façon externe.

- Réseau de contrôle du système (réseau XSCF)

Le réseau de contrôle du système (réseau XSCF) est utilisé dans le cadre de la gestion et de la maintenance du système. Ce réseau est également utilisé lors de l'exploitation du microprogramme XSCF, qui est utilisé pour contrôler et gérer le système, activer/désactiver les opérations, et pour les opérations de remplacement de composants. Pour effectuer des opérations dans le cadre du contrôle à distance du système, le réseau de contrôle du système est configuré dans un environnement adapté pour les opérations.

Le réseau de contrôle du système peut également être connecté à un réseau

utilisateur pour lequel des mesures de sécurité, telles qu'un pare-feu, doivent prises pour éviter les accès externes non valides au réseau de contrôle du système.

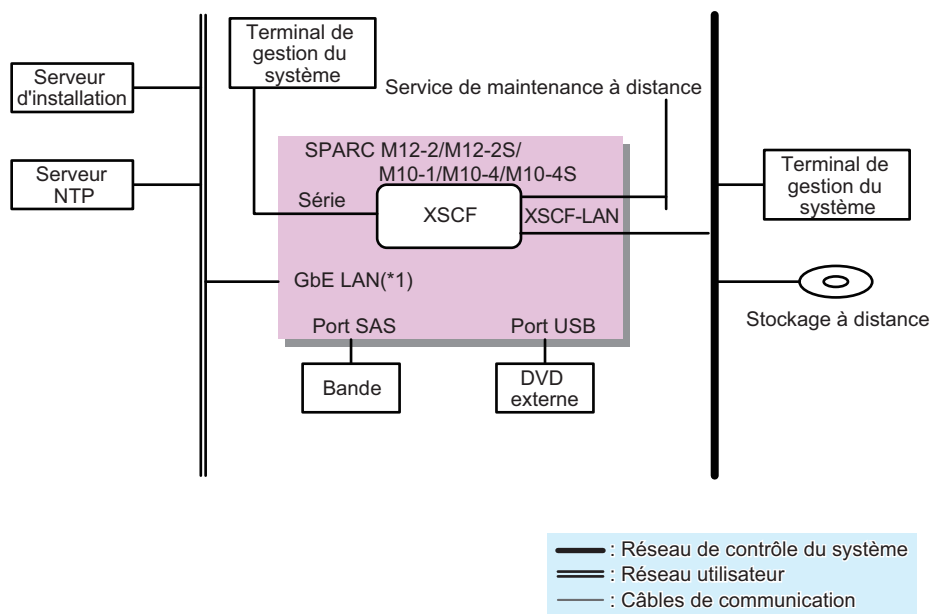
Le terminal utilisé pour effectuer la maintenance et la gestion du système (terminal de gestion du système) est connecté via un port série ou LAN, selon le cas. Pour plus d'informations sur les types de terminal de gestion de système, consultez « 2.1 Connexion du terminal de gestion du système ».

L'exemple suivant présente la configuration d'un système SPARC M12/M10.

Figure 1-9 présente une configuration qui utilise un SPARC M12/M10.

Le terminal de gestion du système est connecté au port XSCF-LAN via le port série ou le réseau de contrôle du système. Le stockage à distance est connecté au port XSCF-LAN via le réseau de contrôle du système. Les ports LAN GbE ou LAN 10GbE sont connectés au serveur d'installation et à d'autres via le réseau utilisateur. De plus, les ports SAS sont connectés aux périphériques externes à interface SAS tels que les unités à bande, et les ports USB sont connectés aux périphériques externes à interface USB, tels que les lecteurs DVD externes.

Figure 1-9 Exemple de configuration des connexions de la configuration d'unité unique du SPARC M12-1/M12-2/M12-2S/M10-1/M10-4/M10-4S

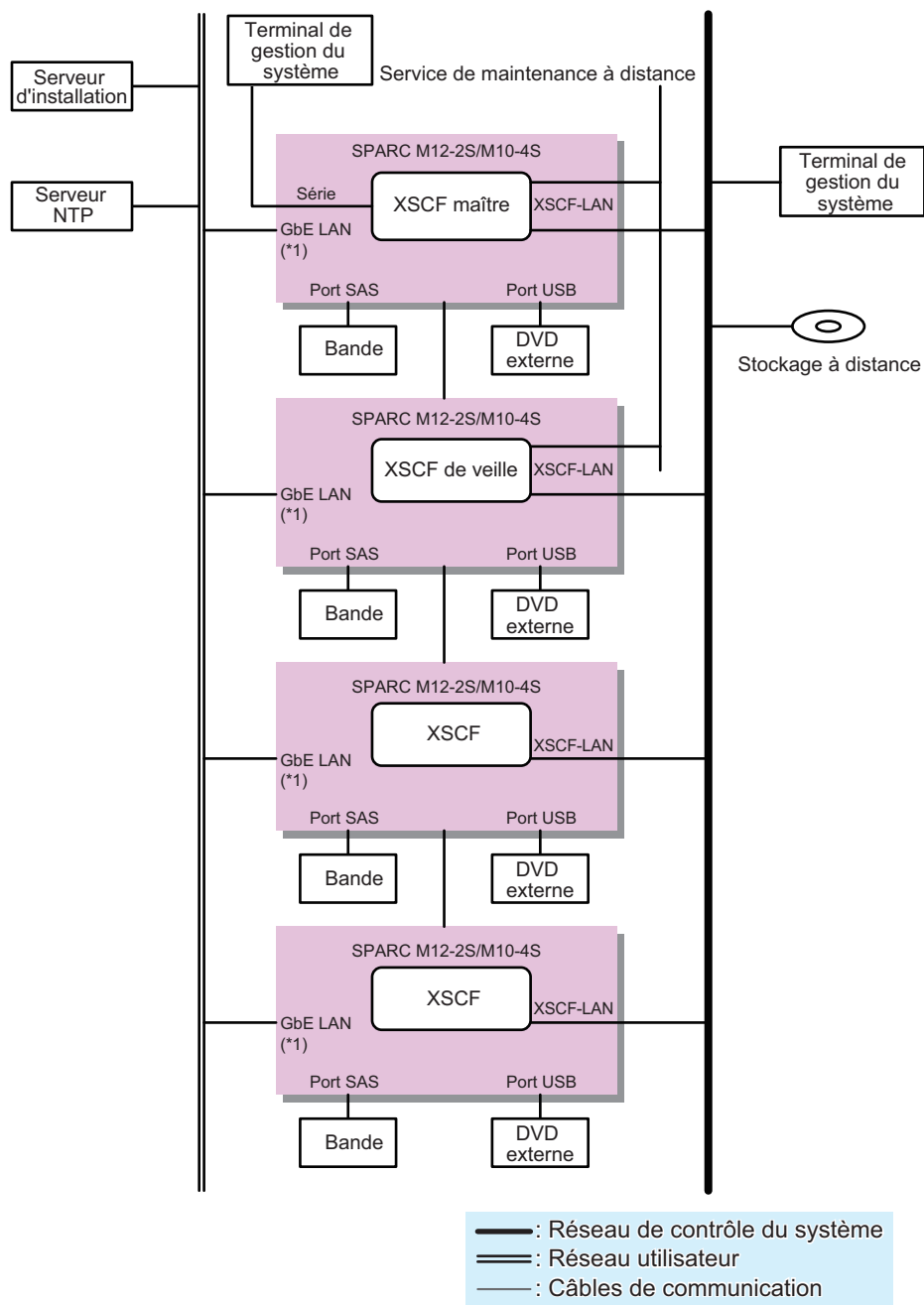


*1 LAN 10GbE pour SPARC M12-1/M12-2/M12-2S

Figure 1-10 présente une configuration qui comprend quatre unités SPARC M12-2S ou SPARC M10-4S connectées sans avoir recours aux boîtiers à barre transversale. Le terminal de gestion du système est connecté au port série du XSCF maître ou aux ports XSCF-LAN du XSCF maître et du XSCF de veille via le réseau de contrôle du système. Le port LAN 10GbE de quatre unités SPARC M12-2S ou le port LAN GbE de quatre unités SPARC M10-4S est connecté au serveur d'installation et à d'autres via le réseau utilisateur. De plus, les ports SAS sont connectés aux périphériques

externes à interface SAS tels que les unités à bande, et les ports USB sont connectés aux périphériques externes à interface USB, tels que les lecteurs DVD externes.

Figure 1-10 Exemple de configuration des connexions SPARC M12-2S/M10-4S (sans boîtier à barre transversale)



*1 LAN 10GbE pour SPARC M12-2S

Figure 1-11 présente une configuration qui comprend plusieurs unités SPARC M12-2S ou SPARC M10-4S connectées grâce à des boîtiers à barre transversale. Le terminal de gestion du système est connecté au port série du XSCF maître dans le boîtier à barre transversale ou aux ports XSCF-LAN du XSCF maître et du XSCF de veille via le réseau de contrôle du système. Le stockage à distance est connecté au XSCF-LAN de chaque unité SPARC M12-2S ou SPARC M10-4S via le réseau de contrôle du système.

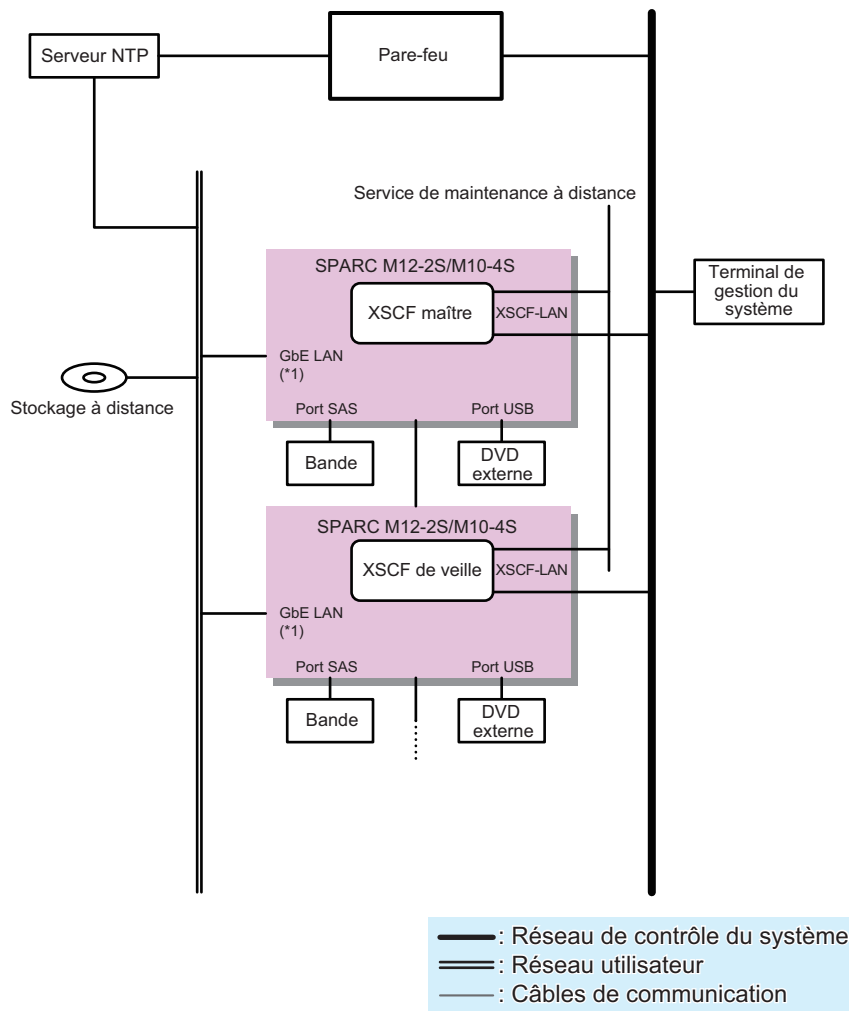
Le port LAN 10GbE du SPARC M12-2S ou le port LAN GbE du SPARC M10-4S est connecté au serveur d'installation et à d'autres via le réseau utilisateur. De plus, les ports SAS des unités SPARC M12-2S ou SPARC M10-4S sont connectés aux périphériques externes à interface SAS tels que les unités à bande, et les ports USB sont connectés aux périphériques externes à interface USB, tels que les lecteurs DVD externes.

Figure 1-12 présente une configuration qui connecte le réseau de contrôle du système et le réseau utilisateur par l'intermédiaire du pare-feu.

Ici, pour utiliser un serveur NTP afin de synchroniser l'heure des XSCF, le serveur NTP sur le réseau utilisateur est connecté par l'intermédiaire du pare-feu. La connexion par l'intermédiaire du pare-feu peut protéger les XSCF contre les menaces de sécurité sur le réseau utilisateur.

Pour le stockage à distance placé sur le réseau utilisateur, vous pouvez le connecter au XSCF-LAN tout en le protégeant contre les menaces de sécurité en configurant l'accès au stockage à distance dans le pare-feu.

Figure 1-12 Configuration permettant de connecter le réseau de contrôle du système et le réseau utilisateur



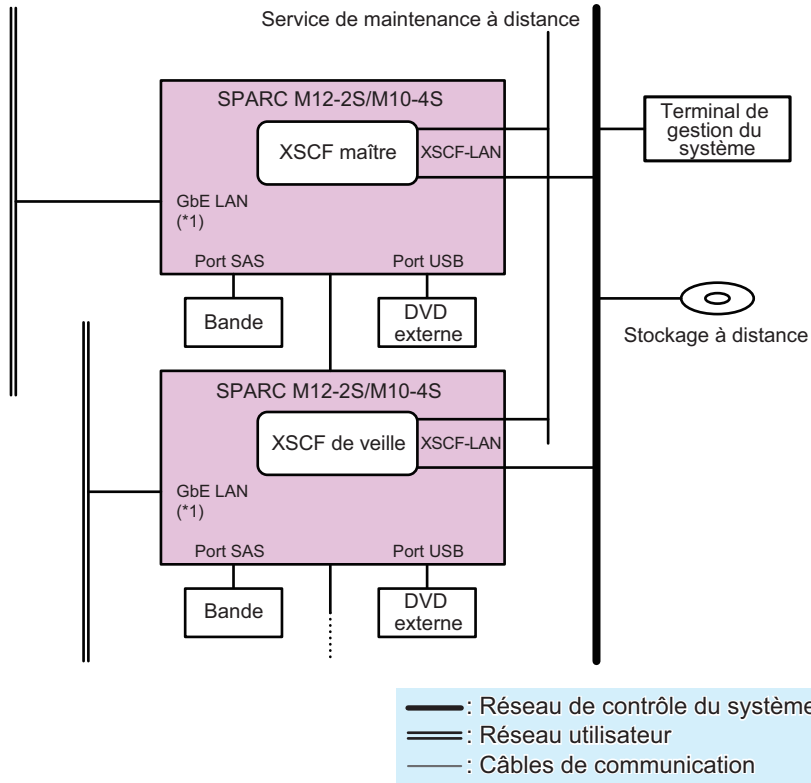
*1 LAN 10GbE pour SPARC M12-2S

Figure 1-13 présente un système dans une configuration de bloc de construction où chaque unité SPARC M12-2S ou SPARC M10-4S est connectée à un réseau utilisateur

séparé.

Séparer le segment du réseau utilisateur connecté au LAN 10GbE de chaque unité SPARC M12-2S ou le segment du réseau utilisateur connecté au LAN GbE de chaque unité SPARC M10-4S réduit le risque de menaces de sécurité sur les réseaux utilisateurs. Le réseau de contrôle du système ne peut pas être séparé pour chaque unité SPARC M12-2S ou SPARC M10-4S dans une configuration de bloc de construction.

Figure 1-13 Configuration permettant de séparer le segment du réseau utilisateur de chaque serveur



*1 LAN 10GbE pour SPARC M12-2S

1.3.2 Numéros et fonctions des ports XSCF-LAN et pare-feu

Tableau 1-1 répertorie les numéros de ports utilisés avec les ports XSCF-LAN et les fonctions utilisés par XSCF. Pour protéger le XSCF des accès non autorisés et des attaques lorsqu'il est connecté à un réseau externe, il est recommandé de configurer un pare-feu. Lors de la mise en place d'un pare-feu, vous devez autoriser le passage de paquets entre les ports, comme nécessaire.

Tableau 1-1 Numéros de port de XSCF-LAN, fonctions et direction de la connexion

Numéro de port/ Protocole	Fonction	Direction de la connexion(*)
21/TCP	Transfert externe du shell XSCF (FTP)	XSCF -> Réseau externe (21)
22/TCP	Shell XSCF (SSH)	Réseau externe -> XSCF (22)
	Transfert externe du shell XSCF (SSH)	XSCF -> Réseau externe (22)
23/TCP	Shell XSCF (Telnet)	Réseau externe -> XSCF (23)
25/TCP	E-mail de notification et service de maintenance à distance	XSCF -> Réseau externe (25)
53/TCP 53/UDP	DNS	XSCF (53) -> Réseau externe (53)
80/TCP	Transfert externe du shell XSCF (HTTP)	XSCF -> Réseau externe (80)
110/TCP	E-mail de notification et authentification POP, Service de maintenance à distance par authentification POP	XSCF -> Réseau externe (110)
123/UDP	Synchronisation de l'heure via le serveur NTP	XSCF (123) -> Réseau externe (123)
	Synchronisation de l'heure via le client NTP	Réseau externe (123) -> XSCF (123)
161/UDP	Fonction SNMP	Réseau externe -> XSCF (161)
162/UDP	Fonction d'interruption SNMP	XSCF -> Réseau externe (162)
389/TCP	Authentification par LDAP et Active Directory	XSCF -> Réseau externe (389)
443/TCP	XSCF Web (HTTPS)	Réseau externe -> XSCF (443)
	Transfert externe du shell XSCF (HTTPS)	XSCF -> Réseau externe (443)
465/TCP	Service de maintenance à distance (SMTP sur SSL)	XSCF -> Réseau externe (465)
587/TCP	E-mail de notification et authentification SMTP, Service de maintenance à distance par authentification SMTP	XSCF -> Réseau externe (587)
623/UDP	Fonction de gestion d'alimentation à distance utilisant IPMI	XSCF (623) <-> Réseau externe (623)
636/TCP	Authentification par LDAP sur SSL, Active Directory	XSCF -> Réseau externe (636)
3260/TCP	Stockage à distance	XSCF -> Réseau externe (3260)
6481/TCP	Fonction d'Auto Service Request (ASR) (étiquette de service)	Réseau externe (6481) -> XSCF (6481)
6481/UDP	(*2)	

*1 Chaque symbole et numéro entre parenthèses a la signification suivante :

Symbol -> : Indique la direction de gauche à droite. <-> : Indique la direction de gauche à droite ou de droite à gauche.

Nombre entre parenthèses : numéro de port de connexion. Pour une connexion à un réseau externe, le numéro du port du réseau peut être modifié sur le XSCF. Pour plus de détails, consultez la section de la fonction correspondante dans ce document. Pour une connexion au stockage à distance, le numéro de port du stockage est fixe (3260).

*2 La fonction ASR est un service de maintenance à distance qui utilise le logiciel Oracle Auto Service Request fourni par l'entreprise Oracle. Pour plus d'informations sur la fonction ASR, consultez le *Oracle Auto Service Request Installation and Operations Guide* relatif à la version du logiciel que vous utilisez.

1.4 Bases du microprogramme superviseur

Cette section donne un aperçu du microprogramme superviseur intégré aux systèmes SPARC M12/M10.

Le microprogramme superviseur est destiné à la mise en place de la virtualisation. Il est monté sur la mémoire CPU.

Des microprogrammes et logiciels différents tels que le microprogramme XSCF et Oracle Solaris, qui est installé sur les domaines logiques, fonctionnent sur chaque système SPARC M12/M10. Ces microprogrammes et logiciels gèrent tout le système. Le microprogramme superviseur est placé entre le microprogramme XSCF et Oracle Solaris pour fonctionner comme une interface afin de poster des informations de réglage de XSCF vers les domaines logiques et d'informer le XSCF de l'état des domaines logiques.

Ci-après, les principales fonctions du microprogramme superviseur.

- Transmission d'informations entre les partitions physiques gérées par XSCF et les domaines logiques gérés par Oracle VM Server pour SPARC
Oracle VM Server pour SPARC configure les domaines logiques en fonction des informations de configuration PPAR (PCL) transmises par le XSCF au domaine de commande. De plus, les informations de configuration du domaine logique et les informations liées aux ressources matérielles reconfigurées sont transmises au microprogramme XSCF via le superviseur.

Pour en savoir plus sur les informations de configuration PPAR, consultez « [11.2.2 Vérification de la configuration de la partition physique](#) ».

- Transmission des informations relatives au blocage ou à une panne du domaine logique
Si un domaine logique est bloqué ou en panne, le superviseur informe le XSCF de l'état du domaine logique.
- Transmission d'informations sur la date et l'heure de XSCF et du domaine logique
Le superviseur informe le XSCF des heures de configuration des domaines logiques. Le XSCF enregistre l'heure de chaque domaine logique afin de la différencier de l'heure de configuration de tout le système.

1.5 Bases d'Oracle VM Server pour SPARC

Cette section résume le logiciel Oracle VM Server pour SPARC.

Le logiciel Oracle VM Server pour SPARC est utilisé pour construire l'environnement du domaine local. Il est installé et utilisé dans l'environnement d'Oracle Solaris.

Un domaine logique est configuré à partir de ressources matérielles telles que les CPU, la mémoire et les dispositifs E/S, qui lui sont distribuées de manière flexible, à partir de la partition physique établie par le microprogramme XSCF. Les ressources sont assignées comme un environnement matériel virtuel. Le domaine logique configuré peut exécuter des applications métier, et chacune correspond à un environnement Oracle Solaris indépendant. La construction de plusieurs environnements matériels virtuels sur une ou plusieurs unités SPARC M12 ou SPARC M10 améliore l'utilisation du serveur et peut réduire les coûts, par rapport à l'intégration du serveur.

Les domaines logiques typiques correspondent au domaine de commande, qui crée et contrôle les autres domaines logiques et les domaines invités utilisés pour les applications pour l'activité. Dans chaque système SPARC M12/M10, un domaine de commande est créé par partition physique pour gérer les autres domaines logiques configurés dans la partition physique. Oracle VM Server pour SPARC s'exécute dans le domaine de commande et est utilisé pour construire et gérer les domaines clients. Le domaine de commande sert également à informer le microprogramme XSCF sur les domaines logiques via le superviseur intégré. Les informations de réglage du XSCF sont également envoyées au domaine de commande via le microprogramme superviseur.

Le processeur, la mémoire, le dispositif E/S, et d'autres ressources matérielles même des domaines logiques déjà appliqués aux tâches, peuvent être configurés, selon l'état de fonctionnement du domaine logique. Oracle VM Server pour SPARC implémente également la reconfiguration des ressources matérielles. L'ajout de ressources matérielles à une tâche augmentant temporairement la charge, peut permettre de maintenir une haute disponibilité des ressources matérielles et d'éviter le débordement des tâches.

Pour plus de détails sur la configuration et la reconfiguration des domaines logiques en utilisant Oracle VM Server pour SPARC dans des systèmes SPARC M12/M10, consultez le *Guide de configuration du domaine Fujitsu SPARC M12 et Fujitsu M10/SPARCM10*. Pour plus de détails sur Oracle VM Server pour SPARC, consultez le *Oracle VM Server for SPARC Administration Guide* de la version que vous utilisez.

1.6 Bases d'OpenBoot PROM

Cette section donne un aperçu de OpenBoot PROM.

OpenBoot PROM offre les fonctions de base permettant de démarrer Oracle Solaris.

Sous l'environnement OpenBoot PROM, l'écran de la console affiche une invite de validation. Vous pouvez configurer plusieurs fonctions liées au démarrage d'Oracle Solaris en définissant les variables d'environnement de OpenBoot PROM. Vous pouvez définir les variables de l'environnement OpenBoot PROM à partir de l'une

des commandes suivantes.

- Exécutez la commande `setenv` dans l'environnement OpenBoot PROM (à l'invite de validation).
- Exécutez la commande `eeeprom` dans l'environnement Oracle Solaris.

Par ailleurs, il est possible de remplacer certaines variables de l'environnement OpenBoot PROM à l'aide de la commande `setpparam` du microprogramme XSCF.

Pour plus de détails sur les variables d'environnement et les commandes d'OpenBoot PROM, consultez *OpenBoot 4.x Command Reference Manual* d'Oracle Corporation. Pour plus de détails sur les variables d'environnement et les commandes d'OpenBoot PROM non prises en charge par le SPARC M12/M10, consultez le « [Annexe H Variables d'environnement et commandes d'OpenBoot PROM](#) ».

Connexion à / Déconnexion de XSCF

Ce chapitre décrit les types de connexion du terminal de gestion du système et la méthode de connexion au XSCF.

- [Connexion du terminal de gestion du système](#)
- [Connexion au Shell XSCF](#)
- [Déconnexion du shell XSCF](#)
- [Connexion à XSCF Web](#)
- [Déconnexion de XSCF Web](#)
- [Nombre d'utilisateurs pouvant se connecter](#)

2.1 Connexion du terminal de gestion du système

Cette section décrit les formes de connexion du terminal de gestion du système dans le réseau de contrôle du système. Pour connaître les méthodes de connexion, consultez « [2.2 Connexion au Shell XSCF](#) ».

Les formes de connexion du réseau de contrôle du système sont classées dans les deux types suivants, selon le port raccordé.

- Connexion série
Un câble série est connecté au port série.
- Connexion LAN
Un câble LAN est connecté à un port XSCF-LAN.

Généralement, le terminal de gestion du système avec une connexion au port de série est utilisé pour établir les paramètres initiaux du microprogramme XSCF. Après avoir établi les paramètres réseau de XSCF, une connexion série ou une connexion LAN peut être sélectionnée.

Les sections suivantes décrivent les fonctionnalités de chaque type de connexion.

2.1.1 Connexion avec le port série

Une connexion série est une connexion d'un câble série au port série sur le serveur. Si le SPARC M12-2S ou SPARC M10-4S est dans une configuration de bloc de construction, raccordez le câble série au châssis possédant le XSCF maître. Cet environnement est sûr car le terminal de gestion du système et le XSCF maître sont connectés l'un à l'autre. Lorsque le terminal de gestion du système est connecté par le biais d'une connexion série, l'écran de connexion pour le XSCF maître s'affiche.

Figure 2-1 Port série (SPARC M12-1)

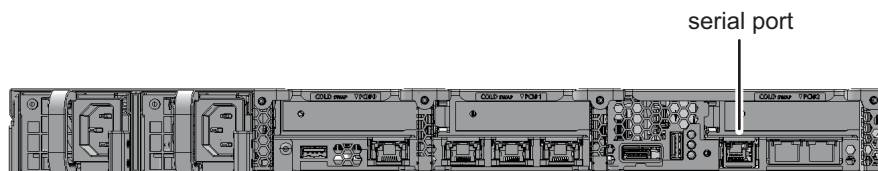


Figure 2-2 Port série (SPARC M12-2)

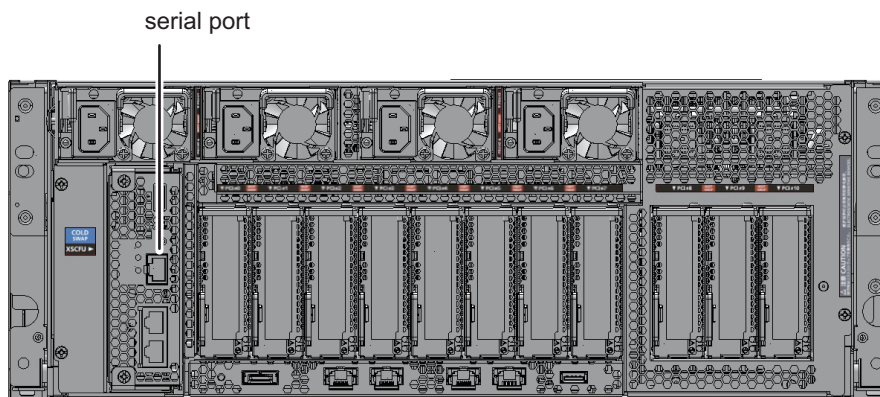


Figure 2-3 Port série (SPARC M12-2S)

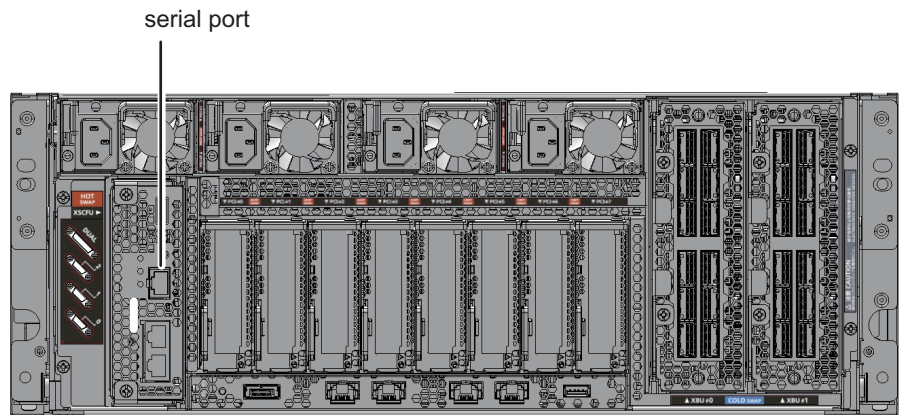


Figure 2-4 Port série (SPARC M10-1)

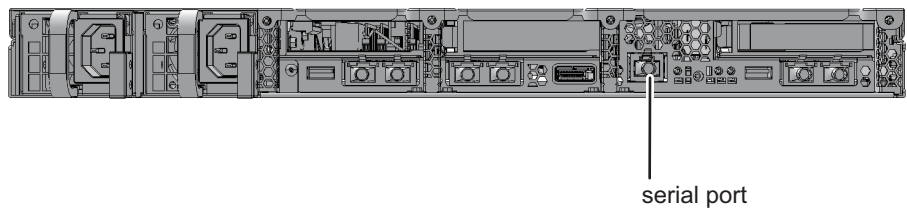


Figure 2-5 Port série (SPARC M10-4S)

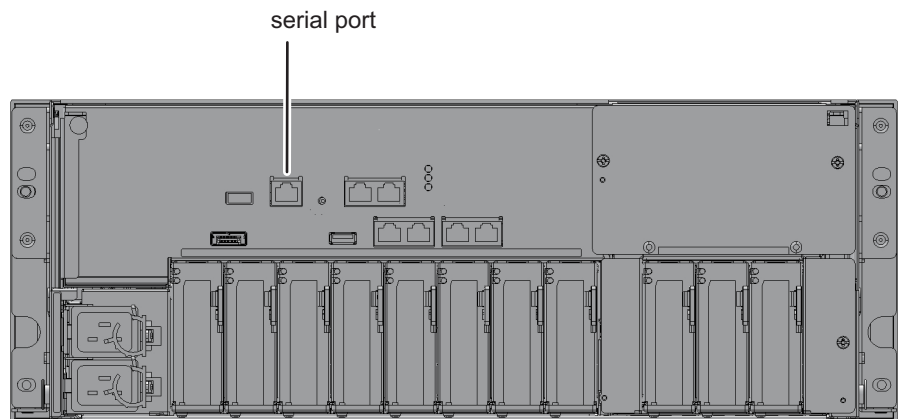
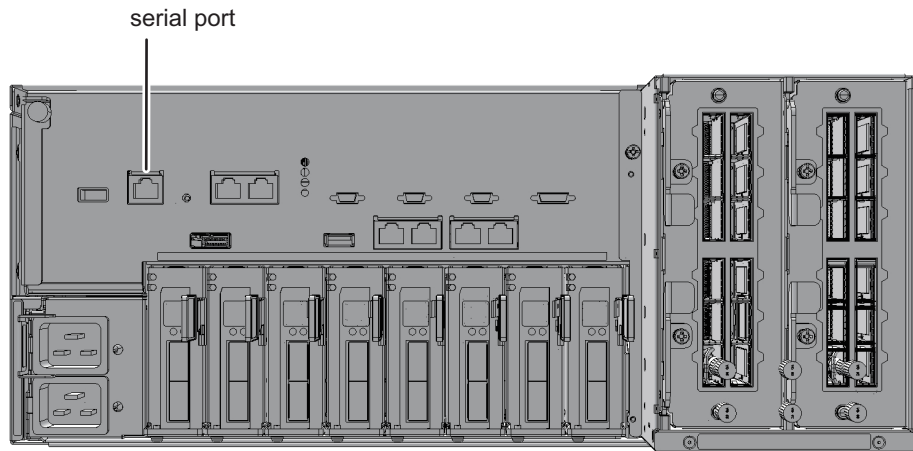


Figure 2-6 Port série (SPARC M10-4S)

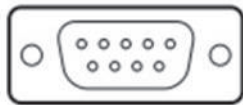


Une fois connecté à XSCF, vous pouvez utiliser le Shell XSCF. Utilisez les commandes XSCF pour surveiller et gérer le système. Si vous devez surveiller ou gérer un domaine logique, vous pouvez passer du Shell XSCF vers la console du domaine de commande. Pour connaître les méthodes d'échange, consultez « [8.3 Passage à la console du domaine de commande depuis le shell XSCF](#) ».

Pour raccorder le port série, les préparations décrites ci-dessous doivent avoir été réalisées.

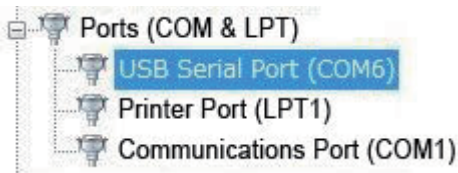
- Préparation d'un câble série
Gardez le câble RS-232C D-Sub à 9 broches fourni à portée de main. Si le terminal utilisé ne dispose pas d'un port série, un câble de conversion RJ-45/RS-232C, un connecteur de conversion ou un câble de conversion USB/série est requis.

Figure 2-7 Connecteur RC-232C D-Sub à 9 broches



- Préparation du logiciel du terminal pour la connexion
Lorsque vous utilisez un shell XSCF, réglez TERM=vt100 pour le logiciel du terminal.
- Confirmation de la reconnaissance du port série
Connectez le câble série au terminal, puis vérifiez la reconnaissance du port série. Spécifiez le port série reconnu comme le port de connexion série avec XSCF.
Dans l'exemple suivant, le port série est le port reconnu comme COM6.

Figure 2-8 Confirmation du port série (avec le gestionnaire de périphériques)



2.1.2 Fonctions disponibles pour les terminaux de la connexion série

Lorsqu'un terminal est connecté au port série, vous pouvez utiliser le Shell XSCF et la console du domaine de commande (console du domaine de commande). Le serveur Web de XSCF n'est pas disponible.

Tableau 2-1 répertorie les terminaux et les consoles pour la connexion série et les fonctions disponibles.

Tableau 2-1 Terminaux et consoles pour la connexion série et fonctions disponibles

Type de terminal	Tâches	Câble
Terminal Shell XSCF	- Vous pouvez utiliser le terminal Shell XSCF immédiatement après l'avoir connecté au port série. - Vous pouvez passer de la fenêtre à la console du domaine de commande à l'aide de la commande console. - Si le Shell XSCF n'est pas utilisé pendant une durée spécifique après la connexion, vous serez automatiquement déconnecté. Pour plus de détails sur le réglage d'expiration de la session XSCF, consultez la page du manuel correspondant à la commande <code>setautologout(8)</code> ou le <i>Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual</i>.	Un câble série croisé RS-232C est nécessaire. Si vous ne disposez que d'un câble LAN, un câble de conversion à 9 broches est nécessaire pour le PC.
Console du domaine de commande (console RW)	- Cette console OS être utilisée pour l'entrée / la sortie. En utilisant la commande console depuis le terminal Shell XSCF, vous pouvez ouvrir la console RW en spécifiant la partition physique et la console accessible en écriture. - Dans une partition physique, seul un utilisateur (une connexion) peut utiliser la console RW à la fois. - Pour plus de détails sur le réglage du délai d'expiration de la session lorsque la console du domaine de commande n'a pas été utilisée pendant un certain temps, consultez l'explication <code>ttymon</code> dans le manuel de référence d'Oracle Solaris.	

Tableau 2-1 Terminals et consoles pour la connexion série et fonctions disponibles (*suite*)

Type de terminal	Tâches	Câble
Console du domaine de commande (console RO)	- Cette console OS est une console de référence uniquement. En utilisant la commande console depuis le terminal Shell XSCF, vous pouvez ouvrir la console RO en spécifiant la partition physique et la console de référence.	

Le nombre maximum autorisé de connexions simultanées aux consoles RW et RO est le suivant :

- SPARC M12-1/M10-1 : 20 consoles
- SPARC M12-2/M10-4 : 40 consoles
- SPARC M12-2S/M10-4S (sans boîtier à barre transversale) : 40 consoles
- SPARC M12-2S/M10-4S (avec boîtiers à barre transversale) : 70 consoles

2.1.3 Connexion avec un port XSCF-LAN

Une connexion XSCF-LAN est la connexion du câble LAN au port XSCF-LAN. Dans une configuration de bloc de construction, raccordez le câble LAN au SPARC M12-2S, au SPARC M10-4S ou au boîtier à barre transversale possédant le XSCF maître ou le XSCF de veille.

Une fois le câble LAN connecté, configurez les paramètres du réseau XSCF et connectez le terminal de gestion du système via le service SSH ou le service Telnet pour afficher l'écran de connexion pour le XSCF maître.

Figure 2-9 Ports XSCF-LAN (SPARC M12-1)

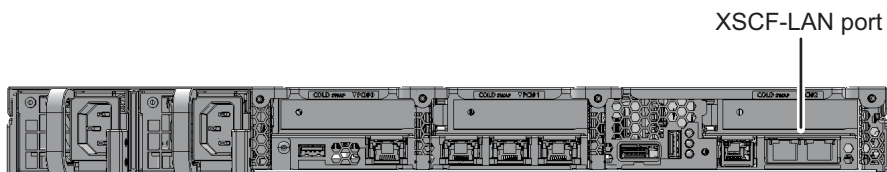


Figure 2-10 Ports XSCF-LAN (SPARC M12-2)

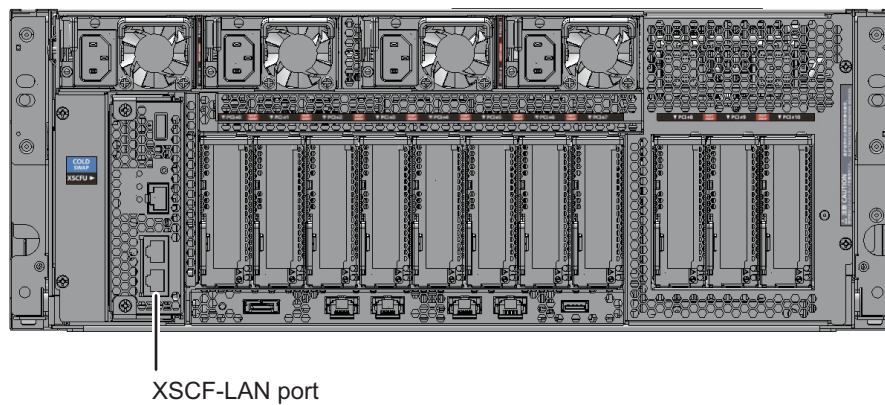


Figure 2-11 Ports XSCF-LAN (SPARC M12-2S)

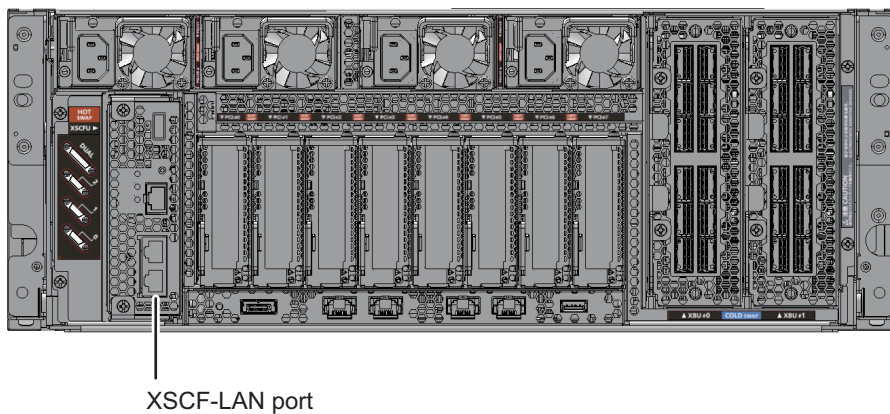


Figure 2-12 Ports XSCF-LAN (SPARC M10-1)

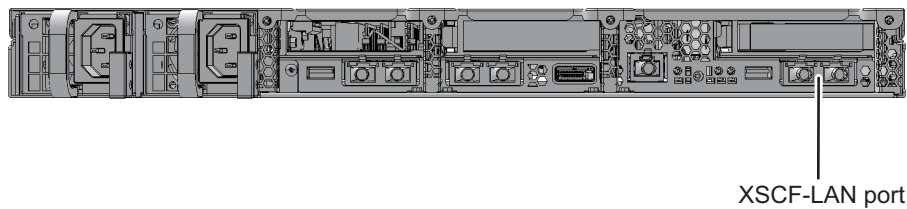


Figure 2-13 Ports XSCF-LAN (SPARC M10-4)

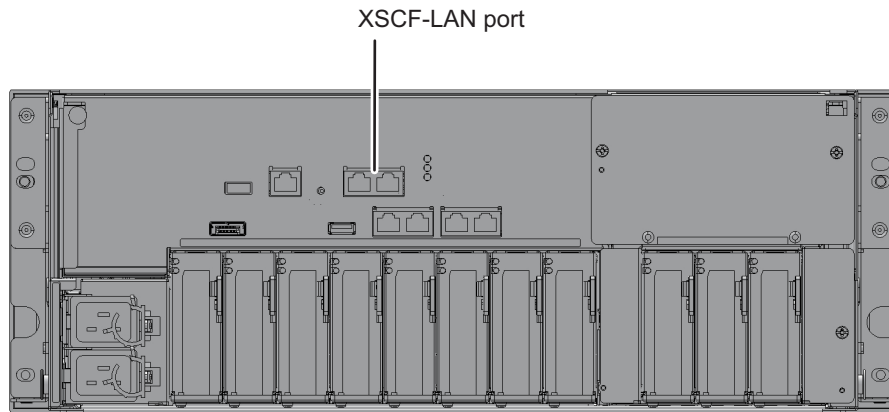
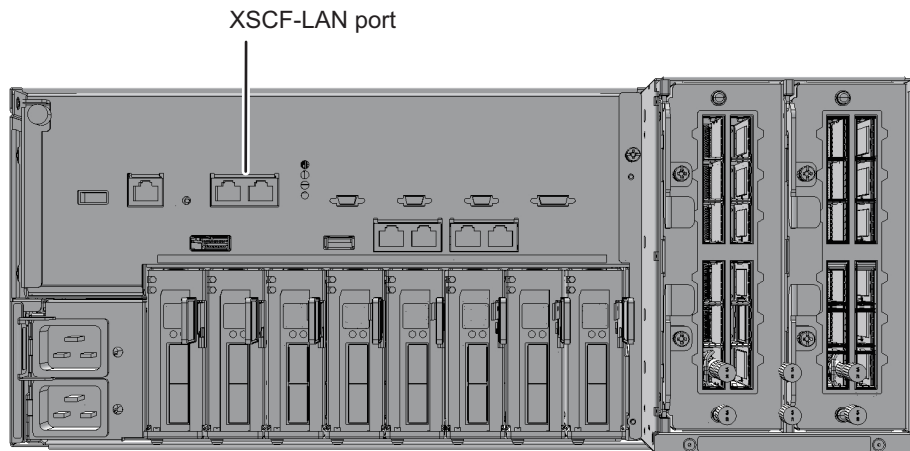


Figure 2-14 Ports XSCF-LAN (SPARC M10-4S)



Vous pouvez utiliser le Shell XSCF sur le terminal de gestion du système avec le raccordement au port XSCF-LAN. Vous pouvez en outre utiliser XSCF Web en configurant un navigateur Internet. Il est possible de configurer les réglages du système en utilisant les commandes XSCF ou XSCF Web.

Une fois le réseau XSCF configuré et le terminal de gestion du système connecté au port XSCF-LAN, vous pouvez utiliser ces fonctions qui nécessitent un environnement de réseau :

- Notification par e-mail
- SNMP
- Service de maintenance à distance
- Connexion et synchronisation à un serveur NTP externe
- Surveillance et gestion de XSCF à distance

Deux ports XSCF-LAN ont été préparés dans chaque système. Vous pouvez utiliser un seul port, utiliser deux ports ou partager l'utilisation des ports en utilisant un port pour un intranet et l'autre pour Internet selon le fonctionnement du système.

Une fois connecté à XSCF, vous pouvez utiliser le Shell XSCF. Utilisez les commandes XSCF pour surveiller et gérer le serveur. Si vous devez surveiller ou gérer un domaine logique, vous pouvez passer du Shell XSCF vers la console du domaine de commande. Pour connaître les méthodes d'échange, consultez « [8.3 Passage à la console du domaine de commande depuis le shell XSCF](#) ».

Pour effectuer une connexion LAN, les préparations décrites ci-dessous doivent avoir été réalisées.

- Préparation d'un câble LAN
Un câble LAN de catégorie 5 ou supérieure est nécessaire.
- Configuration du réseau XSCF
Vous devez configurer le réseau XSCF, SSH, Telnet ainsi que d'autres services. Pour plus de détails, consultez « [3.9 Configuration du réseau XSCF](#) ».
- Préparation d'un navigateur Web (pour l'utilisation de XSCF Web)
Préparez un navigateur Web. Pour les navigateurs Web pris en charge, consultez les dernières *Notes de produit* pour votre serveur.
- Préparation du logiciel du terminal
Lorsque vous utilisez un shell XSCF, réglez TERM=vt100 pour le logiciel du terminal.

2.1.4 Fonctions disponibles pour les terminaux de la connexion XSCF-LAN

Vous pouvez utiliser le terminal Shell XSCF et la console du domaine de commande via les services SSH ou Telnet depuis un terminal connecté au XSCF-LAN.

L'accès par XSCF-LAN permet d'utiliser la fonction de notification par e-mail, la fonction SNMP, la fonction de service de maintenance à distance, la fonction de synchronisation de l'heure via un serveur NTP externe et l'authentification de l'utilisateur par le serveur LDAP, le service de répertoire actif ou le serveur LDAP via le serveur SSL. Selon les paramètres du navigateur Web, vous pouvez également utiliser XSCF Web.

[Tableau 2-2](#) répertorie les terminaux et les consoles pour la connexion XSCF-LAN et les fonctions disponibles.

Tableau 2-2 Terminals et consoles pour la connexion XSCF-LAN et fonctions disponibles

Type de terminal	Tâches	Numéro de port/ câble
Terminal Shell XSCF	- Une fois connecté au service SSH ou au service Telnet, le Shell XSCF peut être utilisé. - Vous pouvez passer de la fenêtre à la console du domaine de commande de la même manière qu'avec le port série. - Si le Shell XSCF n'est pas utilisé pendant une durée spécifique après la connexion, vous serez automatiquement déconnecté, de la même manière qu'avec le port série.	SSH:22 Telnet:23 Un câble LAN est requis.
Console du domaine de commande (console RW)	- Cette console OS être utilisée pour l'entrée / la sortie. En utilisant la commande console depuis le terminal Shell XSCF, vous pouvez ouvrir la console RW en spécifiant la partition physique et la console accessible en écriture. - Dans une partition physique, seul un utilisateur (une connexion) peut utiliser la console RW à la fois. - Pour plus de détails sur le réglage du délai d'expiration de la session lorsque la console du domaine de commande n'a pas été utilisée pendant un certain temps, consultez l'explication ttymon dans le manuel de référence d'Oracle Solaris.	
Console du domaine de commande (console RO)	- Cette console OS est une console de référence uniquement. En utilisant la commande console depuis le terminal Shell XSCF, vous pouvez ouvrir la console RO en spécifiant la partition physique et la console de référence.	
Console XSCF Web	Vous pouvez utiliser la console XSCF Web en spécifiant l'URL sur un navigateur Web.	HTTPS:443 Un câble LAN est requis.

Le nombre maximum autorisé de connexions simultanées aux consoles RW et RO est le suivant :

- SPARC M12-1/M10-1 : 20 consoles
- SPARC M12-2/M10-4 : 40 consoles
- SPARC M12-2S/M10-4S (sans boîtier à barre transversale) : 40 consoles
- SPARC M12-2S/M10-4S (avec boîtiers à barre transversale) : 70 consoles

2.2 Connexion au Shell XSCF

Cette section décrit la connexion au XSCF avec le Shell XSCF.

En utilisant le compte utilisateur par défaut au moment de l'installation initiale, créez un nouveau compte d'utilisateur pour l'authentification. Connectez-vous avec le nouveau compte d'utilisateur. Pour plus de détails sur la méthode d'authentification

avec le compte par défaut, consultez « Réalisation d'un diagnostic initial du système » dans le *Guide d'installation* de votre serveur. Pour plus de détails sur la création d'un nouveau compte, consultez « [3.5 Création/gestion des utilisateurs XSCF](#) ».

2.2.1 Comment se connecter au shell XSCF avec une connexion série

Cette section décrit comment connecter un terminal au port série et la connexion au Shell XSCF.

1. **Vérifiez que le câble série est connecté au port série du XSCF maître et qu'il est correctement connecté au PC ou à la station de travail utilisée.**
2. **Vérifiez que les valeurs suivantes correspondent aux paramètres du logiciel du terminal :**
 - Débit en bauds : 9600 bps
 - Longueur des données : 8 bits
 - Parité : aucune
 - Bit d'arrêt : 1 bit
 - Contrôle de flux : aucun
 - Délai de transmission : non nul

[Figure 2-15](#) montre un exemple de configuration du logiciel du terminal. Si une connexion ne peut pas être établie, augmentez le délai.

Figure 2-15 Exemple de réglages du logiciel du terminal

Port: COM1

Baud rate: 9600

Data: 8 bit

Parity: none

Stop: 1 bit

Flow control: none

OK

Cancel

Help

Transmit delay

10 msec/char 10 msec/line

3. **Établissez la connexion série, puis appuyez sur la touche [Entrée].**
Le terminal devient le terminal Shell XSCF et l'invite de connexion s'affiche.
4. **Entrez un compte d'utilisateur et le mot de passe XSCF pour vous connecter au XSCF.**

```
login: jsmith
Password: xxxxxxxx
```

5. **Vérifiez que l'invite du Shell XSCF (XSCF>) s'affiche.**
Vous pouvez maintenant utiliser le Shell XSCF.

Remarque - Si l'utilisateur qui s'est connecté au Shell XSCF en connexion série la dernière fois a mis fin à cette connexion pendant que la commande de console était en cours d'exécution, l'invite du Shell XSCF peut ne pas apparaître. Si l'invite du Shell XSCF n'apparaît pas, saisissez « #. ». Si l'invite « XSCF> » s'affiche pendant que la commande de console était en cours d'exécution.

```
XSCF>
```

2.2.2 Comment se connecter au shell XSCF avec une connexion SSH via XSCF-LAN

La procédure décrite dans cette section suppose que le service SSH décrit dans « [3.7 Configuration du service SSH/Telnet pour la connexion à XSCF](#) » est activé.

Cette section décrit comment se connecter au Shell XSCF via SSH avec un port XSCF-LAN.

1. **Vérifiez que le câble LAN est connecté à un port XSCF-LAN du XSCF maître et qu'il est correctement connecté au PC ou à la station de travail utilisée.**
2. **Avant de se connecter via SSH, vérifiez les empreintes sauvegardées à l'avance.**
Si aucune empreinte n'a été sauvegardée, établissez une connexion via le port série, exécutez la commande `showssh`, prenez note de l'empreinte de la clé publique d'hôte, puis gardez-la à portée de main comme référence.
3. **Démarrez le client SSH, puis spécifiez l'adresse IP (adresse IP physique) qui est attribuée au XSCF-LAN ou le nom d'hôte et, si besoin, spécifiez le numéro de port et établissez une connexion au service SSH.**
Dans les systèmes à plusieurs XSCF, spécifiez l'adresse IP de prise de contrôle (adresse IP virtuelle) si nécessaire.
4. **Entrez un compte d'utilisateur et la phrase de passe XSCF pour se connecter au Shell XSCF.**
5. **Une question concernant la validité de l'empreinte de la clé publique d'hôte peut s'afficher. Vérifiez les empreintes que vous avez gardées à portée de main comme référence, confirmez la connexion du XSCF adapté puis entrez « yes ».**
6. **Vérifiez que l'invite du Shell XSCF (XSCF>) s'affiche.**
Vous pouvez maintenant utiliser le Shell XSCF.
L'exemple suivant représente une identification.

```
[foo@phar foo]% ssh june@192.168.0.2
The authenticity of host '192.168.0.2 (192.168.0.2)' can't be
established.
RSA key fingerprint is
03:4b:b4:b2:3d:4d:0c:24:03:ca:f1:63:f2:a7:f3:35.
Are you sure you want to continue connecting? [yes|no] : yes
Warning: Permanently added '192.168.0.2' (RSA) to the list of
known
hosts.
foo@phar's password: xxxxxx
XSCF>
```

Pour établir la connexion SSH avec une clé d'utilisateur, enregistrez la clé publique d'utilisateur à l'avance avec le XSCF. Pour savoir comment enregistrer une clé publique d'utilisateur, consultez « [3.7 Configuration du service SSH/Telnet pour la connexion à XSCF](#) ».

L'exemple suivant représente une identification avec une clé publique d'utilisateur.

```
[client]# ssh nana@192.168.1.12
Enter passphrase for key '/home/nana/.ssh/id_rsa': xxxxxxxx
Warning: No xauth data; using fake authentication data for X11
forwarding.
Last login: Mon Sep 1 10:19:37 2012 from client
XSCF>
```

Remarque : pour plus de détails sur le démarrage de SSH, consultez les manuels de SSH.

2.2.3 Comment se connecter au shell XSCF avec une connexion Telnet via XSCF-LAN

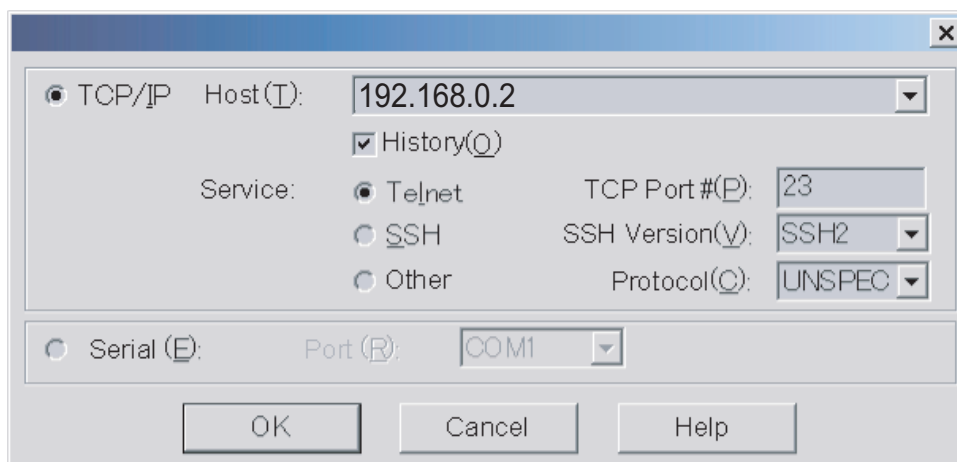
La procédure décrite dans cette section suppose que le service Telnet décrit dans « [3.7 Configuration du service SSH/Telnet pour la connexion à XSCF](#) » est activé.

Cette section décrit comment se connecter au Shell XSCF via Telnet avec un port XSCF-LAN.

1. **Vérifiez que le câble LAN est connecté à un port XSCF-LAN du XSCF maître et qu'il est correctement connecté au PC ou à la station de travail utilisée.**
2. **Démarrez le logiciel du terminal, spécifiez l'adresse IP (adresse IP physique) qui est attribuée au XSCF-LAN ou le nom d'hôte et le port numéro 23 pour établir une connexion service Telnet, et ouvrez le terminal du Shell XSCF.**
Dans les systèmes à plusieurs XSCF, spécifiez l'adresse IP de prise de contrôle (adresse IP virtuelle) si nécessaire.

[Figure 2-16](#) montre un exemple de configuration du logiciel du terminal.

Figure 2-16 Exemple de réglages du logiciel du terminal



3. **Entrez un compte d'utilisateur et le mot de passe XSCF pour vous connecter au Shell XSCF.**
4. **Vérifiez que l'invite du Shell XSCF (XSCF>) s'affiche.**
Vous pouvez maintenant utiliser le Shell XSCF.
L'exemple suivant indique une réussite de la connexion.

```
login:jsmith  
Password:xxxxxxx  
XSCF>
```

2.3 Déconnexion du shell XSCF

Cette section décrit comment se déconnecter de XSCF Web.

1. **Exécutez la commande exit pour vous déconnecter.**

```
XSCF> exit
```

Vous êtes déconnecté du XSCF et la session XSCF est terminée.

Si le Shell XSCF n'est pas utilisé pendant une durée spécifique après la connexion, vous serez automatiquement déconnecté. La valeur d'expiration d'une session XSCF est définie à l'aide de la commande setautologout. Pour plus de détails, consultez la page du manuel correspondant à la commande setautologout(8) ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

2.4 Connexion à XSCF Web

Cette section décrit comment se connecter au XSCF avec XSCF Web.

Vous pouvez utiliser XSCF Web selon les paramètres du navigateur Web du PC connecté au XSCF-LAN. XSCF Web ne peut pas être connecté depuis le port série.

L'accès par XSCF-LAN permet également d'utiliser la fonction de notification par e-mail, la fonction SNMP, la fonction de service de maintenance à distance, la fonction de synchronisation de l'heure via un serveur NTP externe et l'authentification de l'utilisateur par le serveur LDAP, le service de répertoire actif ou le serveur LDAP via le serveur SSL.

XSCF Web est connecté à un serveur connecté via le réseau utilisateur avec les protocoles HTTPS et SSL/TLS. Il permet un affichage de l'état des serveurs, le contrôle des périphériques utilisés et une consultation des informations de

configuration sur le Web.

Lorsqu'un utilisateur enregistré se connecte à XSCF Web sur un navigateur Web depuis un PC et qu'il se connecte à XSCF, le navigateur affiche l'arborescence et les pages d'index disponibles. Pour plus de détails sur les informations de la page XSCF Web, consultez « [Annexe C Liste des pages de XSCF Web](#) ».

2.4.1 Éléments devant être définis à l'avance

XSCF Web est désactivé dans les réglages initiaux. Avant d'utiliser XSCF Web, les paramètres suivants doivent être configurés à l'avance.

- Enregistrement d'un compte d'utilisateur XSCF
- Activation du service HTTPS pour utiliser XSCF Web
- Enregistrement d'un certificat de serveur Web en utilisant le paramètre de service HTTPS
- Configuration de la notification par e-mail (paramètre recommandé pour la notification en cas de panne)

Pour savoir comment activer le service HTTPS, consultez « [3.8 Configuration du service HTTPS pour la connexion à XSCF](#) ».

2.4.2 Navigateurs pris en charge

XSCF Web prend en charge les navigateurs Web répertoriés dans [Tableau 2-3](#).

Tableau 2-3 Navigateurs Web pris en charge

Nom du navigateur Web	Version
Microsoft Internet Explorer	8.0, 9.0, 10.0 et 11.0
Mozilla Firefox version 32 bits	10.0 à ESR 52

Pour plus de détails sur les navigateurs Web utilisés, consultez les dernières *Notes de produit* de votre serveur.

2.4.3 Fonctions devant être activées dans le navigateur Web

Les fonctions suivantes seront utilisées dans le navigateur Web et doivent donc être définies pour être activées.

- Transport Layer Security (TLS) Ver. 1,2
- JavaScript
- Cookies (pour la gestion de session)

2.4.4 Comment se connecter avec XSCF Web

Cette section décrit comment se connecter au XSCF avec XSCF Web.

1. **Vérifiez que le câble LAN est connecté à un port XSCF-LAN du XSCF maître et qu'il est correctement connecté au PC ou à la station de travail utilisée.**
2. **Pour l'URL du navigateur Web, spécifiez l'adresse IP ou le nom d'hôte du XSCF pour vous connecter à celui-ci.**

- Exemple de saisie d'URL sur un navigateur Web

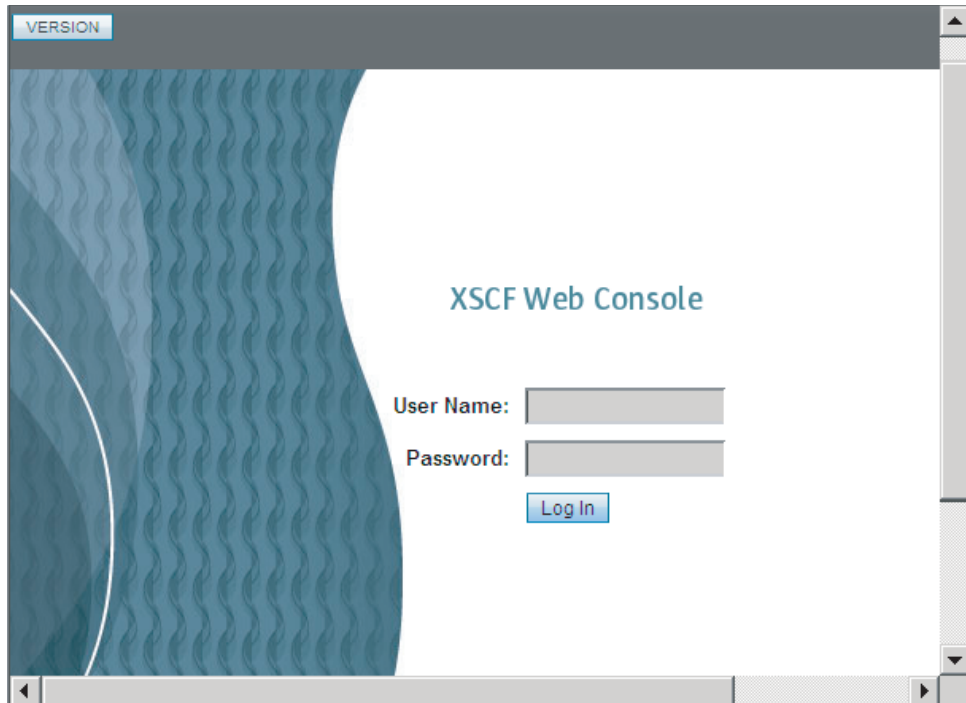
```
https://192.168.111.111 (Saisissez l'adresse IP de XSCF  
<numéros>)/  
Ou bien,  
https://XSCF-host-name (Remarque : différent du nom de l'hôte  
du domaine)/
```

Remarque : il pourra vous être demandé de confirmer le certificat lorsque la communication sera établie. Confirmez le contenu et acceptez le certificat à ce moment. Lorsqu'une connexion HTTPS est effectuée, le navigateur Web continue d'afficher un avertissement jusqu'à la fin de l'installation du certificat.

3. **Entrez un compte d'utilisateur et le mot de passe XSCF sur la page de connexion pour vous connecter au XSCF.**

[Figure 2-17](#) montre un exemple de la page de connexion.

Figure 2-17 Exemple de la page de connexion de XSCF Web



Après connexion, la page par défaut apparaît. La page par défaut affiche une arborescence permettant de sélectionner des pages et une page seule.

Cas d'erreur d'authentification

En cas d'échec de la connexion, un message indiquant que la connexion a échoué s'affiche. La tentative de connexion ayant échoué est consignée dans le journal des événements et dans le journal d'audit.

2.5 Déconnexion de XSCF Web

Cette section décrit comment se déconnecter de XSCF Web.

1. **Cliquez sur le bouton [LOG OUT] de la page XSCF Web pour vous déconnecter.**
Une fois déconnecté de XSCF, vous êtes redirigé vers la page de connexion de XSCF Web.

Surveillance de l'état de l'accès

XSCF Web surveille l'état d'utilisation des comptes d'utilisateur XSCF connectés. Si le compte n'est pas utilisé pendant une durée spécifique après la connexion, XSCF Web détecte que l'authentification a expiré pour ce compte. Ainsi, si vous accédez à XSCF

Web avec un compte dont l'authentification a expiré, une boîte de dialogue indiquant cette expiration s'affiche et vous êtes dirigé vers la page du haut. Pour continuer à utiliser XSCF Web, vous devez vous connecter de nouveau.

Vous pouvez modifier le délai d'expiration de l'authentification sur les pages XSCF Web. Le délai d'expiration de l'authentification par défaut est de 10 minutes. Ce délai varie de 1 minute à 255 minutes. Pour modifier ce délai, sélectionnez [Menu] - [Settings] - [Autologout].

2.6 Nombre d'utilisateurs pouvant se connecter

Cette section présente le nombre d'utilisateurs pouvant être connectés au XSCF. L'exécution de la commande `who` répertorie les comptes d'utilisateur connectés au XSCF.

- SPARC M12-1/M10-1
Le nombre maximal d'utilisateurs connectés est de 20. Lorsque 20 utilisateurs sont connectés simultanément au XSCF, l'accès est refusé à tout utilisateur qui tente d'établir une autre connexion (21ème).
- Système SPARC M12-2/M12-2S/M10-4/M10-4S (sans boîtier à barre transversale)
Le nombre maximal d'utilisateurs connectés est de 40. Lorsque 40 utilisateurs sont connectés simultanément au XSCF, l'accès est refusé à tout utilisateur qui tente d'établir une autre connexion (41ème).
- Système SPARC M12-2S/M10-4S (avec boîtiers à barre transversale)
Le nombre maximal d'utilisateurs connectés est de 70. Lorsque 70 utilisateurs sont connectés simultanément au XSCF, l'accès est refusé à tout utilisateur qui tente d'établir une autre connexion (71ème).

Configuration du système

Ce chapitre décrit les procédures de réglage requises pour utiliser le XSCF.

- [Tâches préparatoires pour la configuration de XSCF](#)
- [Comprendre le contenu des paramètres du microprogramme XSCF](#)
- [Configuration depuis le shell XSCF](#)
- [Configuration depuis le XSCF Web](#)
- [Création/gestion des utilisateurs XSCF](#)
- [Réglage de l'heure/date du XSCF](#)
- [Configuration du réseau XSCF](#)
- [Configuration du service SSH/Telnet pour la connexion à XSCF](#)
- [Configuration du service HTTPS pour la connexion à XSCF](#)
- [Configuration de l'audit pour renforcer la sécurité de XSCF](#)

3.1 Tâches préparatoires pour la configuration de XSCF

Cette section décrit ce qu'il faut vérifier et effectuer avant la configuration du XSCF.

Pour ce faire, elle part du principe que l'installation du serveur, le raccordement des câbles, le diagnostic initial du système et les autres tâches d'installation ont été effectués.

3.1.1 Tâches initiales avant configuration

Avant de démarrer la configuration du XSCF, le raccordement des câbles, l'identification initiale auprès du serveur et d'autres tâches doivent avoir été effectués de manière à ce que vous puissiez vous connecter au XSCF de n'importe quel terminal disposant d'une connexion en série ou LAN.

L'administrateur système et les techniciens sur site doivent configurer le XSCF après avoir accompli les tâches suivantes.

Tableau 3-1 Tâches à accomplir avant la configuration du XSCF

Tâches	Voir
Effectuer une identification initiale auprès du XSCF en utilisant son compte d'utilisateur par défaut.	« Connexion à XSCF » dans le <i>Guide d'installation</i> de votre serveur.
Enregistrez au moins un compte d'utilisateur disposant du privilège d'utilisateur platadm ou useradm.	« 3.5 Création/gestion des utilisateurs XSCF »

Durant le fonctionnement normal, placez le commutateur de mode sur la position verrouillée pour éviter des erreurs d'opération.
Pour plus d'information sur la méthode de commutation du commutateur de mode, consultez « [13.2 Changer le mode de fonctionnement](#) ».

3.1.2 Informations complémentaires

Avant de configurer le XSCF, veuillez à lire l'ensemble des dernières *Notes de produit* pour votre serveur pour vérifier les exigences matérielles et les informations complémentaires.

3.1.3 Interface utilisateur pour la configuration et méthode d'accès

Pour configurer le XSCF, connectez un PC au XSCF maître. Pour effectuer plusieurs paramétrages, accédez au XSCF à partir du shell XSCF, une interface en ligne de commande, ou de XSCF Web, une interface utilisateur basée sur un navigateur.

Tableau 3-2 Interfaces utilisateur et accès au XSCF

Interface utilisateur	Comment accéder au XSCF
Shell XSCF (interface de ligne de commande)	Identifiez-vous depuis un PC connecté au port série. Identifiez-vous depuis un PC connecté au port LAN destiné au XSCF (XSCF-LAN) via le service SSH ou Telnet.
XSCF Web (interface utilisateur basée sur un navigateur)	Identifiez-vous à l'aide du service HTTPS depuis un PC disposant d'un navigateur web installé et connecté au XSCF-LAN.

Pour utiliser XSCF Web, vous devez d'abord le configurer à l'aide du shell XSCF. Prenez note du fait que les paramètres de certaines fonctions, comme le réglage d'altitude et la double alimentation ne sont pas pris en charge par XSCF Web. Lorsque vous recourez à ces fonctions, utilisez le shell XSCF pour effectuer les

paramétrages. Pour plus de détails sur les fonctions prises en charge par XSCF Web, consultez « [Annexe C Liste des pages de XSCF Web](#) ».

Procédure de réglage

La procédure de paramétrage varie en fonction de l'interface utilisateur connectée.

- En utilisant le shell XSCF
Consultez « [3.3 Configuration depuis le shell XSCF](#) ».
- En utilisant XSCF Web
Consultez « [3.4 Configuration depuis le XSCF Web](#) ».

Informations de réglage

Une fois le XSCF configuré, le paramètre réglé est automatiquement sauvegardé sur le XSCF et l'unité de fond de panier PSU ou l'unité de fond de panier à barre transversale. Une fois que le XSCF est configuré, une gestion quotidienne n'est donc pas nécessaire. Cependant, dans la mesure où les informations sauvegardées sur le serveur peuvent être endommagées, sauvegardez/restaurer régulièrement les informations de réglages du XSCF. Pour plus de détails concernant la façon de sauvegarder/restaurer les informations de réglages du XSCF, consultez « [10.10 Sauvegarde/restauration des informations des réglages de XSCF](#) ».

3.1.4 Configuration de manière fluide

Cette section décrit ce qu'il vous est nécessaire de comprendre avant de configurer le XSCF.

Dans de nombreux cas, le système peut fonctionner avec les paramètres et les valeurs par défaut datant de la première installation. Cependant, le serveur doit être configuré pour s'adapter à l'environnement de l'utilisateur. Vous pouvez réduire la durée requise pour la configuration en vérifiant les tâches déjà effectuées à l'aide du *Guide d'installation* de votre serveur ainsi que les éléments définis par avance. Pour les réglages, prenez en compte les points suivants.

- Répertoriez, s'il y a lieu, les éléments déjà configurés lors de l'installation initiale. Pour chaque élément mentionné ci-dessous, affichez les informations de réglage et vérifiez si une reconfiguration est nécessaire.
- Assurez-vous que les comptes d'utilisateur requis sont prêts en vérifiant leur maintenance, l'administrateur système, les partitions physiques, etc. Vous devez également décider par avance si vous utiliserez comme compte d'utilisateur le compte local sauvegardé sur le XSCF ou les données de compte sauvegardées sur un serveur à distance.
- Vérifiez de nouveau la configuration du serveur. Vérifiez qu'aucun élément relatif aux adresses réseau, aux configurations de domaines, au nombre d'activations de processeurs (CPU), etc. ne soit indéfini ou vide. Des mesures, de vérification par exemple, doivent être prises pour vous assurer de l'adéquation de certains réglages à l'environnement de l'utilisateur, comme l'adresse de réseau.
- Vous pouvez utiliser plusieurs services en vous connectant au réseau XSCF. Définissez par avance comment traiter les accès non autorisés ou limiter l'accès à

l'hôte ainsi que les moyens d'utiliser le service de maintenance à distance, par exemple pour la notification, et l'approche à adopter pour l'heure standard.

- L'environnement opérationnel du serveur est un critère nécessaire à la mise en œuvre de mesures d'économie d'énergie. Selon la superficie et la température de la salle du serveur, combinées à d'autres éléments de l'environnement d'installation, définissez les intervalles de démarrage du serveur. Définissez également la valeur maximale de consommation d'énergie et d'autres valeurs comparables.

3.2 Comprendre le contenu des paramètres du microprogramme XSCF

Cette section décrit dans le détail les procédures de configuration du microprogramme XSCF.

3.2.1 Éléments de réglage destinés à l'utilisation du XSCF

Les différents élément de réglage du XSCF possèdent les buts suivants :

- Paramètres d'utilisation du microprogramme XSCF
- Paramètres de configuration des partitions physiques et des domaines logiques
- Paramètres de gestion/commande matérielle du système
- Autres paramètres, comme la notification d'évènement

Cette section décrit les paramètres d'utilisation du microprogramme XSCF. Pour les paramètres de configuration des partitions physiques et des domaines logiques, consultez « [Chapitre 7 Contrôle des partitions physiques](#) » et « [Chapitre 8 Contrôle des domaines logiques](#) » ainsi que le *Guide de configuration du domaine Fujitsu SPARC M12 et Fujitsu M10/SPARCM10*. Pour les paramètres d'administration/commande du matériel, comme l'alimentation électrique, consultez « [Chapitre 4 Configuration du système selon le type d'utilisation](#) » et « [Chapitre 15 Extension de la configuration du système](#) ». En outre, concernant les autres paramètres, consultez le chapitre correspondant.

Tableau 3-3 présente les éléments de réglage destinés à l'utilisation du microprogramme XSCF. Pour plus de détails sur chacun de ces éléments, consultez les sections indiquées dans le tableau.

Tableau 3-3 Éléments de réglage destinés à l'utilisation du XSCF

Élément de réglage	Paramétrage requis ou optionnel	Voir
Gestion d'utilisateurs	Requis	3.5
Durée	Requis	3.6

Tableau 3-3 Éléments de réglage destinés à l'utilisation du XSCF (*suite*)

Élément de réglage	Paramétrage requis ou optionnel	Voir
Réseau	Requis	3.9
Service SSH/Telnet	Optionnel	3.7
Service HTTPS	Optionnel	3.8
Audit	Optionnel	3.10
Service LDAP	Optionnel	3.5.12
Service Active Directory	Optionnel	3.5.13
Service LDAP sur SSL	Optionnel	3.5.14

Remarque : les services relatifs aux éléments de réglage suivants ont été activés en usine.

- Gestion d'utilisateurs
- Heure
- Réseau
- Audit

3.2.2 Vérification du XSCF maître

Pour le SPARC M12-1/M12-2/M10-1/M10-4 et le SPARC M12-2S/M10-4S dans une configuration d'unité unique, le XSCF de ce châssis est le XSCF maître. Pour le SPARC M12-2S ou le SPARC M10-4S dans une configuration de bloc de construction, seul le XSCF maître ou le XSCF de veille est accessible aux utilisateurs. Configurez le XSCF depuis le XSCF maître. En principe, le XSCF maître dans une configuration de bloc de construction est le XSCF installé dans le SPARC M12/M10 dont l'identifiant (BB-ID) est 0 ou 1 ou dans le châssis du boîtier à barre transversale 80 ou 81. Le XSCF de veille est également le XSCF installé dans le châssis possédant les mêmes numéros.

Si l'on bascule du XSCF maître au XSCF de veille pendant le fonctionnement du système, le XSCF maître passe de l'unité dans le châssis disposant du BB-ID 0 à celle située dans le châssis possédant 1 comme BB-ID. De même, le XSCF de veille passe de l'unité située dans le châssis possédant le BB-ID 1 à celle située dans le châssis disposant du 0.

Dans un système comportant plusieurs XSCF, le XSCF maître et le XSCF de veille possèdent les numéros d'installation de composants suivants :

- Système SPARC M12-2S ou SPARC M10-4S (sans boîtier à barre transversale)
 - XSCF maître : BB#00 ; XSCF de veille : BB#01
- Ou bien,
 - XSCF maître : BB#01 ; XSCF de veille : BB#00
- Système SPARC M12-2S ou SPARC M10-4S (avec boîtiers à barre transversale)
 - XSCF maître : XBBOX#80 ; XSCF de veille : XBBOX#81

Ou bien,

- XSCF maître : XBBOX#81 ; XSCF de veille : XBBOX#80

Pour vérifier et connecter le XSCF maître dans un système comportant plusieurs XSCF, la méthode est la suivante.

- Vérification de la DEL MAÎTRE et installation d'une connexion en série
Grâce à l'énergie fournie au SPARC M12-2S ou SPARC M10-4S ou aux boîtiers à barre transversale, la fin de l'initialisation du XSCF maître allume la DEL MAÎTRE sur le panneau arrière de l'unité XSCF. En connectant un PC au port série de ce même panneau, vous pouvez vous identifier sur le XSCF maître.

- Indication de l'adresse IP de prise de contrôle ou du XSCF maître pour établir une connexion

Le XSCF maître et le XSCF de veille dispose respectivement des ports XSCF LAN#0 et LAN#1. LAN#0 et LAN#1 sont dédoublés dans la mesure où ils sont connectés l'un à l'autre via le même sous-réseau.

Pour vous connecter au XSCF maître, spécifiez l'adresse IP de prise de contrôle LAN#0 ou LAN#1. Même lorsqu'une commutation a eu lieu entre le XSCF maître et le XSCF de veille, vous pouvez vous connecter au XSCF maître en spécifiant la même adresse IP de prise de contrôle.

Comme méthode alternative de connexion au XSCF maître, vous pouvez spécifier l'adresse IP LAN#0 ou LAN#1 du XSCF maître. Cette méthode de connexion peut être employée lorsque le système ne comporte qu'un seul XSCF ou lorsque du fait d'opérations de maintenance, le XSCF de veille est inaccessible.

Après vous être connecté et vous être identifié sur le XSCF maître à l'adresse IP indiquée, exécutez la commande `showhardconf`. Vous pouvez vérifier quel châssis de SPARC M12-2S, SPARC M10-4S ou boîtier à barre transversale dispose du XSCF maître.

Dans l'exemple suivant, BB-ID 0 est le XSCF maître.

```
XSCF> showhardconf
SPARC M10-4S;
      + Serial: 2081208013; Operator_Panel_Switch:Locked;
:
      BB#00 Status:Normal; Role:Master Ver: 0101h; Serial:
      7867000297;
      + FRU-Part-Number: CA20393-B50X A2 ;
:
      BB#01 Status:Normal; Role:Standby Ver:0101h; Serial:
      7867000297;
      + FRU-Part-Number: CA20393-B50X A2 ;
:
```

Dans l'exemple suivant, le boîtier à barre transversale 80 est le XSCF maître.

```
XSCF> showhardconf
SPARC M10-4S;
      + Serial:PAxxxxxxxx; Operator_Panel_Switch:Locked;
:
      XBBOX#80 Status:Normal; Role:Master Ver:0101h; Serial:
```

```
7867000297;  
+ FRU-Part-Number:CA20393-B50X A2 ;  
:  
XBB0X#81 Status:Normal; Role:Standby Ver:0101h; Serial:  
7867000297;  
+ FRU-Part-Number:CA20393-B50X A2 ;  
:
```

Remarque : les paramètres réalisés sur le XSCF maître sont répercutés sur le XSCF de veille.

3.2.3 Fonctions exécutables sur le XSCF de veille

Cette section décrit les fonctions et commandes exécutables sur le XSCF de veille.

Tableau 3-4 Fonctions exécutables sur le XSCF de veille

Fonction	Commande
Sortie du XSCF	exit
Affichage de pages du manuel	man
Redémarrage du XSCF	rebootxscf
Paramétrage d'un privilège d'utilisateur	setprivileges
Affichage d'état d'un châssis	showbbstatus
Affichage d'état final d'une commande	showresult
Affichage des informations relatives à un utilisateur	showuser
Vidange du microprogramme	snapshot
Commutation du XSCF	switchscf
Affichage d'un audit	viewaudit
Affichage des utilisateurs connectés	who

Pour plus de détails sur chaque commande, consultez la page du manuel correspondante ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

3.2.4 Vérification détaillée des options de commande sur les pages de manuel

À l'aide de la commande `man(1)`, vous pouvez vérifier les pages de manuel concernant les opérandes, les options, etc. des commandes XSCF lors de la configuration du XSCF. Le contenu des pages de manuel affichées est le même que celui des informations relatives aux commandes du *Fujitsu SPARC M12 and Fujitsu*

```
XSCF> man showhardconf
System Administration                showhardconf(8)
NAME
    showhardconf - display information about field replaceable
    unit (FRU) installed in the system

SYNOPSIS
    showhardconf [-u] [-M]
    showhardconf -h

DESCRIPTION
    showhardconf(8) command displays information about each
    FRU.
    :
```

3.3 Configuration depuis le shell XSCF

Cette section décrit la procédure de configuration réalisée depuis le shell XSCF.

Pour plus de détails sur chaque étape, consultez la section indiquée par le titre entre guillemets. De plus, selon l'environnement de l'utilisateur, déterminez si les paramètres (optionnels) doivent être activés ou non.

1. **Connectez-vous au shell XSCF depuis n'importe quel terminal disposant d'une connexion série.**

Configurez un environnement sécurisé avec une connexion série au serveur.

Pour plus de détails, consultez « [2.2.1 Comment se connecter au shell XSCF avec une connexion série](#) ».

2. **Connectez-vous au shell XSCF.**

Connectez-vous au shell XSCF avec un nouveau compte d'utilisateur créé lors de la première identification.

Pour plus de détails sur la connexion, consultez « [2.2 Connexion au Shell XSCF](#) ».

Pour plus de détails sur la création d'un nouveau compte d'utilisateur lors de la première identification, consultez « [3.5 Création/gestion des utilisateurs XSCF](#) ».

3. **Définissez une stratégie de mot de passe.**

Indiquez les attributs des mots de passe des comptes d'utilisateur XSCF comme leur date d'expiration ou leur nombre de caractères.

Pour plus de détails, consultez « [3.5 Création/gestion des utilisateurs XSCF](#) ».

4. **Configurez les éléments d'audit (optionnel).**

La fonction d'audit archive les connexions et déconnexions au XSCF ainsi que divers autres événements dans le journal d'audit. La fonction d'audit est activée

par défaut. Le privilège d'utilisateur `auditadm` est nécessaire pour les paramètres d'audit.

Pour plus de détails, consultez « [3.10 Configuration de l'audit pour renforcer la sécurité de XSCF](#) ».

5. **Définissez l'heure.**

Définissez l'heure du XSCF, qui sera l'heure standard du système. Une fois l'heure du système mise à jour, le XSCF est redémarré et la session XSCF terminée. Connectez-vous à nouveau.

Pour plus de détails, consultez « [3.6 Réglage de l'heure/date du XSCF](#) ».

Remarque : cette tâche de paramétrage a été effectuée pendant l'installation initiale. Si la valeur doit être modifiée, paramétrez-la de nouveau.

6. **Configurez le service SSH/Telnet.**

Il est possible d'activer SSH et Telnet simultanément. Cependant, les connexions réalisées à l'aide du service Telnet ne constituent pas un protocole de communication sûr. Nous vous recommandons de désactiver le service Telnet lorsque le service SSH est activé.

Le service SSH/Telnet est désactivé par défaut.

Pour plus de détails, consultez « [3.7 Configuration du service SSH/Telnet pour la connexion à XSCF](#) ».

7. **Confirmez la clé publique d'hôte du XSCF.**

Pour utiliser le service SSH avec une connexion XSCF-LAN, exécutez la commande `showssh` et notez l'empreinte. L'étape 11 renvoie au contenu de l'empreinte notée pendant la connexion au shell XSCF via un service SSH. Copiez les données texte de la clé publique d'hôte sur un fichier dans un répertoire donné du client.

```
XSCF> showssh
SSH status: enabled
RSA key:
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAt0IG3wfpQnGr51znS9XtzwHcBBb/UU0LN08S
ilUXE6j+avlxdY7AFqBflwGxLF+Tx5pTa6HuZ8o8yUBbDZVJAAAFQCfKPxarV+/
5qzK4A43Qaigkqu/6QAAAIbMLQl22G8pwibESrh5JmOhSxpLzl3P26ksI8qPr+7B
xmjlR0k=
Fingerprint:
1024 e4:35:6a:45:b4:f7:e8:ce:b0:b9:82:80:2e:73:33:c4
/etc/ssh/ssh_host_rsa_key.pub
DSA key:
ssh-dss
AAAAB3NzaC1kc3MAAACBAJSy4GxD7Tk4fxFvyW1D0NUDqZQPY3PuY2IG7QC4BQ1k
ewDnb1B8/JEqI+8pnfbWzmOWU37KHL19OEYNAv6v+WZT6RElU5Pyb8F16uq96L8Q
DMswFlICMzgrn+ilJNStr6r8KDJfwoQMmK0eeDFj2mL40NOvaLQ83+rRwW6Ny/yF
1Rgv6PUpUqRLw4Verb+uOfmPRpe6/kb4z++lOhtpWI9bay6CK0nrFRok+z54ez7B
rDFBQVuNZx9PyEFezJG9ziEYVUag/23LIAiLxxBmW9pqa/WxC21Ja4RQVN3009km
VwAAAIaON1LR/9Jdd7yyG18+Ue7eBBJHrCA0pkSzvfzzFFj5XUzQBdabh5p5Rwz+
1vriawFIZI9j2uhM/3HQdrvYSVBEDMjaasF9hB6T/uFwP8yqtJf6Y9GdjBAhWuH8
```

```
F13pX4BtvK9IeldqCscnOuu0e2rlUoI6GICMr64FL0YYBSwfbwLIz6PSA/yKQe23
dwfkSfcwQZNq/5pThGFi3tob5Qev2KCK2OyEDMCAOvVlMhqHuPNpX+hE19nPdBFG
zQ==
Fingerprint:
1024 9e:39:8e:cb:8a:99:ff:b4:45:12:04:2d:39:d3:28:15
/etc/ssh/ssh_host_dsa_key.pub
```

Pour plus de détails, consultez « [3.7 Configuration du service SSH/Telnet pour la connexion à XSCF](#) ».

8. **Enregistrez la clé publique d'utilisateur.**

Pour utiliser une clé d'utilisateur de service SSH via une connexion XSCF-LAN, créez une clé secrète et une clé publique d'utilisateur pour un compte d'utilisateur enregistré sur le PC et enregistrez la clé publique d'utilisateur avec le XSCF.

Pour plus de détails, consultez « [3.7 Configuration du service SSH/Telnet pour la connexion à XSCF](#) ».

9. **Configurez le réseau destiné au XSCF.**

Configurez le réseau XSCF, dont l'adresse IP XSCF-LAN et SSCP. Plusieurs utilisateurs peuvent simultanément accéder au XSCF via SSH, Telnet ou HTTPS.

Exécutez la commande `applynetwork` pour diffuser les paramètres du réseau. Ensuite, exécutez la commande `rebootxscf` pour redémarrer le XSCF et finaliser la configuration. Une fois le XSCF redémarré, la session XSCF est terminée. Connectez-vous à nouveau.

Pour plus de détails, consultez « [3.9 Configuration du réseau XSCF](#) ».

10. **Connectez-vous au shell XSCF depuis n'importe quel terminal disposant d'une connexion XSCF-LAN (optionnel).**

À partir de cette étape, les tâches de paramétrage peuvent être également effectuée via une connexion XSCF-LAN. Ici, connectez-vous au XSCF depuis un PC connecté au XSCF-LAN en spécifiant son adresse IP, puis identifiez-vous à nouveau.

Pour continuer à utiliser la connexion série pour les paramétrages, reportez-vous à l'étape 12.

Le service Telnet ne doit pas être considéré comme une forme sûre de communication. Nous vous recommandons d'utiliser un service SSH. En vous identifiant via un service SSH, il se peut que la validité de l'empreinte de la clé publique d'hôte fasse l'objet d'une question. Vérifiez que l'empreinte est la même que celle notée à l'étape 7 et répondez « **yes** ». Si les empreintes ne correspondent pas, il est possible que l'adresse IP ne soit pas correcte ou soit unique à la destination de connexion, ou cela peut impliquer une usurpation d'identité. Vérifiez à nouveau l'adresse IP.

```
RSA key fingerprint is xxxxxx
Connecting? [yes|no] : yes
```

Pour utiliser un service SSH avec authentification de clé d'utilisateur lorsqu'une phrase secrète est définie, saisissez la phrase secrète.


```
Enter passphrase for key '/home/nana/.ssh/id_rsa' :xxxxxxx
Warning: No xauth data; using fake authentication data for X11
forwarding.
Last login: Fri Sep 1 10:19:37 2011 from client
```

11. Configurez NTP (optionnel).

Configurez le NTP de sorte que le XSCF fonctionne comme serveur ou client NTP. Vous pouvez également configurer NTP après avoir configuré un domaine.

Pour plus de détails, consultez « [3.6 Réglage de l'heure/date du XSCF](#) ».

Les procédures suivantes permettent de configurer les paramètres de gestion d'un compte d'utilisateur. Pour gérer un compte d'utilisateur, déterminez à l'avance si vous allez configurer un compte d'utilisateur local sauvegardé sur le XSCF ou paramétrer les données de compte sauvegardées dans une base de données de répertoire sur un réseau à l'aide de Lightweight Directory Access Protocol (LDAP), Active Directory ou LDAP sur SSL. Pour configurer une base de données de répertoire sur un réseau, paramétrez les comptes d'utilisateur de manière à ce qu'ils soient authentifiés d'après cette base de données.

Pour utiliser le serveur LDAP, Active Directory ou LDAP sur SSL, vous devez télécharger un certificat, créer une clé publique et finaliser par avance l'enregistrement en tant qu'utilisateur dans la base de données de répertoire de votre environnement. Dans la mesure où un utilisateur d'Active Directory ou LDAP sur SSL ne peut télécharger aucune clé publique d'utilisateur sur le XSCF, vous devez vous identifier après vous être connecté au XSCF via SSH à l'aide d'un mot de passe.

Ce manuel ne fournit pas les détails relatifs à LDAP, Active Directory et LDAP sur SSL. Consultez les manuels disponibles sur LDAP, Active Directory et LDAP sur SSL.

Remarque : pour la version de microprogramme XCP prenant en charge les services LDAP, Active Directory et LDAP sur SSL, consultez les dernières *Notes de produit* pour votre serveur.

12. Configurez les paramètres du service LDAP (optionnel).

Configurez le XSCF en tant que client LDAP. Pour plus de détails, consultez « [3.5.12 Gestion de comptes d'utilisateur XSCF à l'aide de LDAP](#) ».

13. Configurez les paramètres du service Active Directory (optionnel).

Configurez le XSCF en tant que client Active Directory. Pour plus de détails, consultez « [3.5.13 Gestion de comptes d'utilisateur XSCF à l'aide d'Active Directory](#) ».

14. Configurez les paramètres du service LDAP sur SSL (optionnel).

Configurez le XSCF en tant que client LDAP sur SSL. Pour plus de détails, consultez « [3.5.14 Gestion de comptes d'utilisateur XSCF à l'aide de LDAP sur SSL](#) ».

15. Configurez des comptes d'utilisateur XSCF.

Enregistrez les comptes d'utilisateur XSCF contenus localement sur le serveur en fonction de l'environnement de l'utilisateur.

- Pour ajouter un compte d'utilisateur, exécutez la commande `showuser` en spécifiant l'option `-l`, puis vérifiez que la liste des comptes d'utilisateur ne comprend pas de compte invalide.
- Pour prendre en compte les travaux de maintenance, veillez à préparer un

compte d'utilisateur pour technicien sur site (FE) disposant du privilège d'utilisateur fieldeng.

Pour plus de détails, consultez « [3.5 Création/gestion des utilisateurs XSCF](#) ».

16. **Configurez SMTP (optionnel).**

Configurez le SMTP pour utiliser la fonction de notification par e-mail du XSCF.

Pour plus de détails, consultez « [10.2 Réception de notifications par e-mail lorsqu'une panne se produit](#) ».

17. **Configurez les éléments relatifs au protocole SNMP pour utiliser la fonction d'agent SNMP (optionnel).**

Pour plus de détails, consultez « [10.3 Surveillance/Gestion de l'état du système avec l'agent SNMP](#) ».

18. **Configurez les éléments permettant d'utiliser le service de maintenance à distance (optionnel).**

Ce document ne décrit pas en détail la fonction de service de maintenance à distance. Pour des informations sur la fonction de service de maintenance à distance, consultez les dernières *Notes de produit* pour votre serveur.

Les étapes suivantes permettent de configurer les éléments de gestion du matériel dans la totalité du système.

19. **Définissez l'altitude.**

Pour plus de détails, consultez « [4.1 Paramétrage / vérification de l'altitude du système](#) ».

Remarque : cette tâche de paramétrage a été effectuée pendant l'installation initiale. Si la valeur doit être modifiée, paramétrez-la de nouveau.

20. **Configurez la limitation de l'alimentation (optionnel).**

Pour plus de détails, consultez « [4.4 Diminution de la consommation électrique](#) ».

21. **Configurez le mode de mise en miroir de la mémoire (optionnel).**

Pour plus de détails, consultez « [14.1 Configuration de la mise en miroir de la mémoire](#) ».

22. **Définissez la durée d'attente de la climatisation (optionnel).**

Définissez cette durée de telle sorte que le processus de mise sous tension attende que les installations de climatisation adaptent l'environnement à la température ambiante.

Pour plus de détails, consultez « [4.2.2 Réglage/Vérification du temps d'attente au démarrage](#) ».

Les étapes suivantes permettent de configurer les éléments de gestion des partitions physiques.

23. **Configurez les partitions physiques (optionnel).**

Paramétrez les informations de gestion de la configuration du domaine.

Pour plus de détails, consultez « [11.2 Vérification d'une partition physique](#) » et le *Guide de configuration du domaine Fujitsu SPARC M12 et Fujitsu M10/SPARCM10*.

24. **Paramétrez le mode de partition physique (optionnel).**
Pour plus de détails, consultez « [7.2 Réglage des modes de fonctionnement de la partition physique](#) » et le *Guide de configuration du domaine Fujitsu SPARC M12 et Fujitsu M10/SPARCM10*.
25. **Effectuez les réglages permettant l'activation du processeur (CPU).**
Pour plus de détails, consultez « [Chapitre 5 Activation de processeur](#) ».
26. **Définissez le délai de préchauffage (optionnel).**
Définissez un délai permettant de retarder le processus de mise sous tension pendant une durée déterminée avant le démarrage d'Oracle Solaris. Cette durée s'applique après le démarrage du processus de mise sous tension du serveur. Ce paramètre est utilisé pour attendre que le serveur ait effectué son préchauffage et que les périphériques soient mis sous tension.

Si la commande `setpowercapping` a défini une valeur maximale de consommation électrique, il se peut que l'électricité consommée par toutes les partitions physiques fonctionnant simultanément dépasse cette valeur maximale. Pour éviter cela, vous pouvez utiliser ce paramètre pour échelonner les périodes de fonctionnement de chaque partition physique.

Pour plus de détails, consultez « [4.2.1 Réglage/Vérification du délai de préchauffage](#) ».
27. **Paramétrez la planification d'alimentation (optionnel).**
Définissez les informations de planification d'alimentation pour chacune des partitions physiques.

Pour paramétrer une planification d'alimentation, utilisez les commandes `setpowerschedule`, `addpowerschedule` et `deletepowerschedule` du microprogramme XSCF. Pour plus de détails sur chaque commande, consultez la page du manuel correspondant à la commande ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

3.4 Configuration depuis le XSCF Web

Cette section décrit la procédure de configuration nécessaire depuis XSCF Web. Pour plus de détails sur chaque étape, consultez la section indiquée par le titre entre guillemets.

Pour utiliser XSCF Web, le service HTTPS doit avoir au préalable été activé dans les paramètres réalisés à l'aide du shell XSCF.

1. **Connectez-vous au shell XSCF depuis n'importe quel terminal disposant d'une connexion série.**
Pour plus de détails, consultez « [2.2 Connexion au Shell XSCF](#) ».
2. **Effectuez les étapes 2 à 11 dans « [3.3 Configuration depuis le shell XSCF](#) ».**
Si vous avez déjà effectué les étapes 2 à 11 à l'aide du shell XSCF dans la section 7.2, passez à l'étape suivante dans cette section.
3. **Configurez HTTPS.**

Pour plus de détails, consultez « [3.8 Configuration du service HTTPS pour la connexion à XSCF](#) ».

4. **Connectez-vous au XSCF depuis un navigateur web.**

Connectez-vous à XSCF Web depuis un PC sur lequel un navigateur web est installé et raccordé à XSCF-LAN en indiquant le nom d'hôte ou l'adresse IP.

- Exemple de saisie d'URL sur un navigateur Web

```
https://192.168.111.111 (Saisissez l'adresse IP de XSCF
<numéros>)/
Ou bien,
https://XSCF-host-name (Remarque : différent du nom de l'hôte du
domaine)/
```

5. **Connectez-vous au XSCF depuis la console XSCF Web.**

Identifiez-vous avec un compte d'utilisateur créé.

```
<Image d'entrée d'authentification de connexion sur un navigateur Web>
login:yyyy
Password:xxxxxxxx
```

La fenêtre du navigateur de XSCF Web est appelée console XSCF Web.

Pour plus de détails, consultez « [2.4 Connexion à XSCF Web](#) ».

6. **Les éléments de réglage sont les mêmes que ceux du shell XSCF. Configurez-les depuis la console XSCF Web de la même façon qu'à l'étape 12 et ultérieurement dans « [3.3 Configuration depuis le shell XSCF](#) ».**

Pour plus de détails sur le menu XSCF Web, consultez « [Annexe C Liste des pages de XSCF Web](#) ».

Remarque : pour les paramètres non compris dans le menu XSCF Web, comme l'altitude ou la double alimentation, utilisez le shell XSCF.

3.5 Création/gestion des utilisateurs XSCF

Cette section décrit comment créer/gérer les comptes d'utilisateur, les mots de passe, les privilèges d'utilisateur ainsi que la stratégie de mot de passe employée pour la connexion au XSCF. Pour la gestion des comptes d'utilisateur, vous pouvez configurer un compte d'utilisateur local XSCF ou un compte d'utilisateur pour vous identifier sur une base de données de répertoire sur un réseau à l'aide de LDPA, Active Directory ou LDAP sur SSL.

3.5.1 Comptes d'utilisateur XSCF

Utilisation des scénarios

Les comptes d'utilisateur XSCF sont utilisés pour s'identifier sur le shell XSCF via SSH ou Telnet ou sur XSCF Web.

Utilisateurs pouvant enregistrer un compte d'utilisateur XSCF

Pour enregistrer un compte d'utilisateur XSCF, vous devez vous connecter avec un compte d'utilisateur disposant du privilège d'utilisateur useradm.

Noms de compte d'utilisateur XSCF disponibles

Aucun des noms de compte d'utilisateur XSCF suivants n'est disponible dans la mesure où ceux-ci sont réservés au système :

root, bin, daemon, adm, operator, nobody, sshd, rpc, rpcuser, ldap, ntp, admin, default, proxyuser

Si le compte d'utilisateur XSCF est géré à l'aide du service LDAP, Active Directory ou LDAP sur SSL, son nom et, si cela est spécifié, l'identifiant d'utilisateur (UID) ne doivent pas être déjà utilisés sur le XSCF, LDAP, Active Directory ou LDAP sur SSL. Pour plus de détails sur les caractères disponibles, consultez la page de manuel correspondant à la commande adduser(8) ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

Nombre de comptes d'utilisateur

Le nombre de comptes d'utilisateur pouvant être spécifiés s'élève à 100 en supposant qu'en moyenne chaque compte d'utilisateur compte 10 caractères. Lorsqu'elle est exécutée, la commande adduser enregistre un compte d'utilisateur auquel est automatiquement attribué un identifiant appelé UID. Cet UID est un nombre entier supérieur ou égal à 100. Un numéro choisi arbitrairement peut également être spécifié en tant qu'UID. Dans ce cas, déterminez un UID compris entre 100 et 60 000.

Cas d'échec d'authentification de connexion

Si l'authentification échoue, le compte d'utilisateur peut être verrouillé pendant une durée déterminée. La fonction permettant de débloquent un compte est appelée fonction de déverrouillage de compte d'utilisateur XSCF. L'administrateur système peut activer et désactiver les comptes d'utilisateur XSCF utilisés.

3.5.2 Mots de passe et stratégie de mot de passe

Lors de l'enregistrement d'un compte d'utilisateur XSCF, enregistrez également un mot de passe. Un compte d'utilisateur nouvellement créé ne possède pas de mot de passe défini. En conséquence, avant qu'une commande de mot de passe ou une clé publique attribuée par Secure Shell (SSH) ne soit paramétrée pour l'utilisateur, le compte d'utilisateur ne peut être utilisé pour une identification.

Les mots de passe obéissent à certaines restrictions en termes de longueur ou de type de caractères. Ces attributs de mots de passe se conforment à des règles appelées stratégie de mot de passe. Après création d'un compte d'utilisateur, la stratégie actuelle de mot de passe s'applique au compte d'utilisateur créé. Lorsque vous redéfinissez la stratégie de mot de passe, celle-ci s'applique aux utilisateurs ajoutés ultérieurement. Vous pouvez vérifier la stratégie actuelle de mot de passe en exécutant la commande `showpasswordpolicy`.

Tableau 3-5 présente les éléments de réglage de la stratégie de mot de passe.

Tableau 3-5 Éléments de la stratégie de mot de passe

Élément de réglage	Signification
Mindays	Nombre minimal de jours entre deux modifications de mot de passe. 0 indique le mot de passe peut être modifié à n'importe quel moment.
Maxdays	Nombre maximal de jours durant lesquels un mot de passe est valide
Warn	Un avertissement prévenant du nombre de jours avant expiration du mot de passe est transmis avant expiration effective de celui-ci
Inactive	Nombre de jours après expiration du mot de passe précédant le verrouillage du compte
Expiry	Nombre de jours durant lesquels le compte demeure valide. La valeur par défaut est 0. 0 signifie que le compte n'expire jamais.
Retry	Nombre de tentatives autorisées pour modifier un mot de passe
Difok	Nombre de caractères non compris dans l'ancien mot de passe mais devant être intégrés au nouveau
Minlen	Longueur minimale de mot de passe acceptée
Dcredit	Un mot de passe qui contient des caractères numériques peut être plus court que la longueur minimale acceptable de mot de passe (Minlen). Le nombre de caractères baisse en fonction du nombre de caractères numériques compris dans le mot de passe. Ici, vous pouvez régler la valeur maximale de cette diminution.
Ucredit	Un mot de passe qui contient des majuscules peut être plus court que la longueur minimale acceptable de mot de passe (Minlen). Le nombre de caractères baisse en fonction du nombre de majuscules comprises dans le mot de passe. Ici, vous pouvez régler la valeur maximale de cette diminution.

Tableau 3-5 Éléments de la stratégie de mot de passe *(suite)*

Élément de réglage	Signification
Lcredit	Un mot de passe qui contient des minuscules peut être plus court que la longueur minimale acceptable de mot de passe (Minlen). Le nombre de caractères baisse en fonction du nombre de minuscules comprises dans le mot de passe. Ici, vous pouvez régler la valeur maximale de cette diminution.
Ocredit	Un mot de passe qui contient des caractères non alphanumériques peut être plus court que la longueur minimale acceptable de mot de passe (Minlen). Le nombre de caractères baisse en fonction du nombre de caractères non alphanumériques compris dans le mot de passe. Ici, vous pouvez régler la valeur maximale de cette diminution.
Remember	Nombre de mots de passe pouvant être stockés dans l'historique de mot de passe

3.5.3 Types de privilège d'utilisateur

Lors de l'ajout d'un compte d'utilisateur XSCF, définissez un privilège d'utilisateur pour celui-ci. L'octroi de privilèges d'utilisateur répond aux objectifs suivants :

- Fournir des privilèges opérationnels sur la totalité du système à l'administrateur système
- Restreindre les opérations à une partition physique déterminée
- Gérer les comptes d'utilisateur
- Configurer l'audit
- Restreindre les opérations sur le serveur des techniciens sur site

Plusieurs privilèges d'utilisateur peuvent être paramétrés pour un seul compte d'utilisateur. Attribuez des privilèges d'utilisateur aux comptes en fonctions de l'environnement de l'utilisateur et de l'objectif. [Tableau 3-6](#) répertorie les privilèges d'utilisateur.

Tableau 3-6 Privilèges d'utilisateur

Privilège d'utilisateur	Résumé	Descriptif du privilège
pparop@n	Référencement de tous les états d'une partition physique déterminée.	- Autorisé à référencer tous les états du matériel installé sur une partition physique déterminée (PPAR-ID :n). - Autorisé à référencer tous les états d'une partition physique déterminée (PPAR-ID:n).

Tableau 3-6 Privilèges d'utilisateur (*suite*)

Privilège d'utilisateur	Résumé	Descriptif du privilège
pparmgr@n	Autorisation de gérer l'alimentation et référencement uniquement de l'état d'une partition physique déterminée.	- Autorisé à mettre sous/hors tension et redémarrer une partition physique déterminée (PPAR-ID :n). - Autorisé à référencer tous les états du matériel installé sur une partition physique déterminée (PPAR-ID :n). - Autorisé à référencer tous les états d'une partition physique déterminée (PPAR-ID:n).
pparadm@n	Autorisation uniquement de gérer une partition physique déterminée.	- Autorisé à commander tout le matériel installé sur une partition physique déterminée (PPAR-ID :n). - Autorisé à référencer tous les états du matériel installé sur une partition physique déterminée (PPAR-ID :n). - Autorisé à commander toutes les partitions physiques déterminées (PPAR-ID :n). - Autorisé à référencer tous les états d'une partition physique déterminée (PPAR-ID:n).
platop	Référencement de l'état de la totalité du système.	Peut référencer tous les états du serveur sans pouvoir les modifier.
platadm	Gestion de la totalité du système.	- Autorisé à effectuer toutes les opérations sur le matériel pour le système. - Autorisé à manipuler tous les paramètres XSCF hormis ceux nécessitant les privilèges useradm et d'audit XSCF. - Peut ajouter/supprimer du matériel sur la partition physique. - Peut effectuer des opérations d'alimentation sur la partition physique. - Autorisé à référencer tous les états du serveur.
useradm	Gestion des comptes d'utilisateur.	- Autorisé à créer, supprimer, activer et désactiver des comptes d'utilisateur. - Autorisé à modifier des mots de passe d'utilisateur et des profils de mot de passe. - Autorisé à modifier des privilèges d'utilisateur.
auditop	Référencement de l'état d'audit.	Autorisé à référencer l'état d'audit du XSCF et les méthodes d'audit.
auditadm	Commande de l'audit.	- Autorisé à commander l'audit du XSCF. - Autorisé à supprimer des méthodes d'audit du XSCF.
fieldeng	Permet l'utilisation par les techniciens sur site.	Restreint l'autorisation des techniciens sur site aux seules tâches de maintenance et aux modifications de configuration des périphériques.

Tableau 3-6 Privilèges d'utilisateur (*suite*)

Privilège d'utilisateur	Résumé	Descriptif du privilège
none	Vous ne disposez d'aucun privilège d'utilisateur.	Lorsqu'un compte d'utilisateur stocké sur le XSCF est réglé sur « none », le privilège de ce compte d'utilisateur n'est pas pris en compte sur LDAP. En conséquence, même si un privilège d'utilisateur a été paramétré pour le compte sur LDAP, ce privilège est considéré équivalent à « none ».

Un privilège d'utilisateur destiné à une partition physique ciblée comporte le suffixe « @numéro de PPAR » ajouté à son nom. (exemple : pparadm pour PPAR-ID 01 devient pparadm@1)

Un compte d'utilisateur peut disposer de privilèges sur plusieurs partitions physiques dont celle souhaitée. Pour plus de détails sur les paramètres de privilège d'utilisateur, consultez la page de manuel correspondant à la commande `setprivileges(8)` ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

3.5.4 Vérification des éléments de réglage et des commandes liées aux comptes d'utilisateur XSCF

Tableau 3-7 répertorie les éléments de réglage relatifs aux comptes d'utilisateur XSCF et les commandes du shell XSCF correspondantes.

Tableau 3-7 Éléments de réglage liés aux comptes d'utilisateur XSCF

Élément de réglage	Paramétrage requis ou optionnel	Commande liée
Ajout/suppression d'un compte d'utilisateur	Requis	<code>showuser(8)</code> , <code>adduser(8)</code> , <code>deleteuser(8)</code>
Activation/désactivation d'un compte d'utilisateur	Requis	<code>enableuser(8)</code> , <code>disableuser(8)</code>
Définition de la stratégie de mot de passe	Optionnel	<code>setpasswordpolicy(8)</code> , <code>showpasswordpolicy(8)</code>
Paramétrage d'un mot de passe	Requis	<code>password(8)</code>
Attribution d'un privilège d'utilisateur	Requis	<code>setprivileges(8)</code> , <code>showuser(8)</code>
Configuration de la fonction de verrouillage	Optionnel	<code>setloginlockout(8)</code> , <code>showloginlockout(8)</code>

Tableau 3-8 Éléments de réglage liés aux comptes d'utilisateur pour le service de répertoire

Élément de réglage	Paramétrage requis ou optionnel	Commande liée
Paramétrage du client LDAP	Optionnel	<code>showldap(8)</code> , <code>setldap(8)</code>

Tableau 3-8 Éléments de réglage liés aux comptes d'utilisateur pour le service de répertoire *(suite)*

Élément de réglage	Paramétrage requis ou optionnel	Commande liée
Paramétrage du client Active Directory	Optionnel	showad(8), setad(8)
Paramétrage du client LDAP sur SSL	Optionnel	showldapssl(8), setldapssl(8)

Remarque : pour la version de microprogramme XCP prenant en charge les services LDAP, Active Directory et LDAP sur SSL, consultez les dernières *Notes de produit* pour votre serveur.

3.5.5 Procédure d'enregistrement d'un compte d'utilisateur XSCF

Le compte d'utilisateur par défaut paramétré à la sortie d'usine est « default ». Afin d'utiliser un autre compte d'utilisateur pour des opérations sur le système, enregistrez-le à l'aide du XSCF.

Le compte d'utilisateur « default » dispose des privilèges suivants :

- privilèges « default » : useradm et platadm

En vous identifiant avec ce compte par défaut lors de l'installation initiale, enregistrez au moins un compte d'utilisateur disposant du privilège useradm ou platadm. Pour plus de détails sur l'authentification avec le compte d'utilisateur par défaut, consultez « Connexion à XSCF » dans le *Guide d'installation* de votre serveur.

Procédure d'enregistrement

Pour gérer le compte d'utilisateur XSCF via un service de répertoire sur un réseau à l'aide du service LDAP, Active Directory ou LDAP sur SSL, consultez « [3.5.12 Gestion de comptes d'utilisateur XSCF à l'aide de LDAP](#) », « [3.5.13 Gestion de comptes d'utilisateur XSCF à l'aide d'Active Directory](#) » ou « [3.5.14 Gestion de comptes d'utilisateur XSCF à l'aide de LDAP sur SSL](#) ».

L'administrateur système enregistre un compte d'utilisateur en effectuant les procédures suivantes. Pour plus de détails, consultez les sections correspondantes indiquées.

1. **Connectez-vous au XSCF avec un compte d'utilisateur disposant du privilège useradm (voir section 3.5.6).**
Le compte d'utilisateur par défaut « default » dispose du privilège useradm.
2. **Vérifiez les utilisateurs enregistrés (voir showuser(8) dans la section 3.5.6).**
Lors de l'ajout d'un compte d'utilisateur, exécutez la commande showuser en spécifiant l'option -l, puis vérifiez que la liste des comptes d'utilisateur ne comprenne pas de compte invalide.
3. **Vérifiez/modifiez la stratégie de mot de passe (voir showpasswordpolicy(8) ou setpasswordpolicy(8) dans la section 3.5.7).**

4. **Enregistrez le compte d'utilisateur XSCF (voir adduser(8) dans la section 3.5.8).**
À l'aide de la commande adduser, enregistrez le compte d'utilisateur adapté à l'environnement de l'utilisateur.
5. **Définissez un mot de passe (voir password(8) dans la section 3.5.8).**
6. **Enregistrez un privilège d'utilisateur (voir setprivileges(8) dans la section 3.5.9).**

Pour plus de détails sur chaque commande, consultez la page du manuel correspondante ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

3.5.6 Vérification des utilisateurs enregistrés

Pour vérifier les utilisateurs enregistrés sur le système, utilisez la commande showuser. Pour afficher des informations sur les autres comptes d'utilisateur, un compte d'utilisateur disposant du privilège useradm doit être utilisé afin de pouvoir exécuter la commande.

1. **Exécutez la commande showuser pour afficher les informations sur un compte d'utilisateur XSCF.**
Dans l'exemple suivant, toutes les informations sur un compte d'utilisateur XSCF sont affichées en spécifiant l'option -l.

```
XSCF> showuser -l
User Name:          user001
UID:                101
Status:             Enabled
Minimum:            0
Maximum:            99999
Warning:            7
Inactive:           -1
Last Change:        Jul 11, 2012
Password Expires:   Never
Password Inactive:  Never
Account Expires:    Never
Privileges:         platadm
```

Dans l'exemple suivant, toutes les informations sur les privilèges d'utilisateur sont affichées en spécifiant l'option -l.

```
XSCF> showuser -p
User Name:          jsmith
Privileges:         pparadm@1,3-6,8,9
                   platadm
```

3.5.7

Vérification/Modification de la stratégie de mot de passe

Une fois la stratégie de mot de passe définie, elle s'applique à tous les utilisateurs ajoutés ultérieurement. Utilisez la commande `showpasswordpolicy` pour vérifier la stratégie de mot de passe actuellement définie. Après avoir vérifié la stratégie de mot de passe, si vous souhaitez la modifier, utilisez la commande `setpasswordpolicy`. Exécutez la commande `setpasswordpolicy` avec un compte d'utilisateur disposant du privilège `useradm`.

La commande `setpasswordpolicy` définit la stratégie de mot de passe avec les options suivantes.

Tableau 3-9 Options de la commande `setpasswordpolicy`

Option	Stratégie de mot de passe	Contenu du réglage
-n	Mindays	Nombre minimal de jours entre deux modifications de mot de passe. 0 indique le mot de passe peut être modifié à n'importe quel moment.
-M	Maxdays	Nombre maximal de jours durant lesquels un mot de passe est valide
-w	Warn	Un avertissement prévenant du nombre de jours avant expiration du mot de passe est transmis avant expiration effective de celui-ci
-i	Inactive	Nombre de jours après expiration du mot de passe précédant le verrouillage du compte
-e	Expiry	Nombre de jours durant lesquels le compte demeure valide
-y	Retry	Nombre de tentatives autorisées pour modifier un mot de passe
-k	Difok	Nombre de caractères non compris dans l'ancien mot de passe mais devant être intégrés au nouveau
-m	Minlen	Longueur minimale de mot de passe acceptée
-d	Dcredit	Un mot de passe qui contient des caractères numériques peut être plus court que la longueur minimale acceptable de mot de passe (Minlen). Le nombre de caractères baisse en fonction du nombre de caractères numériques compris dans le mot de passe. Ici, vous pouvez régler la valeur maximale de cette diminution.

Tableau 3-9 Options de la commande setpasswordpolicy (suite)

Option	Stratégie de mot de passe	Contenu du réglage
-u	Ucredit	Un mot de passe qui contient des majuscules peut être plus court que la longueur minimale acceptable de mot de passe (Minlen). Le nombre de caractères baisse en fonction du nombre de majuscules comprises dans le mot de passe. Ici, vous pouvez régler la valeur maximale de cette diminution.
-l	Lcredit	Un mot de passe qui contient des minuscules peut être plus court que la longueur minimale acceptable de mot de passe (Minlen). Le nombre de caractères baisse en fonction du nombre de minuscules comprises dans le mot de passe. Ici, vous pouvez régler la valeur maximale de cette diminution.
-o	Ocredit	Un mot de passe qui contient des caractères non alphanumériques peut être plus court que la longueur minimale acceptable de mot de passe (Minlen). Le nombre de caractères baisse en fonction du nombre de caractères non alphanumériques compris dans le mot de passe. Ici, vous pouvez régler la valeur maximale de cette diminution.
-r	Remember	Nombre de mots de passe pouvant être stockés dans l'historique de mot de passe

Procédure de fonctionnement

1. **Exécutez la commande showpasswordpolicy pour vérifier la stratégie de mot de passe.**

```
XSCF> showpasswordpolicy
Mindays:          0
Maxdays:         90
Warn:             7
Inactive:        -1
Expiry:           0
Retry:            5
Difok:            1
Minlen:           8
Dcredit:          0
Ucredit:          0
Lcredit:          0
Ocredit:          0
Remember:         4
```

2. **Si nécessaire, exécutez la commande setpasswordpolicy pour opérer des modifications dans les paramètres de la stratégie de mot de passe.**

L'exemple ci-dessous spécifie ce qui suit :

- 3 tentatives au maximum
- Une longueur de mot de passe à 6 caractères ou plus si le mot de passe contient 2 caractères numériques. Une longueur de mot de passe à 8 caractères ou plus si le mot de passe ne contient pas de caractères numériques
- Un délai d'expiration de 60 jours
- Un préavis de 15 jours avant expiration pour les avertissements
- Possibilité de mémoriser 3 mots de passe

```
XSCF> setpasswordpolicy -y 3 -m 8 -d 2 -u 0 -l 0 -o 0 -M 60 -w 15 -r 3
```

3. Exécutez la commande showpasswordpolicy, puis vérifiez les paramètres.

```
XSCF> showpasswordpolicy
Mindays:                0
Maxdays:                60
Warn:                   15
Inactive:               -1
Expiry:                 0
Retry:                  3
Difok:                  1
Minlen:                 8
Dcredit:                2
Ucredit:                0
Lcredit:                0
Ocredit:                0
Remember:               3
```

Remarque : la stratégie de mot de passe du système ne s'applique lorsqu'un mot de passe est modifié par une commande password dont l'opérande spécifiée est un autre utilisateur. Lors de la modification du mot de passe d'un autre utilisateur, assurez-vous de spécifier un mot de passe se conformant à la stratégie du système.

3.5.8 Ajout d'un compte d'utilisateur XSCF et réglage d'un mot de passe

Pour ajouter un compte d'utilisateur, utilisez la commande adduser. Exécutez la commande avec un compte d'utilisateur disposant du privilège useradm. Pour plus de détails concernant les noms pouvant être utilisés pour les comptes d'utilisateur, consultez « [3.5.1 Comptes d'utilisateur XSCF](#) ».

Pour le compte d'utilisateur ajouté, utilisez la commande password pour définir un mot de passe. La commande password définit la durée de validité du mot de passe à l'aide des options suivantes.

Tableau 3-10 Options de la commande password

Option	Contenu du réglage
-e	Définit la durée de validité du compte d'utilisateur ou sa date d'expiration. Lorsqu'elle est réglée sur « NEVER », la date d'expiration du compte d'utilisateur est supprimée.
-i	Définit le nombre de jours après expiration du mot de passe précédant le verrouillage du compte
-M	Définit le nombre maximal de jours durant lesquels un mot de passe est valide
-n	Définit le nombre minimal de jours durant lesquels un mot de passe est valide
-w	Définit le nombre de jours après lesquels un avertissement concernant l'expiration du mot de passe est transmis avant expiration effective de celui-ci

Procédure de fonctionnement

1. **Exécutez la commande adduser pour ajouter un compte d'utilisateur.**
L'exemple suivant indique que le nom du compte d'utilisateur est jsmith. Si la spécification de l'UID est omise, un UID est attribué automatiquement.

```
XSCF> adduser jsmith
```

Dans l'exemple suivant, un compte d'utilisateur est ajouté avec un UID spécifié à l'aide de l'option -u.

```
XSCF> adduser -u 359 jsmith
```

2. **Exécutez la commande password et spécifiez un mot de passe.**

```
XSCF> password jsmith
Password:
Retype new password:
passwd: password updated successfully
XSCF>
```

L'exemple suivant indique que 60 jours ont été définis comme durée d'expiration et 15 jours avant expiration comme date de départ pour les avertissements.

```
XSCF> password -M 60 -w 15 jsmith
```

3.5.9 Réglage d'un privilège d'utilisateur

Pour paramétrer des privilèges d'utilisateur, utilisez la commande `setprivileges`. Exécutez la commande `setprivileges` avec un compte d'utilisateur disposant du privilège `useradm`. Pour plus d'informations sur les types de privilèges d'utilisateur, consultez [Tableau 3-6](#).

1. **Exécutez la commande `showuser` pour afficher les informations sur un compte d'utilisateur activé.**

```
XSCF> showuser -p jsmith
User Name:      jsmith
Privileges:     None
```

2. **Exécutez la commande `setprivileges` pour attribuer un privilège à un compte d'utilisateur.**

Dans l'exemple suivant, les privilèges d'utilisateur `useradm` et `auditadm` sont attribués au compte `jsmith`.

```
XSCF> setprivileges jsmith useradm auditadm
```

Remarque : la commande `setprivileges` attribue le privilège d'utilisateur à l'opérande spécifiée. Pour ajouter un nouveau privilège à un compte d'utilisateur disposant déjà d'un privilège, spécifiez également le privilège d'utilisateur existant.

3. **Exécutez la commande `showuser`, puis vérifiez les privilèges d'utilisateur.**

```
XSCF> showuser -p jsmith
User Name:      jsmith
Privileges:     useradm
                  auditadm
```

3.5.10 Activation/Désactivation d'un compte d'utilisateur

Les comptes d'utilisateur enregistrés avec la commande `adduser` sont activés immédiatement après leur enregistrement. Si nécessaire, vous pouvez désactiver des comptes d'utilisateur XSCF enregistrés, puis les réactiver.

Pour désactiver un compte d'utilisateur, utilisez la commande `disableuser`. Pour réactiver un compte d'utilisateur désactivé, utilisez la commande `enableuser`. Exécutez les commandes `disableuser` et `enableuser` avec un compte d'utilisateur disposant du privilège `useradm`.

1. **Exécutez la commande `showuser` pour afficher les informations sur un compte d'utilisateur activé.**


```
XSCF> showuser -p jsmith
User Name:          jsmith
:
```

2. **Exécutez la commande disableuser pour désactiver un compte d'utilisateur.**
Dans l'exemple suivant, le compte d'utilisateur à désactiver est spécifié.

```
XSCF> disableuser jsmith
```

3. **Pour utiliser de nouveau ce compte d'utilisateur, exécutez la commande enableuser pour le réactiver.**
Dans l'exemple suivant, le compte d'utilisateur à activer est spécifié.

```
XSCF> enableuser jsmith
```

4. **Exécutez la commande showuser pour vérifier les informations sur un compte d'utilisateur activé.**

```
XSCF> showuser -p jsmith
User Name:          jsmith
:
```

3.5.11 Activation/Désactivation de la fonction de verrouillage d'identification

Lorsque la fonction de verrouillage d'identification est activée et que l'utilisateur échoue à trois reprises successives à se connecter, ce dernier ne pourra pas se connecter avant qu'une durée déterminée ne soit écoulée. Dans les paramètres par défaut, la fonction de verrouillage d'identification est désactivée.

Pour définir une durée de verrouillage et activer la fonction de verrouillage d'identification, utilisez la commande setloginlockout. Pour activer la fonction de verrouillage, définissez une durée autre que 0 minutes. Toute valeur comprise entre 0 et 1 440 minutes peut être définie comme durée de verrouillage. Pour désactiver la fonction de verrouillage une fois que celle-ci a été activée, indiquez une durée de verrouillage de 0 minute. Utilisez la commande showloginlockout pour vérifier la durée de verrouillage paramétrée. Exécutez les commandes setloginlockout et showloginlockout avec un compte d'utilisateur disposant du privilège useradm.

1. **Exécutez la commande showloginlockout pour afficher les paramètres de la fonction de verrouillage.**

```
XSCF> showloginlockout
90 minutes
```

2. **Exécutez la commande `setloginlockout` pour configurer la fonction de verrouillage.**

Dans l'exemple suivant, une durée de verrouillage de 20 minutes est spécifiée et la fonction de verrouillage activée.

```
XSCF> setloginlockout -s 20
```

Dans l'exemple suivant, la fonction de verrouillage est désactivée.

```
XSCF> setloginlockout -s 0
```

La durée de verrouillage définie est appliquée dès la connexion suivante. Si la durée spécifiée est de 0 minute, la fonction de verrouillage est désactivée à compter de la connexion suivante.

La fonction de verrouillage est activée sur les XSCF maître et de veille. Si un compte d'utilisateur est verrouillé, un message est sauvegardé dans le journal d'audit.

Si la fonction de verrouillage est désactivée, le nombre de tentatives de connexion effectuées par les utilisateurs n'est pas limité.

Si vous devez utiliser un compte d'utilisateur bloqué avant expiration du verrouillage, l'administrateur peut désactiver la fonction de verrouillage. Après avoir réussi à vous connecter à ce compte d'utilisateur, l'administrateur système devra définir de nouveau la durée de verrouillage et réactiver la fonction de verrouillage.

3.5.12 Gestion de comptes d'utilisateur XSCF à l'aide de LDAP

Lightweight Directory Access Protocol (LDAP) est un protocole utilisé pour accéder à un service de répertoire sur réseau. En principe, l'authentification et le privilège d'utilisateur d'un compte d'utilisateur XSCF sur les systèmes SPARC M12/M10 sont gérés par le XSCF maître local. Cependant, en utilisant LDAP, ils peuvent être gérés par un service de répertoire (serveur LDAP) sur un réseau. En outre, si plusieurs systèmes SPARC M12/M10 sont installés, le compte d'utilisateur XSCF commun à tous ces systèmes peut être utilisé avec LDAP.

Pour gérer les paramètres de compte d'utilisateur XSCF, tels que l'authentification et les privilèges d'utilisateur, à partir du protocole LDAP, configurez le XSCF comme un client LDAP.

Cette section décrit comment gérer les paramètres de compte d'utilisateur XSCF par l'intermédiaire d'un service de répertoire sur réseau à l'aide de LDAP.

Remarque : cette section ne décrit pas la configuration et la gestion du serveur LDAP. Un administrateur déjà familier des serveurs LDAP devra concevoir le serveur LDAP.

Remarque : pour la version de microprogramme XCP prenant en charge LDAP, consultez les dernières *Notes de produit* pour votre serveur.

Dans les paramètres de LDAP, les éléments relatifs à un client LDAP sont définis. Les

réglages couvrent le serveur LDAP, l'identifiant lié, le mot de passe, la base de recherche, etc. Les informations d'utilisateur XSCF sont gérées sur le serveur LDAP.

Tableau 3-11 répertorie les termes liés aux paramètres de LDAP.

Tableau 3-11 Termes liés à LDAP

Terme	Description
LDAP	Abréviation de Lightweight Directory Access Protocol. LDAP est un protocole utilisé pour accéder à un service de répertoire sur un réseau.
baseDN	Abréviation de base Distinguished Name. Dans LDAP, les informations de répertoire sont organisées hiérarchiquement. Pour effectuer une recherche, indiquez l'arborescence inférieure à passer en revue dans la structure hiérarchique. À ce moment-là, spécifiez le nom unique (« distinguished name » ou DN) en haut de l'arborescence inférieure ciblée. Ce nom unique (DN) est qualifié de base de recherche (baseDN).
Chaîne de certificats	Liste des certifications, comprenant entre autres un certificat d'utilisateur et le certificat délivré par l'autorité de certification. Les certificats OpenSSL et TLS ne doivent pas être téléchargés à l'avance.
TLS	Abréviation de Transport Layer Security. C'est un protocole de chiffrement des informations destinées à être transmises/reçues via internet.

Tâches de paramétrage de LDAP

Cette section décrit les tâches permettant de configurer le XSCF en tant que client LDAP.

1. **Activez LDAP.**
2. **Saisissez les informations de configuration du serveur LDAP.**
 - L'adresse IP ou le nom d'hôte ainsi que le numéro de port du répertoire LDAP primaire
 - En option : jusqu'à deux adresses IP ou le nom d'hôte ainsi que le port des répertoires LDAP alternatifs
 - Le nom unique (DN) en tant que base de recherche et référence
 - Utilisation ou non de Transport Layer Security (TLS)
3. **Vérifiez si LDAP fonctionne normalement.**

Paramètres requis sur le serveur LDAP

- Ajoutez des descriptions liées aux privilèges d'utilisateur sur un fichier de schéma LDAP.
Pour configurer le XSCF en tant que client LDAP, créez un schéma LDAP relatif aux privilèges d'utilisateur du XSCF sur un serveur LDAP. Ajoutez les descriptions

suivantes au fichier de schéma.

```
attributetype ( 1.3.6.1.1.1.1.40 NAME 'spPrivileges'  
    DESC 'Service Processor privileges'  
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.26  
    SINGLE-VALUE )  
objectclass ( 1.3.6.1.1.1.2.13 NAME 'serviceProcessorUser' SUP top  
AUXILIARY  
    DESC 'Service Processor user'  
    MAY spPrivileges )
```

- Ajoutez les attributs requis pour les utilisateurs à un fichier LDIF.
Ajoutez les attributs suivants, requis pour chaque utilisateur, à un fichier LDIF (LDAP Data Interchange Format) sur un serveur LDAP.

Tableau 3-12 Attributs requis pour un fichier LDIF

Nom de champ	Description
spPrivileges	Privilège d'utilisateur valide sur le XSCF
uidNumber	Identifiant d'utilisateur (UID) valide sur le XSCF L'identifiant d'utilisateur doit être une valeur numérique supérieure à 100. Utilisez la commande showuser pour afficher un UID.

L'exemple suivant montre une saisie de fichier de schéma LDAP.

```
spPrivileges: platadm  
uidNumber: 150
```

Mécanisme d'authentification de l'utilisateur lors de la configuration du XSCF comme client LDAP

Si des clients LDAP sont configurés sur le XSCF et activés, l'authentification de l'utilisateur est d'abord effectuée localement, puis sur le serveur LDAP. Si la commande setprivileges est exécutée sans spécifier un privilège pour l'utilisateur, toutes les données locales relatives aux privilèges de l'utilisateur sont supprimées. Après cela, si la référencement des privilèges est activé sur LDAP, le privilège d'utilisateur est référencé sur LDAP. Lorsqu'aucun privilège n'est spécifié pour l'utilisateur, celui-ci ne dispose d'aucun privilège même s'il possède des données l'indiquant sur LDAP.

Les commandes suivantes sont utilisées pour gérer LDAP sur le XSCF.

- setlookup
- setldap

Les méthodes de chiffrement Unix crypt ou MD5 sont utilisées pour les mots de passe sauvegardés dans le référentiel LDAP.

Une fois que vous avez configuré le XSCF afin d'utiliser LDAP, vous n'avez plus

besoin d'une gestion quotidienne.

Éléments de réglage de LDAP et commandes de shell à utiliser

Tableau 3-13 répertorie les éléments de réglage de LDAP et les commandes de shell correspondantes.

Tableau 3-13 Éléments de réglage de LDAP et commandes à utiliser

Élément de réglage	Description de la fonction	Commande de shell	Remarques
Affichage d'utilisation de LDAP	Affiche l'état concernant l'utilisation d'un serveur LDAP pour l'authentification et la recherche de privilèges d'utilisateur.	showlookup	
Activation/désactivation de l'utilisation de LDAP	Active/désactive l'utilisation d'un serveur LDAP pour l'authentification et la recherche de privilèges d'utilisateur.	setlookup	S'il est spécifié que les données relatives à l'authentification et aux privilèges d'utilisateur sont placées sur un serveur LDAP, le système cherche d'abord dans la zone locale. Si les données ciblées ne sont pas trouvées localement, la recherche se poursuit alors sur le serveur LDAP.
Affichage du client	Affiche les informations de configuration du client LDAP.	showldap	
Identifiant associé	Enregistre un identifiant lié pour se connecter (authentifier) au serveur LDAP.	setldap	La longueur maximale d'un identifiant lié est de 128 caractères.
Mot de passe	Définit un mot de passe utilisé pour se connecter au serveur LDAP.		Un mot de passe peut comprendre de 8 à 16 caractères.
Base de recherche	Définit une base de recherche par arborescence LDAP (baseDN).		- Si cet élément est omis, la commande débute sa recherche par le sommet de l'arborescence. - La longueur maximale autorisée pour la base de recherche est de 128 caractères.

Tableau 3-13 Éléments de réglage de LDAP et commandes à utiliser (suite)

Élément de réglage	Description de la fonction	Commande de shell	Remarques
Chaîne de certificats	Importe la chaîne de certificats d'un serveur LDAP. Importe la chaîne de certificats (scp) depuis un fichier à distance en utilisant une copie sécurisée.		- La chaîne de certificats doit être sous format PEM. (*1) - Il se peut qu'un mot de passe doive être saisi pour importer le certificat depuis un fichier à distance en utilisant scp.
Serveur/port LDAP	Spécifie les adresses IP et les numéros de port des serveurs LDAP primaire et secondaire. Spécifie les adresses IP ou les noms d'hôtes pour ces adresses. (exemples : ldap://foobar.east, ldaps://10.8.31.14:636)		Lorsque le numéro de port n'est pas spécifié, les numéros de port LDAP par défaut sont 636 pour ldaps:// et 389 pour ldap://.
Expiration	Définit la durée maximale (en secondes) autorisée pour une recherche LDAP.		
LDAP test	Reste la connexion à un serveur LDAP.		

*1 PEM : Abréviation de Privacy Enhanced Mail. Le message à envoyer est crypté pour une protection accrue de la vie privée.

Activation/désactivation de l'utilisation d'un serveur LDAP

- Exécutez la commande showlookup pour afficher la méthode de recherche de l'authentification et des privilèges d'utilisateur.**
Dans l'exemple suivant, la recherche n'est effectuée que sur le serveur XSCF pour l'authentification d'utilisateur et sur les serveurs XSCF et LDAP pour les privilèges d'utilisateur.

```
XSCF> showlookup
Privileges lookup: Local only
Authentication lookup: Local and LDAP
```

- Exécutez la commande setlookup pour activer/désactiver l'utilisation d'un serveur LDAP.**
Dans l'exemple suivant, un serveur LDAP est activé à la fois pour l'authentification et les privilèges d'utilisateur.

```
XSCF> setlookup -a ldap
XSCF> setlookup -p ldap
```

- Exécutez la commande showlookup, puis vérifiez la méthode de recherche.**

```
XSCF> showlookup
Privileges lookup: Local and LDAP
Authentication lookup: Local and LDAP
```

Paramétrage du serveur LDAP, du numéro de port, de l'identifiant lié, du mot de passe lié, de la base de recherche (baseDN) et de la durée de recherche (période d'expiration)

1. **Exécutez la commande showldap pour afficher les paramètres du client LDAP.**

```
XSCF> showldap
Bind Name: Not set
Base Distinguished Name: Not set
LDAP Search Timeout: 0
Bind Password: Not set
LDAP Servers: Not set
CERTS: None
```

2. **Exécutez la commande setldap pour configurer les paramètres du client LDAP.**
Dans l'exemple suivant, un identifiant lié et une base de recherche (baseDN) sont spécifiés.

```
XSCF> setldap -b "cn=Directory Manager" -B "ou=People,dc=users,dc=apl,dc=com,o=isp"
```

Dans l'exemple suivant, un mot de passe lié est spécifié.

```
XSCF> setldap -p
Password:xxxxxxxx
```

Dans l'exemple suivant, les serveurs LDAP primaire et secondaire ainsi que les numéros de port sont spécifiés.

```
XSCF> setldap -s ldap://onibamboo:389,ldaps://company2.com:636
```

Dans l'exemple suivant, la durée de validité pour la recherche LDAP est spécifiée.

```
XSCF> setldap -T 60
```

3. **Exécutez la commande showldap, puis vérifiez les paramètres.**

```
XSCF> showldap
Bind Name: cn=Directory Manager
Base Distinguished Name: ou=People,dc=users,dc=apl,dc=com,o=isp
```

```
LDAP Search Timeout:    60
Bind Password:         Set
LDAP Servers:          ldap://onibamboo:389 ldaps://company2.com:636
CERTS:                 None
```

Installation de la chaîne de certificats d'un serveur LDAP

1. **Exécutez la commande `showldap` pour afficher les paramètres de LDAP.**

```
XSCF> showldap
Bind Name:              cn=Directory Manager
Base Distinguished Name: ou=People,dc=users,dc=apl,dc=com,o=isp
LDAP Search Timeout:    60
Bind Password:         Set
LDAP Servers:          ldap://onibamboo:389 ldaps://company2.com:636
CERTS:                 None
```

2. **Exécutez la commande `setldap` pour importer la chaîne de certificats.**

```
XSCF> setldap -c hhhh@example.com:Cert.pem
```

3. **Exécutez la commande `showldap`, puis vérifiez que la chaîne de certificats a été importée.**

```
XSCF> showldap
Bind Name:              cn=Directory Manager
Base Distinguished Name: ou=People,dc=users,dc=apl,dc=com,o=isp
LDAP Search Timeout:    60
Bind Password:         Set
LDAP Servers:          ldap://onibamboo:389 ldaps://company2.com:636
CERTS:                 Exists
```

Test de connexion à un serveur LDAP

1. **Exécutez la commande `setldap` pour effectuer le test.**

```
XSCF> setldap -t sysadmin
onibamboo:389          PASSED
```

2. **Connectez-vous en tant qu'utilisateur enregistré au serveur LDAP. Confirmez l'authentification en utilisant le mot de passe saisi.**

```
login: sysadmin
Password:xxxxxxx
```


3. Exécutez la commande `showuser`, puis vérifiez si le privilège d'utilisateur affiché est le même que celui créé sur le serveur LDAP.

```
XSCF> showuser
User Name:      sysadmin (nonlocal)
UID:            110
Privileges:     platadm
```

3.5.13 Gestion de comptes d'utilisateur XSCF à l'aide d'Active Directory

Dans les paramètres d'Active Directory, les éléments relatifs à un client Active Directory sont définis. Les réglages couvrent le serveur Active Directory, le chargement d'un certificat de serveur, le nom de groupe, le privilège d'utilisateur, le domaine d'utilisateur, le journal, la requête d'index DNS, etc. Les informations d'utilisateur XSCF sont gérées sur le serveur Active Directory.

Remarque : cette section ne décrit pas la configuration et la gestion du serveur Active Directory. Un administrateur déjà familier des serveurs Active Directory devra concevoir le serveur Active Directory.

Remarque : pour la version de microprogramme XCP prenant en charge Active Directory, consultez les dernières *Notes de produit* pour votre serveur.

Tableau 3-14 répertorie les termes liés aux paramètres d'Active Directory.

Tableau 3-14 Termes liés à Active Directory

Terme	Description
Active Directory	Active Directory est un service de répertoire distribué développé par Microsoft Corporation et disponible sous les systèmes d'exploitation Windows. Comme le service de répertoire LDAP, il est utilisé pour l'authentification de l'utilisateur.
Domaine d'utilisateur	Le domaine d'utilisateur est le domaine d'authentification utilisé pour identifier un utilisateur.
Requête d'index DNS	La requête est utilisée pour questionner un serveur DNS au sujet du serveur Active Directory afin d'authentifier un utilisateur.

Active Directory fournit à la fois l'authentification du certificat d'utilisateur et l'autorisation du niveau d'accès de l'utilisateur aux ressources du réseau. Active Directory utilise l'authentification pour identifier des utilisateurs déterminés avant qu'ils n'accèdent aux ressources système et pour octroyer des privilèges d'accès définis aux utilisateur afin de contrôler leurs droits d'accès aux ressources du réseau.

Les privilèges d'utilisateur sont configurés sur le XSCF ou obtenus depuis un serveur sur un domaine de réseau basé sur l'appartenance au groupe de chacun des

utilisateurs. Un utilisateur peut appartenir à plusieurs groupes. Le domaine d'utilisateur est le domaine d'authentification utilisé pour identifier un utilisateur. Active Directory authentifie les utilisateurs dans l'ordre selon lequel les domaines d'utilisateur sont configurés.

Une fois l'authentification réalisée, les privilèges d'utilisateur peuvent être définis selon les manières suivantes :

- Dans le cas le plus simple, les privilèges d'utilisateur sont définis par les paramètres Active Directory sur le XSCF. Il existe un paramètre defaultrole pour Active Directory. Si le paramètre defaultrole est configuré ou défini, tous les utilisateurs authentifiés via Active Directory se voient attribuer les privilèges d'utilisateur définis dans celui-ci. Les utilisateurs paramétrés sur le serveur Active Directory n'ont besoin que d'un mot de passe quelle que soit leur appartenance à un groupe.
- Si le paramètre defaultrole n'est pas configuré ou défini, un privilège d'utilisateur est obtenu sur le serveur Active Directory en se fondant sur l'appartenance de l'utilisateur à un groupe. Sur le XSCF, le paramètre group doit correspondre au nom de groupe d'un serveur Active Directory. Chaque groupe dispose d'un privilège d'utilisateur configuré sur le XSCF et qui lui est associé. Une fois qu'un utilisateur est authentifié, l'appartenance à un groupe de celui-ci est utilisée pour déterminer ses privilèges.

Éléments de réglage d'Active Directory et commandes de shell à utiliser

Tableau 3-15 répertorie les éléments de réglage et les commandes de shell correspondantes.

Tableau 3-15 Éléments de réglage liés à Active Directory et commandes à utiliser

Élément de réglage	Description de la fonction	Commande de shell	Remarques
Affichage d'état d'Active Directory	Affiche l'état actuel d'Active Directory, comme son activation/désactivation et le mode d'index DNS.	showad	
Activation/désactivation de l'utilisation d'Active Directory	Spécifie si l'utilisation d'Active Directory pour la gestion de l'authentification et des privilèges d'utilisateur est activée ou non.	setad	Il est désactivé par défaut.
Affichage du serveur Active Directory	Affiche la configuration du serveur Active Directory primaire ou de jusqu'à cinq serveurs Active Directory alternatifs.	showad	Un numéro de port de « 0 » indique que le port par défaut d'Active Directory est utilisé.

Tableau 3-15 Éléments de réglage liés à Active Directory et commandes à utiliser *(suite)*

Élément de réglage	Description de la fonction	Commande de shell	Remarques
Serveur/port Active Directory	Spécifie les adresses IP et numéros de port du serveur primaire et de jusqu'à cinq serveurs alternatifs Active Directory. Spécifie les adresses IP ou les noms d'hôtes pour ces adresses. Pour spécifier des noms d'hôte pour les serveurs Active Directory, les noms de serveur doivent être compatibles avec le serveur DNS.	setad	Lorsqu'aucun numéro de port n'est spécifié, le port par défaut est utilisé.
Chargement/suppression du certificat du serveur	Charge ou supprime les certificats du serveur primaire et de jusqu'à cinq serveurs alternatifs.	setad	Le mode strictcertmode doit être désactivé pour permettre la suppression d'un certificat.
Activation/désactivation du mode d'index DNS	Active ou désactive le mode d'index DNS.	setad	Il est désactivé par défaut.
Affichage de requête d'index DNS	Affiche la configuration d'un nombre maximal de cinq requêtes d'index DNS.	showad	
Requête d'index DNS	Configure les requêtes d'index DNS. La requête d'index DNS est utilisée pour questionner un serveur DNS afin de définir un serveur Active Directory destiné à être utilisé pour l'authentification des utilisateurs.	setad	DNS et le mode d'index DNS doivent être activés pour permettre à la requête d'index DNS de fonctionner.
Activation/désactivation du mode de recherche étendue	Active ou désactive le mode de recherche étendue. Le mode de recherche étendue est uniquement activé dans le cas d'un environnement spécifique, où le compte d'utilisateur n'est pas sous format UserPrincipalName (UPN).	setad	Il est désactivé par défaut.
Activation/désactivation du mode strictcertmode	Active/désactive le mode strictcertmode. Si le mode strictcertmode est activé, le certificat d'un serveur doit auparavant avoir été téléchargé sur le serveur de sorte que les signatures puissent avoir été validées lorsque le certificat du serveur est présenté.	setad	Il est désactivé par défaut.
Affichage du certificat du serveur	Affiche les données suivantes : - Informations de certificat pour le serveur primaire et un nombre maximal de cinq serveurs alternatifs. - Intégralité du contenu du certificat	showad	
Affichage du domaine d'utilisateur	Affiche les domaines d'utilisateur.	showad	

Tableau 3-15 Éléments de réglage liés à Active Directory et commandes à utiliser (*suite*)

Élément de réglage	Description de la fonction	Commande de shell	Remarques
Domaine d'utilisateur	Configure jusqu'à cinq domaines d'utilisateur donnés. Spécifiez un domaine d'utilisateur sous format UPN dans lequel noms d'utilisateur et de domaine sont associés à l'aide du symbole « @ » ou sous forme de nom unique (DN) avec « uid = nom d'utilisateur, ou = unité d'organisation et dc = nom de domaine »	setad	Si un nom de domaine est directement indiqué en utilisant le formulaire UPN sur l'invite de connexion, comme par exemple « login: ima.admin@dc01.example.com », le domaine d'utilisateur est utilisé uniquement pour cette connexion.
Affichage de defaultrole	Affiche le paramètre defaultrole.	showad	
defaultrole	Spécifie les privilèges attribués à tous les utilisateurs authentifiés via Active Directory.	setad	
Affichage des groupes	Affiche la configuration du groupe d'administrateurs, du groupe d'opérateurs et du groupe personnalisé.	showad	
Groupe d'administrateurs	Attribue des noms de groupe à un nombre maximal de cinq groupes d'administrateurs. Le groupe d'administrateurs dispose des privilèges platadm, useradm et auditadm. Ces privilèges ne peuvent pas être modifiés.	setad	
Groupe d'opérateurs	Attribue des noms de groupe à un nombre maximal de cinq groupes d'opérateurs. Le groupe d'opérateurs dispose des privilèges platop et auditop. Ces privilèges ne peuvent pas être modifiés.	setad	
Groupe personnalisé	Attribue des noms de groupe et des privilèges d'utilisateur à un nombre maximal de cinq groupes.	setad	
Expiration	Définit le délai d'expiration de la transaction en secondes. Vous pouvez spécifier une valeur numérique comprise entre 1 et 20.	setad	La valeur par défaut est de 4 secondes. Si un délai d'expiration spécifié est trop bref pour la configuration, le processus d'identification ou la récupération du paramètre de privilège d'utilisateur peut échouer.
Activation/désactivation du journal	Active/désactive l'archivage des messages d'authentification et de diagnostic d'autorisation d'Active Directory.	setad	Ce journal est effacé lorsque le XSCF est redémarré.
Affichage de journal	Affiche les messages d'authentification et de diagnostic d'autorisation d'Active Directory.	showad	

Tableau 3-15 Éléments de réglage liés à Active Directory et commandes à utiliser (*suite*)

Élément de réglage	Description de la fonction	Commande de shell	Remarques
Suppression de journal	Efface les journaux de messages d'authentification et de diagnostic d'autorisation d'Active Directory.	setad	
Valeur par défaut	Fait revenir les paramètres d'Active Directory à leur valeur par défaut à la sortie d'usine.	setad	

Avant de configurer les paramètres d'Active Directory

Prenez note des points suivants avant de configurer les paramètres d'Active Directory.

- Vérifiez qu'une version de XCP prenant en charge Active Directory est utilisée. Pour connaître les versions de XCP prenant en charge Active Directory, consultez les dernières *Notes de produit*.
- Le privilège d'utilisateur useradm est nécessaire pour les paramètres d'Active Directory.
- Si le XSCF est configuré pour utiliser LDAP, Active Directory ou LDAP sur SSL pour des données de compte d'utilisateur, son nom et, si cela est spécifié, l'identifiant d'utilisateur (UID) ne doivent pas être déjà utilisés sur le XSCF, LDAP, Active Directory ou LDAP sur SSL.
- Afin d'utiliser un nom d'hôte pour un serveur Active Directory, les paramètres DNS doivent être configurés de manière adaptée avant de paramétrer Active Directory.
- Sur Active Directory, le compte système appelé proxyuser est utilisé. Vérifiez qu'aucun compte d'utilisateur portant ce nom n'existe. S'il existe un compte d'utilisateur portant le nom de proxyuser, supprimez ce compte à l'aide de la commande deleteuser. Une fois ce compte supprimé, redémarrez le XSCF avant d'utiliser Active Directory.
- Si Active Directory est activé et que vous essayez de vous connecter via Telnet, les requêtes au second serveur et au serveur alternatif suivant peuvent expirer et provoquer l'échec de la connexion.
- Si la valeur définie par l'opérande timeout est faible est que vous vous connectez au XSCF, il se peut que le privilège d'utilisateur ne vous soit pas attribué. Dans ce cas, augmentez la valeur de réglage de timeout et réessayez.
- Si vous êtes un utilisateur Active Directory, vous pouvez télécharger une clé publique d'utilisateur sur le XSCF. Les utilisateurs Active Directory peuvent s'identifier en se connectant au XSCF via SSH et en utilisant l'authentification par mot de passe.

Activation/désactivation de l'utilisation d'un serveur Active Directory

1. **Exécutez la commande `showad` pour afficher l'utilisation du serveur Active Directory.**

```
XSCF> showad
dnslocator mode: disabled
expsearch mode: disabled
state: disabled
strictcert mode: disabled
timeout: 4
logdetail: none
```

2. **Exécutez la commande `setad` pour activer/désactiver l'utilisation du serveur Active Directory.**

Dans l'exemple suivant, l'utilisation du serveur Active Directory est activée.

```
XSCF> setad enable
```

Dans l'exemple suivant, l'utilisation du serveur Active Directory est désactivée.

```
XSCF> setad disable
```

3. **Exécutez la commande `showad`, puis vérifiez si Active Directory est activé ou non.**

Dans l'exemple suivant, Active Directory est activé.

```
XSCF> showad
dnslocator mode: disabled
expsearch mode: disabled
state: enabled
strictcert mode: disabled
timeout: 4
logdetail: none
```

Paramétrage des serveurs Active Directory et des numéros de port

1. **Exécutez la commande `showad` pour afficher les paramètres du serveur Active Directory.**

```
XSCF> showad server
Primary Server
  address: (none)
  port: 0
XSCF> showad server -i
Alternate Server 1
  address: (none)
  port: 0
Alternate Server 2
  address: (none)
  port: 0
Alternate Server 3
  address: (none)
  port: 0
Alternate Server 4
  address: (none)
  port: 0
Alternate Server 5
  address: (none)
  port: 0
```

2. **Exécutez la commande setad pour paramétrer les serveurs Active Directory.**
Dans l'exemple suivant, le serveur primaire et le numéro de port sont spécifiés.

```
XSCF> setad server 10.24.159.150:8080
```

Dans l'exemple suivant, des serveurs alternatifs sont spécifiés.

```
XSCF> setad server -i 1 10.24.159.151
```

3. **Exécutez la commande showad, puis vérifiez les paramètres d'Active Directory.**

```
XSCF> showad server
Primary Server
  address: 10.24.159.150
  port: 8080
XSCF> showad server -i
Alternate Server 1
  address: 10.24.159.151
  port: 0
Alternate Server 2
  address: (none)
  port: 0
Alternate Server 3
  address: (none)
  port: 0
Alternate Server 4
  address: (none)
  port: 0
Alternate Server 5
  address: (none)
```

Chargement/Suppression du certificat du serveur

1. **Exécutez la commande `showad` pour afficher les informations de certificat du serveur.**

```
XSCF> showad cert
Primary Server:
certstatus = certificate not present
issuer = (none)
serial number = (none)
subject = (none)
valid from = (none)
valid until = (none)
version = (none)

XSCF> showad cert -i
Alternate Server 1:
certstatus = certificate not present
issuer = (none)
serial number = (none)
subject = (none)
valid from = (none)
valid until = (none)
version = (none)

Alternate Server 2:
... <snip>

Alternate Server 5:
certstatus = certificate not present
issuer = (none)
serial number = (none)
subject = (none)
valid from = (none)
valid until = (none)
version = (none)
```

2. **Exécutez la commande `setad` pour charger le certificat du serveur sur le XSCF.**

Dans l'exemple suivant, le certificat du serveur primaire est chargé en utilisant le nom d'utilisateur et le mot de passe.

```
XSCF> setad loadcert -u yoshi http://domain_2/UID_2333/testcert
Warning: About to load certificate for Primary Server.
Continue? [y|n]: y
Password:
```

Dans l'exemple suivant, le contenu du certificat est copié et collé sur l'écran, puis

le certificat du serveur alternatif 1 est chargé depuis une console. Après avoir appuyé sur la touche [Entrée], appuyez sur les touches [Ctrl] et [D] pour finaliser le chargement.

```
XSCF> setad loadcert console
Warning: About to load certificate for Alternate Server 1:
Continue? [y|n]: y
Please enter the certificate:
-----BEGIN CERTIFICATE-----
MIIEtjCCAzagAwIBAgIBADANBgkqhkiG9w0BAQQFADB8MQswCQYDVQQGEwJVUzET
MBEGA1UECBMKQ2FsaWZvcn5pYTESMBAGA1UEBxMJU2FuIERpZWdvMRkwFwYDVQQK
ExBTdW4gTWljam9zeXN0ZW1zMRUwEwYDVQQLEwxTeXN0ZW0gR3JvdXAxEjAQBgNV
...
-----END CERTIFICATE-----
[Enter]
[Ctrl]+[D]
```

3. **Exécutez la commande showad, puis vérifiez si le certificat du serveur est chargé.**

```
XSCF> showad cert
Primary Server:
certstatus = certificate present
issuer = DC = local, DC = xscf, CN = apl
serial number = 55:1f:ff:c4:73:f7:5a:b9:4e:16:3c:fc:e5:66:5e:5a
subject = DC = local, DC = xscf, CN = apl
valid from = Mar 9 11:46:21 2010 GMT
valid until = Mar 9 11:46:21 2015 GMT
version = 3 (0x02)

XSCF> showad cert -i 1
Alternate Server 1:
certstatus = certificate present
issuer = DC = local, DC = aplle, CN = aplle.local
serial number = 0b:1d:43:39:ee:4b:38:ab:46:47:de:0a:b4:a9:ea:04
subject = DC = local, DC = aplle, CN = aplle.local
valid from = Aug 25 02:38:15 2009 GMT
valid until = Aug 25 02:44:48 2014 GMT
version = 3 (0x02)
```

4. **Exécutez la commande setad pour supprimer le certificat du serveur primaire.**

```
XSCF> setad rmcert
Warning: About to delete certificate for Primary Server.
Continue? [y|n]: y
```

5. **Exécutez la commande showad, puis vérifiez si le certificat du serveur a été supprimé.**

```
XSCF> showad cert
Primary Server:
certstatus = certificate not present
issuer = (none)
serial number = (none)
subject = (none)
valid from = (none)
valid until = (none)
version = (none)
```

Le mode strictcertmode doit être désactivé pour permettre la suppression d'un certificat.

Activation/désactivation du mode d'index DNS

1. **Exécutez la commande showad pour afficher l'état d'activation/désactivation du mode d'index DNS.**

```
XSCF> showad
dnslocatormode: disabled
expsearchmode: disabled
state: enabled
strictcertmode: disabled
timeout: 4
logdetail: none
```

2. **Exécutez la commande setad pour activer/désactiver le mode d'index DNS.**
Dans l'exemple suivant, le mode d'index DNS est activé.

```
XSCF> setad dnslocatormode enable
```

Dans l'exemple suivant, le mode d'index DNS est désactivé.

```
XSCF> setad dnslocatormode disable
```

3. **Exécutez la commande showad, puis vérifiez si le mode d'index DNS est activé/désactivé.**

Dans l'exemple suivant, le mode d'index DNS est activé.

```
XSCF> showad
dnslocatormode: enabled
expsearchmode: disabled
state: enabled
strictcertmode: disabled
timeout: 4
logdetail: none
```

Configuration de la requête d'index DNS

Remarque : avant de paramétrer la requête d'index DNS, activez le mode d'index DNS.

1. **Exécutez la commande `showad` pour afficher la configuration de la requête d'index DNS.**

```
XSCF> showad dnslocatorquery -i 1
service 1: (none)
XSCF> showad dnslocatorquery -i 2
service 2: (none)
```

2. **Exécutez la commande `setad` pour configurer la requête d'index DNS.**

```
XSCF> setad dnslocatorquery -i 1 '_ldap._tcp.gc._msdcs..'
```

3. **Exécutez la commande `showad` et vérifiez la requête d'index DNS.**

```
XSCF> showad dnslocatorquery -i 1
service 1: _ldap._tcp.gc._msdcs..
```

DNS et le mode d'index DNS doivent être activés pour permettre à la requête d'index DNS de fonctionner.

Activation/désactivation du mode de recherche étendue

1. **Exécutez la commande `showad` pour afficher l'état d'activation/désactivation du mode de recherche étendue.**

```
XSCF> showad
dnslocatormode: enabled
expsearchmode: disabled
state: enabled
strictcertmode: disabled
timeout: 4
logdetail: none
```

2. **Exécutez la commande `setad` pour activer/désactiver le mode de recherche étendue.**

Dans l'exemple suivant, le mode de recherche étendue est activé.

```
XSCF> setad expsearchmode enable
```

Dans l'exemple suivant, le mode de recherche étendue est désactivé.

```
XSCF> setad expsearchmode disable
```

3. **Exécutez la commande showad, puis vérifiez si le mode de recherche étendue est activé/désactivé.**

Dans l'exemple suivant, le mode de recherche étendue est activé.

```
XSCF> showad  
dnslocator mode: enabled  
expsearch mode: enabled  
state: enabled  
strictcert mode: disabled  
timeout: 4  
logdetail: none
```

Activation/Désactivation du mode strictcertmode

1. **Exécutez la commande showad pour afficher l'état d'activation/désactivation du mode strictcertmode.**

```
XSCF> showad  
dnslocator mode: enabled  
expsearch mode: enabled  
state: enabled  
strictcert mode: disabled  
timeout: 4  
logdetail: none
```

2. **Exécutez la commande setad pour activer/désactiver le mode strictcertmode.**
Dans l'exemple suivant, le mode strictcertmode est activé.

```
XSCF> setad strictcertmode enable
```

Dans l'exemple suivant, le mode strictcertmode est désactivé.

```
XSCF> setad strictcertmode disable
```

3. **Exécutez la commande showad, puis vérifiez si le mode strictcertmode est activé/désactivé.**

Dans l'exemple suivant, le mode strictcertmode est activé.

```
XSCF> showad  
dnslocator mode: enabled  
expsearch mode: enabled
```

```
state: enabled
strictcertmode: enabled
timeout: 4
logdetail: none
```

Pour activer le mode `strictcertmode`, le certificat du serveur doit avoir auparavant été chargé sur le XSCF.

Réglage d'un domaine d'utilisateur

1. **Exécutez la commande `showad` pour afficher les domaines d'utilisateur.**

```
XSCF> showad userdomain
domain 1: (none)
domain 2: (none)
domain 3: (none)
domain 4: (none)
domain 5: (none)
```

2. **Exécutez la commande `setad` pour paramétrer les domaines d'utilisateur.**
Dans l'exemple suivant, le domaine d'utilisateur 1 est paramétré.

```
XSCF> setad userdomain -i 1 '@davidc.example.aCompany.com'
```

Dans l'exemple suivant, le domaine d'utilisateur 2 est paramétré.

```
XSCF> setad userdomain -i 2 'CN=<USERNAME>,CN=Users,DC=davidc,DC=example,
DC=aCompany,DC=com'
```

3. **Exécutez la commande `showad`, puis vérifiez les domaines d'utilisateur.**

```
XSCF> showad userdomain
domain 1: <USERNAME>@davidc.example.aCompany.com
domain 2: CN=<USERNAME>,CN=Users,DC=davidc,DC=example,
DC=aCompany,
DC=com
domain 3: (none)
domain 4: (none)
domain 5: (none)
```

Si un nom de domaine est directement indiqué sur l'invite de connexion, comme par exemple « login: ima.admin@dc01.example.com », le domaine d'utilisateur est utilisé uniquement pour cette connexion.

Réglage des privilèges par défaut

1. **Exécutez la commande `showad` pour afficher les privilèges par défaut.**

```
XSCF> showad defaultrole
Default role: (none)
```

2. **Exécutez la commande `setad` pour paramétrer un privilège par défaut.**

```
XSCF> setad defaultrole platadm platop
```

3. **Exécutez la commande `showad`, puis vérifiez le privilège par défaut.**

```
XSCF> showad defaultrole
Default role: platadm platop
```

Réglage des noms et des privilèges de groupe

1. **Exécutez la commande `showad` pour afficher les noms de groupe.**

L'exemple suivant montre des groupes d'administrateurs.

```
XSCF> showad group administrator
Administrator Group 1
    name: (none)
Administrator Group 2
    name: (none)
Administrator Group 3
    name: (none)
Administrator Group 4
    name: (none)
Administrator Group 5
    name: (none)
```

L'exemple suivant montre des groupes d'opérateurs.

```
XSCF> showad group operator
Operator Group 1
    name: (none)
Operator Group 2
    name: (none)
Operator Group 3
    name: (none)
Operator Group 4
    name: (none)
Operator Group 5
```

```
name: (none)
```

L'exemple suivant montre des groupes personnalisés.

```
XSCF> showad group custom
Custom Group 1
  name: (none)
  roles: (none)
Custom Group 2
  name: (none)
  roles: (none)
Custom Group 3
  name: (none)
  roles: (none)
Custom Group 4
  name: (none)
  roles: (none)
Custom Group 5
  name: (none)
  roles: (none)
```

2. **Exécutez la commande `setad` pour paramétrer les noms et privilèges de groupe.**
Dans l'exemple suivant, le groupe d'administrateurs 1 est paramétré.

```
XSCF> setad group administrator -i 1 name CN=SpSuperAdmin,OU=Groups,DC=davidc,
DC=example,DC=aCompany,DC=com
```

Dans l'exemple suivant, le groupe d'opérateurs 1 est paramétré.

```
XSCF> setad group operator -i 1 name CN=OpGroup1,OU=SCFTEST,DC=aplle,DC=local
```

Dans l'exemple suivant, le groupe personnalisé 1 est paramétré.

```
XSCF> setad group custom -i 1 name CN=CtmGroup1,OU=SCFTEST,DC=aplle,DC=local
```

Dans l'exemple suivant, le privilège du groupe personnalisé 1 est paramétré.

```
XSCF> setad group custom -i 1 roles platadm,platop
```

3. **Exécutez la commande `showad`, puis vérifiez les noms et privilèges de groupe.**
Dans l'exemple suivant, les groupes d'administrateurs sont vérifiés.

```
XSCF> showad group administrator
Administrator Group 1
  name: CN=<USERNAME>,CN=SpSuperAdmin,OU=Groups,DC=davidc,DC=example,
DC=aCompany,DC=com
Administrator Group 2
```

```
name: (none)
Administrator Group 3
name: (none)
Administrator Group 4
name: (none)
Administrator Group 5
name: (none)
```

Dans l'exemple suivant, les groupes d'opérateurs sont vérifiés.

```
XSCF> showad group operator
Operator Group 1
name: CN=OpGroup1,OU=SCFTEST,DC=aplle,DC=local
Operator Group 2
name: (none)
Operator Group 3
name: (none)
Operator Group 4
name: (none)
Operator Group 5
name: (none)
```

Dans l'exemple suivant, les groupes personnalisés sont vérifiés.

```
XSCF> showad group custom
Custom Group 1
name: CN=CtmGroup1,OU=SCFTEST,DC=aplle,DC=local
roles: platadm platop
Custom Group 2
name: (none)
roles: (none)
Custom Group 3
name: (none)
roles: (none)
Custom Group 4
name: (none)
roles: (none)
Custom Group 5
name: (none)
roles: (none)
```

Le groupe d'administrateurs dispose des privilèges platadm, useradm et auditadm. Ces privilèges ne peuvent pas être modifiés. Le groupe d'opérateurs dispose également des privilèges platop et auditop. Ces privilèges ne peuvent pas être modifiés.

Réglage de l'inactivité

1. **Exécutez la commande showad pour afficher le délai d'expiration.**


```
XSCF> showad
dnslocatormode: enabled
expsearchmode: enabled
state: enabled
strictcertmode: enabled
timeout: 4
logdetail: none
```

2. **Exécutez la commande `setad` pour paramétrer le délai d'expiration.**
Dans l'exemple suivant, le délai d'expiration a été fixé à 10 secondes.

```
XSCF> setad timeout 10
```

3. **Exécutez la commande `showad`, puis vérifiez le délai d'expiration.**

```
XSCF> showad
dnslocatormode: enabled
expsearchmode: enabled
state: enabled
strictcertmode: enabled
timeout: 10
logdetail: none
```

Activation/désactivation des journaux de messages d'authentification et de diagnostic d'autorisation d'Active Directory.

1. **Exécutez la commande `showad` pour afficher le niveau de détail du journal.**

```
XSCF> showad
dnslocatormode: enabled
expsearchmode: enabled
state: enabled
strictcertmode: enabled
timeout: 10
logdetail: none
```

2. **Exécutez la commande `setad` pour définir le niveau de détail du journal.**
Dans l'exemple suivant, le journal est activé et son niveau de détail est réglé sur « trace ».

```
XSCF> setad logdetail trace
```

Dans l'exemple suivant, le journal est désactivé.

```
XSCF> setad logdetail none
```

3. **Exécutez la commande showad, puis vérifiez le niveau de détail du journal.**
Dans l'exemple suivant, le niveau de détail du journal est réglé sur trace.

```
XSCF> showad  
dnslocatormode: enabled  
expsearchmode: enabled  
state: enabled  
strictcertmode: enabled  
timeout: 10  
logdetail: trace
```

Affichage des journaux de messages de diagnostic et suppression des fichiers de journal

1. **Exécutez la commande showad pour afficher le niveau de détail du journal.**

```
XSCF> showad  
dnslocatormode: enabled  
expsearchmode: enabled  
state: enabled  
strictcertmode: enabled  
timeout: 10  
logdetail: trace
```

2. **Exécutez la commande showad pour afficher les messages de diagnostic.**
Dans l'exemple suivant, les messages de diagnostic sont affichés en temps réel.

```
XSCF> showad log -f  
Mon Nov 16 14:47:53 2009 (ActDir): module loaded, OPL  
Mon Nov 16 14:47:53 2009 (ActDir): --error-- authentication  
status:  
auth-ERROR  
Mon Nov 16 14:48:18 2009 (ActDir): module loaded, OPL  
...
```

3. **Exécutez la commande setad pour effacer le fichier de journal des messages de diagnostic.**

```
XSCF> setad log clear  
Warning: About to clear log file.  
Continue? [y|n]: y
```

Réinitialisation des paramètres d'Active Directory à leur valeur par défaut

1. **Exécutez la commande `showad` pour afficher l'état des paramètres d'Active Directory.**

```
XSCF> showad
dnslocatormode: enabled
expsearchmode: enabled
state: enabled
strictcertmode: enabled
timeout: 10
logdetail: trace
```

2. **Exécutez la commande `setad` pour réinitialiser les paramètres d'Active Directory à leur valeur par défaut.**

```
XSCF> setad default -y
Warning: About to reset settings to default.
Continue? [y|n]: y
```

3. **Exécutez la commande `showad`, puis vérifiez que les paramètres d'Active Directory ont été ramenés à leur valeur par défaut.**

```
XSCF> showad
dnslocatormode: disabled
expsearchmode: disabled
state: disabled
strictcertmode: disabled
timeout: 4
logdetail: none
```

Connexion avec un compte d'utilisateur Active Directory

Après finalisation de chaque paramètre, vérifiez si la connexion avec le compte d'utilisateur Active Directory est possible.

3.5.14 Gestion de comptes d'utilisateur XSCF à l'aide de LDAP sur SSL

Dans les paramètres de LDAP sur SSL, les éléments relatifs à un client LDAP sur SSL sont définis. Les réglages couvrent le serveur LDAP sur SSL, le chargement d'un certificat de serveur, le nom de groupe, le privilège d'utilisateur, le domaine

d'utilisateur, le journal, la requête d'index DNS, etc. Les informations d'utilisateur XSCF sont gérées sur le serveur LDAP sur SSL.

Remarque : cette section ne décrit pas la configuration et la gestion du serveur LDAP sur SSL. Un administrateur familier des serveurs LDAP sur SSL devra concevoir le serveur LDAP sur SSL.

Remarque : pour connaître les versions du microprogramme XCP prenant en charge LDAP sur SSL, consultez les dernières *Notes de produit*.

Tableau 3-16 répertorie les termes liés aux paramètres de LDAP sur SSL.

Tableau 3-16 Termes liés à LDAP sur SSL

Terme	Description
LDAP sur SSL	LDAP sur SSL est un service de répertoire distribué comme Active Directory. LDAP sur SSL offre une sécurité accrue aux utilisateurs LDAP grâce à la technologie Secure Socket Layer (SSL) / Transport Layer Security (TLS). Comme le service de répertoire LDAP, LDAP sur SSL est utilisé pour l'authentification de l'utilisateur.

LDAP sur SSL fournit à la fois l'authentification du certificat d'utilisateur et l'autorisation du niveau d'accès de l'utilisateur aux ressources du réseau. LDAP sur SSL utilise l'authentification pour identifier des utilisateurs déterminés avant qu'ils n'accèdent aux ressources système et pour octroyer des privilèges d'accès définis aux utilisateur afin de contrôler leurs droits d'accès aux ressources du réseau.

Les privilèges d'utilisateur sont configurés sur le XSCF ou obtenus depuis un serveur sur un domaine de réseau basé sur l'appartenance au groupe de chacun des utilisateurs. Un utilisateur peut appartenir à plusieurs groupes. Le domaine d'utilisateur est le domaine d'authentification utilisé pour identifier un utilisateur. LDAP sur SSL authentifie les utilisateurs dans l'ordre selon lequel les domaines d'utilisateur sont configurés.

Une fois l'authentification réalisée, les privilèges d'utilisateur peuvent être définis selon les manières suivantes :

- Dans le cas le plus simple, les privilèges d'utilisateur sont définis par les paramètres LDAP sur SSL sur le XSCF. Il existe un paramètre defaultrole pour LDAP sur SSL. Si le paramètre defaultrole est configuré ou défini, tous les utilisateurs authentifiés via LDAP sur SSL se voient attribuer les privilèges d'utilisateur définis dans celui-ci. Les utilisateurs paramétrés sur le serveur LDAP sur SSL n'ont besoin que d'un mot de passe quelle que soit leur appartenance à un groupe.
- Si le paramètre defaultrole n'est pas configuré ou défini, le privilège d'utilisateur est obtenu sur le serveur LDAP sur SSL en se fondant sur l'appartenance de l'utilisateur à un groupe. Sur le XSCF, le paramètre group doit correspondre au nom de groupe d'un serveur LDAP sur SSL. Chaque groupe dispose d'un privilège d'utilisateur configuré sur le XSCF et qui lui est associé. Une fois qu'un utilisateur est authentifié, l'appartenance à un groupe de celui-ci est utilisée pour

déterminer ses privilèges.

Éléments de réglage de LDAP sur SSL et commandes de shell à utiliser

Tableau 3-17 répertorie les éléments de réglage et les commandes de shell correspondantes.

Tableau 3-17 Éléments de réglage de LDAP sur SSL et commandes à utiliser

Élément de réglage	Description de la fonction	Commande de shell	Remarques
Affichage d'état de LDAP sur SSL	Affiche l'état actuel de LDAP sur SSL, comme son état d'activation/désactivation et le mode usemapmode.	showldapssl	
Activation/désactivation de l'utilisation de LDAP sur SSL	Spécifie si l'utilisation de LDAP sur SSL pour la gestion de l'authentification et des privilèges d'utilisateur est activée ou non.	setldapssl	Il est désactivé par défaut.
Affichage du serveur LDAP sur SSL	Affiche la configuration du serveur primaire ou d'un nombre maximal de cinq serveurs alternatifs LDAP sur SSL.	showldapssl	Un numéro de port de « 0 » indique que le port par défaut de LDAP sur SSL est utilisé.
Serveur/port LDAP sur SSL	Spécifie les adresses IP et numéros de port du serveur primaire et de jusqu'à cinq serveurs alternatifs LDAP sur SSL. Spécifie les adresses IP ou les noms d'hôtes pour ces adresses. Pour spécifier des noms d'hôte pour les serveurs LDAP sur SSL, les noms de serveur doivent être compatibles avec le serveur DNS.	setldapssl	Lorsqu'aucun numéro de port n'est spécifié, le port par défaut est utilisé.
Chargement/suppression du certificat du serveur	Charge ou supprime les certificats du serveur primaire et de jusqu'à cinq serveurs alternatifs.	setldapssl	Le mode strictcertmode doit être désactivé pour permettre la suppression d'un certificat.
Activation/désactivation du mode usemapmode	Active/désactive le mode usemapmode. Lorsqu'il est désactivé, les attributs d'utilisateur spécifiés à l'aide de l'opérande usermap, de préférence au domaine d'utilisateur, sont utilisés pour l'authentification de l'utilisateur.	setldapssl	Il est désactivé par défaut.
Affichage de usermap	Affiche le paramètre usermap.	showldapssl	
usermap	Configure le paramètre usermap. Le paramètre usermap est utilisé pour l'authentification de l'utilisateur.	setldapssl	Le mode usemapmode doit être activé pour permettre l'utilisation de usermap.

Tableau 3-17 Éléments de réglage de LDAP sur SSL et commandes à utiliser (*suite*)

Élément de réglage	Description de la fonction	Commande de shell	Remarques
Activation/désactivation du mode strictcertmode	Active/désactive le mode strictcertmode. Si le mode strictcertmode est activé, le certificat d'un serveur doit auparavant avoir été téléchargé sur le serveur de sorte que les signatures puissent avoir été validées lorsque le certificat du serveur est présenté.	setldapssl	Il est désactivé par défaut.
Affichage du certificat du serveur	Affiche les données suivantes : - Informations de certificat pour le serveur primaire et un nombre maximal de cinq serveurs alternatifs. - Intégralité du contenu du certificat	showldapssl	
Affichage du domaine d'utilisateur	Affiche les domaines d'utilisateur.	showldapssl	
Domaine d'utilisateur	Configure jusqu'à cinq domaines d'utilisateur donnés. Le domaine d'utilisateur est spécifié sous la forme de nom unique (DN).	setldapssl	
Affichage de defaultrole	Affiche le paramètre defaultrole.	showldapssl	
defaultrole	Spécifie les privilèges attribués à tous les utilisateurs authentifiés via LDAP sous SSL.	setldapssl	
Affichage des groupes	Affiche la configuration du groupe d'administrateurs, du groupe d'opérateurs et du groupe personnalisé.	showldapssl	
Groupe d'administrateurs	Attribue des noms de groupe à un nombre maximal de cinq groupes d'administrateurs. Le groupe d'administrateurs dispose des privilèges platadm, useradm et auditadm. Ces privilèges ne peuvent pas être modifiés.	setldapssl	
Groupe d'opérateurs	Attribue des noms de groupe à un nombre maximal de cinq groupes d'opérateurs. Le groupe d'opérateurs dispose des privilèges platop et auditop. Ces privilèges ne peuvent pas être modifiés.	setldapssl	
Groupe personnalisé	Attribue des noms de groupe et des privilèges d'utilisateur à un nombre maximal de cinq groupes.	setldapssl	

Tableau 3-17 Éléments de réglage de LDAP sur SSL et commandes à utiliser (*suite*)

Élément de réglage	Description de la fonction	Commande de shell	Remarques
Expiration	Définit le délai d'expiration de la transaction en secondes. Vous pouvez spécifier une valeur numérique comprise entre 1 et 20.	setldapssl	La valeur par défaut est de 4 secondes. Si un délai d'expiration spécifié est trop bref pour la configuration, le processus d'identification ou la récupération du paramètre de privilège d'utilisateur peut échouer.
Activation/désactivation du journal	Active/désactive les journaux de messages d'authentification et de diagnostic d'autorisation de LDAP sur SSL.	setldapssl	Ce journal est effacé lorsque le XSCF est redémarré.
Affichage de journal	Affiche les messages d'authentification et de diagnostic d'autorisation de LDAP sur SSL.	showldapssl	
Suppression de journal	Supprime les journaux de messages d'authentification et de diagnostic d'autorisation de LDAP sur SSL.	setldapssl	
Valeur par défaut	Fait revenir les paramètres de LDAP sur SSL à leur valeur par défaut à la sortie d'usine.	setldapssl	

Avant de configurer les réglages de LDAP sur SSL

Prenez note des points suivants avant de configurer les paramètres de LDAP sur SSL.

- Vérifiez qu'une version de XCP prenant en charge LDAP sur SSL est utilisée. Pour connaître les versions de XCP prenant en charge LDAP sur SSL, consultez les dernières *Notes de produit*.
- Le privilège d'utilisateur useradm est nécessaire pour les paramètres de LDAP sur SSL.
- Si le XSCF est configuré pour utiliser LDAP, Active Directory ou LDAP sur SSL pour des données de compte d'utilisateur, son nom et, si cela est spécifié, l'identifiant d'utilisateur (UID) ne doivent pas être déjà utilisés sur le XSCF, LDAP, Active Directory ou LDAP sur SSL.
- Afin d'utiliser un nom d'hôte pour un serveur LDAP sur SSL, les paramètres DNS doivent être configurés de manière adaptée avant de paramétrer LDAP sur SSL.
- Sur LDAP sur SSL, le compte système appelé proxyuser est utilisé. Vérifiez qu'aucun compte d'utilisateur portant ce nom n'existe. S'il existe un compte d'utilisateur portant le nom de proxyuser, supprimez ce compte à l'aide de la commande deleteuser. Une fois ce compte supprimé, redémarrez le XSCF avant d'utiliser LDAP sur SSL.
- Si la valeur définie par l'opérande timeout est faible est que vous vous connectez

au XSCF, il se peut que le privilège d'utilisateur ne vous soit pas attribué. Dans ce cas, augmentez la valeur de réglage de timeout et réessayez.

- Les utilisateurs de LDAP sur SSL ne peuvent pas télécharger une clé publique d'utilisateur sur le XSCF. Les utilisateurs de LDAP sur SSL peuvent s'identifier en se connectant au XSCF via SSH et en utilisant l'authentification par mot de passe.

Activation/Désactivation de l'utilisation du serveur LDAP sur SSL

1. **Exécutez la commande `showldapssl` pour afficher l'utilisation du serveur LDAP sur SSL.**

```
XSCF> showldapssl
usermapmode: disabled
state: disabled
strictcertmode: disabled
timeout: 4
logdetail: none
```

2. **Exécutez la commande `setldapssl` pour activer/désactiver l'utilisation du serveur LDAP sur SSL.**

Dans l'exemple suivant, l'utilisation du serveur LDAP sur SSL est activée.

```
XSCF> setldapssl enable
```

Dans l'exemple suivant, l'utilisation du serveur LDAP sur SSL est désactivée.

```
XSCF> setldapssl disable
```

3. **Exécutez la commande `showldapssl`, puis vérifiez si LDAP sur SSL est activé ou non.**

Dans l'exemple suivant, LDAP sur SSL est activé.

```
XSCF> showldapssl
usermapmode: disabled
state: enabled
strictcertmode: disabled
timeout: 4
logdetail: none
```

Réglage des serveurs et des numéros de port de LDAP sur SSL

1. **Exécutez la commande `showldapssl` pour afficher les paramètres du serveur**

LDAP sur SSL.

```
XSCF> showldapssl server
Primary Server
  address: (none)
  port: 0
XSCF> showldapssl server -i
Alternate Server 1
  address: (none)
  port: 0
Alternate Server 2
  address: (none)
  port: 0
Alternate Server 3
  address: (none)
  port: 0
Alternate Server 4
  address: (none)
  port: 0
Alternate Server 5
  address: (none)
  port: 0
```

2. Exécutez la commande `setldapssl` pour paramétrer les serveurs LDAP sur SSL.

Dans l'exemple suivant, le serveur primaire et le numéro de port sont spécifiés.

```
XSCF> setldapssl server 10.18.76.230:4041
```

Dans l'exemple suivant, des serveurs alternatifs sont spécifiés.

```
XSCF> setldapssl server -i 1 10.18.76.231
```

3. Exécutez la commande `showldapssl`, puis vérifiez les paramètres du serveur LDAP sur SSL.

```
XSCF> showldapssl server
Primary Server
  address: 10.18.76.230
  port: 4041

XSCF> showldapssl server -i
Alternate Server 1
  address: 10.18.76.231
  port: 0
Alternate Server 2
  address: (none)
  port: 0
Alternate Server 3
  address: (none)
```

```
port: 0
Alternate Server 4
address: (none)
port: 0
Alternate Server 5
address: (none)
port: 0
```

Chargement/Suppression du certificat du serveur

1. **Exécutez la commande `showldapssl` pour afficher les informations de certificat du serveur.**

```
XSCF> showldapssl cert
Primary Server:
certstatus = certificate not present
issuer = (none)
serial number = (none)
subject = (none)
valid from = (none)
valid until = (none)
version = (none)

XSCF> showldapssl cert -i
Alternate Server 1:
certstatus = certificate not present
issuer = (none)
serial number = (none)
subject = (none)
valid from = (none)
valid until = (none)
version = (none)

Alternate Server 2:
... <snip>

Alternate Server 5:
certstatus = certificate not present
issuer = (none)
serial number = (none)
subject = (none)
valid from = (none)
valid until = (none)
version = (none)
```

2. **Exécutez la commande `setldapssl` pour charger le certificat du serveur sur le XSCF.**

Dans l'exemple suivant, le certificat du serveur primaire est chargé en utilisant le nom d'utilisateur et le mot de passe.

```
XSCF> setldapssl loadcert -u yoshi http://domain_3/UID_2333/testcert
Warning: About to load certificate for Primary Server.
Continue? [y|n]: y
Password:
```

Dans l'exemple suivant, le contenu du certificat est copié et collé sur l'écran, puis le certificat du serveur alternatif 1 est chargé depuis une console. Après avoir appuyé sur la touche [Entrée], appuyez sur les touches [Ctrl] et [D] pour finaliser le chargement.

```
XSCF> setldapssl loadcert console
Warning: About to load certificate for Alternate Server 1:
Continue? [y|n]: y
Please enter the certificate:
-----BEGIN CERTIFICATE-----
MIIEtjCCAzagAwIBAgIBADANBgkqhkiG9w0BAQQFADB8MQswCQYDVQQGEwJVUzET
MBEGA1UECBMKQ2FsaWZvcml5pYTESMBAg1UEBxMJU2FuIERpZWdvMRkwFwYDVQQK
ExBTdW4gTWljbmc9zeXN0ZWlzMRUwEwYDVQQLEwxTeXN0ZW0gR3JvdXAx EjAQBgNV
...
-----END CERTIFICATE-----
[Enter]
[Ctrl]+[D]
```

3. **Exécutez la commande showldapssl, puis vérifiez si le certificat du serveur est chargé.**

```
XSCF> showldapssl cert
Primary Server:
certstatus = certificate present
issuer = DC = local, DC = xscf, CN = apl
serial number = 55:1f:ff:c4:73:f7:5a:b9:4e:16:3c:fc:e5:66:5e:5a
subject = DC = local, DC = xscf, CN = apl
valid from = Mar 9 11:46:21 2010 GMT
valid until = Mar 9 11:46:21 2015 GMT
version = 3 (0x02)

XSCF> showldapssl cert -i 1
Alternate Server 1:
certstatus = certificate present
issuer = DC = local, DC = ap1le, CN = ap1le.local
serial number = 0b:1d:43:39:ee:4b:38:ab:46:47:de:0a:b4:a9:ea:04
subject = DC = local, DC = ap1le, CN = ap1le.local
valid from = Aug 25 02:38:15 2009 GMT
valid until = Aug 25 02:44:48 2014 GMT
version = 3 (0x02)
```

4. **Exécutez la commande setldapssl pour supprimer le certificat du serveur primaire.**

```
XSCF> setldapssl rmcert  
Warning: About to delete certificate for Primary Server.  
Continue? [y|n]: y
```

5. **Exécutez la commande showldapssl, puis vérifiez si le certificat du serveur a été supprimé.**

```
XSCF> showldapssl cert  
Primary Server:  
certstatus = certificate not present  
issuer = (none)  
serial number = (none)  
subject = (none)  
valid from = (none)  
valid until = (none)  
version = (none)
```

Le mode strictcertmode doit être désactivé pour permettre la suppression d'un certificat.

Activation/Désactivation du mode usermapmode

1. **Exécutez la commande showldapssl pour afficher l'état d'activation/désactivation du mode usermapmode.**

```
XSCF> showldapssl  
usermapmode: disabled  
state: enabled  
strictcertmode: disabled  
timeout: 4  
logdetail: none
```

2. **Exécutez la commande setldapssl pour activer/désactiver le mode usermapmode.**

Dans l'exemple suivant, le mode usermapmode est activé.

```
XSCF> setldapssl usermapmode enable
```

Dans l'exemple suivant, le mode usermapmode est désactivé.

```
XSCF> setldapssl usermapmode disable
```

3. **Exécutez la commande showldapssl pour vérifier l'état d'activation/désactivation du mode usermapmode.**

Dans l'exemple suivant, le mode usermapmode est activé.

```
XSCF> showldapssl
usermapmode: enabled
state: enabled
strictcertmode: disabled
timeout: 4
logdetail: none
```

Réglage ou suppression de usermap

1. **Exécutez la commande showldapssl pour afficher la configuration de usermap.**

```
XSCF> showldapssl usermap
attributeInfo: (none)
binddn: (none)
bindpw: (none)
searchbase: (none)
```

2. **Exécutez la commande setldapssl pour configurer le paramètre usermap.**
Dans l'exemple suivant, les informations d'attribut sont paramétrées.

```
XSCF> setldapssl usermap attributeInfo '(&(objectclass=person)(uid=))'
```

Dans l'exemple suivant, le DN lié est paramétré.

```
XSCF> setldapssl usermap binddn CN=SuperAdmin,DC=aCompany,DC=com
```

Dans l'exemple suivant, le mot de passe lié est paramétré.

```
XSCF> setldapssl usermap bindpw b.e9s#n
```

Dans l'exemple suivant, la base de recherche est paramétrée.

```
XSCF> setldapssl usermap searchbase OU=yoshi,DC=aCompany,DC=com
```

3. **Exécutez la commande showldapssl, puis vérifiez le paramètre usermap.**

```
XSCF> showldapssl usermap
attributeInfo: (&(objectclass=person)(uid=))
binddn: CN=SuperAdmin,DC=aCompany,DC=com
bindpw: Set
searchbase: OU=yoshi,DC=aCompany,DC=com
```

4. **Exécutez la commande setldapssl pour supprimer le paramètre usermap.**
Dans l'exemple suivant, les informations d'attribut sont supprimées.

```
XSCF> setldapssl usermap attributeInfo
```

Dans l'exemple suivant, le DN lié est supprimé.

```
XSCF> setldapssl usermap binddn
```

Dans l'exemple suivant, le mot de passe lié est supprimé.

```
XSCF> setldapssl usermap bindpw
```

Dans l'exemple suivant, la base de recherche est supprimée.

```
XSCF> setldapssl usermap searchbase
```

5. **Exécutez la commande showldapssl, puis vérifiez si le paramètre usermap est supprimé.**

```
XSCF> showldapssl usermap
attributeInfo: (none)
binddn: (none)
bindpw: (none)
searchbase: (none)
```

Le mode usermapmode doit être activé pour permettre l'utilisation de usermap.

Activation/Désactivation du mode strictcertmode

1. **Exécutez la commande showldapssl pour afficher l'état d'activation/désactivation du mode strictcertmode.**

```
XSCF> showldapssl
usermapmode: enabled
state: enabled
strictcertmode: disabled
timeout: 4
logdetail: none
```

2. **Exécutez la commande setldapssl pour activer/désactiver le mode strictcertmode.**

Dans l'exemple suivant, le mode strictcertmode est activé.

```
XSCF> setldapssl strictcertmode enable
```

Dans l'exemple suivant, le mode strictcertmode est désactivé.

```
XSCF> setsetldapssl strictcertmode disable
```

3. **Exécutez la commande `showldapssl`, puis vérifiez si le mode `strictcertmode` est activé/désactivé.**

Dans l'exemple suivant, le mode `strictcertmode` est activé.

```
XSCF> showldapssl  
usermapmode: enabled  
state: enabled  
strictcertmode: enabled  
timeout: 4  
logdetail: none
```

Pour activer le mode `strictcertmode`, le certificat du serveur doit avoir auparavant été chargé sur le XSCF.

Réglage d'un domaine d'utilisateur

1. **Exécutez la commande `showldapssl` pour afficher les domaines d'utilisateur.**

```
XSCF> showldapssl userdomain  
domain 1: (none)  
domain 2: (none)  
domain 3: (none)  
domain 4: (none)  
domain 5: (none)
```

2. **Exécutez la commande `setldapssl` pour paramétrer les domaines d'utilisateur.**
Dans l'exemple suivant, le domaine d'utilisateur 1 est paramétré.

```
XSCF> setldapssl userdomain -i 1 '@davidc.example.aCompany.com'
```

Dans l'exemple suivant, le domaine d'utilisateur 2 est paramétré.

```
XSCF> setldapssl userdomain -i 2 'CN=<USERNAME>,CN=Users,DC=davidc,DC=example,DC=aCompany,DC=com'
```

3. **Exécutez la commande `showldapssl`, puis vérifiez les domaines d'utilisateur.**

```
XSCF> showldapssl userdomain  
domain 1: <USERNAME>@davidc.example.aCompany.com  
domain 2: CN=<USERNAME>,CN=Users,DC=davidc,DC=example,  
DC=aCompany,  
DC=com  
domain 3: (none)
```

```
domain 4: (none)
domain 5: (none)
```

Réglage des privilèges par défaut

1. **Exécutez la commande `showldapssl` pour afficher les privilèges par défaut.**

```
XSCF> showldapssl defaultrole
Default role: (none)
```

2. **Exécutez la commande `setldapssl` pour paramétrer un privilège par défaut.**

```
XSCF> setldapssl defaultrole platadm platop
```

3. **Exécutez la commande `showldapssl`, puis vérifiez le privilège par défaut.**

```
XSCF> showldapssl defaultrole
Default role: platadm platop
```

Réglage des noms et des privilèges de groupe

1. **Exécutez la commande `showldapssl` pour afficher les noms de groupe.**
L'exemple suivant montre des groupes d'administrateurs.

```
XSCF> showldapssl group administrator
Administrator Group 1
    name: (none)
Administrator Group 2
    name: (none)
Administrator Group 3
    name: (none)
Administrator Group 4
    name: (none)
Administrator Group 5
    name: (none)
```

L'exemple suivant montre des groupes d'opérateurs.

```
XSCF> showldapssl group operator
Operator Group 1
    name: (none)
Operator Group 2
    name: (none)
Operator Group 3
```



```
name: (none)
Operator Group 4
name: (none)
Operator Group 5
name: (none)
```

L'exemple suivant montre des groupes personnalisés.

```
XSCF> showldapssl group custom
Custom Group 1
name: (none)
roles: (none)
Custom Group 2
name: (none)
roles: (none)
Custom Group 3
name: (none)
roles: (none)
Custom Group 4
name: (none)
roles: (none)
Custom Group 5
name: (none)
roles: (none)
```

2. **Exécutez la commande `setldapssl` pour paramétrer les noms et privilèges de groupe.**

Dans l'exemple suivant, le groupe d'administrateurs 1 est paramétré.

```
XSCF> setldapssl group administrator -i 1 name CN=SpSuperAdmin,OU=Groups,
DC=davidc,DC=example,DC=aCompany,DC=com
```

Dans l'exemple suivant, le groupe d'opérateurs 1 est paramétré.

```
XSCF> setldapssl group operator -i 1 name CN=OpGroup1,OU=SCFTEST,DC=aplle,DC=local
```

Dans l'exemple suivant, le groupe personnalisé 1 est paramétré.

```
XSCF> setldapssl group custom -i 1 name CN=CtmGroup1,OU=SCFTEST,DC=aplle,DC=local
```

Dans l'exemple suivant, le privilège du groupe personnalisé 1 est paramétré.

```
XSCF> setldapssl group custom -i 1 roles platadm,platop
```

3. **Exécutez la commande `showldapssl`, puis vérifiez les noms et privilèges de groupe.**

Dans l'exemple suivant, les groupes d'administrateurs sont vérifiés.

```
XSCF> showldapssl group administrator
Administrator Group 1
    name: CN=<USERNAME>,CN=SpSuperAdmin,OU=Groups,DC=davidc,
DC=example,DC=aCompany,DC=com
Administrator Group 2
    name: (none)
Administrator Group 3
    name: (none)
Administrator Group 4
    name: (none)
Administrator Group 5
    name: (none)
```

Dans l'exemple suivant, les groupes d'opérateurs sont vérifiés.

```
XSCF> showldapssl group operator
Operator Group 1
    name: CN=OpGroup1,OU=SCFTEST,DC=aplle,DC=local
Operator Group 2
    name: (none)
Operator Group 3
    name: (none)
Operator Group 4
    name: (none)
Operator Group 5
    name: (none)
```

Dans l'exemple suivant, les groupes personnalisés sont vérifiés.

```
XSCF> showldapssl group custom
Custom Group 1
    name: CN=CtmGroup1,OU=SCFTEST,DC=aplle,DC=local
    roles: platadm platop
Custom Group 2
    name: (none)
    roles: (none)
Custom Group 3
    name: (none)
    roles: (none)
Custom Group 4
    name: (none)
    roles: (none)
Custom Group 5
    name: (none)
    roles: (none)
```

Le groupe d'administrateurs dispose des privilèges platadm, useradm et auditadm. Ces privilèges ne peuvent pas être modifiés. Le groupe d'opérateurs dispose également des privilèges platop et auditop. Ces privilèges ne peuvent pas être modifiés.

Réglage de l'inactivité

1. **Exécutez la commande `showldapssl` pour afficher le délai d'expiration.**

```
XSCF> showldapssl
dnslocator mode: enabled
expsearch mode: enabled
state: enabled
strictcert mode: enabled
timeout: 4
logdetail: none
```

2. **Exécutez la commande `setldapssl` pour définir le délai d'expiration.**
Dans l'exemple suivant, le délai d'expiration est fixé à 10 secondes.

```
XSCF> setldapssl timeout 10
```

3. **Exécutez la commande `showldapssl`, puis vérifiez le délai d'expiration.**

```
XSCF> showldapssl
dnslocator mode: enabled
expsearch mode: enabled
state: enabled
strictcert mode: enabled
timeout: 10
logdetail: none
```

Activation/Désactivation des journaux de messages d'authentification et de diagnostic d'autorisation de LDAP sur SSL

1. **Exécutez la commande `showldapssl` pour afficher le niveau de détail du journal.**

```
XSCF> showldapssl
dnslocator mode: enabled
expsearch mode: enabled
state: enabled
strictcert mode: enabled
timeout: 10
logdetail: none
```

2. **Exécutez la commande `setldapssl` pour définir le niveau de détail du journal.**
Dans l'exemple suivant, le journal est activé et son niveau de détail est réglé sur « trace ».

```
XSCF> setldapssl logdetail trace
```

Dans l'exemple suivant, le journal est désactivé.

```
XSCF> setldapssl logdetail none
```

3. **Exécutez la commande `showldapssl`, puis vérifiez le niveau de détail du journal.**
Dans l'exemple suivant, le niveau de détail du journal est réglé sur trace.

```
XSCF> showldapssl  
dnslocator mode: enabled  
expsearch mode: enabled  
state: enabled  
strictcert mode: enabled  
timeout: 10  
logdetail: trace
```

Affichage des journaux de messages de diagnostic et suppression des fichiers de journal

1. **Exécutez la commande `showldapssl` pour afficher le niveau de détail du journal.**

```
XSCF> showldapssl  
dnslocator mode: enabled  
expsearch mode: enabled  
state: enabled  
strictcert mode: enabled  
timeout: 10  
logdetail: trace
```

2. **Exécutez la commande `showldapssl` pour afficher les messages de diagnostic.**
Dans l'exemple suivant, les messages de diagnostic sont affichés en temps réel.

```
XSCF> showldapssl log -f  
Mon Nov 16 14:47:53 2009 (LdapSSL): module loaded, OPL  
Mon Nov 16 14:47:53 2009 (LdapSSL): --error-- authentication status:  
auth-ERROR  
Mon Nov 16 14:48:18 2009 (LdapSSL): module loaded, OPL  
...
```

3. **Exécutez la commande `setldapssl` pour effacer le fichier de journal des messages de diagnostic.**

```
XSCF> setldapssl log clear
Warning: About to clear log file.
Continue? [y|n]: y
```

Réinitialisation des réglages de LDAP sur SSL à leur valeur par défaut

1. **Exécutez la commande `showldapssl` pour afficher l'état des paramètres de LDAP sur SSL.**

```
XSCF> showldapssl
dnslocator mode: enabled
expsearch mode: enabled
state: enabled
strictcert mode: enabled
timeout: 10
logdetail: trace
```

2. **Exécutez la commande `setldapssl` pour réinitialiser les paramètres de LDAP sur SSL à leur valeur par défaut.**

```
XSCF> setldapssl default -y
Warning: About to reset settings to default.
Continue? [y|n]: y
```

3. **Exécutez la commande `showldapssl`, puis vérifiez que les paramètres de LDAP sur SSL ont été ramenés à leur valeur par défaut.**

```
XSCF> showldapssl
dnslocator mode: disabled
expsearch mode: disabled
state: disabled
strictcert mode: disabled
timeout: 4
logdetail: none
```

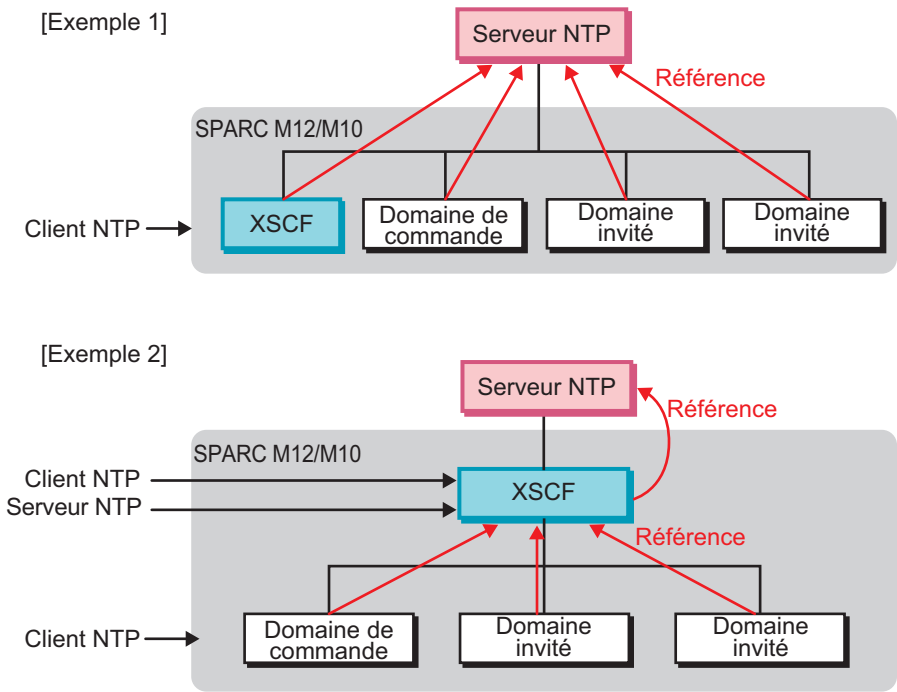
Connexion avec un compte d'utilisateur LDAP sur SSL

Après finalisation de chaque paramètre, vérifiez si la connexion avec le compte d'utilisateur LDAP sur SSL est possible.

3.6 Réglage de l'heure/date du XSCF

Cette section décrit comment régler l'heure de ce système. Le système utilise l'horloge du XSCF comme temps de référence pour toutes les partitions physiques. Le XSCF peut être configuré de manière à fonctionner à la fois comme serveur et client NTP. Si le XSCF n'est pas configuré en tant que client NTP, l'horloge interne Realtime Clock (RTC) de chaque châssis du SPARC M12/M10 est utilisée pour l'heure du XSCF. Dans ce cas, pour modifier l'heure du XSCF, utilisez la commande `setdate`. [Figure 3-1](#) présente quelques exemples de schémas de fonctionnement liés à l'heure dans ce système. Dans l'exemple 1, le XSCF et le domaine logique sont exécutés en tant que clients NTP. Dans l'exemple 2, le XSCF fonctionne à la fois comme client et serveur NTP.

Figure 3-1 Exemples de schémas de fonctionnement liés à l'heure



Remarque : il est demandé au client de définir le schéma de fonctionnement du serveur NTP. Pour plus de détails sur NTP, consultez les manuels relatifs à NTP.

3.6.1

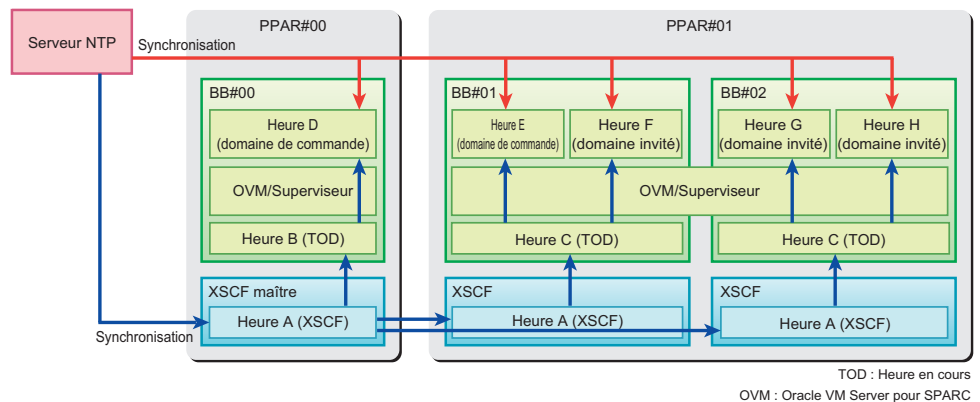
Compréhension de la relation entre l'heure du XSCF et l'heure des partitions physiques

Le XSCF conserve le décalage temporel entre XSCF et la partition physique. Cela évite que le décalage entre les domaines logiques et le XSCF ne change même lors de la réinitialisation d'une partition physique. Même si l'heure du XSCF est modifiée en utilisant la commande `setdate` du microprogramme XSCF, le décalage temporel entre celui-ci et la partition physique est conservé.

L'heure XSCF et l'heure de la partition physique sont gérées de la manière suivante.

- Lorsque la partition physique est sous tension, les données de décalage temporel entre le XSCF et la partition physique sont ajoutées à l'heure XSCF, et cette valeur est définie comme heure matérielle de la partition physique (TOD).
- Lors du démarrage d'Oracle Solaris, l'heure du domaine logique est définie à partir de l'heure matérielle de la partition physique (TOD).

Figure 3-2 Réglage de l'heure pour le XSCF et le domaine logique



Remarque : n'utilisez pas la commande `resetdateoffset` sauf lors de la configuration initiale d'une partition physique, car elle affecte le contrôle temporel mentionné ci-dessus. La commande `resetdateoffset` est uniquement utilisée lors de la configuration initiale d'une partition physique.
Pour plus d'informations sur l'utilisation de la commande `resetdateoffset` lors de la configuration initiale d'une partition physique, consultez le *Guide d'installation* de votre serveur.

3.6.2

Stratégie de gestion du temps d'un domaine logique

Vous pouvez définir des stratégies individuelles de gestion du temps pour les domaines logiques. En conséquence, le temps peut être géré de manière différente

selon le domaine logique. Les stratégies de gestion du temps des domaines sont décrites ci-dessous.

- Lors du démarrage d'un domaine logique, l'heure est définie à partir de l'heure XSCF.
- Un domaine logique peut être configuré en tant que client NTP d'un serveur NTP externe. Dans ce cas, après la définition initiale de l'heure du domaine logique à partir de l'heure XSCF, celle-ci est synchronisée avec le serveur NTP.
- Un domaine logique peut être configuré en tant que client NTP du XSCF fonctionnant comme serveur NTP. Dans ce cas, au démarrage du domaine logique l'heure est synchronisée avec l'heure XSCF.
- Si, dans un domaine logique, l'heure est définie par la commande date d'Oracle Solaris, le décalage temporel entre le domaine logique et la partition physique est conservé après redémarrage.

Remarque : pour synchroniser l'heure à l'aide de NTP, spécifiez le même serveur NTP pour tous les domaines logiques situés dans une même partition physique. Pour plus de détails sur la façon de définir le serveur NTP d'un domaine, consultez *Oracle Solaris Administration: Network Services* (Oracle Solaris 10) ou *Introduction to Oracle Solaris 11 Network Services* (Oracle Solaris 11).

3.6.3 Vérification des éléments de réglage et commandes liés à l'heure

Tableau 3-18 répertorie les éléments de réglage liés à l'heure et les commandes de shell XSCF correspondantes.

Tableau 3-18 Éléments de réglage liés à l'heure		
Élément de réglage	Paramétrage requis ou optionnel	Commande liée
Fuseau horaire	Optionnel	settimezone(8), showtimezone(8)
Heure d'été	Optionnel	settimezone(8), showtimezone(8)
Heure du système	Requis	setdate(8), showdate(8)
Serveur NTP	Optionnel	setad(8), showad(8)
Tourniquet DNS	Optionnel	setad(8), showad(8)
Favori, couche	Optionnel	setad(8), showad(8)
Horloge locale	Optionnel	setad(8), showad(8)

3.6.4 Réglage du fuseau horaire

Pour vérifier quel fuseau horaire a été défini, exécutez la commande showtimezone

en spécifiant l'option `-c tz`. Pour définir le fuseau horaire, utilisez la commande `settimezone`. En spécifiant l'option `-a` avec la commande `settimezone`, vous pouvez répertorier les fuseaux horaires pouvant être définis. Exécutez la commande `settimezone` avec un compte d'utilisateur disposant du privilège `platadm` ou `fieldeng`.

Les fuseaux horaires prédéfinis comme standard se conforment à la norme POSIX. La liste des fuseaux peut être modifiée chaque année.

1. **Exécutez la commande `showtimezone` pour afficher le fuseau horaire.**

```
XSCF> showtimezone -c tz
America/Chicago
```

2. **Exécutez la commande `settimezone` pour définir le fuseau horaire du XSCF.**
Dans l'exemple suivant, les options `-c settz` et `-a` ont été spécifiées pour afficher une liste des fuseaux horaires.

```
XSCF> settimezone -c settz -a
Africa/Abidjan
Africa/Accra
:
Asia/Thimphu
Asia/Tokyo
Asia/Ujung_Pandang
:
Europe/Lisbon
Europe/Ljubljana
Europe/London
:
```

Dans l'exemple suivant, l'heure de Asia/Tokyo est définie comme fuseau horaire.

```
XSCF> settimezone -c settz -s Asia/Tokyo
Asia/Tokyo
```

3. **Exécutez la commande `showtimezone`, puis vérifiez le paramètre.**

Remarque : le fuseau horaire (nom de région/géographique) reconnu par XSCF peut être modifié pour prendre en compte les informations de fuseau horaire les plus récentes. Si le fuseau horaire précédemment défini devient indisponible sur le système, XSCF basculera vers le temps universel coordonné (UTC).

Si le fuseau horaire défini est modifié pour fonctionner avec UTC, exécutez la commande `settimezone -c settz -a` pour vérifier quel fuseau horaire peut être spécifié. Si la liste de fuseaux horaires n'inclut pas celui que vous aviez défini précédemment, réinitialisez le fuseau horaire.

3.6.5 Réglage de l'heure d'été

Pour vérifier ou paramétrer les informations relatives à l'heure d'été, utilisez les commandes `showtimezone` et `settimezone`.

1. **Exécutez la commande `showtimezone` pour afficher le fuseau horaire.**

Dans l'exemple suivant, le fuseau horaire est affiché.

```
XSCF> showtimezone -c tz
Asia/Tokyo
```

Dans l'exemple suivant, les informations relatives à l'heure d'été paramétrées sont affichées. Dans cet exemple, le fuseau horaire défini est l'heure du Japon (JST), le décalage horaire avec UTC de +9 heures, l'heure d'été est en avance d'1 heure par rapport à l'heure du Japon (JDT) sur une période s'étalant du dernier dimanche de mars à 2:00 (JST) au dernier dimanche d'octobre à 2:00 (JDT).

```
XSCF> showtimezone -c dst -m custom
JST-9JDT,M3.5.0,M10.5.0
```

2. **Exécutez la commande `settimezone` pour paramétrer les informations relatives à l'heure d'été sur le XSCF.**

Dans l'exemple suivant, les informations relatives à l'heure d'été sont paramétrées : l'abréviation du fuseau horaire est JST (heure du Japon), dont le décalage horaire avec UTC est de +9 heures, l'heure d'été est fixée sur JDT (heure d'été du Japon) avec un décalage horaire par rapport à UTC de +10 heures sur une période s'étalant du premier dimanche d'avril à 0:00 (JST) au premier dimanche de septembre à 0:00 (JDT).

```
XSCF> settimezone -c adddst -b JST -o GMT-9 -d JDT -p GMT-10 -f
M4.1.0/00:00:00 -t M9.1.0/00:00:00
JST-9JDT-10,M4.1.0/00:00:00,M9.1.0/00:00:00
```

Dans l'exemple suivant, les informations relatives à l'heure d'été paramétrées sont supprimées.

```
XSCF> settimezone -c deldst -b JST -o GMT-9
```

Pour appliquer les informations relatives à l'heure d'été modifiées par l'option `-c adddst` ou `-c deldst`, déconnectez-vous puis connectez-vous de nouveau.

3. **Exécutez la commande `showtimezone`, puis vérifiez le paramètre.**

3.6.6 Réglage de l'heure du système

Définissez l'heure locale ou utilisez le temps universel coordonné (UTC) pour l'horloge, la date et l'heure du XSCF. Une fois l'heure réglée, le XSCF est redémarré. Pour vérifier la date et l'heure de l'horloge du XSCF, utilisez la commande `showdate`. Utilisez la commande `setdate` pour régler la date et l'heure de l'horloge du XSCF. Exécutez la commande `setdate` avec un compte d'utilisateur disposant du privilège `platadm` ou `fieldeng`.

Remarque : l'heure du système est paramétrée au cours de l'installation initiale.

1. **Exécutez la commande `showdate` pour afficher l'heure du XSCF.**

L'exemple suivant montre l'heure actuelle fixée sur l'heure locale.

```
XSCF> showdate
Mon Jan 23 14:53:00 JST 2012
```

Dans l'exemple suivant, l'option `-u` est spécifiée pour afficher l'heure locale conformément à UTC.

```
XSCF> showdate -u
Mon Jan 23 05:56:15 UTC 2012
```

2. **Exécutez la commande `setdate` pour régler l'heure.**

Dans l'exemple suivant, l'heure actuelle est fixée sur l'heure locale, 16:59:00, 27 janvier 2012.

```
XSCF> setdate -s 012716592012.00
Fri Jan 27 16:59:00 JST 2012
The XSCF will be reset. Continue? [y|n]:y
Fri Jan 27 07:59:00 UTC 2012
```

Dans l'exemple suivant, l'heure actuelle est fixée sur UTC, 07:59:00, 27 janvier 2012.

```
XSCF> setdate -u -s 012707592012.00
Fri Jan 27 07:59:00 UTC 2012
The XSCF will be reset. Continue? [y|n]:y
Fri Jan 27 07:59:00 UTC 2012
```

Le XSCF est redémarré une fois que l'heure est réglée. La session XSCF est interrompue à ce moment-là. Reconnectez-vous au XSCF, puis identifiez-vous de nouveau.

Remarque : si l'alimentation en entrée a été désactivée et qu'une tâche de maintenance a été

effectuée, assurez-vous de bien vérifier l'heure du XSCF à l'aide de la commande `showdate` une fois l'alimentation réactivée. Si elle ne correspond pas à l'heure actuelle, réglez-la sur cette dernière à l'aide de la commande `setdate`.

3.6.7 Synchronisation des heures du domaine de commande et du XSCF

Cette section présente deux méthodes de synchronisation des heures du domaine de commande et du XSCF une fois que l'heure du domaine de commande a été définie par la commande `date` d'Oracle Solaris :

- Définition du XSCF comme serveur NTP du domaine de commande
- Définition du même serveur NTP pour le domaine de commande et XSCF

Réglage du XSCF comme serveur NTP du domaine de commande

1. **Définissez le XSCF comme serveur NTP.**
Pour plus de détails, consultez « [3.6.8 Spécification du XSCF comme serveur NTP](#) ».
2. **Spécifiez l'identifiant de la partition physique ciblée, puis exécutez la commande console pour basculer sur la console du domaine de commande de cette même partition physique.**

```
XSCF> console -p xx
```

3. **Spécifiez que le XSCF est le serveur NTP du domaine de commande.**
Pour plus de détails sur les paramètres de serveur NTP d'Oracle Solaris, consultez *Oracle Solaris Administration: Network Services* (Oracle Solaris 10) ou *Introduction to Oracle Solaris 11 Network Services* (Oracle Solaris 11).
4. **Redémarrez le domaine de commande.**
5. **Exécutez la commande `date` d'Oracle Solaris pour afficher l'heure du domaine de commande.**
6. **Sur la console du domaine de commande de la partition physique, appuyez sur `#` ou toute autre commande d'échappement pour revenir au shell XSCF.**
7. **Exécutez la commande `showdate` pour afficher l'heure du XSCF, puis vérifiez si l'heure du domaine de commande de la partition physique ciblée correspond à l'heure du XSCF.**

Spécification du même serveur NTP pour le domaine de commande et XSCF

1. **Configurez le XSCF en tant que client NTP.**
Pour plus de détails, consultez « [3.6.9 Spécification du XSCF comme client NTP](#) ».

2. **Enregistrez un serveur NTP externe avec XSCF.**
Pour plus de détails sur les paramètres de serveur NTP du XSCF, consultez « [3.6.10 Configuration des serveurs NTP utilisés par le XSCF](#) ».
3. **Spécifiez l'identifiant de la partition physique ciblée, puis exécutez la commande console pour basculer sur la console du domaine de commande de cette même partition physique.**

```
XSCF> console -p xx
```

4. **Spécifiez le même serveur NTP externe pour le domaine de commande et le XSCF.**
Pour plus de détails sur les paramètres de serveur NTP d'Oracle Solaris, consultez *Oracle Solaris Administration: Network Services* (Oracle Solaris 10) ou *Introduction to Oracle Solaris 11 Network Services* (Oracle Solaris 11).
5. **Redémarrez le domaine de commande.**
6. **Exécutez la commande date d'Oracle Solaris pour afficher l'heure du domaine de commande.**
7. **Sur la console du domaine de commande de la partition physique, appuyez sur # ou toute autre commande d'échappement pour revenir au shell XSCF.**
8. **Affichez l'heure du XSCF à l'aide de la commande showdate, puis vérifiez si l'heure du domaine de commande de la partition physique ciblée correspond à l'heure du XSCF.**

Remarque : en spécifiant également le même serveur NTP pour les domaines invités, le XSCF et le domaine de commande, vous pouvez synchroniser les heures de tous ces domaines sur le XSCF.

3.6.8 Spécification du XSCF comme serveur NTP

Configurez le XSCF en tant que serveur NTP fournissant le service NTP aux autres clients. Par défaut, le XSCF ne se comporte pas comme un serveur NTP fournissant ses services aux autres clients.

Utilisez la commande `showntp` pour vérifier les informations NTP d'un réseau XSCF. Pour que le XSCF se comporte comme un serveur NTP et fournisse le service NTP, utilisez la commande `setntp` en spécifiant l'option `-s server`. Exécutez la commande `setntp` avec un compte d'utilisateur disposant du privilège `platadm`.

1. **Exécutez la commande `showntp` pour afficher l'état du service NTP de XSCF.**

```
XSCF> showntp -a
client : disable
server : disable
```

2. **Exécutez la commande `setntp` pour configurer le XSCF en tant que serveur**

NTP fournissant son service aux autres clients.

Dans l'exemple suivant, les options `-s server` et `-c enable` ont été spécifiées, de sorte que le XSCF se comporte comme un serveur NTP et fournisse le service NTP.

```
XSCF> setntp -s server -c enable  
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

3. **Exécutez la commande `rebootxscf` pour redémarrer le XSCF.**

```
XSCF> rebootxscf -a  
The XSCF will be reset. Continue? [y|n] :y
```

La session XSCF est interrompue à ce moment-là. Reconnectez-vous au XSCF, puis identifiez-vous de nouveau.

4. **Exécutez la commande `showntp`, puis vérifiez que le XSCF est défini comme serveur NTP.**

```
XSCF> showntp -a  
client : disable  
server : enable
```

3.6.9 Spécification du XSCF comme client NTP

Pour que le XSCF utilise un serveur NTP, configurez-le comme client NTP. Par défaut, le XSCF ne se comporte pas comme un client NTP recevant l'heure du serveur NTP. Pour définir le XSCF comme client NTP, utilisez la commande `setntp` en spécifiant l'option `-s client`.

1. **Exécutez la commande `showntp` pour afficher l'état du XSCF en tant que client NTP.**

```
XSCF> showntp -a  
client : disable  
server : enable
```

2. **Exécutez la commande `setntp` pour configurer XSCF comme un client NTP.**

```
XSCF> setntp -s client -c enable  
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

3. **Exécutez la commande `rebootxscf` pour redémarrer le XSCF.**

```
XSCF> rebootxscf -a
The XSCF will be reset. Continue? [y|n] :y
```

La session XSCF est interrompue à ce moment-là. Reconnectez-vous au XSCF, puis identifiez-vous de nouveau.

4. **Exécutez la commande `showntp`, puis vérifiez que le XSCF est défini comme client NTP.**

```
XSCF> showntp -a
client : enable
server : enable
```

Remarque : si le décalage temporel entre le XSCF et le serveur NTP atteint 1000 secondes (environ 17 minutes) ou plus, le démon ntp du client XSCF s'arrête. En conséquence, la synchronisation avec le serveur NTP devient impossible. Pour vérifier si le démon ntp est arrêté, exécutez la commande `showntp -l`. Si « NTP is unavailable » apparaît, le démon ntp est arrêté.

Pour redémarrer le démon ntp, exécutez la commande `rebootxscf`, qui redémarre le XSCF.

▪ **Lorsque le démon ntp est arrêté**

```
XSCF> showntp -l
XSCF> NTP is unavailable.
```

▪ **Lorsque le démon ntp fonctionne**

```
XSCF> showntp -l
remote          refid          st t when poll reach delay  offset jitter
=====
*192.168.10.10  10.0.20.20  4 u 805 1024  377   19.429 0.083  0.917
127.127.1.0     .LOCL.      5 l 7   64   377    0.000 0.000  0.008
XSCF>
```

3.6.10 Configuration des serveurs NTP utilisés par le XSCF

Jusqu'à trois serveurs NTP peuvent être enregistrés pour recevoir l'heure du XSCF depuis un serveur NTP de niveau supérieur. Pour enregistrer un serveur NTP, utilisez la commande `setntp` en spécifiant l'option `-c add`.

À ce moment-là, le XSCF doit être configuré en tant que client NTP. Pour plus de détails sur la façon de configurer le XSCF en tant que client NTP, consultez « [3.6.9 Spécification du XSCF comme client NTP](#) ».

Lorsqu'un serveur NTP est enregistré, les paramètres préexistants sont effacés ou écrasés par ceux du serveur NTP spécifié. Pour spécifier un serveur NTP en utilisant

son nom d'hôte, les serveurs DNS doivent être capables de comprendre le nom de serveur.

1. **Exécutez la commande `showntp` pour afficher les serveurs NTP utilisés avec le XSCF.**

```
XSCF> showntp -a
client : disable
server : enable

server ntp1.example.com prefer
server ntp2.example.com
```

2. **Exécutez la commande `showntp` pour vérifier la synchronisation et afficher l'état.**

```
XSCF> showntp -l
remote      refid      st t when poll reach delay offset jitter
=====
*192.168.0.27 192.168.1.56 2 u  27  64  377 12.929 -2.756 1.993
+192.168.0.57 192.168.1.86 2 u  32  64  377 13.030 2.184 94.421
127.127.1.0   .LOCL.       5 l  44  64  377 0.000 0.000 0.008
```

3. **Exécutez la commande `setntp` pour ajouter un serveur NTP.**

Dans l'exemple suivant, trois adresses IP sont ajoutées en tant que serveurs NTP de niveau supérieur pour le XSCF : 192.168.1.2, 130.34.11.111, et 130.34.11.117.

```
XSCF> setntp -c add 192.168.1.2 130.34.11.111 130.34.11.117
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

Dans l'exemple suivant, deux noms d'hôtes sont ajoutés en tant que serveurs NTP de niveau supérieur pour le XSCF : ntp1.red.com et ntp2.blue.com.

```
XSCF> setntp -c add ntp1.red.com ntp2.blue.com
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

4. **Exécutez la commande `setntp` pour supprimer un serveur NTP du XSCF.**

Dans l'exemple suivant, ntp2.example.com, serveur NTP pour le XSCF, est supprimé.

```
XSCF> setntp -c del ntp2.example.com
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

5. **Exécutez la commande `rebootxscf` pour redémarrer le XSCF et diffuser les paramètres définis.**


```
XSCF> rebootxscf -a
The XSCF will be reset. Continue? [y|n] :y
```

La session XSCF est interrompue à ce moment-là. Reconnectez-vous au XSCF, puis identifiez-vous de nouveau.

6. **Exécutez la commande `showntp`, puis vérifiez les serveurs NTP.**

```
XSCF> showntp -a
client : enable
server : disable

server ntp1.red.com prefer
server ntp2.blue.com
```

3.6.11 Configuration du tourniquet DNS du serveur NTP

Si vous avez enregistré le serveur NTP par son nom d'hôte, vous pouvez utiliser le tourniquet DNS (round-robin) avec ce nom d'hôte. Pour utiliser le tourniquet DNS, utilisez la commande `setntp` en spécifiant l'option `-c pool`. Le serveur NTP que vous voulez configurer doit avoir été enregistré au préalable avec le XSCF. Pour plus de détails sur l'enregistrement du serveur NTP, consultez « [3.6.10 Configuration des serveurs NTP utilisés par le XSCF](#) ».

1. **Exécutez la commande `showntp` pour afficher les paramètres du tourniquet DNS.**

```
XSCF> showntp -a
client : enable
server : disable

server ntp1.example.com prefer
server ntp2.example.com
```

2. **Exécutez la commande `setntp` pour configurer le tourniquet DNS.**
Dans l'exemple suivant, le tourniquet DNS du serveur NTP est activé.

```
XSCF> setntp -c pool ntp2.example.com
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

Dans l'exemple suivant, le tourniquet DNS du serveur NTP est désactivé.

```
XSCF> setntp -c server ntp2.example.com
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

3. **Exécutez la commande `rebootxscf` pour redémarrer le XSCF et diffuser les paramètres définis.**

```
XSCF> rebootxscf -a  
The XSCF will be reset. Continue? [y|n] :y
```

La session XSCF est interrompue à ce moment-là. Reconnectez-vous au XSCF, puis identifiez-vous de nouveau.

4. **Exécutez la commande `showntp` pour afficher les paramètres du tourniquet DNS.**

L'exemple suivant montre le serveur `ntp2.example.com` avec le tourniquet DNS activé.

```
XSCF> showntp -a  
client : enable  
server : disable  
  
server ntp1.example.com prefer  
pool ntp2.example.com
```

3.6.12 Spécification/annulation de la préférence pour un serveur NTP

Si plusieurs serveurs NTP sont configurés, la spécification `-m prefer=on` accorde la priorité au serveur NTP enregistré comme premier par la commande `setntp` lorsque les serveurs NTP sont synchronisés. À partir de ce moment, le serveur enregistré avec le tourniquet DNS activé sera exclu de la synchronisation. Par défaut, l'option `prefer` est définie sur « on (activée) ».

1. **Exécutez la commande `showntp` pour afficher les paramètres de préférence.**

```
XSCF> showntp -m  
prefer : on  
localaddr : 0
```

2. **Exécutez la commande `setntp` pour paramétrer la préférence.**

Dans l'exemple suivant, la préférence est spécifiée pour les serveurs NTP.

```
XSCF> setntp -m prefer=on  
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

Dans l'exemple suivant, la préférence est annulée pour les serveurs NTP.

```
XSCF> setntp -m prefer=off  
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

3. **Exécutez la commande `rebootxscf` pour redémarrer le XSCF et diffuser les paramètres définis.**

```
XSCF> rebootxscf -a  
The XSCF will be reset. Continue? [y|n] :y
```

La session XSCF est interrompue à ce moment-là. Reconnectez-vous au XSCF, puis identifiez-vous de nouveau.

4. **Exécutez la commande `showntp`, puis vérifiez les paramètres de préférence.**
Dans l'exemple suivant, l'indication de préférence est annulée.

```
XSCF> showntp -m  
prefer : off  
localaddr : 0
```

Dans l'exemple suivant, aucune préférence n'est spécifiée.

```
XSCF> showntp -a  
client : enable  
server : disable  
  
server ntp1.red.com  
server ntp2.blue.com
```

3.6.13 Réglage de la valeur de couche du XSCF

Afin de définir une valeur de couche pour le XSCF, utilisez la commande `setntp` en spécifiant l'option `-c stratum`. Toute valeur comprise entre 1 et 15 peut être définie comme valeur de couche. La valeur par défaut est de 5.

1. **Exécutez la commande `showntp` pour afficher la valeur de couche définie pour le XSCF.**

```
XSCF> showntp -s  
stratum : 5
```

2. **Exécutez la commande `setntp` pour modifier la valeur de couche.**
Dans l'exemple suivant, la valeur de couche utilisée sur le réseau XSCF est fixée à 7.

```
XSCF> setntp -c stratum -i 7  
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

3. **Exécutez la commande `rebootxscf` pour redémarrer le XSCF et diffuser les paramètres définis.**

```
XSCF> rebootxscf -a  
The XSCF will be reset. Continue? [y|n] :y
```

La session est interrompue à ce moment-là. Reconnectez-vous à une nouvelle interface, puis identifiez-vous de nouveau.

4. **Exécutez la commande `showntp`, puis vérifiez la valeur de couche.**

```
XSCF> showntp -s
stratum : 7
```

3.6.14 Modification de l'adresse de l'horloge locale du XSCF

Définissez l'adresse d'horloge de l'horloge locale du XSCF elle-même. Vous pouvez indiquer une valeur comprise entre 0 et 3 pour l'octet le moins significatif de l'adresse de l'horloge locale. L'adresse de l'horloge locale par défaut est 127.127.1.0.

1. **Exécutez la commande `showntp` pour afficher l'adresse de l'horloge locale du XSCF.**

```
XSCF> showntp -m
prefer : on
localaddr : 0

XSCF> showntp -l
remote          refid          st t when poll reach  delay  offset  jitter
=====
*192.168.0.27 192.168.1.56    2 u   27   64   377 12.929 -2.756  1.993
+192.168.0.57 192.168.1.86    2 u   32   64   377 13.030  2.184 94.421
127.127.1.0   .LOCL.          5 l   44   64   377  0.000  0.000  0.008
```

2. **Exécutez la commande `setntp` pour modifier l'adresse de l'horloge locale de XSCF.**

Dans l'exemple suivant, l'octet le moins significatif de l'adresse d'horloge est défini comme 1.

```
XSCF> setntp -m localaddr=1
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

3. **Exécutez la commande `rebootxscf` pour redémarrer le XSCF et diffuser les paramètres définis.**

```
XSCF> rebootxscf -a
The XSCF will be reset. Continue? [y|n] :y
```

La session XSCF est interrompue à ce moment-là. Reconnectez-vous au XSCF, puis identifiez-vous de nouveau.

4. **Exécutez la commande `showntp` pour afficher l'adresse de l'horloge locale du**

XSCF.

```
XSCF> showntp -m
prefer : on
localaddr : 1

XSCF> showntp -l
remote          refid          st t when poll reach  delay  offset  jitter
=====
*192.168.0.27 192.168.1.56    2 u  27   64   377 12.929 -2.756  1.993
+192.168.0.57 192.168.1.86    2 u  32   64   377 13.030  2.184 94.421
127.127.1.1   .LOCL.          5 l  44   64   377  0.000  0.000  0.008
```

Remarques concernant les serveurs NTP se référant à l'horloge locale

En supposant que le XSCF se réfère au serveur NTP qui lui-même se réfère à l'heure du système (horloge locale) du serveur, et que « 127.127.1.0 » soit l'adresse définie pour l'horloge locale, il se peut que la synchronisation de l'heure sur le XSCF soit impossible.

L'adresse de l'horloge locale du XSCF est définie comme « 127.127.1.0 ». Ainsi, si le XSCF se réfère à un serveur NTP dont l'horloge locale possède comme adresse définie « 127.127.1.0 », l'adresse de la source d'horloge (refid) se trouve être la même que celle de l'horloge locale du XSCF. Un tel serveur NTP n'est pas soumis à la synchronisation de l'heure du XSCF.

En exécutant la commande `showntp -l`, vous pouvez afficher l'adresse de la source d'horloge de chaque serveur NTP tel que configurée sur le XSCF ainsi que l'adresse de l'horloge locale du XSCF.

```
XSCF> showntp -l
remote          refid          st t when poll reach  delay  offset  jitter
=====
192.168.1.2    LOCAL(0)        3 u  10 1024   377  0.000  0.000  0.000
*127.127.1.0   .LOCL.          5 l  28   64   377  0.000  0.000  0.008
```

Sur les deux serveurs NTP en sortie, le premier serveur (192.168.1.2) est le serveur configuré par la commande `setntp`. Le refid de ce serveur NTP est LOCAL(0), de sorte que la source d'horloge définie pour le serveur NTP est l'horloge locale dont l'adresse est « 127.127.1.0 ». La source du second serveur est l'horloge locale du XSCF. L'adresse de l'horloge locale du XSCF est définie comme « 127.127.1.0 ». Comme le serveur NTP (192.168.1.2) n'est pas soumis à la synchronisation de l'heure du XSCF, il en découle que le XSCF synchronise l'heure sur sa propre horloge locale.

En prenant l'une des mesures suivantes pour éviter les problèmes, vous pouvez disposer d'une heure correctement synchronisée sur les serveurs NTP configurés à l'aide de la commande `setntp`.

- Modifiez les sources d'horloge auxquelles se réfèrent les serveurs NTP configurés pour le XSCF.
Utilisez la commande `showntp -l` pour vérifier les sources d'horloge des serveurs

NTP configurés pour le XSCF. Le serveur NTP dont le refid est LOCAL(0), mentionné plus haut, se réfère à l'horloge locale dont l'adresse est « 127.127.1.0 ». En conséquent, opérez une modification pour que le serveur se réfère à une autre source d'horloge. Avant de modifier la source d'horloge d'un serveur NTP, vérifiez que cette modification n'affectera pas les autres clients NTP.

- Modifiez l'adresse de l'horloge locale du serveur NTP.
Changez l'adresse de l'horloge locale du serveur NTP auquel se réfère le XSCF en « 127.127.1.1 », « 127.127.1.2 », ou « 127.127.1.3 ». Modifiez /etc/inet/ntp.conf d'Oracle Solaris. Pour appliquer les modifications, redémarrez le démon ntp. Avant de modifier l'adresse de l'horloge locale d'un serveur NTP, vérifiez que cette modification n'affectera pas les autres clients NTP.
- Modifiez la valeur de couche d'un serveur NTP.
Modifiez la valeur de couche d'un serveur NTP que XSCF référence à 1. Le serveur NTP dont la valeur de couche est 1 est la source d'horloge la plus significative sans refid. Par conséquent, son adresse n'est jamais la même que celle de l'horloge locale du XSCF. Avant de modifier la valeur de couche d'un serveur NTP, vérifiez que cette modification n'affectera pas les autres clients NTP.
- Modifiez l'adresse de l'horloge locale du XSCF.
Utilisez la commande `setntp -m localaddr=`value pour modifier l'adresse de l'horloge locale du XSCF. Comme valeur, indiquez l'octet le moins significatif de l'adresse d'horloge locale « 127.127.1.x ». Vous pouvez spécifier une valeur numérique comprise entre 0 et 3. Si la valeur spécifiée pour une valeur est comprise entre 1 et 3, l'adresse du serveur NTP se référant à l'horloge locale ne correspond plus à l'adresse de l'horloge locale interne du XSCF. En conséquence, même un serveur se référant à l'horloge locale peut être configuré comme serveur NTP pour le XSCF.

3.7 Configuration du service SSH/Telnet pour la connexion à XSCF

Cette section décrit comment configurer les services SSH et Telnet. Pour utiliser le terminal du shell XSCF et la console du domaine de commande d'une partition physique donnée, utilisez SSH ou Telnet. Activez/désactivez SSH et Telnet, définissez la clé d'hôte SSH et paramétrez le délai d'expiration automatique pour les utilisateurs connectés. De plus, enregistrez la clé publique d'utilisateur avec le XSCF.

Il est possible d'activer SSH et Telnet simultanément. Toutefois, les communications utilisant le service Telnet ne peuvent pas être considérées comme sécurisées. Nous vous recommandons de désactiver le service Telnet lorsque le service SSH est activé.

Client SSH

Ce système peut utiliser la fonction SSH avec les logiciels clients suivants :

- Oracle Solaris Secure Shell
- OpenSSH

- PuTTY
- UTF-8 TeraTerm Pro avec TTSSH2

Pour connaître les conditions d'utilisation des logiciels, consultez leurs manuels respectifs.

Numéro de port

Le numéro du port SSH est 22 et le numéro du port Telnet, 23.

Clé publique d'utilisateur

Pour utiliser une clé d'utilisateur SSH via une connexion XSCF-LAN, créez une clé d'utilisateur secrète et une clé publique d'utilisateur pour un compte d'utilisateur enregistré sur le PC client, puis enregistrez la clé publique d'utilisateur avec le XSCF. Pour afficher, enregistrer ou supprimer une clé publique d'utilisateur SSH après avoir indiqué un nom d'utilisateur, le privilège useradm est requis.

Remarque : pour UTF-8 TeraTerm Pro avec TTSSH2 4.66 ou une version plus récente, 2048-bit DSA n'est pas pris en charge pour les clés publiques d'utilisateur.

Console

Les systèmes SPARC M12/M10 peuvent être utilisés avec une console de domaine de commande accessible en écriture (RW) ou uniquement référençable (RO) pour une partition physique. Vous pouvez utiliser une console RW par partition physique. Utilisez la commande console pour utiliser la console de domaine de commande. Pour plus de détails sur la console, consultez « [Chapitre 2 Connexion à / Déconnexion de XSCF](#) ».

3.7.1 Vérification des éléments de réglage et des commandes liés à SSH et Telnet

[Tableau 3-19](#) répertorie les éléments de réglage liés à SSH et Telnet et les commandes du shell XSCF correspondantes.

Tableau 3-19 Éléments de réglage à SSH et Telnet

Élément de réglage	Paramétrage requis ou optionnel	Commande liée
Activation/désactivation de SSH	Optionnel	setssh(8), showssh(8)
Génération d'une clé d'hôte	Optionnel	setssh(8), showssh(8)
Enregistrement/suppression d'une clé publique d'utilisateur	Optionnel	setssh(8), showssh(8)
Activation/désactivation de Telnet	Optionnel	settelnet(8), showtelnet(8)
Délai d'expiration	Optionnel	setautologout(8), showautologout(8)

3.7.2 Activation/Désactivation des services SSH et Telnet

Afin de vérifier les services SSH et Telnet paramétrés pour le réseau XSCF, utilisez les commandes `showssh` et `showtelnet`. En outre, pour configurer les services SSH et Telnet, utilisez les commandes `setssh` et `settelnet`.

Lors de l'utilisation des commandes `setssh` ou `settelnet` pour activer/désactiver les services SSH ou Telnet, le paramètre est diffusé immédiatement après que la commande a été exécutée.

1. **Exécutez la commande `showssh` pour afficher les paramètres SSH ou `showtelnet` pour afficher les paramètres Telnet.**

Dans l'exemple suivant, les paramètres du service SSH sont affichés.

```
XSCF> showssh
SSH status: enabled
RSA key:
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAt0IG3wfpQnGr51znS9XtzWcBBb/UU0LN08S
ilUXE6j+av1xdY7AFqBflwGxLF+Tx5pTa6HuZ8o8yUBbDZVJAAAAFQCfKPxarV+/
5qzK4A43Qaigkqu/6QAAAIbMLQl22G8pwibESrh5JmOhSxpLzl3P26ksI8qPr+7B
xmjlR0k=
Fingerprint:
1024 e4:35:6a:45:b4:f7:e8:ce:b0:b9:82:80:2e:73:33:c4
/etc/ssh/ssh_host_rsa_key.pub
DSA key:
ssh-dss
AAAAB3NzaC1kc3MAAACBAJSy4GxD7Tk4fxFvyWlD0NUDqZQPY3PuY2IG7QC4BQ1k
ewDnblB8/JEqI+8pnfbWzmOWU37KHL19OEYNv6v+WZT6RElU5Pyb8F16uq96L8Q
DMswFlICMZgrn+ilJNStr6r8KDJfwOQMmK0eeDFj2mL40NOvaLQ83+rRwW6Ny/yF
1Rgv6PUpUqRLw4VeRb+uOfmPRpe6/kb4z++lOhtp
WI9bay6CK0nrFRok+z54ez7BrDFBQVuNZx9PyEFezJG9ziEYVUag/23LIAiLxxBm
W9pqa/WxC21Ja4RQVN3009kmVwAAAIaON1LR/9Jdd7yyG18+Ue7eBBJHrCA0pkSz
vfzzFFj5XUzQBdabh5p5Rwz+lvriawFIZI9j2uhM/3HQdrvYSVBEDmJaasF9hB6T
/uFwP8yqtJf6Y9GdjBAhWuH8F13pX4BtvK9IeldqCscnOuu0e2rlUoI6GICMr64F
L0YYBSwfbwLiZ6PSA/yKQe23dwfkSfcwQZNq/5pThGPi3tob5Qev2KCK2OyEDMCA
OvVlMhqHuPNpX+hE19nPdBFGzQ==
Fingerprint:
1024 9e:39:8e:cb:8a:99:ff:b4:45:12:04:2d:39:d3:28:15
/etc/ssh/ssh_host_dsa_key.pub
```

Dans l'exemple suivant, les paramètres du service Telnet sont affichés.

```
XSCF> showtelnet
Telnet status: disabled
```

2. **Exécutez la commande `setssh` pour configurer le service SSH ou `settelnet` pour configurer le service Telnet.**

Dans l'exemple suivant, l'activation du service SSH est spécifiée.


```
XSCF> setssh -c enable  
Continue? [y|n] :y
```

Dans l'exemple suivant, la désactivation du service Telnet est spécifiée.

```
XSCF> settelnet -c disable  
Continue? [y|n] :y
```

3.7.3 Réglage d'une clé d'hôte du service SSH

Pour activer et commencer à utiliser le service SSH, générez tout d'abord une clé d'hôte.

Lors de l'utilisation du service SSH via une connexion XSCF-LAN, notez l'empreinte. Copiez les données texte de la clé publique d'hôte générée sur un fichier dans un répertoire donné du client.

1. **Exécutez la commande showssh pour afficher la clé d'hôte et l'empreinte.**
Une clé d'hôte est générée lorsque vous le service SSH est activé pour la première fois.

```
XSCF> showssh  
SSH status: enabled  
RSA key:  
ssh-rsa  
AAAAB3NzaC1yc2EAAAABIwAAAIEAt0IG3wfpQnGr51znS9XtzwHcBBb/UU0LN08S  
ilUXE6j+avlxY7AFqBflwGxLF+Tx5pTa6HuZ8o8yUBbDZVJAAAFQCfKPxarV+/  
5qzK4A43Qaigkqu/6QAAAIbMLQ122G8pwibESrh5JmOhSxpLzl3P26ksI8qPr+7B  
xmjlR0k=  
Fingerprint:  
1024 e4:35:6a:45:b4:f7:e8:ce:b0:b9:82:80:2e:73:33:c4  
/etc/ssh/ssh_host_rsa_key.pub  
DSA key:  
ssh-dss  
AAAAB3NzaC1kc3MAAACBAJSy4GxD7Tk4fxFvyW1D0NUdQZQPY3PuY2IG7QC4BQ1k  
ewDnb1B8/JEqI+8pnfbWzmOWU37KHL19OEYNAv6v+WZT6RE1U5Pyb8F16uq96L8Q  
DMswFlICMZgrn+ilJNStr6r8KDJfwQMmK0eeDFj2mL40NOvaLQ83+rRwW6Ny/yF  
1Rgv6PUPuqRLw4Verb+uOfmPRpe6/kb4z++lOhtp  
WI9bay6CK0nrFRok+z54ez7BrDFBQVuNZx9PyEFezJG9ziEYVUag/23LIAiLxxBm  
W9pqa/WxC21Ja4RQVN3009kmVwAAAIaON1LR/9Jdd7yyG18+Ue7eBBJHrCA0pkSz  
vfzzFFj5XUzQBdabh5p5Rwz+lvriawFIZI9j2uhM/3HQdrvYSVBEdMjaasF9hB6T  
/uFwP8yqtJf6Y9GdjBAhWuH8F13pX4BtvK9IeldqCscnOuu0e2rlUoI6GICMr64F  
L0YYBSwfbwLIz6PSA/yKQe23dwfkSfcwQZNq/5pThGPi3tob5Qev2KCK2OyEDMCA  
OvVlMhqHuPNpX+hE19nPdBFGzQ==  
Fingerprint:  
1024 9e:39:8e:cb:8a:99:ff:b4:45:12:04:2d:39:d3:28:15  
/etc/ssh/ssh_host_dsa_key.pub
```

2. **Exécutez la commande setssh pour générer une clé d'hôte.**
Dans l'exemple suivant, une clé d'hôte est générée et utilisée pour remplacer la

clé actuelle.

```
XSCF> setssh -c genhostkey
Host key already exists. The key will be updated. Continue? [y|n]
: y
```

3.7.4 Enregistrement/Suppression d'une clé publique d'utilisateur pour le service SSH

Pour utiliser une clé d'utilisateur pour le service SSH via une connexion XSCF-LAN, créez une clé d'utilisateur secrète et une clé publique d'utilisateur pour un compte d'utilisateur enregistré sur le PC client, puis enregistrez la clé publique d'utilisateur avec le XSCF.

1. **Exécutez la commande showssh pour afficher les clés publiques d'utilisateur.**
Dans l'exemple suivant, l'option -c pubkey est spécifiée pour afficher la clé publique d'utilisateur. Cependant, aucune réponse n'est reçue car aucune clé d'utilisateur n'a été enregistrée.

```
XSCF> showssh -c pubkey
```

2. **Créez une clé secrète et une clé publique d'utilisateur pour un compte d'utilisateur XSCF enregistré sur le client.**
Pour plus détails sur la façon de créer une clé d'utilisateur et de spécifier une phrase secrète sur le client, consultez le manuel du logiciel client utilisé. Nous vous recommandons de définir une phrase secrète.
3. **Pour enregistrer la clé publique d'utilisateur, exécutez la commande setssh en spécifiant l'option -c addpubkey, puis copiez la clé publique d'utilisateur créée à l'étape 2 et collez-la dans la fenêtre.**
Après avoir appuyé sur la touche [Entrée], appuyez sur les touches [Ctrl] et [D] pour finaliser le l'enregistrement.

Dans l'exemple suivant, la clé publique de l'utilisateur efgh est enregistrée.

```
XSCF> setssh -c addpubkey -u efgh
Please input a public key:
ssh-rsa AAAAB3NzaClyc2EAAAABIwAAAIEAzFh95SohrDgpnN7zFCJCVNy+
jaZPTjNDxcidQGbiHYDCBttI4151Y0Sv85FJwDpSNHNKoVLMYLjtBmUMPbGgGV
B61qskSv/Fev44hefNCZMiXGItIIpKP0nBK4XJpCFoFbPXNUHDwlrTD9icD5U/
wRFGSRRxFI+Ub5oLRxN8+A8= efgh@example.com
<Appuyez sur [Ctrl] et [D] keys>
XSCF>
```

4. **Exécutez la commande showssh, puis vérifiez la clé publique d'utilisateur et son numéro.**
L'exemple suivant montre une clé d'utilisateur enregistrée sous le numéro 1.

```
XSCF> showssh -c pubkey
Public key:
1 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAzFh95SohrDgpnN7zFCJCVNy+
jaZPTjNDxcidQGbiHYDCBttI4151Y0Sv85FJwDpSNHNKoVLMYLjtBmUMPbGgGV
B6lqskSv/Fev44hefNCZMiXGItIIPKP0nBK4XJpCFoFbPXNUHDwlrTD9icD5U/
wRFGSRRxFI+Ub5oLRxN8+A8= efgh@example.com
```

Lors de la connexion suivante au shell XSCF, établissez une connexion SSH depuis le PC client en utilisant un compte d'utilisateur XSCF. Vérifiez que vous pouvez vous connecter au shell XSCF en vous identifiant avec la clé d'utilisateur.

5. **Pour supprimer une clé publique d'utilisateur, exécutez la commande setssh en spécifiant son numéro.**

Dans l'exemple suivant, l'option -c delpubkey est spécifiée, de même que le numéro de clé d'utilisateur avec l'option -s, pour pouvoir supprimer la clé publique d'utilisateur.

```
XSCF> setssh -c delpubkey -s 1
1 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAzFh95SohrDgpnN7zFCJCVNy+
jaZPTjNDxcidQGbiHYDCBttI4151Y0Sv85FJwDpSNHNKoVLMYLjtBmUMPbGgGV
B6lqskSv/Fev44hefNCZMiXGItIIPKP0nBK4XJpCFoFbPXNUHDwlrTD9icD5U/
wRFGSRRxFI+Ub5oLRxN8+A8= efgh@example.com
```

6. **Exécutez la commande showssh, puis vérifiez que la clé publique d'utilisateur a été supprimée.**

```
XSCF> showssh -c pubkey
```

3.7.5 Réglage du délai d'expiration des services SSH/Telnet

1. **Exécutez la commande showautologout pour afficher le délai d'expiration.**

```
XSCF> showautologout
30min
```

2. **Exécutez la commande setautologout pour définir le délai d'expiration.**
Dans l'exemple suivant, le délai d'expiration est fixé à 255 minutes.

```
XSCF> setautologout -s 255
255min
```

Le délai d'expiration défini est appliqué à compter de la connexion suivante.

3.8 Configuration du service HTTPS pour la connexion à XSCF

Cette section décrit comment configurer le service HTTPS.

Les paramètres du service HTTPS sont configurés pour l'utilisation de XSCF Web avec une connexion au XSCF-LAN et d'une fenêtre de navigateur web. Utilisez les paramètres décrits ici pour activer/désactiver et utiliser HTTPS. HTTPS est désactivé par défaut dans ces systèmes. La console XSCF Web peut être une console sécurisée.

Sélection d'une autorité de certification

En prenant compte du système du client et de l'environnement du navigateur web, sélectionnez l'une des autorités de certification suivantes :

- Autorité de certification externe
- Autorité de certification sur l'intranet
- Autorité de certification autonome

Si l'environnement du client ne dispose d'aucune autorité de certification externe ou sur l'intranet, utilisez l'autorité de certification autonome de XSCF. (Consultez « [3.8.2 Flux d'utilisation de l'autorité de certification autonome](#) ».)

L'autorité de certification autonome de XSCF est une autorité de certification autonome configurée avec le XSCF et ne peut être utilisée comme autorité de certification externe pour d'autres systèmes.

Durée de validité d'un certificat autonome

Un certificat autonome dispose de la durée de validité fixe suivante :

- Certificat de serveur : 10 ans

Après expiration de la durée de validité d'un certificat de serveur web ou modification de celui-ci, configurez de nouveau le service HTTPS.

Nom unique (DN)

Pour créer une demande de signature de certificat (CSR) de serveur web, spécifiez le nom unique (DN) de la manière suivante :

Remarque : dans l'autorité de certification autonome de XSCF, la longueur de la clé pour la certification autonome utilisée pour la signature du certificat de serveur Web est 2048-bit. La longueur de la clé ne peut pas être modifiée.

- Code de pays à 2 lettres (ex. : US ou JP)
- Région
- Ville
- Nom d'organisation (entreprise), nom de service ou de département
- Nom courant (nom d'utilisateur, nom d'hôte du serveur Web)

- Adresse e-mail de l'administrateur

Hormis le code de pays, les champs mentionnés ci-dessus peuvent comporter jusqu'à 64 caractères. Pour plus de détails sur le DN, consultez la page de manuel correspondant à la commande `sethttps(8)` ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

3.8.1 Flux pour l'utilisation d'une autorité de certification externe ou sur l'intranet

Cette section décrit la procédure de paramétrage à suivre pour utiliser une autorité de certification externe ou sur l'intranet.

1. **Créez une clé secrète de serveur web de XSCF.**
2. **Créez une demande de signature de certificat (CSR) de serveur web sur le XSCF.**
3. **Demandez à l'autorité de certification de délivrer un certificat pour la demande de signature de certificat du serveur XSCF Web.**
4. **Importez le certificat du serveur Web signé par l'autorité de certification vers XSCF.**
5. **Activez HTTPS.**

Au cours des étapes 1 à 5 mentionnées ci-dessus, spécifiez leurs options respectives dans la commande `sethttps`. Si XSCF Web est utilisé pour les paramètres, sélectionnez les éléments de réglage respectifs.

Si le système comporte plusieurs XSCF, les paramètres sont diffusés automatiquement par le XSCF de veille.

3.8.2 Flux d'utilisation de l'autorité de certification autonome

Cette section décrit la procédure de paramétrage à suivre pour utiliser une autorité de certification autonome.

S'il n'existe ni clé secrète de serveur web, ni certificat de serveur web autonome, vous pouvez spécifier l'option « enable » pour l'authentification autonome dans la commande `sethttps` afin de finaliser automatiquement et en une seul fois les paramètres définis au cours des étapes 1 à 4.

S'il existe une clé secrète de serveur web et un certificat de serveur web autonome, suivez les étapes 1 à 4.

1. **Configurez l'autorité de certification autonome de XSCF.**
2. **Générez une clé secrète de serveur Web de XSCF.**
3. **Créez un certificat de serveur web autonome sur le XSCF.**
4. **Activez HTTPS.**

Si le système comporte plusieurs XSCF, les paramètres sont diffusés automatiquement

par le XSCF de veille.

3.8.3 Vérification des éléments de réglage et commandes liés à HTTPS

Tableau 3-20 répertorie les éléments de réglage liés à HTTPS et les commandes de shell XSCF correspondantes.

Tableau 3-20 Éléments de réglage liés à HTTPS

Élément de réglage	Paramétrage requis ou optionnel	Commande liée
Activation/désactivation de HTTPS	Optionnel	sethttps(8), showhttps(8)
Certificat externe - Création d'une clé secrète de serveur web sur le XSCF - Création d'une CSR de serveur web sur le XSCF et demande de délivrance de certificat à l'autorité - Importation d'un certificat de serveur web sur le XSCF	Optionnel	sethttps(8), showhttps(8)
Authentification autonome - Configuration d'une autorité de certification autonome - Création d'une clé secrète de serveur web - Création d'un certificat de serveur web autonome	Optionnel	sethttps(8), showhttps(8)

3.8.4 Activation/Désactivation du service HTTPS

Pour vérifier que le service HTTPS est paramétré pour le réseau XSCF, utilisez la commande shownetwork. En outre, pour configurer le service HTTPS, utilisez la commande sethttps. Exécutez la commande sethttps avec un compte d'utilisateur disposant du privilège platadm.

1. **Exécutez la commande showhttps pour afficher les paramètres du service HTTPS.**
Dans l'exemple suivant, les paramètres du service HTTPS sont affichés.

```
XSCF> showhttps
HTTPS status: enabled
Server key: installed in Apr 24 12:34:56 JST 2006
CA key: installed in Apr 24 12:00:34 JST 2006
CA cert: installed in Apr 24 12:00:34 JST 2006
CSR:
-----BEGIN CERTIFICATE REQUEST-----
```

```

MIIBwjCCASsCAQAwgYExCzAJBgNVBAYTAmpqMQ4wDAYDVQQIEwVzdGF0ZTERMA8G
A1UEBxMIbG9jYWxpdHkxFTATBgNVBAoTDG9yZ2FuaXphdGlvbjEPMA0GA1UECxMG
b3JnYW5pMQ8wDQYDVQQDEWZjb21tb24xFTJAUBgkqhkiG9w0BCQEWB2VlLm1haWww
gZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJ5D57X/k42LcipTWBwzv2GrxaVM
5GEyx3bdBW8/7WZhnd3uiZ9+ANlvRAuw/Yy7I/pAD+NQJesBcBjujy9x+IiJl9F
MrI5fR8pOIywVodbMPCar09rrU45bVeZhTyi+uQOdWLoX/Dhq0fm2BpYuh9WukT5
pTEg+2dABg8UdHmNagMBAAGgADANBgkqhkiG9w0BAQQFAAOBgQAux1jH3dyB6Xho
PgBuVIakDzIKEPipK9qQfC57YI43uRBGRubu0AHEcLVue5yTu6G5SxHTCq07tV5g
38UHSg5Kqy9QuWHWMri/hxm0kQ4gBpApjNb6F/B+ngBE3j/thGbEuvJb+0wbycvu
5jrhB/ZV9k8X/MbDOxSx/U5nF+Zuyw==
-----END CERTIFICATE REQUEST-----

```

2. Exécutez la commande **sethttps** pour configurer HTTPS.

Dans l'exemple suivant, le service HTTPS est activé.

```

XSCF> sethttps -c enable
Continue? [y|n] : y

```

En l'absence de clé secrète de serveur Web ou de certificat de serveur Web signé de façon autonome, cette commande « activer » automatiquement spécifiée configure l'authentification autonome, génère une clé secrète de serveur Web, crée un certificat de serveur Web et active HTTPS pour exécuter cette tâche de manière simultanée.

Dans l'exemple suivant, le service HTTPS est désactivé.

```

XSCF> sethttps -c disable
Continue? [y|n] : y

```

3.8.5 Importation d'un certificat de serveur web à l'aide d'une autorité de certification sur l'intranet ou externe

1. Exécutez la commande **sethttps** pour générer une clé secrète de serveur web.

Dans l'exemple suivant, l'option **-c genserverkey** est spécifiée pour générer une clé secrète de serveur web.

```

XSCF> sethttps -c genserverkey
Server key already exists. Do you still wish to update? [y|n] :y
Enter passphrase: xxxxxxxx
Verifying - Enter passphrase: xxxxxxxx

```

2. Exécutez la commande **sethttps** en spécifiant le DN (nom unique) pour générer une CSR (demande de signature de certificat).

Dans l'exemple suivant, l'option **-c gencsr** est spécifiée, de même que le DN (JP, Kanagawa, Kawasaki, Example, development, scf-host, abc@example.com) afin

de générer une CSR.

```
XSCF> sethttps -c gencsr JP Kanagawa Kawasaki Example
development scfhost abc@example.com
```

3. Exécutez la commande `showhttps` pour afficher la CSR. Copiez et sauvegardez la CSR affichée (du DÉBUT à la FIN) sur un fichier texte.

```
XSCF> showhttps
HTTPS status: disabled
Server key: installed in Jul 11 06:33:25 UTC 2006
CA key: installed in Jul 11 06:33:21 UTC 2006
CA cert: installed in Jul 11 06:33:21 UTC 2006
CSR:
-----BEGIN CERTIFICATE REQUEST-----
MIIByzCCATQCAQAwYoxCzAJBgNVBAYTAkpQMREwDwYDVQQIEWhLYW5hZ2F3YTER
MA8GA1UEBxMIS2F3YXNha2kxEDAOBgNVBAoTB0ZVSklUU1UxDDAKBgNVBAsTA0VQ
:
uni/n3g2/F5Ftnjg+M4HtfzT6VwEhG01FGP4IIImqKg==
-----END CERTIFICATE REQUEST-----
```

4. Envoyez la CSR copiée à l'autorité de certification pour lui demander de délivrer un certificat de serveur web.
5. Pour effectuer l'importation, exécutez la commande `setssh` en spécifiant l'option `-c importca`, puis copiez le certificat de serveur web signé à l'étape 4 et collez-le dans la fenêtre.
Appuyez sur la touche [Entrée] pour l'importer, puis sur les touches [Ctrl] et [D] pour finaliser cette étape.

```
XSCF> sethttps -c importca
Please import a certificate:
-----BEGIN CERTIFICATE-----
MIIDdTCCAt6gAwIBAgIBATANBgkqhkiG9w0BAQQFADCBgTELMAkGAlUEBhMCamox
:
R+OpXAVQvb2tjIn3k099dq+begEC04mwknWlt7QI7A1BkcW2/MkOolIRa6iP1Zwg
JoPmwAbrGyAvGUtdzUoyIH0jl7dRQrVIRA==
-----END CERTIFICATE-----
<Appuyez sur [Ctrl] et [D] keys>
```

6. Exécutez la commande `sethttps` pour activer HTTPS.

```
XSCF> sethttps -c enable
Continue? [y|n] : y
```

7. Depuis le client, accédez à XSCF Web en spécifiant HTTPS. Vérifiez qu'aucune fenêtre de dialogue signalant un avertissement de sécurité n'apparaît sur l'écran et que le certificat est correct.

3.8.6

Configuration d'une autorité de certification autonome et création d'un certificat de serveur web

En l'absence de clé secrète de serveur web et de certificat de serveur web signé de façon autonome

1. **Exécutez la commande `sethttps` en spécifiant l'option `-c enable` pour démarrer le service HTTPS.**

```
XSCF> sethttps -c enable
Continue? [y|n] : y
```

Cette commande configure automatiquement l'authentification autonome, génère une clé secrète de serveur web, crée un certificat de serveur web et active HTTPS en finalisant simultanément les processus.

Lorsqu'une clé secrète de serveur web et un certificat de serveur web signé de façon autonome sont disponibles

La clé secrète de serveur web existante et le certificat seront écrasés.

1. **Exécutez la commande `sethttps` en spécifiant le DN (nom unique) pour créer un certificat de serveur web signé de façon autonome.**

Dans l'exemple suivant, l'option `-c selfsign` est spécifiée, de même que le DN (JP, Kanagawa, Kawasaki, Example, development, scf-host, abc@example.com) afin de créer un certificat de serveur web signé de façon autonome.

```
XSCF> sethttps -c selfsign JP Kanagawa Kawasaki Example
development scf-host abc@example.com
CA key and CA cert already exist. Do you still wish to update?
[y|n] :y
Enter passphrase: xxxxxxxx
Verifying - Enter passphrase: xxxxxxxx
```

2. **Exécutez la commande `showhttps` en spécifiant l'option `-t`, puis vérifiez que le certificat de serveur web signé de façon autonome a été créé.**

```
XSCF> showhttps -t
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      cb:92:cc:ee:79:6c:d3:09
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=JP, ST=Kanagawa, O=Fujitsu, OU=Fujitsu, CN=XSCF
    Validity
      Not Before: May 24 07:15:17 2017 GMT
      Not After : May 22 07:15:17 2027 GMT
```

```
Subject: C=JP, ST=Kanagawa, O=Fujitsu, OU=Fujitsu, CN=XSCF/  
emailAddress=hoge@hoge  
Subject Public Key Info:  
Public Key Algorithm: rsaEncryption  
Public-Key: (2048 bit)  
Modulus:  
    00:c7:5f:f1:61:ad:ba:4b:64:25:7e:49:ba:7a:6c:  
    d4:5c:b1:8c:2d:15:9f:8a:2f:70:c8:cc:4a:3d:2c:  
    bd:0a:b7:f8:1d:4a:12:93:ea:22:d5:be:85:69:d7:  
    0b:31:a8:1a:ae:34:c6:f6:e8:a1:c8:cc:02:08:be:  
    bc:2b:e9:34:8f:f2:ee:4a:93:26:a0:47:93:7e:b7:  
    f8:3f:73:24:55:45:02:14:f7:c2:d8:56:f7:a1:cf:  
    2f:2d:3e:d4:ff:05:1a:82:25:34:1f:f2:1a:83:91:  
    a7:35:98:7d:2a:92:53:6b:19:75:91:86:b5:2e:ef:  
    :  
    :
```

3. Exécutez la commande `sethttps` pour activer HTTPS.

```
XSCF> sethttps -c enable  
Continue? [y|n] : y
```

Si le système comporte plusieurs XSCF, les paramètres sont diffusés automatiquement par le XSCF de veille.

3.9 Configuration du réseau XSCF

Cette section décrit comment configurer le réseau XSCF pour ce système.

Les paramètres réseau de XSCF sont les paramètres de l'interface du réseau de XSCF, tels que ceux du XSCF-LAN et du protocole de communication SP à SP (SSCP), les paramètres d'acheminement et les paramètres liés au DNS.

3.9.1 Utilisation de services via le réseau XSCF

Avec une connexion au réseau XSCF, vous pouvez utiliser divers services et informations de serveur par l'intermédiaire du shell XSCF et des interfaces XSCF Web. Pour plus de détails sur chaque service, consultez les sections correspondantes indiquées ci-dessous :

- Fonctionnement du serveur, affichage d'état et modification de configuration (voir [Chapitre 10](#) et [Chapitre 11](#).)
- Service NTP (voir la section [3.6](#).)
- Service Telnet (voir la section [3.7](#).)
- Service SSH (voir la section [3.7](#).)

- Service HTTPS (voir la section [3.8.](#))
- Service SMTP (voir la section [10.2.](#))
- Service SNMP (voir la section [10.3.](#))
- Service de maintenance à distance (voir les *Notes de produit.*)
- Service LDAP (voir la section [3.5.12.](#))
- Service Active Directory (voir la section [3.5.13.](#))
- Service LDAP sur SSL (voir la section [3.5.14.](#))

3.9.2 Compréhension des interfaces du réseau XSCF

Port Ethernet XSCF

Chaque châssis SPARC M12/M10 et chaque boîtier à barre transversale possède deux ports Ethernet XSCF. Ces ports sont nommés XSCF-LAN#0 et XSCF-LAN#1.

Tous les deux utilisent un connecteur RJ-45 prenant en charge 10Base-T/100Base-TX/1000Base-T. Les ports XSCF-LAN sont des ports destinés à une connexion LAN utilisée par l'administrateur système pour effectuer des opérations à l'aide du shell XSCF ou de XSCF Web. Ces opérations comprennent l'affichage d'état du serveur, le fonctionnement d'un domaine et l'affichage d'une console.

Pour vous connecter au réseau XSCF, spécifiez les adresses IP de ces ports Ethernet. Les utilisateurs peuvent procéder à la maintenance ou à la gestion du serveur en utilisant les deux chemins LAN.

Pour un système comprenant plusieurs XSCF, les ports XSCF-LAN des XSCF esclaves ne sont pas utilisés à des fins de maintenance/gestion du serveur. Les ports XSCF-LAN des XSCF esclaves sont connectés au réseau uniquement lorsque le stockage à distance est utilisé. Pour plus de détails sur le stockage à distance, consultez « [4.6 Utilisation du stockage à distance](#) ».

Adresse IP de reprise entre XSCD maître et XSCF de veille

Si le système comporte plusieurs XSCF, les ports XSCF-LAN#0 et XSCF-LAN#1 des XSCF maître et de veille sont respectivement regroupés de sorte qu'une seule adresse IP de reprise (adresse IP virtuelle) puisse être définie ces groupes. En conséquence, même si les châssis comprenant le XSCF maître et le XSCF de veille sont commutés, les utilisateurs n'ont pas besoin de s'inquiéter des adresses IP du XSCF maître et du XSCF de veille. En continuant d'utiliser l'adresse IP de reprise, ils peuvent accéder au XSCF maître même après le basculement.

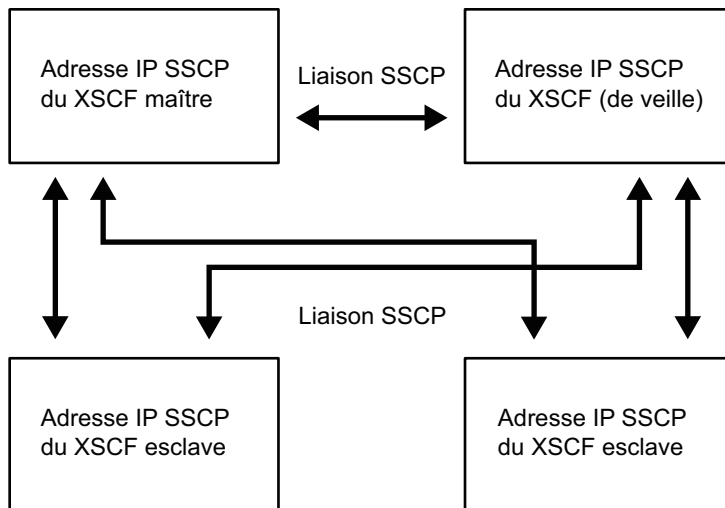
Protocole de communication inter-processeur de service (SSCP)

Si le système comporte plusieurs XSCF, un réseau reliant ces XSCF est configuré. Le protocole de cette interface de réseau reliant les XSCF est appelé protocole de communication inter-processeur de service (SSCP) ou réseau de liaison SSCP. Grâce à ses chemins de communication, les XSCF sont interconnectés, se surveillent mutuellement et échangent des informations sur le système.

[Figure 3-3](#) indique un réseau de liaison SSCP utilisant un système SPARC M12-2S ou

SPARC M10-4S dans la configuration 4BB, avec des châssis directement interconnectés.

Figure 3-3 Réseau de liaison SSCP



Pour configurer le SSCP, les câbles correspondant raccordent le XSCF maître au XSCF de veille, le XSCF maître aux XSCF esclaves et le XSCF de veille aux XSCF esclaves. Pour le raccordement entre le XSCF maître et le XSCF de veille, les ports de contrôle XSCF DUAL sont connectés l'un à l'autre. Le port SSCP destiné à raccorder le XSCF maître ou de veille à chaque esclave est appelé port de contrôle XSCF BB. Les XSCF esclaves ne sont pas interconnectés. Pour les détails sur les connexions de câble pour configurer le SSCP, consultez « Chapitre 4 Réglage du SPARC M12-2S dans une configuration de bloc de construction » dans le *Guide d'installation Fujitsu SPARC M12-2S* ou « Chapitre 4 Configuration des connexions des blocs de construction » dans le *Guide d'installation Fujitsu M10-4S/SPARC M10-4S*.

L'adresse IP de SSCP a été préalablement définie par défaut à la sortie d'usine. Si vous souhaitez définir une adresse IP de SSCP différente, le paramétrage doit être effectué en même temps que les réglages initiaux du système. Pour plus de détails sur les adresses IP de SSCP, consultez « [3.9.5 Compréhension des adresses IP définies avec SSCP](#) ».

3.9.3 Configuration de l'interface réseau XSCF

Cette section décrit les interfaces réseau XSCF suivantes :

- Le réseau de commande du système qui fournit l'accès au XSCF (XSCF-LAN) aux utilisateurs
- Réseau de liaison pour assurer la communication entre XSCF (SSCP) (dans un système comportant plusieurs XSCF)

Dans un système comportant un seul SPARC M12/M10, deux adresses IP sont définies pour le XSCF-LAN afin d'accéder au XSCF. Le XSCF-LAN ne peut utiliser qu'un seul port LAN.

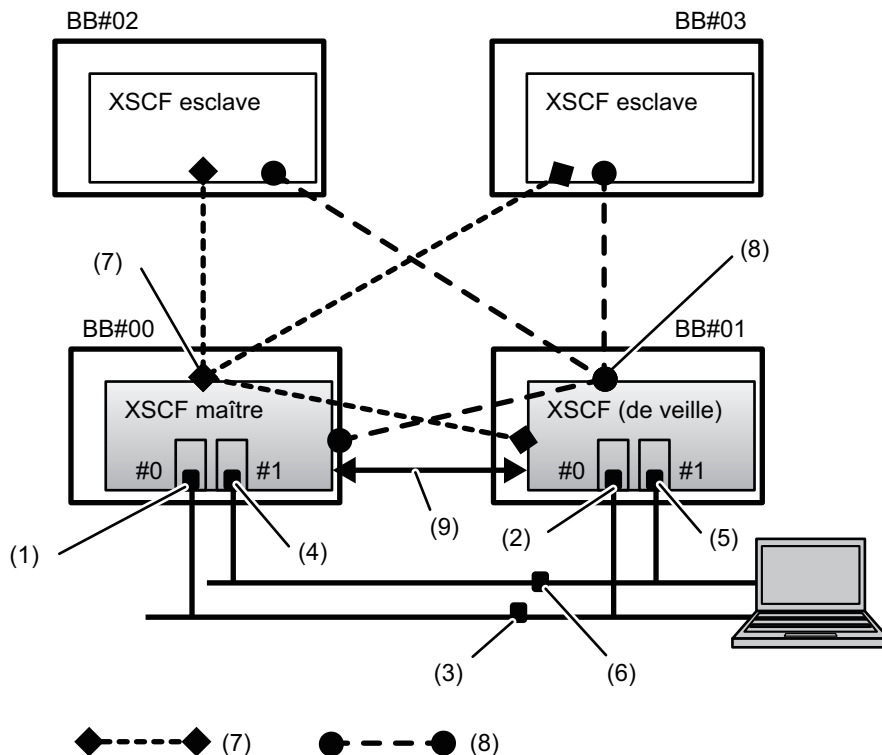
Dans les systèmes SPARC M12-2S comportant quatre châssis ou les systèmes SPARC M10-4S comportant quatre châssis directement connectés, quatre adresses IP sont définies pour le XSCF-LAN, deux comme adresses IP de reprise et 10 pour SSCP, soit un total de 16 adresses IP.

Dans les systèmes SPARC M12-2S comportant 16 châssis ou les systèmes SPARC M10-4S comportant 16 châssis connectés par quatre boîtiers à barre transversale, quatre adresses IP sont définies pour le XSCF-LAN, deux comme adresses IP de reprise et 44 pour SSCP, soit un total de 50 adresses IP.

Remarque : si le système comporte plusieurs XSCF, ceux-ci ne peuvent pas être configurés depuis le XSCF de veille. Les commandes permettant de configurer tous les XSCF sont uniquement exécutées depuis le XSCF maître.

Figure 3-4 présente les interfaces réseau nécessaires pour configurer le réseau XSCF pour un système SPARC M12-2S ou SPARC M10-4S dans une configuration 4BB, comportant des châssis directement interconnectés.

Figure 3-4 Réseau XSCF dans la configuration 4BB

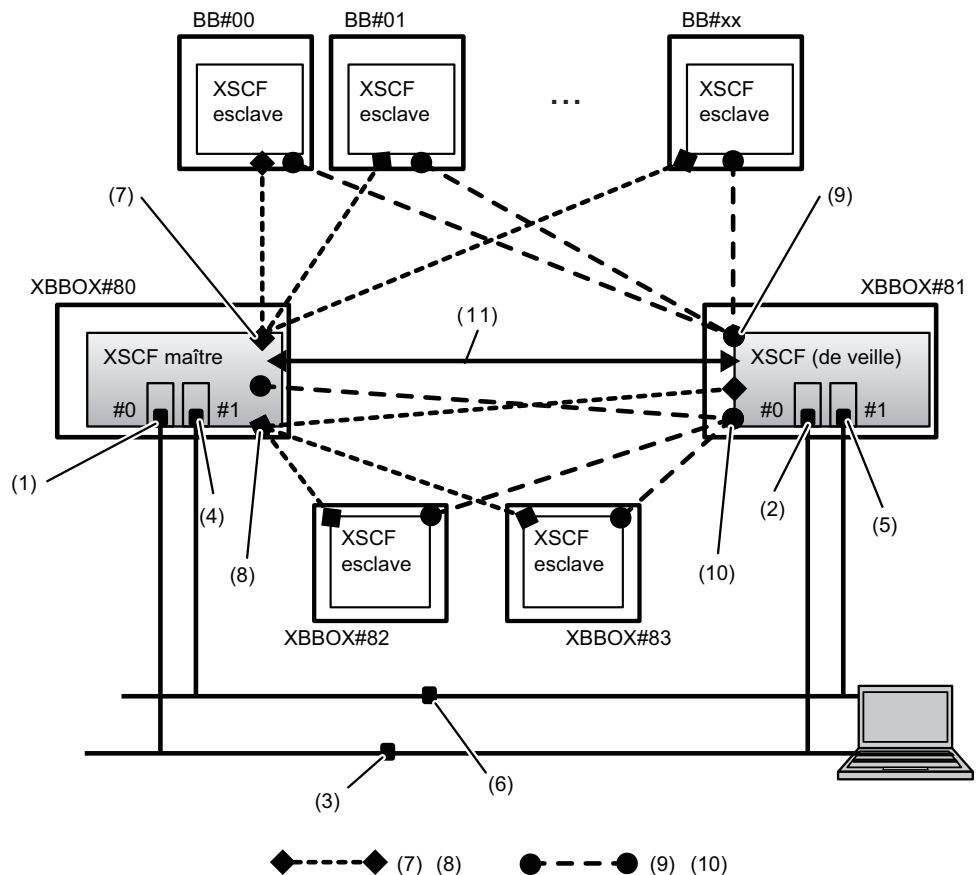


N°	Paramètre de l'adresse	N°	Paramètre de l'adresse
1	Adresse XSCF-LAN#0 (du côté du XSCF maître)	6	Adresse IP de reprise inter-XSCF-LAN#1

N°	Paramètre de l'adresse	N°	Paramètre de l'adresse
2	Adresse XSCF-LAN#0 (du côté du XSCF de veille)	7	Adresse SSCP (XSCF maître et XSCF dans chaque BB#xx) : 4 adresses
3	Adresse IP de reprise inter-XSCF-LAN#0	8	Adresse SSCP (XSCF de veille et XSCF dans chaque BB#xx) : 4 adresses
4	Adresse XSCF-LAN#1 (du côté du XSCF maître)	9	Adresse SSCP pour la duplication (XSCF maître et de veille) : 2 adresses
5	Adresse XSCF-LAN#1 (du côté du XSCF de veille)		

Figure 3-5 présente un exemple des interfaces réseau nécessaires à la configuration du réseau XSCF pour un système SPARC M12-2S ou SPARC M10-4S comportant des boîtiers à barre transversale.

Figure 3-5 Réseau XSCF dans une configuration de système comportant des boîtiers à barre transversale



N°	Paramètre de l'adresse	N°	Paramètre de l'adresse
1	Adresse XSCF-LAN#0 (du côté du XSCF maître)	7	Adresse SSCP (XSCF maître et XSCF dans chaque BB#xx) : 17 adresses
2	Adresse XSCF-LAN#0 (du côté du XSCF de veille)	8	Adresse SSCP (XSCF maître et XSCF dans chaque XBBOX#xx) : 4 adresses
3	Adresse IP de reprise inter-XSCF-LAN#0	9	Adresse SSCP (XSCF de veille et XSCF dans chaque BB#xx) : 17 adresses
4	Adresse XSCF-LAN#1 (du côté du XSCF maître)	10	Adresse SSCP (XSCF de veille et XSCF dans chaque XBBOX#xx) : 4 adresses
5	Adresse XSCF-LAN#1 (du côté du XSCF de veille)	11	Adresse SSCP pour la duplication (XSCF maître et de veille) : 2 adresses
6	Adresse IP de reprise inter-XSCF-LAN#1		

3.9.4 Compréhension des sous-réseaux des groupes de réseaux

Les adresses réseau des adresses IP dans le groupe suivant de connexions réseau XSCF doivent être définies en tant qu'adresses différentes :

- XSCF-LAN#0
- XSCF-LAN#1
- Liaison SSCP entre le XSCF maître et chaque BB
- Liaison SSCP entre le XSCF de veille et chaque BB
- Liaison SSCP entre le XSCF maître et les XSCF de chaque XBBOX
- Liaison SSCP entre le XSCF de veille et les XSCF de chaque XBBOX
- Liaison SSCP entre le XSCF maître et le XSCF de veille (DUAL)

Pour les systèmes SPARC M12-2S ou SPARC M10-4S dans la configuration 4BB, comportant des châssis directement interconnectés, trois types de sous-réseaux sont nécessaires comme adresses de réseau SSCP (identifiant du réseau de liaison SSCP 0-2). Les liaisons SSCP indiquées par les nombres 7, 8 et 9 dans [Figure 3-4](#) doivent être configurées avec différentes adresses IP de sous-réseau.

Un système comportant des boîtiers à barre transversale nécessite jusqu'à cinq types de sous-réseau. (Chaque sous-réseau dispose d'un identifiant de réseau de liaison SSCP compris entre 0 et 4.) Les cinq types de liaisons SSCP indiqués par les nombres 7 à 11 dans [Figure 3-5](#) doivent être configurés avec différentes adresses IP de sous-réseau.

3.9.5

Compréhension des adresses IP définies avec SSCP

Les adresses IP utilisées avec SSCP sont ordonnées et définies dans les groupes suivants. Ces groupes se distinguent par leur identifiant de réseau de liaison SSCP. Au moins deux adresses IP doivent être définies par port SSCP. (Voir [Figure 3-4](#) et [Figure 3-5](#).)

- Groupe constitué du XSCF maître et des XSCF de chaque BB ([Figure 3-4](#), N° 7, [Figure 3-5](#), N° 7)
- Groupe constitué du XSCF de veille et des XSCF de chaque BB ([Figure 3-4](#), N° 8, [Figure 3-5](#), N° 9)
- Groupe constitué du XSCF maître et des XSCF de chaque XBBOX ([Figure 3-5](#), N° 8)
- Groupe constitué du XSCF de veille et des XSCF de chaque XBBOX ([Figure 3-5](#), N° 10)
- Groupe constitué du XSCF maître et du XSCF de veille ([Figure 3-4](#), N° 9, [Figure 3-5](#), N° 11)

Le système SPARC M12-1/M12-2/M10-1/M10-4 dans une configuration ne comportant qu'un XSCF ne possède pas de paramètres SSCP.

[Tableau 3-21](#) répertorie l'emplacement, la quantité, l'identifiant et la valeur par défaut d'adresse IP de chaque adresse IP de SSCP définie pour un système SPARC M12-2S ou SPARC M10-4S dans la configuration 4BB, comportant des châssis directement interconnectés. Exécutez la commande showsscp pour vérifier les adresses IP actuellement définies.

Tableau 3-21 Adresses IP de SSCP (dans la configuration 4BB)

Emplacement	Quantité	Liaison SSCP Identifiant de réseau	Adresse IP par défaut
<u>Connexion entre le XSCF maître et les XSCF de chaque BB#xx</u>	4	0	
BB#00 (maître)			169.254.1.1
BB#01			169.254.1.2
BB#02			169.254.1.3
BB#03			169.254.1.4
<u>Connexion entre le XSCF de veille et chaque BB#xx</u>	4	1	
BB#00			169.254.1.9
BB#01 (veille)			169.254.1.10
BB#02			169.254.1.11
BB#03			169.254.1.12

Tableau 3-21 Adresses IP de SSCP (dans la configuration 4BB) (*suite*)

Emplacement	Quantité	Liaison SSCP Identifiant de réseau	Adresse IP par défaut
<u>Connexion pour duplication entre le XSCF maître et le XSCF de veille</u>	2	2	
BB#00 (maître)			169.254.1.17
BB#01 (veille)			169.254.1.18
Total	10		

[Tableau 3-22](#) répertorie l'emplacement, la quantité, l'identifiant et la valeur par défaut d'adresse IP de chaque adresse IP de SSCP définie pour un système SPARC M12-2S ou SPARC M10-4S dans la configuration maximale (configuration de 16BB et 4-XBBOX).

Tableau 3-22 Adresse IP de SSCP (dans la configuration à 16BB et 4-XBBOX)

Emplacement	Quantité	Liaison SSCP Identifiant de réseau	Adresse IP par défaut
<u>Connexion entre le XSCF maître et les XSCF de chaque BB#xx</u>	17	0	
XBBOX#80 (maître)			169.254.1.1
De BB#00 à BB#15			169.254.1.2 à 169.254.1.17
<u>Connexion entre le XSCF de veille et les XSCF de chaque BB#xx</u>	17	1	
XBBOX#81 (veille)			169.254.1.33
De BB#00 à BB#15			169.254.1.34 à 169.254.1.49
<u>Connexion entre le XSCF maître et les XSCF de chaque XBBOX#xx</u>	4	2	
XBBOX#80 (maître)			169.254.1.65
XBBOX#81			169.254.1.66
XBBOX#82			169.254.1.67
XBBOX#83			169.254.1.68
<u>Connexion entre le XSCF de veille et les XSCF de chaque XBBOX#xx</u>	4	3	
XBBOX#80			169.254.1.73
XBBOX#81 (veille)			169.254.1.74
XBBOX#82			169.254.1.75
XBBOX#83			169.254.1.76
<u>Connexion pour duplication entre le XSCF maître et le XSCF de veille</u>	2	4	
XBBOX#80 (maître)			169.254.1.81
XBBOX#81 (veille)			169.254.1.82
Total	44		

3.9.6 Vérification des éléments de réglage et des commandes liés au réseau XSCF

Tableau 3-23 répertorie les éléments de réglage liés au réseau XSCF et les commandes du shell XSCF correspondantes.

Un redémarrage du XSCF est nécessaire pour parachever la configuration du réseau. Utilisez la commande `rebootxscf` pour redémarrer le XSCF. Le redémarrage du XSCF

interrompt la session XSCF, aussi, connectez-vous de nouveau au XSCF.

Tableau 3-23 Éléments de réglage liés au compte d'utilisateur XSCF

Élément de réglage	Paramétrage requis ou optionnel	Commande liée
Adresse IP du réseau XSCF - XSCF-LAN - Adresse IP de reprise - SSCP	Requis	setnetwork(8), shownetwork(8) setsscp(8), showsscp(8)
Activation/désactivation du réseau	Optionnel	setnetwork(8), shownetwork(8)
Masque de réseau	Requis	setnetwork(8), shownetwork(8) setsscp(8), showsscp(8)
Nom d'hôte / Nom de domaine	Optionnel	sethostname(8), showhostname(8)
Ajout/suppression d'un accès au réseau - Adresse IP de destination - Passerelle - Masque de réseau	Requis	setroute(8), showroute(8)
Ajout/suppression d'un DNS - Serveur de noms - Chemin de recherche	Optionnel	setnameserver(8), shownameserver(8)
Règle de filtrage du paquet IP	Optionnel	setpacketfilters(8), showpacketfilters(8)
Application au réseau	Requis	applynetwork(8)

3.9.7 Flux de configuration du réseau XSCF

Cette section décrit la procédure de configuration du réseau XSCF. Les références aux procédures détaillées sont présentées dans ces étapes.

1. Définissez une adresse IP Ethernet (XSCF-LAN) (adresse IP physique).

Deux ports XSCF-LAN peuvent être utilisés en fonction de la configuration du réseau.

Dans les systèmes comportant un seul XSCF, paramétrez soit l'une soit les deux adresses IP suivantes :

- XSCF-LAN#0 de BB#00 (XSCF maître)
- XSCF-LAN#1 de BB#00 (XSCF maître)

Dans les systèmes comportant plusieurs XSCF, commencez par définir chaque adresse IP de XSCF-LAN du côté du XSCF maître, puis définissez l'adresse IP de XSCF-LAN du côté du XSCF de veille (voir [shownetwork\(8\)](#), [setnetwork\(8\)](#), et [3.9.8](#)).

Pour pouvoir connecter l'un des XSCF en cas de panne de XSCF, définissez la même adresse de réseau pour les ports LAN avec le même numéro sur chaque XSCF.

Différentes adresses de réseau doivent être définies pour les adresses IP de XSCF-LAN#0 et XSCF-LAN#1.

2. **Si le système comporte plusieurs XSCF, définissez l'adresse IP de reprise (adresse IP virtuelle).**

Le paramétrage d'une adresse IP de reprise permet la reprise de l'adresse IP après une commutation entre XSCF maître et XSCF de veille dans le cas d'une panne de XSCF. Les utilisateurs peuvent toujours se connecter au XSCF maître en accédant à l'adresse IP de reprise sans devoir prendre en compte le basculement de XSCF.

Une fois les adresses IP respectives de XSCF-LAN#0 et XSCF-LAN#1 paramétrées, définissez une adresse IP de reprise pour les ports LAN respectifs de ces derniers, qui sont redondants (voir `shownetwork(8)`, `setnetwork(8)`, and [3.9.9](#)).

3. **Si le système comporte plusieurs XSCF, spécifiez les adresses IP de SSCP.**

SSCP est utilisé dans les réseaux pour communiquer entre XSCF dupliqués, aussi les paramètres d'adresse IP sont-ils nécessaires. La valeur de l'adresse IP de SSCP a été définie auparavant à la sortie d'usine (voir [Tableau 3-21](#) et [Tableau 3-22](#)).

Si les paramètres d'adresse IP de XSCF-LAN sont à l'origine de conflits avec les adresse de réseau par défaut de SSCP, les adresses IP de SSCP doivent être redéfinies. Les adresses IP de SSCP doivent être des adresses au sein d'un même réseau d'un même groupe ou des adresse de réseau différentes extérieures au groupe. Pour plus de détails sur les sous-réseaux, consultez « [3.9.4 Compréhension des sous-réseaux des groupes de réseaux](#) ». Les utilisateurs ne peuvent pas accéder au réseau SSCP (voir `showsscp(8)`, `setsscp(8)` et [3.9.10](#)).

4. **Paramétrez le nom d'hôte, l'accès et DNS.**

Dans les systèmes comportant plusieurs XSCF, commencez par paramétrer le nom d'hôte et l'accès du côté du XSCF maître, puis définissez-les du côté du XSCF de veille (voir `showhostname(8)`, `sethostname(8)`, `showroute(8)`, `setroute(8)`, `shownameserver(8)`, `setnameserver(8)`, [3.9.11](#), [3.9.12](#) et [3.9.13](#)).

5. **Définissez des règles de filtrage de paquets IP.**

Définissez des règles de filtrage de paquets IP pour le XSCF-LAN (voir `showpacketfilters(8)`, `setpacketfilters(8)` et [3.9.14](#)).

Pour les paramètres de connexion d'un stockage à distance à un XSCF esclave, consultez « [4.6.10 Configuration du XSCF-LAN utilisé avec le stockage à distance](#) ».

6. **Appliquez les paramètres du réseau.**

Pour parachever la configuration du réseau, les paramètres doivent être diffusés et le XSCF redémarré. Le redémarrage du XSCF interrompt la session XSCF, aussi, identifiez-vous de nouveau (voir `applynetwork(8)`, `rebootxscf(8)` et [3.9.15](#)).

Remarque : si un redémarrage ou une panne de XSCF se produit durant l'exécution d'une commande de paramétrage concernant tous les XSCF, il se peut que la configuration ne s'achève pas correctement. Connectez-vous de nouveau au XSCF maître, puis vérifiez si les paramètres sont corrects. S'ils sont incorrects, effectuez de nouveau la configuration.

3.9.8 Activation/Désactivation du réseau XSCF et réglage des adresses IP de XSCF-LAN et des masques de réseau

Pour vérifier les informations relatives à l'interface réseau définies pour le XSCF, utilisez la commande `shownetwork`. En outre, pour configurer l'interface réseau utilisée par le XSCF, utilisez la commande `setnetwork`. Exécutez la commande `setnetwork` avec un compte d'utilisateur disposant du privilège `platadm`.

1. **Exécutez la commande `shownetwork` pour afficher les informations sur la totalité des interfaces réseau XSCF.**

```
XSCF> shownetwork -a
bb#00-lan#0
    Link encap:Ethernet HWaddr 00:00:00:12:34:56
    inet addr: 192.168.11.10 Bcast: 192.168.11.255 Mask:255.255.255.0
    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
    RX packets:54424 errors:0 dropped:0 overruns:0 frame:0
    TX packets:14369 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:12241827 (11.3 MiB) TX bytes:1189769 (0.9 MiB)
    Base address:0x1000
lan#0
    Link encap:Ethernet HWaddr 00:00:00:12:34:56
    inet addr:192.168.11.11 Bcast:192.168.11.255 Mask:255.255.255.0
    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
    Base address:0xe000
bb#00-lan#1
:
```

2. **Affichez les informations sur XSCF-LAN#0 ou XSCF-LAN#1.**

Dans l'exemple suivant, les informations d'interface réseau de XSCF-LAN#1 pour BB#00 (XSCF maître) sont affichées.

```
XSCF> shownetwork bb#00-lan#1
bb#00-lan#1
    Link encap:Ethernet HWaddr 00:00:00:12:34:57
    inet addr:192.168.10.10 Bcast: 192.168.10.255 Mask:255.255.255.0
    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
    RX packets:54424 errors:0 dropped:0 overruns:0 frame:0
    TX packets:14369 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:20241827 (19.3 MiB) TX bytes:2089769 (1.9 MiB)
    Base address:0x1000
```

3. **Exécutez la commande `setnetwork` en spécifiant les informations d'interface réseau.**

Dans l'exemple suivant, l'adresse IP est définie comme 192.168.1.10 et le masque de réseau comme 255.255.255.0 pour XSCF-LAN#0 de BB#00 afin d'activer le XSCF-LAN.

```
XSCF> setnetwork bb#00-lan#0 -m 255.255.255.0 192.168.1.10
```

Dans l'exemple suivant, XSCF-LAN#1 de BB#00 est désactivé.

```
XSCF> setnetwork bb#00-lan#1 -c down
```

Dans l'exemple suivant, le masque de réseau et l'adresse IP définie pour XSCF-LAN#1 de BB#00 sont supprimés.

```
XSCF> setnetwork -r bb#00-lan#1
You specified '-r' interface remove option.
So, we delete routing information that interface corresponds.
Continue? [y|n] :y
If you choose 'y'es, you must execute 'applynetwork' command for application.
Or you choose 'y'es, but you don't want to apply, you execute 'rebootxscf' for
reboot.
```

4. Exécutez les commandes **applynetwork** et **rebootxscf** pour diffuser les réglages opérés pour l'interface réseau XSCF.

Remarque : vous pouvez également diffuser l'adresse IP de reprise, l'adresse IP de SSCP, le nom d'hôte XSCF, le nom de domaine XSCF, l'accès au XSCF, DNS pour le XSCF et les autres paramètres définis en exécutant les commandes **applynetwork** et **rebootxscf**.

```
XSCF> applynetwork
The following network settings will be applied:
bb#00 hostname      :hostname-0
bb#01 hostname      :hostname-1
DNS domain name     :example.com
nameserver          :10.23.4.3

interface           :bb#00-lan#0
status              :up
IP address          :10.24.144.214
netmask             :255.255.255.0
route               : -n 0.0.0.0 -m 0.0.0.0 -g 10.24.144.1
(Omis)
XSCF> rebootxscf -a
The XSCF will be reset. Continue? [y|n] :y
```

Le redémarrage du XSCF interrompt la session XSCF, aussi, identifiez-vous à nouveau.

5. Exécutez la commande **shownetwork**, puis vérifiez les informations d'interface réseau de XSCF.

3.9.9 Réglage de l'adresse IP de reprise

Afin de définir une adresse IP de reprise (adresse IP virtuelle) pour le XSCF maître et le XSCF de veille, utilisez la commande `setnetwork`.

1. **Exécutez la commande `shownetwork` pour afficher les informations sur la totalité des interfaces réseau XSCF.**

```
XSCF> shownetwork -a
```

2. **Affichez les informations relatives à l'adresse IP de reprise de XSCF-LAN#0 ou XSCF-LAN#1.**

Dans l'exemple suivant, les informations relatives à l'adresse IP de reprise de XSCF-LAN#0 sont affichées.

```
XSCF> shownetwork lan#0
lan#0 Link encap:Ethernet HWaddr 00:00:00:12:34:56
inet addr:192.168.1.10 Bcast:192.168.1.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
Base address:0xe000
```

3. **Paramétrez les informations relatives à l'adresse IP de reprise de XSCF-LAN#0 ou XSCF-LAN#1.**

Dans l'exemple suivant, l'adresse IP de reprise est définie comme 192.168.11.10 et le masque de réseau comme 255.255.255.0 pour XSCF-LAN#0.

```
XSCF> setnetwork lan#0 -m 255.255.255.0 192.168.11.10
```

4. **Exécutez les commandes `applynetwork` et `rebootxscf` pour diffuser les réglages opérés pour l'interface réseau XSCF.**

Remarque : vous pouvez également diffuser l'adresse IP de SSCP, le nom d'hôte XSCF, le nom de domaine XSCF, l'accès au XSCF, DNS pour le XSCF et les autres paramètres définis en exécutant les commandes `applynetwork` et `rebootxscf`.

```
XSCF> applynetwork
The following network settings will be applied:
bb#00 hostname      :hostname-0
bb#01 hostname      :hostname-1
DNS domain name     :example.com
nameserver           :10.23.4.3

interface            :bb#00-lan#0
status               :up
IP address           :10.24.144.214
netmask              :255.255.255.0
```

```

route                : -n 0.0.0.0 -m 0.0.0.0 -g 10.24.144.1
(Omis)
XSCF> rebootxscf -a
The XSCF will be reset. Continue? [y|n] :y

```

Le redémarrage du XSCF interrompt la session XSCF, aussi, identifiez-vous à nouveau.

5. **Exécutez la commande `shownetwork`, puis vérifiez les informations d'interface réseau de XSCF.**

3.9.10 Définition d'une adresse IP de SSCP

Afin de vérifier l'adresse IP attribuée au protocole de communication inter-processeur de service (SSCP), utilisez la commande `showsscp`. La commande `setsscp` est utilisée pour configurer l'adresse IP de SSCP. Exécutez la commande `setsscp` avec un compte d'utilisateur disposant du privilège `platadm` ou `fieldeng`.

1. **Exécutez la commande `shownetwork` pour afficher les informations sur la totalité des interfaces réseau XSCF.**

```

XSCF> shownetwork -a

```

2. **Exécutez la commande `showsscp` pour afficher les informations relatives à l'adresse de SSCP.**

Dans l'exemple suivant, les informations concernant toutes les adresses de SSCP d'un système SPARC M10-4S dans la configuration 4BB, comportant des châssis directement interconnectés, sont affichées.

```

XSCF> showsscp -a
SSCP network ID:0 address 169.254.1.0
SSCP network ID:0 netmask 255.255.255.248
Location Address
-----
bb#00-if#0 169.254.1.1
bb#01-if#0 169.254.1.2
bb#02-if#0 169.254.1.3
bb#03-if#0 169.254.1.4
SSCP network ID:1 address 169.254.1.8
SSCP network ID:1 netmask 255.255.255.248
Location Address
-----
bb#00-if#1 169.254.1.9
bb#01-if#1 169.254.1.10
bb#02-if#1 169.254.1.11
bb#03-if#1 169.254.1.12
SSCP network ID:2 address 169.254.1.16
SSCP network ID:2 netmask 255.255.255.252
Location Address
-----

```



```
bb#00-if#2 169.254.1.17
bb#01-if#2 169.254.1.18
```

Dans l'exemple suivant, les informations définies pour le XSCF maître disposant de l'identifiant de réseau SSCP 0 dans BB#00 sont affichées.

```
XSCF> showsscp -b 0 -N 0
SSCP network ID:0 address 169.254.1.0
SSCP network ID:0 netmask 255.255.255.248

Location Address
-----
bb#00-if#0 169.254.1.1
```

Dans l'exemple suivant, les informations de SSCP définies du côté du XSCF de veille sont affichées.

```
XSCF> showsscp -b 1 -N 1
SSCP network ID:1 address 169.254.1.8
SSCP network ID:1 netmask 255.255.255.248

Location Address
-----
bb#01-if#1 169.254.1.10
```

Dans l'exemple suivant, les informations paramétrées pour la liaison SSCP destinée à la duplication des XSCF maître et de veille sont affichées.

```
XSCF> showsscp -N 2
SSCP network ID:2 address 169.254.1.16
SSCP network ID:2 netmask 255.255.255.252

Location Address
-----
bb#00-if#2 169.254.1.17
bb#01-if#2 169.254.1.18
```

3. Définissez l'adresse IP de SSCP (lorsque le paramétrage est requis).

L'adresse IP utilisée dans le réseau SSCP est définie comme valeur par défaut. Cependant, lorsque l'adresse IP de XSCF-LAN et l'adresse de réseau de l'adresse IP par défaut de SSCP sont les mêmes, modifiez l'adresse IP de SSCP à l'aide de la commande setsscp. Dans l'exemple suivant, les adresses SSCP et les masques de réseau du réseau de liaison SSCP sont paramétrés en mode interactif pour un système SPARC M12-2S ou SPARC M10-4S dans la configuration 4BB, comportant des châssis directement interconnectés.

```
XSCF> setsscp
How many BB[4] > 4
SSCP network ID:0 address [169.254.1.0] > 10.1.1.0
```

```

SSCP network ID:0 netmask [255.255.255.248] > 255.255.255.0
bb#00-if#0 address [10.1.1.1 ] >
bb#01-if#0 address [10.1.1.2 ] >
bb#02-if#0 address [10.1.1.3 ] >
bb#03-if#0 address [10.1.1.4 ] >

SSCP network ID:1 address [169.254.1.8 ] > 10.2.1.0
SSCP network ID:1 netmask [255.255.255.248] > 255.255.255.0
bb#00-if#1 address [10.2.1.1 ] >
bb#01-if#1 address [10.2.1.2 ] >
bb#02-if#1 address [10.2.1.3 ] >
bb#03-if#1 address [10.2.1.4 ] >

SSCP network ID:2 address [169.254.1.16 ] >
SSCP network ID:2 netmask [255.255.255.252] >
bb#00-if#2 address [169.254.1.17 ] >
bb#01-if#2 address [169.254.1.18 ] >

```

4. **Exécutez les commandes `applynetwork` et `rebootxscf` afin de diffuser les réglages opérés pour les adresse IP et les masques de réseau.**

Remarque : vous pouvez également diffuser le nom d'hôte XSCF, le nom de domaine XSCF, l'accès au XSCF, DNS pour le XSCF et les autres paramètres définis en exécutant les commandes `applynetwork` et `rebootxscf`.

```

XSCF> applynetwork
The following network settings will be applied:
bb#00 hostname      :hostname-0
bb#01 hostname      :hostname-1
DNS domain name     :example.com
nameserver           :10.23.4.3

interface           :bb#00-lan#0
status               :up
IP address           :10.24.144.214
netmask              :255.255.255.0
route                : -n 0.0.0.0 -m 0.0.0.0 -g 10.24.144.1
(Omis)
XSCF> rebootxscf -a
The XSCF will be reset. Continue? [y|n] :y

```

Le redémarrage du XSCF interrompt la session XSCF, aussi, identifiez-vous à nouveau.

5. **Exécutez la commande `showsscp`, puis vérifiez les informations relatives à l'adresse de SSCP.**

3.9.11

Définition d'un nom d'hôte et d'un nom de domaine XSCF

Afin de vérifier les noms d'hôte définis pour les châssis du XSCF maître et du XSCF de veille, utilisez la commande `showhostname`. En outre, afin de paramétrer les noms d'hôte et de domaine pour les châssis du XSCF maître et du XSCF de veille, utilisez la commande `sethostname`. Exécutez la commande `sethostname` avec un compte d'utilisateur disposant du privilège `platadm`.

1. **Exécutez la commande `showhostname` pour afficher les noms d'hôte.**

```
XSCF> showhostname -a
bb#00: scf-hostname0.example.com
bb#01: scf-hostname1.example.com
```

2. **Exécutez la commande `sethostname` pour paramétrer un nom d'hôte.**

Dans l'exemple suivant, le nom d'hôte défini pour BB#00 est `scf0-hostname`.

```
XSCF> sethostname bb#00 scf0-hostname
```

Dans l'exemple suivant, le nom de domaine défini pour le XSCF maître et le XSCF de veille est `example.com`.

```
XSCF> sethostname -d example.com
```

3. **Exécutez la commande `sethostname`, puis les commandes `applynetwork` et `rebootxscf` pour diffuser les paramètres définis pour les noms d'hôte et de domaine.**

Remarque : vous pouvez également diffuser l'accès au XSCF, DNS pour le XSCF et les autres paramètres définis en exécutant les commandes `applynetwork` et `rebootxscf`.

```
XSCF> applynetwork
The following network settings will be applied:
bb#00 hostname      :hostname-0
bb#01 hostname      :hostname-1
DNS domain name     :example.com
nameserver           :10.23.4.3

interface            :bb#00-lan#0
status               :up
IP address           :10.24.144.214
netmask              :255.255.255.0
route                : -n 0.0.0.0 -m 0.0.0.0 -g 10.24.144.1
(Omis)
XSCF> rebootxscf -a
```

Le redémarrage du XSCF interrompt la session XSCF, aussi, identifiez-vous à nouveau.

4. **Exécutez la commande showhostname, puis vérifiez les noms d'hôte et de groupe.**

3.9.12 Réglage de l'acheminement du XSCF

Cette section présente un exemple de données d'acheminement par un sous-réseau dans un système comportant plusieurs XSCF.

- Configuration d'une passerelle par défaut

XSCF de BB#00		XSCF de BB#01	
bb#00-lan#0	+-----+	bb#01-lan#0	
[192.168.11.10]		[192.168.11.20]	
bb#00-lan#1	+-----+	bb#01-lan#1	
[10.12.108.10]		[10.12.108.20]	
Destination	Passerelle	Masque réseau	Interface
[192.168.11.0]	-	[255.255.255.0]	bb#00-lan#0
[192.168.11.0]	-	[255.255.255.0]	bb#01-lan#0
[10.12.108.0]	-	[255.255.255.0]	bb#00-lan#1
[default]	[10.12.108.1]	[0.0.0.0]	bb#00-lan#1
[10.12.108.0]	-	[255.255.255.0]	bb#01-lan#1
[default]	[10.12.108.1]	[0.0.0.0]	bb#01-lan#1

Remarque : la façon dont l'accès de chaque interface du XSCF est déterminé varie en fonction de l'environnement du réseau et de l'emplacement d'installation. L'environnement du réseau doit être configuré de manière adaptée pour le fonctionnement du système.

Remarque : aucun paramètre d'acheminement ne peut être défini pour une adresse IP de reprise.

- Configuration de deux passerelles par défaut

XSCF de BB#00

bb#00-lan#0 +-----+
[192.168.11.10]

bb#00-lan#1 +-----+
[10.12.108.10]

XSCF de BB#01

bb#01-lan#0
[192.168.11.20]

bb#01-lan#1
[10.12.108.20]

Destination	Passerelle	Masque réseau	Interface
[192.168.11.0]	-	[255.255.255.0]	bb#00-lan#0
[default]	[192.168.11.1]	[0.0.0.0]	bb#00-lan#0
[192.168.11.0]	-	[255.255.255.0]	bb#01-lan#0
[default]	[192.168.11.1]	[0.0.0.0]	bb#01-lan#0
[10.12.108.0]	-	[255.255.255.0]	bb#00-lan#1
[default]	[10.12.108.1]	[0.0.0.0]	bb#00-lan#1
[10.12.108.0]	-	[255.255.255.0]	bb#01-lan#1
[default]	[10.12.108.1]	[0.0.0.0]	bb#01-lan#1

Remarque : si deux passerelles par défaut sont configurées, l'une des deux est automatiquement sélectionnée. Dans ses paramètres, le réseau doit être configuré de telle sorte que les passerelles puissent fonctionner correctement comme passerelle par défaut.

Utilisez la commande `showroute` pour vérifier les informations d'acheminement d'un réseau XSCF. En outre, pour configurer les informations d'acheminement, utilisez la commande `setroute`. Exécutez la commande `setroute` avec un compte d'utilisateur disposant du privilège `platadm`.

Procédure de fonctionnement

1. **Exécutez la commande `showroute` pour afficher l'environnement d'acheminement.**

XSCF> showroute -a				
Destination	Gateway	Netmask	Flags	Interface
192.168.11.0	*	255.255.255.0	U	bb#00-lan#0
10.12.108.0	*	255.255.255.0	U	bb#00-lan#1
default	10.12.108.1	0.0.0.0	UG	bb#00-lan#1
Destination	Gateway	Netmask	Interface	
192.168.11.0	*	255.255.255.0	bb#01-lan#0	
10.12.108.0	*	255.255.255.0	bb#01-lan#1	
default	10.12.108.1	0.0.0.0	bb#01-lan#1	

2. **Exécutez la commande `setroute` en spécifiant l'environnement d'acheminement de l'interface réseau.**

Dans l'exemple suivant, l'accès défini comme la destination 192.168.11.0 et le

masque de réseau défini comme 255.255.255.0 pour XSCF-LAN#0 de BB#00 sont ajoutés.

```
XSCF> setroute -c add -n 192.168.11.0 -m 255.255.255.0 bb#00-lan#0
```

Dans l'exemple suivant, l'accès défini comme la passerelle par défaut 10.12.108.1 pour XSCF-LAN#1 de BB#00 est ajouté.

```
XSCF> setroute -c add -n 0.0.0.0 -g 10.12.108.1 bb#00-lan#1
```

Dans l'exemple suivant, l'accès défini comme la destination 192.168.11.0 pour XSCF-LAN#0 de BB#00 est supprimé.

```
XSCF> setroute -c del -n 192.168.11.0 bb#00-lan#0
```

Dans l'exemple suivant, l'accès défini comme la destination 192.168.1.0 et le masque de réseau défini comme 255.255.255.0 pour XSCF-LAN#0 de BB#00 sont supprimés.

```
XSCF> setroute -c del -n 192.168.1.0 -m 255.255.255.0 bb#00-lan#0
```

Dans l'exemple suivant, l'accès défini comme la passerelle par défaut 10.12.108.1 pour XSCF-LAN#1 de BB#00 est supprimé.

```
XSCF> setroute -c del -n 0.0.0.0 -g 10.12.108.1 bb#00-lan#1
```

3. Exécutez les commandes `applynetwork` et `rebootxscf` pour diffuser les réglages opérés à l'aide de la commande `setroute`.

Remarque : vous pouvez également diffuser DNS pour le XSCF et les autres paramètres définis en exécutant les commandes `applynetwork` et `rebootxscf`.

```
XSCF> applynetwork
The following network settings will be applied:
bb#00 hostname      :hostname-0
bb#01 hostname      :hostname-1
DNS domain name     :example.com
nameserver           :10.23.4.3

interface            :bb#00-lan#0
status               :up
IP address            :10.24.144.214
netmask               :255.255.255.0
route                 : -n 0.0.0.0 -m 0.0.0.0 -g 10.24.144.1
(Omis)
XSCF> rebootxscf -a
```

```
The XSCF will be reset. Continue? [y|n] :y
```

Le redémarrage du XSCF interrompt la session XSCF, aussi, identifiez-vous à nouveau.

4. **Exécutez la commande `showroute`, puis vérifiez les paramètres d'acheminement.**

3.9.13 Paramétrage de DNS pour le XSCF

Utilisez la commande `shownameserver` pour vérifier le serveur de noms et le chemin de recherche utilisés par le réseau XSCF. En outre, pour paramétrer le serveur de noms et le chemin de recherche, utilisez la commande `setnameserver`. Exécutez la commande `setnameserver` avec un compte d'utilisateur disposant du privilège `platadm`. Lorsque vous spécifiez un chemin de recherche, vous devez également paramétrer un serveur de noms.

1. **Exécutez la commande `shownameserver` pour afficher les serveurs de noms et les chemins de recherche.**

Si plusieurs serveurs de noms et chemins de recherche sont enregistrés, ils apparaissent chacun sur une ligne distincte.

Dans l'exemple suivant, trois serveurs de nom et un chemin de recherche enregistrés sont vérifiés et trouvés.

```
XSCF> shownameserver
nameserver 10.0.0.2
nameserver 172.16.0.2
nameserver 192.168.0.2
search      sub.example.com
```

Dans l'exemple suivant, aucun serveur de nom ni chemin de recherche enregistré n'est vérifié et trouvé.

```
XSCF> shownameserver
nameserver ---
search      ---
```

2. **Exécutez la commande `setnameserver` en spécifiant un serveur de noms et un chemin de recherche.**

Dans l'exemple suivant, trois adresses IP sont ajoutées en tant que serveurs de noms : 10.0.0.2, 172.16.0.2, et 192.168.0.2.

```
XSCF> setnameserver 10.0.0.2 172.16.0.2 192.168.0.2
```

Dans l'exemple suivant, tous les serveurs de noms paramétrés sont supprimés.

```
XSCF> setnameserver -c del -a
```

Dans l'exemple suivant, deux des trois paramètres dupliques d'un serveur DNS enregistré sont supprimés.

```
XSCF> shownameserver
nameserver 10.24.1.2
nameserver 10.24.1.2
nameserver 10.24.1.2
XSCF> setnameserver -c del 10.24.1.2 10.24.1.2
XSCF> shownameserver
nameserver 10.24.1.2
```

Dans l'exemple suivant, un nom de domaine, sub.example.com, est ajouté comme chemin de recherche.

```
XSCF> setnameserver -c addsearch sub.example.com
```

Dans l'exemple suivant, tous les chemins de recherche paramétrés sont supprimés.

```
XSCF> setnameserver -c delsearch -a
```

3. **Exécutez les commandes `applynetwork` et `rebootxscf` pour diffuser les réglages opérés sur les serveurs de noms et les chemins de recherche à l'aide de la commande `setnameserver`.**

```
XSCF> applynetwork
The following network settings will be applied:
bb#00 hostname      :hostname-0
bb#01 hostname      :hostname-1
DNS domain name     :example.com
nameserver           :10.23.4.3

interface            :bb#00-lan#0
status               :up
IP address           :10.24.144.214
netmask              :255.255.255.0
route                : -n 0.0.0.0 -m 0.0.0.0 -g 10.24.144.1
(Omis)
XSCF> rebootxscf -a
The XSCF will be reset. Continue? [y|n] :y
```

Le redémarrage du XSCF interrompt la session XSCF, aussi, identifiez-vous à nouveau.

4. **Exécutez la commande `showroute`, puis vérifiez les paramètres d'acheminement.**

3.9.14

Réglage des règles de filtrage des paquets IP pour le réseau XSCF

Afin de vérifier les règles de filtrage des paquets IP définies pour le réseau XSCF, utilisez la commande `showpacketfilters`. En outre, pour définir les règles de filtrage des paquets IP, utilisez la commande `setpacketfilters`. Exécutez la commande `setpacketfilters` avec un compte d'utilisateur disposant du privilège `platadm` ou `fieldeng`.

Vous ne pouvez définir les règles de filtrage des paquets IP pour le réseau XSCF que pour les paquets entrants. Aucune règle comparable ne peut être définie pour les paquets sortants.

1. **Exécutez la commande `showpacketfilters` afin d'afficher les règles de filtrage des paquets IP pour le XSCF-LAN.**

Dans l'exemple suivant, les règles de filtrage des paquets IP définies pour le réseau XSCF sont affichées.

```
XSCF> showpacketfilters -a
-i bb#00-lan#0 -j ACCEPT
-i bb#01-lan#1 -j ACCEPT
-s 173.16.0.0/255.255.0.0 -j ACCEPT
-s 205.168.148.100/255.255.255.255 -j ACCEPT
```

Dans l'exemple suivant, les règles de filtrage des paquets IP appliquées sont affichées.

```
XSCF> showpacketfilters -l
pkts  bytes target    prot  in          source
124   102K ACCEPT    all  bb#00-lan#0 0.0.0.0/0.0.0.0
0      0 ACCEPT    all  bb#00-lan#1 0.0.0.0/0.0.0.0
0      0 ACCEPT    all  *           173.16.0.0/255.255.0.0
0      0 ACCEPT    all  *           205.168.148.100
```

L'exemple suivant montre qu'aucune règle de filtrage des paquets IP n'a été définie.

```
XSCF> showpacketfilters -a
XSCF>
```

2. **Exécutez la commande `setpacketfilters` pour définir une règle de filtrage des paquets IP.**

Parmi les règles de filtrage des paquets IP, l'ordre de priorité suit l'ordre dans lequel elles ont été définies.

Dans l'exemple suivant, les paquets sont autorisés à passer par les adresses IP 192.168.100.0/255.255.255.0.

```
XSCF> setpacketfilters -y -c add -i bb#00-lan#0 -s
192.168.100.0/255.255.255.0 -j ACCEPT
-s 192.168.100.0/255.255.255.0 -i bb#00-lan#0 -j ACCEPT
NOTE: applied IP packet filtering rules.
Continue? [y|n] :y
```

Dans l'exemple suivant, les paquets sont autorisés à passer par les adresses IP 192.168.100.0/255.255.255.0 pour XSCF-LAN#0 de BB#00.

```
XSCF> showpacketfilters -a
-s 192.168.100.0/255.255.255.0 -i bb#00-lan#0 -j ACCEPT
XSCF>
XSCF> setpacketfilters -y -c add -i bb#00-lan#0 -j DROP
-s 192.168.100.0/255.255.255.0 -i bb#00-lan#0 -j ACCEPT
-i bb#00-lan#0 -j DROP
NOTE: applied IP packet filtering rules.
Continue? [y|n] :y
XSCF>
XSCF> showpacketfilters -a
-s 192.168.100.0/255.255.255.0 -i bb#00-lan#0 -j ACCEPT
-i bb#00-lan#0 -j DROP
```

Dans l'exemple suivant, un paramètre de rejet de communication depuis 10.10.10.10 est supprimé.

```
XSCF> showpacketfilters -a
-s 172.16.0.0/255.255.0.0 -i bb#00-lan#0 -j DROP
-s 10.10.10.10 -j DROP
XSCF>
XSCF> setpacketfilters -y -c del -s 10.10.10.10 -j DROP
-s 172.16.0.0/255.255.0.0 -i bb#00-lan#0 -j DROP
NOTE: applied IP packet filtering rules.
Continue? [y|n] :y
XSCF>
XSCF> showpacketfilters -a
-s 172.16.0.0/255.255.0.0 -i bb#00-lan#0 -j DROP
```

Dans l'exemple suivant, toutes les règles de filtrage des paquets IP définies sont supprimées.

```
XSCF> setpacketfilters -c clear
(none)
NOTE: applied IP packet filtering rules.
Continue? [y|n] :y
```

3.9.15 Diffusion des réglages de réseau XSCF

Une fois le paramétrage achevé avec les commandes `setnetwork`, `setsscp`, `sethostname`,

setroute et setnameserver, diffusez les paramètres de réseau.

1. **Exécutez la commande `applynetwork`.**

Les paramètres de réseau sont affichées et leur application confirmée.

```
XSCF> applynetwork
The following network settings will be applied:
bb#00 hostname      :hostname-0
bb#01 hostname      :hostname-1
DNS domain name     :example.com
nameserver           :10.23.4.3

interface           :bb#00-lan#0
status              :up
IP address          :10.24.144.214
netmask             :255.255.255.0
route               : -n 0.0.0.0 -m 0.0.0.0 -g 10.24.144.1

interface           :bb#00-lan#1
status              :down
IP address          :
netmask             :
route               :

interface           :bb#01-lan#0
status              :up
IP address          :10.24.144.215
netmask             :255.255.255.0
route               : -n 0.0.0.0 -m 0.0.0.0 -g 10.24.144.1

interface           :bb#01-lan#1
status              :down
IP address          :
netmask             :
route               :

interface           :lan#0
status              :down
IP address          :
netmask             :

interface           :lan#1
status              :down
IP address          :
netmask             :

SSCP network ID:0 netmask :255.255.255.248

interface           :bb#00-if#0
IP address          :192.168.1.1

interface           :bb#01-if#0
IP address          :192.168.1.2

interface           :bb#02-if#0
```

```

IP address                :192.168.1.3

interface                  :bb#03-if#0
IP address                 :192.168.1.4

SSCP network ID:1 netmask :255.255.255.248

interface                  :bb#00-if#1
IP address                 :192.168.1.10

interface                  :bb#01-if#1
IP address                 :192.168.1.9

interface                  :bb#02-if#1
IP address                 :192.168.1.11

interface                  :bb#03-if#1
IP address                 :192.168.1.12

SSCP network ID:2 netmask :255.255.255.252

interface                  :bb#00-if#2
IP address                 :192.168.1.17

interface                  :bb#01-if#2
IP address                 :192.168.1.18

Continue? [y|n] : y

```

2. **Exécutez la commande `rebootxscf` pour redémarrer le XSCF et finaliser les réglages.**

```

XSCF> rebootxscf -a
The XSCF will be reset. Continue? [y|n] :y

```

La session est interrompue à ce moment-là. Reconnectez-vous à une nouvelle interface, puis identifiez-vous de nouveau.

3. **Exécutez les commandes `shownetwork`, `showsscp`, `showhostname`, `showroute` et `shownameserver` pour afficher les paramètres du réseau et vérifiez les nouvelles informations.**
4. **Exécutez la commande `nslookup`, puis vérifiez les informations relatives au nom d'hôte.**

Dans l'exemple suivant, les informations concernant le nom d'hôte `scf0-hostname` sont affichées.

```

XSCF> nslookup scf0-hostname
Server: server.example.com
Address: 192.168.1.3

Name: scf0-hostname.example.com
Address: 192.168.10.10

```

3.9.16

Vérification de l'état de connexion au réseau XSCF

Pour vérifier la réponse des périphériques du réseau, utilisez la commande ping. En outre, pour vérifier le paramètre d'acheminement du réseau, utilisez la commande traceroute.

1. **Exécutez la commande `shownetwork` pour afficher la connexion au réseau.**

```
XSCF> shownetwork -i
Active Internet connections (without servers)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 xx.xx.xx.xx:telnet xxxx:1617 ESTABLISHED
```

2. **Exécutez la commande `ping` pour vérifier la réponse d'un périphérique du réseau.**

Dans l'exemple suivant, un paquet est envoyé trois fois à l'hôte du nom de `scf0-hostname`.

```
XSCF> ping -c 3 scf0-hostname
PING scf0-hostname (XX.XX.XX.XX): 56 data bytes
64 bytes from XX.XX.XX.XX: icmp_seq=0 ttl=64 time=0.1 ms
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=64 time=0.1 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=64 time=0.1 ms

--- scf0-hostname ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.1/0.1 ms
```

3. **Exécutez la commande `traceroute` pour vérifier l'itinéraire réseau d'un périphérique du réseau.**

Dans l'exemple suivant, les itinéraires réseau menant à l'hôte du nom de `server.example.com` sont affichés.

```
XSCF> traceroute server.example.com
traceroute to server.example.com (XX.XX.XX.XX), 30 hops max, 40
byte packets
 1 XX.XX.XX.1 (XX.XX.XX.1) 1.792 ms 1.673 ms 1.549 ms
 2 XX.XX.XX.2 (XX.XX.XX.2) 2.235 ms 2.249 ms 2.367 ms
 3 XX.XX.XX.3 (XX.XX.XX.3) 2.199 ms 2.228 ms 2.361 ms
 4 XX.XX.XX.4 (XX.XX.XX.4) 2.516 ms 2.229 ms 2.357 ms
 5 XX.XX.XX.5 (XX.XX.XX.5) 2.546 ms 2.347 ms 2.272 ms
 6 server.example.com (XX.XX.XX.XX) 2.172 ms 2.313 ms 2.36 ms
```

3.10 Configuration de l'audit pour renforcer la sécurité de XSCF

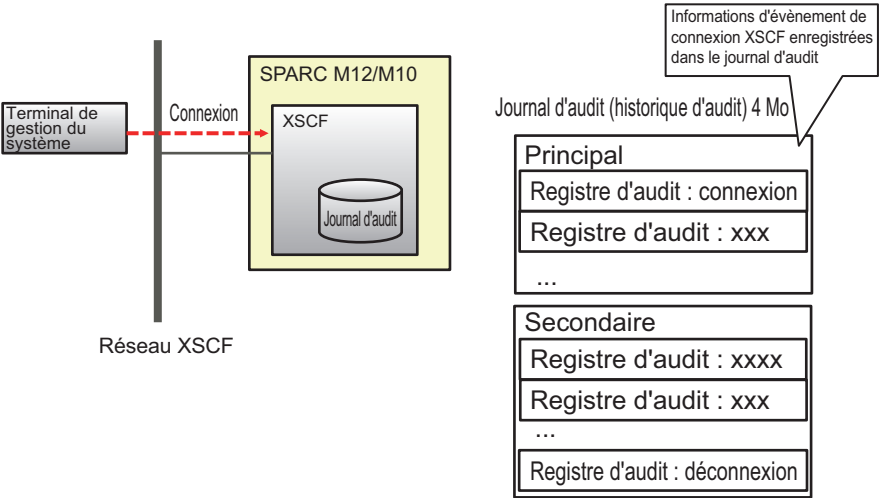
Cette section décrit comment configurer le réseau XSCF pour utiliser l'audit. Les paramètres d'audit sont destinés à l'audit des opérations de réseau effectuées par les utilisateurs et l'archivage détaillé des accès de ceux qui se sont connectés au XSCF, de leur date et heure de connexion et des opérations qu'ils ont réalisées. Les paramètres d'audit sont activés par défaut dans ce système. Les paramètres d'audit déterminent principalement l'activation/désactivation de l'audit et la méthode de gestion de la politique d'audit et du journal d'audit (pistes d'audit).

3.10.1 Mener un audit

Les systèmes SPARC M12/M10 peuvent enregistrer tous les événements XSCF qui peuvent être liés à la sécurité, tels que la connexion et la déconnexion d'un utilisateur et les modifications des privilèges d'utilisateur, ainsi que les opérations, dont le démarrage et l'arrêt du système. Une fois l'audit configuré, l'audit démarre et les informations sur un événement unique, la cause d'occurrence, la date d'occurrence et d'autres informations liées sont enregistrées en tant qu'enregistrement d'audit. Le système possède un journal d'audit (pistes d'audit), qui est une collection d'enregistrements d'audit. L'administrateur système peut consulter un journal d'audit pour vérifier les opérations suspectes ou anormales ou pour identifier la personne qui a effectué un événement spécifique.

Figure 3-6 fournit une vue d'ensemble de la façon dont les informations d'événement de connexion sont enregistrées dans un journal d'audit.

Figure 3-6 Enregistrement dans un journal d'audit



3.10.2 Compréhension des termes liés à l'audit

Tableau 3-24 répertorie les termes liés aux paramètres d'audit de XSCF.

Tableau 3-24 Termes liés à l'audit

Terme	Description
Audit	C'est la fonction de contrôle des accès au système. Cette fonction s'appelle également l'audit.
Évènement d'audit	Un évènement d'audit est une action du système liée à la sécurité pouvant faire l'objet d'un audit. Il est possible de spécifier plusieurs événements d'audit par une valeur numérique ou un nom. (exemple : AEV_LOGIN_SSH, LOGIN_SSH, 0, etc.)
Classe d'audit	Une classe d'audit est un groupe d'événements d'audit pertinents. (par exemple, les événements de la classe d'audit login : connexion SSH, connexion telnet, connexion HTTPS, et déconnexion) Il est possible de spécifier plusieurs classes d'audit. (exemple : CS_AUDIT, AUDIT, 2, etc.)
Enregistrement d'audit	Un enregistrement d'audit est une information identifiant un évènement d'audit. Cela comprend l'évènement lui-même, son heure ou d'autres informations pertinentes. Les enregistrements d'audit sont stockés dans un fichier d'audit.
Journal d'audit	Un journal d'audit correspond aux fichiers de journal qui stockent plusieurs enregistrements d'audit. Un journal d'audit comprend deux zones : primaire et secondaire.
Piste d'audit	Une piste d'audit est également appelée journal d'audit. Les utilisateurs utilisent la commande viewaudit pour analyser le contenu de chaque enregistrement d'audit dans un journal d'audit.
Stratégie d'audit	La stratégie définit le type d'enregistrements d'audit à générer en spécifiant un événement d'audit, une classe d'audit ou un utilisateur. Elle spécifie également d'autres paramètres, tels que les paramètres de notification par e-mail utilisés lorsqu'un journal d'audit atteint la pleine capacité.
Jeton d'audit	Un jeton d'audit est un champ d'un enregistrement d'audit. Le jeton d'audit possède une description d'un attribut d'évènement d'audit, comme l'utilisateur ou le privilège.

3.10.3 Gestion des audits

L'administrateur système détermine quelle classe d'audit, quel événement d'audit ou quel utilisateur utiliser pour l'audit avant d'effectuer l'audit. L'administrateur

système détermine également à quel niveau d'utilisation d'un journal d'audit un avertissement est généré et quelle action est prise lorsque la capacité devient pleine. Ces déterminations sont nommées stratégie d'audit, qui est configurée sur le XSCF avant l'audit. L'administrateur système consulte chaque enregistrement d'audit dans le journal d'audit collecté en fonction de la stratégie d'audit pour rechercher dans les informations d'audit tout accès anormal ou suspect.

Ce qui suit fournit des informations détaillées sur les événements d'audit, la stratégie d'audit, les enregistrements d'audit et le journal d'audit utilisés pour l'audit.

Évènement d'audit

Un évènement d'audit est une opération du système liée à la sécurité pouvant faire l'objet d'un audit.

Les événements d'audit sont décrits ci-dessous.

- Modifications de la configuration XSCF, telles que la modification d'une adresse IP
- Modifications, opérations et affichage du statut de paramètres liés à la partition physique
- Utilisation d'une authentification
- Modifications des attributs de sécurité d'un utilisateur, tels que le mot de passe et les privilèges d'utilisateur
- Lecture des informations d'enregistrement d'audit (dont les tentatives échouées)
- Modifications de la stratégie d'audit
- Modification de la destination de l'e-mail à envoyer lorsque le seuil de capacité du journal d'audit est dépassé
- Modifications apportées par l'administrateur système à un journal d'audit.
- Modifications de l'heure

Stratégie d'audit

La stratégie d'audit détermine comment exécuter la fonction d'audit. Les paramètres suivants de la fonction d'audit peuvent être configurés :

- Activer/désactiver la fonction d'audit
- Types d'événements à auditer
- Un auditeur pour des événements
- Le seuil de capacité du journal d'audit auquel un avertissement est généré et la destination de l'e-mail à envoyer lorsque le seuil est dépassé
- Opération à effectuer lorsqu'un journal d'audit atteint la pleine capacité (Utilisez ce paramètre avec la valeur par défaut.)

Remarque - Si vous voulez utiliser un e-mail pour indiquer que le seuil de capacité du journal d'audit est dépassé, configurez le serveur SMTP avec la commande `setsmtp`.

Enregistrement d'audit et journal d'audit

Les enregistrements d'audit sont enregistrés dans le journal d'audit de 4 Mo du XSCF. Un journal d'audit est enregistré en format binaire, mais peut être exporté au format XML.

Un journal d'audit comprend deux zones : primaire et secondaire. Lorsque ces zones deviennent pleines et un nouvel audit est généré, l'enregistrement n'est pas enregistré mais supprimé.

Pour empêcher que de nouveaux enregistrements d'audit soient supprimés, l'administrateur système supprime les données de la zone secondaire avant que le journal d'audit atteigne la pleine capacité. Après la suppression de la zone secondaire, la zone primaire devient une nouvelle zone secondaire et une nouvelle zone primaire est créée. Lorsqu'un nouvel enregistrement d'audit est généré, l'enregistrement est écrit sur la nouvelle zone primaire.

Remarque : « count » (par défaut) est défini comme l'opération à effectuer lorsqu'un journal d'audit atteint la pleine capacité. Avec ce paramètre, les nouveaux enregistrements d'audit sont supprimés lorsqu'un journal d'audit atteint la pleine capacité et le nombre d'enregistrements supprimés est comptabilisé (décompte des suppressions).

Remarque : si vous spécifiez « suspend », une dégradation due à une erreur peut se produire ou le XSCF peut être redémarré. Spécifiez « count », qui est la valeur par défaut, en tant que stratégie pour écrire dans le journal d'audit. Veuillez également noter que, sur XCP 2250 et les versions ultérieures, spécifier « suspend » aboutit à la même opération que lorsque « count » est spécifié.

Utilisez la stratégie d'audit pour définir le seuil capacité du fichier (tel que 50 %, 75 % ou 80 %) de sorte qu'un avertissement apparaisse avant qu'un journal d'audit atteigne la pleine capacité. Lors de cet avertissement, l'administrateur système archive manuellement le journal d'audit et supprime les enregistrements d'audit pour garantir un nouveau stockage suffisant. Ou il/elle désactive la fonction d'audit. Le fichier le plus ancien des deux zones de journal d'audit est supprimé. Si cette suppression est effectuée deux fois de suite, toutes les données du journal d'audit seront supprimées.

Remarque : pour l'audit de XSCF dans une configuration avec plusieurs systèmes SPARC M12-2S/M10-4S, les deux journaux d'audit sur les XSCF maître et de veille doivent être consultés. Pour plus de détails, consultez « [3.10.10 Gestion du journal d'audit du XSCF de veille](#) ».

3.10.4 Vérification des éléments de réglage et commandes liés à l'audit

Tableau 3-25 répertorie les éléments de réglage liés à l'audit et les commandes de shell XSCF correspondantes.

Tableau 3-25 Éléments de réglage liés à l'audit

Élément de réglage	Paramétrage requis ou optionnel	Commande liée
Activation/désactivation de l'audit	Optionnel	setaudit(8), showaudit(8)
Archivage d'un journal d'audit (*1), suppression des données	Optionnel	setaudit(8), showaudit(8)
Stratégie d'audit	Optionnel	setaudit(8), showaudit(8)
- Spécification de l'activation/désactivation pour les utilisateurs indiqués ou application d'une stratégie globale		setsmtp(8), showsmtp(8)
- Activation/désactivation d'une classe d'audit		
- Activation/désactivation d'un événement d'audit		
- Activation/désactivation de l'audit pour tous les utilisateurs (stratégie globale)		
- Seuil d'avertissement concernant la quantité de journaux d'audit (en %)		
- Adresse électronique de destination utilisée lorsque la quantité de journaux d'audit atteint le seuil		
- Suspension de l'écriture/Suppression des données lorsque le journal d'audit atteint la pleine capacité (*2)		

Tableau 3-25 Éléments de réglage liés à l'audit (*suite*)

Élément de réglage	Paramétrage requis ou optionnel	Commande liée
Affichage d'un journal d'audit - Enregistrements après l'heure spécifiée - Enregistrements avant l'heure spécifiée - Enregistrements dans la plage d'heures spécifiée - Enregistrements à une certaine date (pendant 24 heures sur une certaine date en heure locale) - Classe d'audit - Évènement d'audit - ID de session d'audit - Privilèges d'utilisateur - Valeur retournée (réussite, échec ou aucune) - Utilisateur (nom ou valeur UID numérique) Affichez une piste d'audit en spécifiant le format comme décrit ci-dessous : - Générer les données ligne à ligne - Spécifier un caractère de délimitation (par défaut : virgule) - Suppression de la conversion des UID en noms d'utilisateurs et de la conversion des adresses IP en noms d'hôtes - Génération des données au format XML	Optionnel	viewaudit(8)

*1 L'archivage des journaux d'audit n'est pas pris en charge actuellement.

*2 Lorsqu'un journal d'audit atteint la pleine capacité, seule la stratégie d'audit « count », qui supprime les enregistrements d'audit, est actuellement prise en charge. Ne spécifiez pas « suspend ».

3.10.5 Flux d'un audit

Figure 3-7 indique le déroulement de la configuration des paramètres d'un audit et de l'affichage d'un journal d'audit.

Figure 3-7 Flux du réglage d'un audit et de l'affichage d'un journal

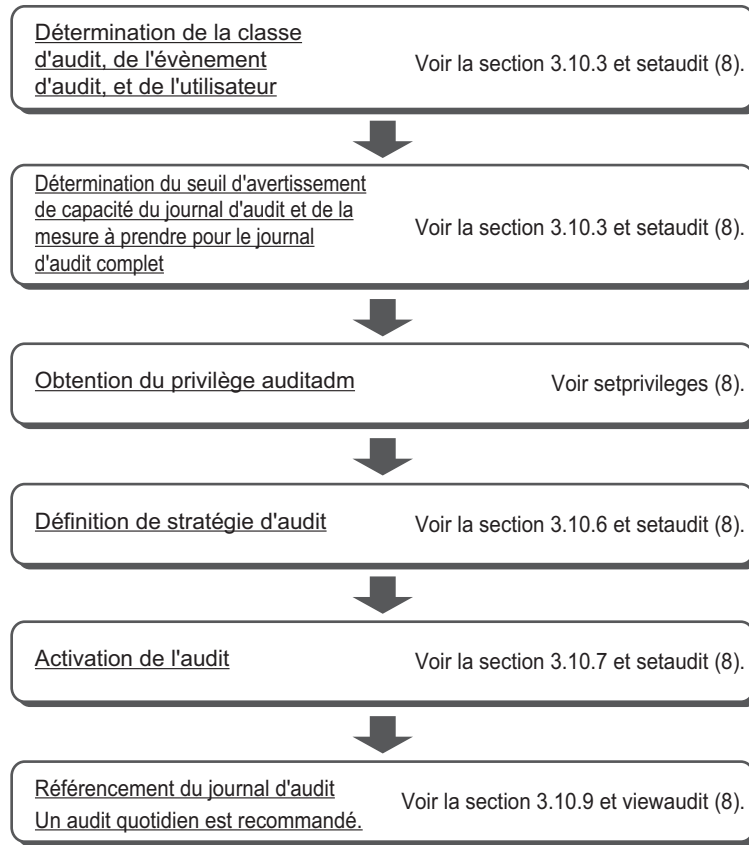
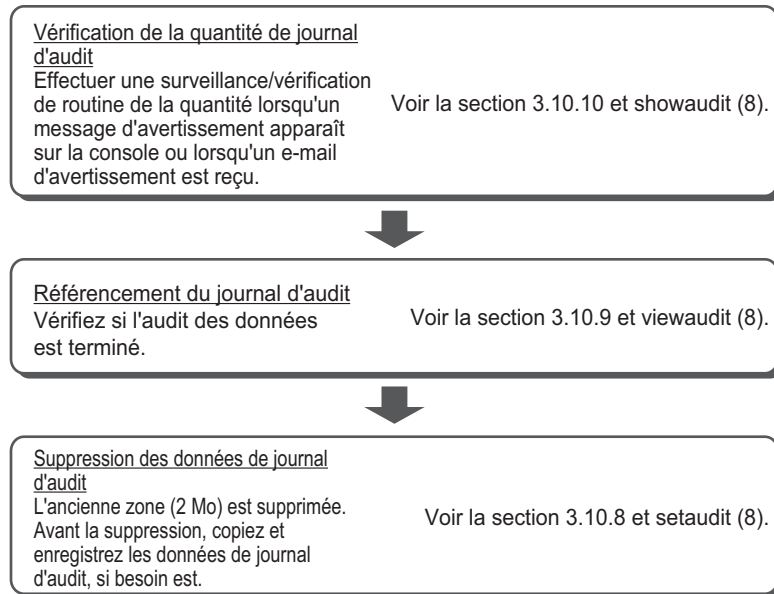


Figure 3-8 indique le déroulement de la suppression des données d'un journal d'audit.

Figure 3-8 Suppression des données de journal d'audit



3.10.6 Affichage/Réglage de la stratégie d'audit

1. **Exécutez la commande showaudit pour afficher les paramètres de la stratégie d'audit.**

```
XSCF> showaudit all
Auditing:                enabled
Audit space used:        13713 (bytes)
Audit space free:        4180591 (bytes)
Records dropped:         0
Policy on full trail:    count
User global policy:     enabled
Mail:
Thresholds:              80% 100%
User policy:
Events:
    AEV_AUDIT_START enabled
    AEV_AUDIT_STOP  enabled
```

2. **Exécutez la commande setaudit pour définir la stratégie d'audit.**
Dans l'exemple suivant, trois utilisateurs (yyyyy, uuuuu et nnnnn) sont spécifiés, AUDIT et LOGIN sont activés pour la classe d'audit, la version est activée pour les événements d'audit et la stratégie globale désactivée pour les utilisateurs.

```
XSCF> setaudit -a yyyyy,uuuuu,nnnnn=enable -c
ACS_AUDIT,ACS_LOGIN=enable -e AEV_version=enable -g disable
```

Dans l'exemple suivant, sont spécifiés une adresse électronique de notification des avertissements, la suppression des nouveaux enregistrements d'audit, le décompte des enregistrements supprimés lorsque la quantité de pistes d'audit atteint la pleine capacité et que les seuils d'avertissement quant à la quantité de fichiers (50 %, 75 % et 90 %).

```
XSCF> setaudit -m yyyy@example.com -p count -t 50,75,90
```

3. Exécutez la commande showaudit, puis vérifiez les paramètres.

```
XSCF> showaudit all
Auditing:                enabled
Audit space used:         13713 (bytes)
Audit space free:         4180591 (bytes)
Records dropped:          0
Policy on full trail:     count
User global policy:       enabled
Mail:                     yyyy@example.com
Thresholds:               50% 75% 90%
User policy:
Events:
    AEV_AUDIT_START       enabled
    AEV_AUDIT_STOP        enabled
    :
    AEV_LOGIN_BUI         enabled
    AEV_LOGIN_CONSOLE     enabled
    AEV_LOGIN_SSH         enabled
    AEV_LOGIN_TELNET      enabled
    AEV_LOGOUT            enabled
    AEV_AUTHENTICATE      enabled
    :
    AEV_version           enabled
    :
```

Lorsque l'option -p count est spécifiée, les nouvelles données d'enregistrement d'audit sont supprimées lorsque le journal d'audit atteint la pleine capacité et le nombre de suppressions d'enregistrements est comptabilisé (décompte des suppressions).

Remarque : lorsqu'un journal d'audit atteint la pleine capacité, seule la stratégie d'audit « count », qui supprime les enregistrements d'audit, est actuellement prise en charge. Par conséquent, ne spécifiez pas « suspend ».

Si la quantité de journaux d'audit dépasse la valeur seuil, un message d'avertissement apparaît sur la console. Si une adresse e-mail de destination d'un avertissement est spécifiée, un avertissement peut également être envoyé en format sécurisé. L'exemple suivant montre un message d'avertissement.

3.10.7 Activation/Désactivation de l'audit

Pour vérifier l'état actuel de l'audit, utilisez la commande `showaudit`. En outre, pour configurer les paramètres d'audit, utilisez la commande `setaudit`. Exécutez la commande `setaudit` avec un compte d'utilisateur disposant du privilège `auditadm`. L'audit est activé par défaut. L'écriture sur le journal d'audit s'arrête lorsque l'audit est désactivé. Elle reprend lorsque celui-ci est réactivé. Dans le processus de redémarrage, l'audit est désactivé avant d'être activé.

1. **Exécutez la commande `showaudit` pour afficher les paramètres d'audit.**

L'exemple suivant affiche l'état complet de l'audit système actuel.

```
XSCF> showaudit all
Auditing:                enabled
Audit space used:         13713 (bytes)
Audit space free:         4180591 (bytes)
Records dropped:          0
Policy on full trail:     count
User global policy:       enabled
Mail:
Thresholds:               80% 100%
User policy:
Events:
    AEV_AUDIT_START enabled
    AEV_AUDIT_STOP enabled
:
```

2. **Exécutez la commande `setaudit` pour régler l'activation/désactivation.**

Dans l'exemple suivant, l'activation de l'écriture des données d'audit est spécifiée.

```
XSCF> setaudit enable
```

Dans l'exemple suivant, la désactivation de l'écriture des données d'audit est spécifiée.

```
XSCF> setaudit disable
```

3.10.8 Suppression des données de journal d'audit

Les données d'un journal d'audit peuvent être supprimées en exécutant la commande `setaudit` dans les cas suivants : lorsque le seuil de capacité du journal d'audit est dépassé, lorsqu'un message d'avertissement apparaît sur la console ou un e-mail

d'avertissement arrive, ou lorsque le journal d'audit atteint la pleine capacité.

1. **Exécute la commande `showaudit` pour vérifier les paramètres d'audit et la quantité de journaux d'audit.**

L'exemple suivant affiche tous les états actuels de l'audit dans le système.

L'exemple montre que la quantité de journaux d'audit est de 3,5 Mo et que le seuil de capacité du niveau d'avertissement de 80 % est dépassé.

```
XSCF> showaudit all
Auditing:                enabled
Audit space used:         3670016 (bytes)
Audit space free:         524288 (bytes)
Records dropped:          0
Policy on full trail:     count
User global policy:       enabled
Mail:
Thresholds:               80% 100%
User policy:
Events:
    AEV_AUDIT_START enabled
    AEV_AUDIT_STOP  enabled
:
```

2. **Exécutez la commande `setaudit` pour effacer les données du journal d'audit.**

La zone de 2 Mo plus ancienne (secondaire) est supprimée.

```
XSCF> setaudit delete
```

Remarque : avant de supprimer les données du journal d'audit, vérifiez si l'audit des données est terminé en utilisant la commande `viewaudit`.

3. **Exécutez la commande `showaudit` pour vérifier les résultats de l'exécution de la commande `setaudit`.**

L'exemple suivant montre que la zone plus ancienne du journal d'audit est supprimée et qu'une capacité disponible d'environ 2 Mo est créée.

```
XSCF> showaudit all
Auditing:                enabled
Audit space used:         2097152 (bytes)
Audit space free:         2097152 (bytes)
Records dropped:          0
Policy on full trail:     count
User global policy:       enabled
Mail:
Thresholds:               80% 100%
User policy:
Events:
    AEV_AUDIT_START enabled
```


Remarque - Après la suppression de la zone secondaire, la zone primaire devient secondaire et une nouvelle zone primaire est créée.

Le système reconnaît alors la quantité de la nouvelle zone secondaire comme 2 Mo, indépendamment de la quantité restante réelle de la zone.

Par conséquent, même une fois que les données d'un journal d'audit ont été supprimées, 2 Mo apparaissent toujours comme étant utilisés lorsque la quantité de journaux d'audit est appelée en utilisant la commande showaudit.

Si cette suppression est effectuée deux fois de suite, toutes les informations dans le journal d'audit seront supprimées.

Même dans ce cas, 2 Mo apparaissent comme étant utilisés lorsque la quantité de journaux d'audit est indiquée à titre de référence en utilisant la commande showaudit.

3.10.9 Référencement d'un journal d'audit

Utilisez la commande viewaudit pour afficher les enregistrements d'audit. Exécutez la commande viewaudit avec un compte d'utilisateur disposant du privilège auditadm ou auditop.

1. Exécutez la commande viewaudit pour visualiser une piste d'audit.

```
XSCF> viewaudit
file,1,2015-06-29 13:42:59.128 +09:00,20150629044259.
0000000000.localhost
header,20,1,audit - start,localhost.localdomain,2015-06-29 13:
42:59.131 +09:00
header,31,1,login - console,localhost.localdomain,2015-06-29
13:45:03.755
+09:00subject,1,default,normal,console
header,60,1,command - showpasswordpolicy,localhost.localdomain,
2015-06-29
13:45:33.653 +09:00
subject,1,default,normal,console
command,showpasswordpolicy
platform access,granted
return,0
:
```

Pour plus de détails concernant la façon de se reporter aux enregistrements d'audit, consultez « [Chapitre 12 Consultation des journaux et des messages](#) ».

3.10.10 Gestion du journal d'audit du XSCF de veille

Les données d'audit du XSCF maître/de veille sont enregistrées dans une zone du journal d'audit du XSCF maître/de veille.

Le journal d'audit peut être appelé en utilisant la commande `viewaudit` depuis chaque XSCF. Cependant, seul le XSCF maître peut être utilisé pour afficher le statut d'audit ou pour supprimer les données du journal d'audit. Par conséquent, pour gérer le journal d'audit du XSCF de veille, basculez le XSCF de veille à maître.

La section suivante décrit comment gérer le journal d'audit sauvegardé sur le XSCF de veille.

Référencement d'un journal d'audit

Exécutez la commande `viewaudit(8)` depuis le XSCF de veille. Pour plus de détails sur la méthode de référencement, consultez « [3.10.9 Référencement d'un journal d'audit](#) ».

Suppression des données de journal d'audit

1. **Exécutez la commande `switchscf(8)` pour échanger le XSCF maître et le XSCF de veille.**
2. **Exécutez la commande `showaudit(8)` pour vérifier la quantité de journaux d'audit pour le précédent XSCF de veille.**
3. **Exécutez la commande `setaudit(8)` pour effacer les données du journal d'audit.** Pour plus de détails sur la suppression des données, consultez « [3.10.8 Suppression des données de journal d'audit](#) ».
4. **Exécutez la commande `showaudit(8)` pour confirmer que le journal d'audit dispose d'espace libre.**
5. **Exécutez la commande `switchscf(8)` pour échanger de nouveau le XSCF maître et le XSCF de veille.**

Configuration du système selon le type d'utilisation

Ce chapitre décrit les éléments permettant de configurer le système de manière appropriée par rapport au type d'utilisation, en portant une attention particulière sur le contrôle de l'alimentation et les connexions d'entraînement.

- Paramétrage / vérification de l'altitude du système
- Contrôle de démarrage du système
- Activation / désactivation de la double alimentation électrique
- Diminution de la consommation électrique
- Connexion d'un lecteur de DVD
- Utilisation du stockage à distance

4.1 Paramétrage / vérification de l'altitude du système

Cette section décrit comment définir et vérifier l'altitude du système.

Les systèmes SPARC M12/M10 contrôlent la vitesse des ventilateurs de refroidissement situés à l'intérieur du système, en fonction de l'altitude et de la température de l'emplacement où le système est installé. L'altitude doit ainsi être paramétrée durant l'installation initiale du système.

Remarque : paramétrez l'altitude du système pendant l'installation initiale. Si la valeur doit être modifiée, paramétrez-la de nouveau.

Pour plus de détails sur les commandes XSCF exécutées dans la procédure suivante, consultez les pages du manuel correspondantes ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

4.1.1 Paramétrage de l'altitude du système

Utilisez la commande `setaltitude` du microprogramme de XSCF afin de paramétrer l'altitude du système.

Exécutez la commande avec un compte d'utilisateur disposant du privilège `platadm` ou `fieldeng`.

```
XSCF> setaltitude -s altitude=value
```

Comme valeur, indiquez l'altitude de l'emplacement du serveur en mètres. Vous pouvez spécifier une valeur par incréments de 100, à partir de 0.

Remarque : une fois l'altitude du système réglée, pour appliquer ce paramètre, il est nécessaire de redémarrer le XSCF avec la commande `rebootxscf`.

Procédure de fonctionnement

1. **Exécutez la commande `setaltitude` pour configurer les paramètres de l'altitude.**
L'exemple suivant définit l'altitude sur 1 000 m.

```
XSCF> setaltitude -s altitude=1000  
1000m
```

2. **Exécutez la commande `rebootxscf` pour redémarrer le XSCF et diffuser le paramètre défini.**

Remarque : lorsque vous poursuivez avec d'autres paramètres, vous pouvez réaliser cette tâche une fois tous les paramètres réalisés.

```
XSCF> rebootxscf -a
```

4.1.2 Vérification des réglages de l'altitude du système

Utilisez la commande `showaltitude` du microprogramme XSCF afin de vérifier l'altitude actuellement définie pour le système.

Exécutez la commande avec un compte d'utilisateur disposant du privilège `platadm` ou `fieldeng`.

```
XSCF> showaltitude
```

La commande affiche l'altitude actuelle du système configuré en mètres.

Procédure de fonctionnement

1. Exécutez la commande `showaltitude` pour afficher l'altitude.

Dans l'exemple suivant, vous pouvez voir que l'altitude est définie sur 1 000 m.

```
XSCF> showaltitude
1000m
```

4.2 Contrôle de démarrage du système

Cette section décrit le délai de préchauffage et le délai d'attente au démarrage permettant de contrôler le démarrage du système.

Le délai de préchauffage et le délai d'attente au démarrage sont utilisés pour les objectifs suivants.

- Vous pouvez empêcher le système de démarrer avant que les périphériques ne soient mis sous tension. Vous pouvez empêcher le système de démarrer avant que le préchauffage soit effectué.
Vous pouvez également définir une durée de fonctionnement différente pour chaque partition physique. Lorsque la valeur de limite supérieure de la consommation électrique est définie, une mise sous tension simultanée peut provoquer le dépassement de limite de consommation électrique. Définissez donc une durée différente pour chaque partition physique. (Consultez « [4.2.1 Réglage/Vérification du délai de préchauffage](#) ».)
- Vous pouvez démarrer le système une fois que la climatisation du centre de données a ajusté la température. (Consultez « [4.2.2 Réglage/Vérification du temps d'attente au démarrage](#) ».)

4.2.1 Réglage/Vérification du délai de préchauffage

Si le délai de préchauffage est défini, OpenBoot PROM démarre après la mise en route de celui-ci, derrière la mise sous tension du serveur et le début du processus de mise sous tension.

Réglage du délai de préchauffage

Utilisez la commande `setpowerupdelay` du microprogramme de XSCF afin de paramétrer le délai de préchauffage.

Exécutez la commande avec un compte d'utilisateur disposant du privilège `platadm` ou `fielddeng`.

```
XSCF> setpowerupdelay {-a|-p ppar-id} -c warmup -s time
```

Si toutes les partitions physiques sont visées, spécifiez -a. Pour viser une partition physique spécifique, spécifiez -p.

Spécifiez maintenant le délai de préchauffage en minutes. Vous pouvez spécifier un entier compris entre 0 et 255. La valeur par défaut est 0.

Remarque : si vous activez la mise sous tension en appuyant sur le commutateur ALIMENTATION du panneau de commande, le délai de préchauffage défini sera ignoré.

Procédure de fonctionnement

1. Exécutez la commande **setpowerupdelay** pour configurer le délai de préchauffage.

L'exemple suivant règle le délai de préchauffage sur 5 minutes pour une partition physique à 0.

```
XSCF> setpowerupdelay -p 0 -c warmup -s 5
```

Si le délai de préchauffage est défini pendant le fonctionnement du système, ce dernier sera activé au prochain système de démarrage.

Vérification du délai de préchauffage

Utilisez la commande **showpowerupdelay** du microprogramme de XSCF afin de vérifier le délai de préchauffage.

Exécutez la commande avec un compte d'utilisateur disposant du privilège **platadm**, **platop** ou **fieldeng**. À défaut, vous pouvez également l'exécuter avec un compte d'utilisateur disposant de **pparadm**, **pparmgr**, ou du privilège **pparop** pour la partition physique cible.

```
XSCF> showpowerupdelay
```

Dans les résultats générés par la commande **showpowerupdelay**, le délai de préchauffage actuellement défini est affiché en minutes dans « délai de préchauffage ». Dans « délai d'attente », le délai d'attente au démarrage est indiqué en minutes.

Procédure de fonctionnement

1. Affichez le délai de préchauffage avec la commande **showpowerupdelay**.

Dans l'exemple suivant, vous pouvez voir que le délai de préchauffage est réglé sur 10 minutes.

```
XSCF> showpowerupdelay
warmup time : 10 minute(s)
wait time : 20 minute(s)
```

4.2.2 Réglage/Vérification du temps d'attente au démarrage

Si le délai d'attente au démarrage est défini, le système suspend la procédure de démarrage jusqu'à ce que la durée définie soit passée. Une fois ce délai d'attente passé et après la mise sous tension du serveur, le système est démarré.

Réglage du délai d'attente au démarrage

Utilisez la commande `setpowerupdelay` du microprogramme de XSCF afin de paramétrer le délai d'attente au démarrage.
Exécutez la commande avec un compte d'utilisateur disposant du privilège `platadm` ou `fieldeng`.

```
XSCF> setpowerupdelay -c wait -s time
```

Spécifiez maintenant le délai d'attente au démarrage en minutes. Vous pouvez spécifier un entier compris entre 0 et 255. La valeur par défaut est 0.

Remarque : si vous activez la mise sous tension en appuyant sur le commutateur ALIMENTATION du panneau de commande, le délai d'attente au démarrage défini sera ignoré.

Procédure de fonctionnement

1. **Définissez le délai d'attente au démarrage avec la commande `setpowerupdelay`.**
Voici un exemple où le délai d'attente au démarrage est réglé sur 5 minutes.

```
XSCF> setpowerupdelay -c wait -s 5
```

Si le délai d'attente au démarrage est défini pendant le fonctionnement du système, ce dernier sera activé au prochain système de démarrage.

Vérification du délai d'attente au démarrage

Utilisez la commande `showpowerupdelay` du microprogramme de XSCF afin de vérifier le délai d'attente au démarrage.
Exécutez la commande avec un compte d'utilisateur disposant du privilège `platadm`, `platop` ou `fieldeng`. À défaut, vous pouvez également l'exécuter avec un compte d'utilisateur disposant de `pparadm`, `pparmgr`, ou du privilège `pparop` pour la partition physique cible.

```
XSCF> showpowerupdelay
```

Dans les résultats générés par la commande `showpowerupdelay`, le délai de préchauffage actuellement défini est affiché en minutes dans « délai de préchauffage ».

». Dans « délai d'attente », le délai d'attente au démarrage est indiqué en minutes.

Procédure de fonctionnement

1. **Affichez le délai d'attente au démarrage avec la commande `showpowerupdelay`.**
Dans l'exemple suivant, vous pouvez voir que le délai d'attente au démarrage est réglé sur 20 minutes.

```
XSCF> showpowerupdelay
warmup time : 10 minute(s)
wait time : 20 minute(s)
```

4.3 Activation / désactivation de la double alimentation électrique

Quatre unités d'alimentation électrique sont installées sur le SPARC M12-2/M12-2S. Pour les systèmes à double alimentation électrique, chaque système possède deux unités d'alimentation électrique.

par ex., PSU#0/PSU#1 pour le système d'alimentation 0, PSU#2/PSU#3 pour le système d'alimentation 1

Lorsque la double alimentation électrique est activée/désactivée, l'état de la PSU et le fonctionnement du système sont identiques à ceux affichés dans [Tableau 4-1](#).

Tableau 4-1 Réglages de la double alimentation électrique et état de l'unité d'alimentation électrique (PSU) assurant le fonctionnement du système pour SPARC M12-2/M12-2S

Réglage de double alimentation électrique	État de la PSU	Fonctionnement du système
Désactivé	2 PSU ou plus en fonctionnement	Utilisable
	Pas plus de 1 PSU en fonctionnement	Non utilisable
Activée	2 PSU en fonctionnement sur au moins 1 des systèmes d'alimentation	Utilisable
	Pas plus de 1 PSU en fonctionnement sur les deux systèmes d'alimentation	Non utilisable

Deux unités d'alimentation électrique (PSU) sont installées sur le SPARC M10 et sur le SPARC M12-1. Étant donné que les PSU sont redondantes, le système peut fonctionner tant qu'au moins une PSU est en fonctionnement. C'est pourquoi même si la fonction de double alimentation électrique est activée/désactivée, cela n'affecte pas le fonctionnement du système.

4.3.1 Activation de la double alimentation électrique

Utilisez la commande `setdualpowerfeed` du microprogramme XSCF afin d'activer la double alimentation électrique.

```
XSCF> setdualpowerfeed {-a|-b bb_id} -s enable
```

Pour viser tous les châssis du système, spécifiez `-a`.

Pour viser un châssis spécifique du système, spécifiez `-b bb_id`. Pour `bb_id`, spécifiez le BB-ID du châssis. Vous pouvez saisir une valeur entière comprise entre 0 et 15 ou 80 et 83, selon la configuration du système.

Procédure de fonctionnement

1. **Activez la double alimentation électrique avec la commande `setdualpowerfeed`.**
L'exemple suivant active la double alimentation électrique pour BB-ID 1.

```
XSCF> setdualpowerfeed -b 1 -s enable  
BB#01:disable -> enable  
NOTE: Dual power feed will be enabled the next time the platform is powered on.
```

4.3.2 Désactivation de la double alimentation électrique

Utilisez la commande `setdualpowerfeed` du microprogramme XSCF afin de désactiver la double alimentation électrique.

```
XSCF> setdualpowerfeed {-a|-b bb_id} -s disable
```

Pour viser tous les châssis du système, spécifiez `-a`.

Pour viser un châssis spécifique du système, spécifiez `-b bb_id`. Pour `bb_id`, spécifiez le BB-ID du châssis. Vous pouvez saisir une valeur entière comprise entre 0 et 15 ou 80 et 83, selon la configuration du système.

Procédure de fonctionnement

1. **Désactivez la double alimentation électrique avec la commande `setdualpowerfeed`.**
Dans l'exemple suivant, tous les châssis sont ciblés.

```
XSCF> setdualpowerfeed -a -s disable  
BB#00:enable -> disable  
BB#01:enable -> disable  
NOTE: Dual power feed will be change the next time the platform is powered on.
```

4.3.3

Vérification du réglage de la double alimentation électrique

Utilisez la commande `showdualpowerfeed` du microprogramme XSCF afin de vérifier le réglage de la double alimentation électrique.

```
XSCF> showdualpowerfeed
```

Selon le statut, plusieurs résultats sont possibles.

- **Résultat lorsque la double alimentation électrique est activée**

```
BB#00: Dual power feed is enabled.
```

- **Résultat lorsque la double alimentation électrique est désactivée**

```
BB#00: Dual power feed is disabled.
```

- **Résultat lorsque la double alimentation électrique est activée puis désactivée**

```
BB#00:enable -> disable  
NOTE: Dual power feed will be change the next time the platform is powered on.
```

- **Résultat lorsque la double alimentation électrique est désactivée puis activée**

```
BB#00:disable -> enable  
NOTE: Dual power feed will be change the next time the platform is powered on.
```

Procédure de fonctionnement

1. **Vérifiez la double alimentation électrique avec la commande `showdualpowerfeed`.**

Dans l'exemple suivant, vous pouvez voir que la configuration du système a été désactivée puis activée avec BB-ID 0 et BB-ID 1.

```
XSCF> showdualpowerfeed  
BB#00:disable -> enable  
BB#01:disable -> enable  
NOTE: Dual power feed will be change the next time the platform is powered on.
```

4.4 Diminution de la consommation électrique

Cette section décrit les différentes fonctions préparées pour diminuer la consommation électrique du SPARC M12/M10.

4.4.1 Réglage de la valeur de limite supérieure de la consommation électrique

Dans le SPARC M12/M10, vous pouvez configurer la valeur de limite supérieure de la consommation électrique ainsi que l'opération à exécuter lorsque la valeur de limite supérieure est dépassée.

Utilisez la commande `setpowercapping` du microprogramme XSCF afin de définir la valeur de limite supérieure de la consommation électrique. Exécutez la commande avec un compte d'utilisateur disposant du privilège `platadm` ou `fieldeng`. La valeur définie est appliquée par XSCF immédiatement après l'exécution de la commande.

```
XSCF> setpowercapping -s option=value [[-s option=value]...]
```

Vous pouvez définir une option et une valeur pour les éléments suivants.

- Activation / désactivation de la fonction de limitation de l'alimentation (`activate_state`)
Spécifiez `enabled` (activé) ou `disabled` (désactivé). La valeur par défaut est désactivée.
- Configuration de la valeur de limite supérieure de la consommation électrique
Spécifiez-la en faisant recours à l'une des méthodes suivantes.
 - Vous pouvez spécifier un nombre en watts (`powerlimit_w`) avec une valeur numérique comprise entre 0 et 999 999.
 - Vous pouvez spécifier un pourcentage (`powerlimit_p`) avec une valeur numérique comprise entre 0 et 100.
- Durée pendant laquelle il est possible de dépasser la limite supérieure (`timelimit`)
Vous pouvez spécifier une extension de durée en secondes avec une valeur numérique comprise entre 10 et 99 999. Vous pouvez également spécifier les valeurs suivantes pour l'extension de la durée :
 - `default` : 30 secondes
 - `none` : pas d'extension de durée
- Opération à exécuter en cas de violation (`violation_actions`)
Spécifiez l'opération à exécuter lorsque l'extension de durée est dépassée après que la valeur de limite supérieure est dépassée. Spécifiez une des opérations suivantes. La valeur par défaut est `none` (aucun).

- aucun

Générez le message.

- arrêt

Génère le message et arrête la partition physique jusqu'à ce que la consommation électrique descende en dessous de la valeur de limite supérieure. Un arrêt commandé est effectué pour les partitions physiques dans l'ordre décroissant des PPAR-ID.

- poff

Génère le message et force l'arrêt de la partition physique jusqu'à ce que la consommation électrique descende en dessous de la valeur de limite supérieure. L'arrêt des partitions physiques est forcé, dans l'ordre décroissant des PPAR-ID.

Remarque : si la configuration de la limite supérieure de la consommation électrique est configurée en fonction de la consommation moyenne observée pendant le fonctionnement, le courant d'appel survenant pendant la mise sous tension ou le test d'autodiagnostic etc. du démarrage du système SPARC M12/M10 peut être un problème. Vous pouvez empêcher la consommation électrique de dépasser la valeur de limite supérieure en utilisant la commande `setpowerupdelay`, une commande XSCF, afin d'échelonner la mise sous tension des multiples partitions physiques et ainsi égaliser le courant d'appel.

Remarque : lorsque l'activité sur le serveur s'intensifie soudainement suite aux opérations des clients, la consommation électrique peut également s'intensifier rapidement. En conséquence, la consommation électrique peut excéder la limite supérieure désignée sur une longue période. Ainsi, avant de démarrer le système de votre activité, définissez la valeur de `violation_actions` sur « none » (par défaut) afin d'éviter d'affecter la continuité de fonctionnement du système. Ensuite, après avoir exécuté un test sur l'environnement client, assurez-vous que la limite supérieure de la consommation électrique (`powerlimit_w`, `powerlimit_p`) n'est pas trop basse et que la durée d'extension (`timelimit`) de la limite supérieure à dépasser n'est pas trop courte. Puis réglez la valeur pour `violation_actions`.

Pour plus de détails sur la commande `setpowercapping`, consultez la page du manuel correspondant à la commande `setpowercapping(8)` ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

Procédure de fonctionnement

1. **Exécutez la commande `showenvironment power` afin de vérifier les informations d'alimentation du système.**

L'utilisation des valeurs pour [Peak Permitted] et [Actual AC power consumption], définit la limite supérieure de la consommation électrique.

```
XSCF> showenvironment power
Power Supply Maximum      :5000W
Installed Hardware Minimum:1268W
Peak Permitted             :2322W
BB#00
    Permitted AC power consumption:5000W
    Actual AC power consumption  :1719W
```

Chaque élément affiche ce qui suit :

- Power Supply Maximum : consommation électrique maximale de l'unité d'alimentation électrique (PSU) pour le système complet
- « Installed Hardware Minimum » (minimum du matériel installé) : la valeur minimale pouvant être définie avec setpowercapping
- « Peak Permitted » (pic autorisé) : valeur de référence supposée pour les pics de consommation
- Permitted AC power consumption : consommation électrique maximale de la PSU (*1)
- Actual AC power consumption : valeur de la consommation électrique réelle du châssis

*1 Dans le SPARC M12, « Available AC power consumption » s'affiche. La consommation électrique nominale de la PSU est également affichée.

2. Exécutez la commande setpowercapping.

L'exemple suivant définit la valeur de limite supérieure à 1800 W pour la consommation électrique et à 90 secondes une l'extension de durée lorsque la valeur de limite supérieure est dépassée.

```
XSCF> setpowercapping -s powerlimit_w=1800 -s timelimit=90
activate_state      : enabled -> -
powerlimit          : 2322w -> 1800w
timelimit           : 30 -> 90
violation_actions   :none -> -
The specified options will be changed.
Continue? [y|n]      :y
configured.
activate_state      :enabled
powerlimit          :1800w
timelimit           :90
violation_actions   :none
```

3. Active la limite de la consommation électrique.

```
XSCF> setpowercapping -s activate_state=enabled
activate_state      :disabled -> enabled
powerlimit          :1800w -> -
timelimit           :90 -> -
violation_actions   :none -> -
The specified options will be changed.
Continue? [y|n]      :y
configured.
activate_state      :enabled
powerlimit          :1800w
timelimit           :90
violation_actions   :none
```

4.4.2 Gestion en cas d'anomalie au niveau de la température/d'une charge due à une alimentation anormale

Une fonction est prévue dans le SPARC M12/M10 afin de réduire la fréquence du processeur et ainsi continuer l'activité lorsqu'une charge causée par une température anormale, une alimentation anormale, ou un autre problème est détecté. Cette fonction est contrôlée pour chaque processeur sur le SPARC M12/M10. Lorsque le problème de température ou alimentation anormale est résolu, la fréquence du processeur retourne automatiquement à sa valeur de départ.

4.4.3 Diminution de la consommation électrique du matériel inutilisé ou peu utilisé

Dans le SPARC M12/M10, vous pouvez configurer le fonctionnement de chaque partition physique pour diminuer la consommation électrique du matériel inutilisé ou peu utilisé (mode d'économie d'énergie).

Lorsqu'une configuration diminuant la consommation électrique est définie, le matériel en question fonctionne avec un faible niveau de consommation électrique, correspondant à son utilisation. Ainsi, l'alimentation du matériel est diminuée tant que son taux d'utilisation est faible, et augmente dès que le taux d'utilisation remonte.

Dans le SPARC M12, la consommation électrique peut également être réduite presque sans affecter la performance de traitement du processeur grâce à l'utilisation du Solaris Power Aware Dispatcher.

Pour les exigences de logiciel du microprogramme XCP et d'Oracle Solaris requises pour l'utilisation du Solaris Power Aware Dispatcher afin de réduire la consommation électrique, consultez la dernière version des *Notes de produit Fujitsu SPARC M12*.

Pour configurer ce mode d'économie d'énergie, utilisez la commande `setpparmode` du microprogramme XSCF. Exécutez la commande avec un compte d'utilisateur disposant du privilège `platadm` ou `ppradm`.

■ SPARC M12

Pour configurer le mode d'économie d'énergie du SPARC M12, utilisez l'option `-m powermgmt_policy`.

```
XSCF> setpparmode -p ppar_id -m powermgmt_policy={elastic|performance|disabled}
```

Avec l'option `powermgmt_policy`, vous pouvez activer (`elastic` ou `performance`) ou désactiver (`disabled`) le mode d'économie d'énergie. La valeur par défaut est désactivée. Le mode est actif dès la fin de l'exécution de la commande.

La signification de chaque valeur de configuration des options est la suivante.

- `elastic`

Active le mode d'économie d'énergie du processeur et de la mémoire. Modifie l'utilisation de l'énergie du système, selon les niveaux d'utilisation actuels des processeurs et de la mémoire. Cela peut réduire la consommation électrique du système.

- performance
Active le mode d'économie d'énergie du processeur. Cela permet d'économiser de l'énergie sans trop affecter les performances, car les processeurs inutilisés et inactifs du système fonctionnent à des vitesses plus faibles ou sont peut-être en état de veille.
- disabled (par défaut)
Désactive le mode d'économie d'énergie du processeur et de la mémoire. Tous les processeurs et la mémoire du système vont fonctionner en continu à la performance la plus élevée.

Remarque : lorsque le mode d'économie d'énergie est activé avec l'option `elastic` spécifiée, la consommation électrique peut diminuer, mais les performances du processeur peuvent décliner. Spécifier la performance diminue la consommation électrique presque sans affecter la performance de traitement du processeur.

Si le microprogramme est mis à jour à partir d'une version antérieure à XCP3040 vers la version XCP3040 ou ultérieure, la fonction Power Aware Dispatcher (fonction PAD), qui consiste à utiliser Solaris Power Aware Dispatcher, est désactivée (off). Lorsque vous spécifiez la performance pour l'option `powermgmt_policy`, vous devez activer (on) la fonction PAD.

Lorsque vous spécifiez `disabled` ou `elastic` pour l'option `powermgmt_policy`, le fait que le paramétrage de la fonction PAD soit activé ou désactivé ne fait aucune différence au niveau du mode d'économie d'énergie.

Pour modifier le paramétrage de la fonction PAD, utilisez l'option `-m pad`.

```
XSCF> setpparmode -p ppar_id -m pad={off|on}
```

Avec « `pad` », vous pouvez activer (on) ou désactiver (off) la fonction PAD. Par défaut, cette fonction est activée (on).

La signification de chaque valeur de configuration des options est la suivante.

- on (par défaut)
Active la fonction PAD.
- off
Désactive la fonction PAD.
Lorsque vous désactivez cette option, l'option `powermgmt_policy` doit être configurée sur `disabled` ou `elastic`.

Effectuez le paramétrage de la fonction PAD lorsque la PPAR est arrêtée.

Lorsque le paramétrage de la fonction PAD passe de l'état désactivé à l'état activé ou vice versa, les informations de configuration du domaine logique sont restaurées à la configuration par défaut après le démarrage de la PPAR. Dans ce cas, les domaines logiques doivent être reconfigurés. Sauvegardez à l'avance les informations de configuration dans un fichier XML.

■ SPARC M10

Pour configurer le mode d'économie d'énergie du SPARC M10, utilisez l'option -m elastic.

```
XSCF> setpparmode -p ppar_id -m elastic={on|off}
```

Vous pouvez activer (« on ») ou désactiver (« off ») le mode d'économie d'énergie avec le paramètre « elastic ». Il est désactivé (« off ») par défaut. Le mode est actif dès la fin de l'exécution de la commande.

La signification de chaque valeur de configuration des options est la suivante.

- on
Active le mode d'économie d'énergie du processeur et de la mémoire. Modifie l'utilisation de l'énergie du système, selon les niveaux d'utilisation actuels des processeurs et de la mémoire. Cela peut réduire la consommation électrique du système.
- off (par défaut)
Désactive le mode d'économie d'énergie du processeur et de la mémoire. Tous les processeurs et la mémoire du système vont fonctionner en continu à la performance la plus élevée.

Remarque : lorsque le mode d'économie d'énergie est activé, la consommation électrique peut diminuer, mais les performances du processeur peuvent décliner.

Pour plus de détails sur la commande setpparmode, consultez la page du manuel correspondant à la commande setpparmode(8) ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

Procédure de fonctionnement

■ SPARC M12

Remarque :

- Lorsque la fonction PAD est désactivée, vous ne pouvez pas modifier le paramétrage du mode d'économie d'énergie sur performance. Après avoir activé la fonction PAD (on), réglez le paramètre sur performance.
 - Lorsque le mode d'économie d'énergie est configuré sur performance, vous ne pouvez pas désactiver la fonction PAD (off). Après avoir configuré le mode d'économie d'énergie sur disabled ou elastic, désactivez la fonction.
-

Ci-dessous se trouve un exemple pour configurer le mode d'économie d'énergie sur performance.

1. **Exécutez la commande showpparmode pour confirmer les paramètres du mode d'économie d'énergie et de la fonction PAD. L'exemple suivant indique que le mode d'économie d'énergie est désactivé et que la fonction PAD est activée.**


```

XSCF> showpparmode -p 0
Host-ID                :90060027
Diagnostic Level        :min
Message Level           :normal
Alive Check             :on
Watchdog Reaction       :reset
Break Signal            :on
Autoboot (Guest Domain) :on
Power Aware Dispatcher  :on
Power Management Policy :disabled
IOreconfigure           :false
CPU Mode                :-
PPAR DR (Current)       :-
PPAR DR (Next)          :off

```

2. **Exécutez la commande setpparmode pour configurer le mode d'économie d'énergie sur performance.**

```

XSCF> setpparmode -p 0 -m powermgmt_policy=performance
Diagnostic Level        :min          -> -
Message Level           :normal       -> -
Alive Check             :on           -> -
Watchdog Reaction       :reset        -> -
Break Signal            :on           -> -
Autoboot (Guest Domain) :on           -> -
Power Aware Dispatcher  :on           -> -
Power Management Policy :disabled     -> performance
IOreconfigure           :false        -> -
CPU Mode                :-
PPAR DR                 :off          -> -
The specified modes will be changed.
Continue? [y|n] :y
configured.
Diagnostic Level        :min
Message Level           :normal
Alive Check             :on (alive check:available)
Watchdog Reaction       :reset (watchdog reaction:reset)
Break Signal            :on (break signal:non-send)
Autoboot (Guest Domain) :on
Power Aware Dispatcher  :on
Power Management Policy :performance
IOreconfigure           :false
CPU Mode                :-
PPAR DR                 :off

```

3. **Exécutez la commande setpparmode, et vérifiez le paramètre.**

```

XSCF> showpparmode -p 0
Host-ID                :90060027
Diagnostic Level        :min
Message Level           :normal
Alive Check             :on

```

Watchdog Reaction	:reset
Break Signal	:on
Autoboot(Guest Domain)	:on
Power Aware Dispatcher	:on
Power Management Policy	:performance
IOreconfigure	:false
CPU Mode	:-
PPAR DR(Current)	:-
PPAR DR(Next)	:off

■ Pour le SPARC M10

Ci-dessous se trouve un exemple pour activer le mode d'économie d'énergie.

1. **Exécutez la commande `showpparmode` pour vérifier si le mode d'économie d'énergie est activé ou désactivé pour le matériel inutilisé ou peu utilisé.**

```
XSCF> showpparmode -p 0
Host-ID                :0f010f10
Diagnostic Level        :min
Message Level           :normal
Alive Check             :on
Watchdog Reaction       :reset
Break Signal            :on
Autoboot(Guest Domain)  :on
Elastic Mode            :off
IOreconfigure           :true
CPU Mode                :auto
PPAR DR(Current)        :-
PPAR DR(Next)           :off
Ethernet Address        :00:0b:5d:e2:01:0c
```

2. **Exécutez la commande `setpparmode` pour activer le mode d'économie d'énergie.**

```
XSCF> setpparmode -p 0 -m elastic=on
Diagnostic Level        :min      -> -
Message Level           :normal   -> -
Alive Check             :on       -> -
Watchdog Reaction       :reset    -> -
Break Signal            :on       -> -
Autoboot(Guest Domain)  :on       -> -
Elastic Mode            :off      -> on
IOreconfigure           :true     -> -
CPU Mode                :auto     -> -
PPAR DR                 :off      -> -
The specified modes will be changed.
Continue? [y|n]:y
configured.
Diagnostic Level        :min
Message Level           :normal
Alive Check             :on (alive check:available)
Watchdog Reaction       :reset (watchdog reaction:reset)
```

Break Signal	:on (break signal:non-send)
Autoboot (Guest Domain)	:on
Elastic Mode	:on
IOreconfigure	:true
CPU Mode	:auto
PPAR DR	:off

3. Exécutez la commande `setpparmode`, et vérifiez le paramètre.

```
XSCF> showpparmode -p 0
Host-ID                :0f010f10
Diagnostic Level        :min
Message Level           :normal
Alive Check             :on
Watchdog Reaction       :reset
Break Signal            :on
Autoboot (Guest Domain) :on
Elastic Mode            :on
IOreconfigure           :true
CPU Mode                :auto
PPAR DR (Current)       :-
PPAR DR (Next)          :off
Ethernet Address        :00:0b:5d:e2:01:0c
```

4.5 Connexion d'un lecteur de DVD

Le SPARC M12/M10 ne dispose pas d'un lecteur DVD interne. Pour installer Oracle Solaris et des applications professionnelles à partir du lecteur DVD, utilisez un lecteur DVD connecté de l'une des façons suivantes :

- Lecteur DVD externe connecté à un port USB
- Lecteur DVD monté sur un terminal connecté au XSCF-LAN

Cette section décrit le lecteur DVD externe connecté à un port USB. Pour utiliser le lecteur DVD monté sur un terminal, consultez « [4.6 Utilisation du stockage à distance](#) ».

4.5.1 Utilisation d'un lecteur DVD externe

Le châssis du SPARC M12/M10 dispose de ports USB à l'avant et à l'arrière. Pour utiliser un lecteur DVD externe, connectez-le à l'un des ports USB. Utilisez un adaptateur CA dédié pour fournir l'alimentation nécessaire au lecteur DVD externe connecté.

Figure 4-1 Port USB (SPARC M12-1) pouvant être connecté à un lecteur DVD

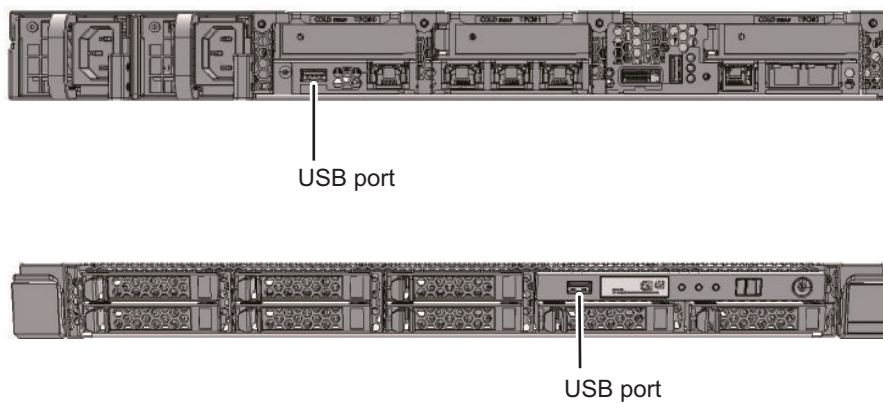


Figure 4-2 Port USB (SPARC M12-2) pouvant être connecté à un lecteur DVD

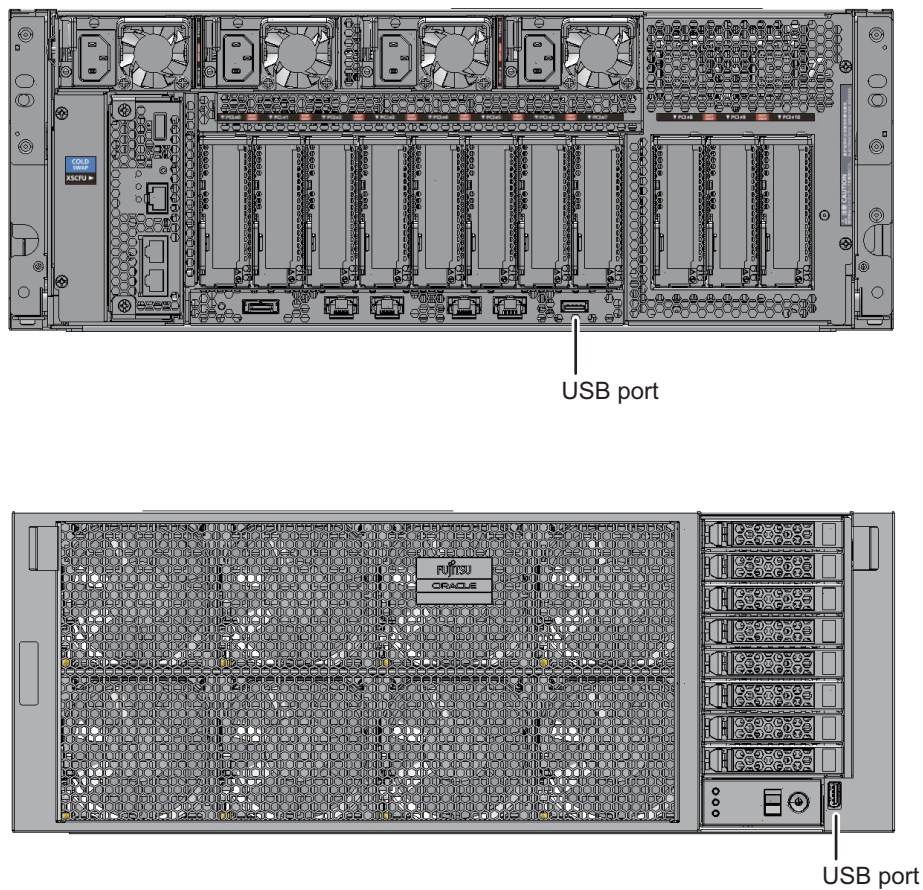


Figure 4-3 Port USB (SPARC M12-2S) pouvant être connecté à un lecteur DVD

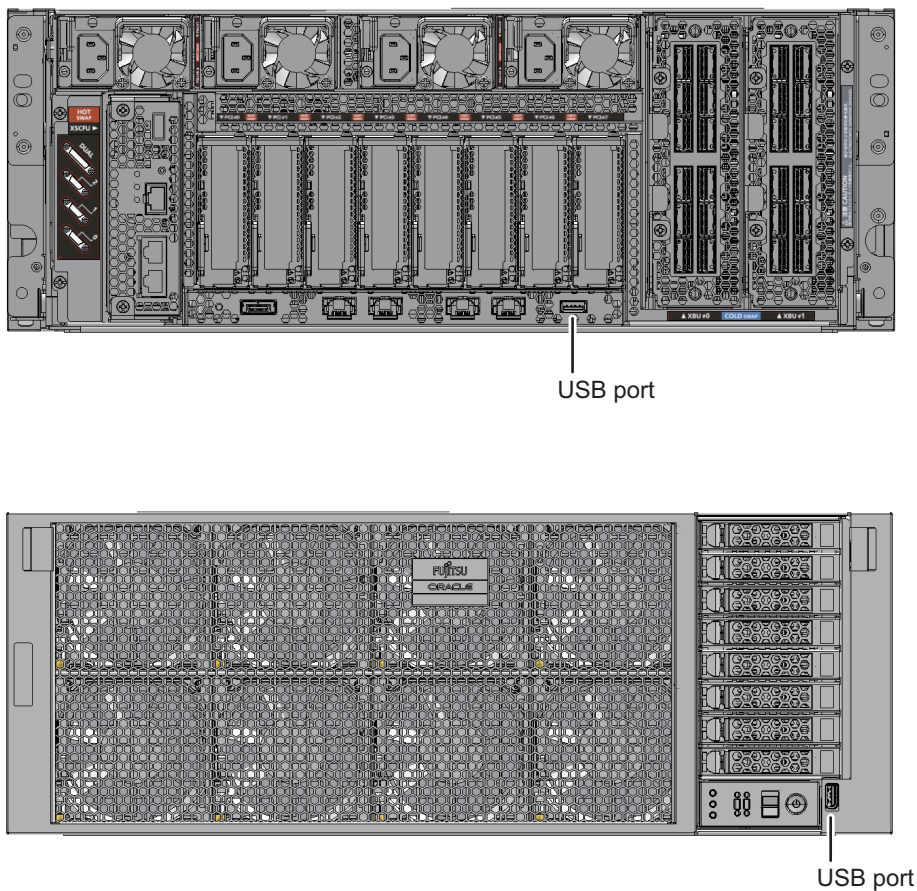


Figure 4-4 Port USB (SPARC M10-1) pouvant être connecté à un lecteur DVD

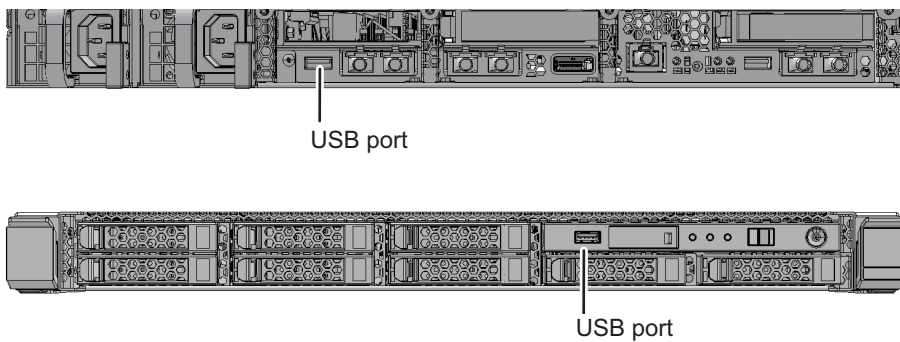
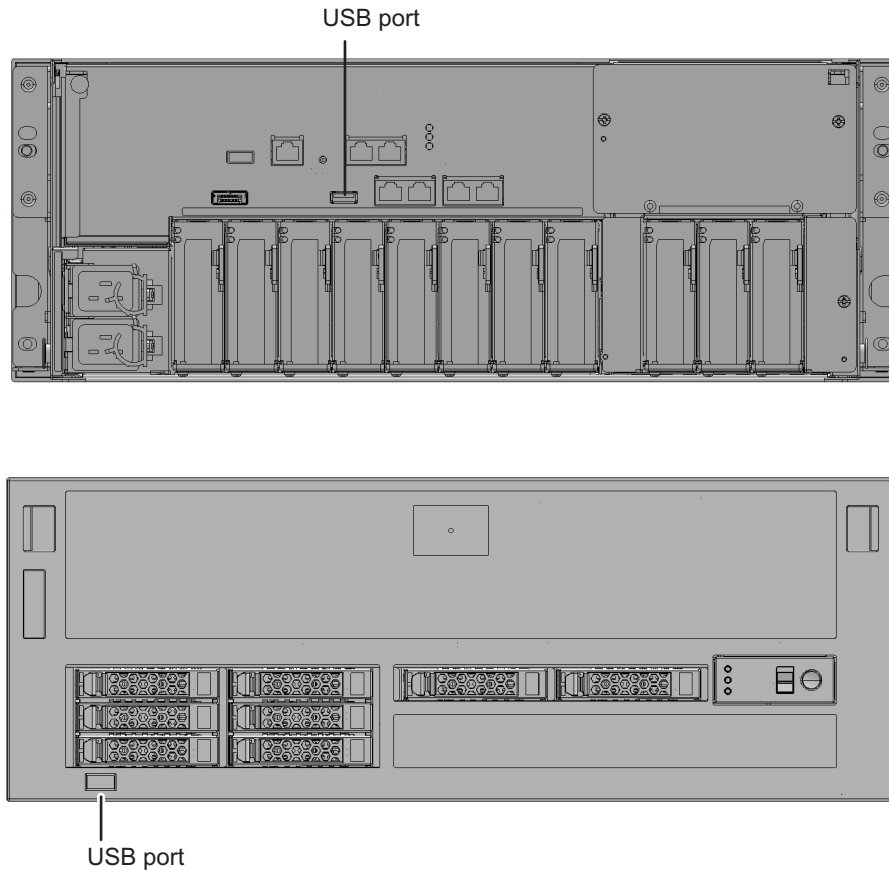


Figure 4-5 Port USB (SPARC M10-4/M10-4S) pouvant être connecté à un lecteur DVD



4.5.2 Utilisation d'un lecteur DVD externe pour installer Oracle Solaris

Lors de l'installation d'Oracle Solaris sur OpenBoot PROM à partir d'un lecteur CD / DVD-ROM, spécifiez le chemin d'accès de périphériques adapté au modèle de SPARC M12/M10 que vous utilisez. Pour plus de détails sur le chemin d'accès de périphériques pour chaque modèle, consultez « [Annexe A Listes des chemins d'accès de périphériques des systèmes SPARC M12/M10](#) ». Pour plus de détails sur les alias du lecteur DVD, consultez « [Annexe J Listes des alias des lecteurs DVD](#) ».

Voici la procédure à suivre afin de spécifier le chemin d'accès de périphériques et d'installer Oracle Solaris.

1. **Connectez un lecteur USB DVD à un port USB à l'avant ou à l'arrière du châssis.**

Si plusieurs lecteurs DVD sont connectés, déconnectez tous les lecteurs DVD

USB qui ne seront pas utilisés pour l'installation.

2. **A partir de l'invite ok de OpenBoot PROM, exécutez la commande show-disks et confirmez le chemin d'accès de périphériques.**

- Exemple de connexion du lecteur DVD USB sur le panneau avant dans le SPARC M12-1

```
{0} ok show-disks
a) /pci@8100/pci@4/pci@0/pci@8/usb@0/cdrom@6/disk
b) /pci@8100/pci@4/pci@0/pci@0/scsi@0/disk
c) /iscsi-hba/disk
q) NO SELECTION
Enter Selection, q to quit: q
```

- Exemple de connexion du lecteur DVD USB (USB3.0) sur le panneau arrière dans le SPARC M12-1

```
{0} ok show-disks
a) /pci@8100/pci@4/pci@0/pci@8/usb@0/hub@1/cdrom@1/disk
b) /pci@8100/pci@4/pci@0/pci@0/scsi@0/disk
c) /iscsi-hba/disk
q) NO SELECTION
Enter Selection, q to quit: q
```

- Exemple de connexion du lecteur DVD USB (USB2.0/1.1) sur le panneau arrière dans le SPARC M12-1

```
{0} ok show-disks
a) /pci@8100/pci@4/pci@0/pci@8/usb@0/hub@5/cdrom@1/disk
b) /pci@8100/pci@4/pci@0/pci@0/scsi@0/disk
d) /iscsi-hba/disk
q) NO SELECTION
Enter Selection, q to quit: q
```

- Exemple de connexion du lecteur DVD USB sur le panneau avant dans le SPARC M12-2/M12-2S

Lorsque deux processeurs sont installés

```
{0} ok show-disks
a) /pci@8100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk
b) /pci@8100/pci@4/pci@0/pci@0/scsi@0/disk
c) /pci@8500/pci@4/pci@0/pci@0/scsi@0/disk
d) /iscsi-hba/disk
q) NO SELECTION
Enter Selection, q to quit: q
```

- Exemple de connexion du lecteur DVD USB (USB3.0) sur le panneau arrière dans le SPARC M12-2/M12-2S

Remarque : si USB3.0 est utilisé, il fonctionne comme un USB2.0.

Lorsque deux processeurs sont installés

```
{0} ok show-disks
a) /pci@8100/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk
b) /pci@8100/pci@4/pci@0/pci@0/scsi@0/disk
c) /pci@8500/pci@4/pci@0/pci@0/scsi@0/disk
d) /iscsi-hba/disk
q) NO SELECTION
Enter Selection, q to quit: q
```

- Exemple de connexion du lecteur DVD USB (USB2.0/1.1) sur le panneau arrière dans le SPARC M12-2/M12-2S

Lorsque deux processeurs sont installés

```
{0} ok show-disks
a) /pci@8100/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk
b) /pci@8100/pci@4/pci@0/pci@0/scsi@0/disk
c) /pci@8500/pci@4/pci@0/pci@0/scsi@0/disk
d) /iscsi-hba/disk
q) NO SELECTION
Enter Selection, q to quit: q
```

- Exemple de connexion du lecteur DVD USB sur le panneau avant dans le SPARC M10-1

```
{0} ok show-disks
a) /pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/cdrom@2/disk
b) /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk
c) /iscsi-hba/disk
q) NO SELECTION
Enter Selection, q to quit: q
```

- Exemple de connexion du lecteur DVD USB sur le panneau arrière dans le SPARC M10-1

```
{0} ok show-disks
a) /pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/cdrom@1/disk
b) /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk
c) /iscsi-hba/disk
q) NO SELECTION
Enter Selection, q to quit: q
```

- Exemple de connexion du lecteur DVD USB sur le panneau avant dans le SPARC M10-4/M10-4S


```
{0} ok show-disks
a) /pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk
b) /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk
c) /iscsi-hba/disk
q) NO SELECTION
Enter Selection, q to quit: q
```

- Exemple de connexion du lecteur DVD USB sur le panneau arrière dans le SPARC M10-4/M10-4S

```
{0} ok show-disks
a) /pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/cdrom@1/disk
b) /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk
c) /iscsi-hba/disk
q) NO SELECTION
Enter Selection, q to quit: q
```

3. **Spécifiez le chemin d'accès de périphériques indiqué dans le a) de l'étape 2, exécutez la commande boot et installez Oracle Solaris.**

- Exemple de spécification de lecteur DVD USB connecté sur le panneau avant dans le SPARC M12-1

```
{0} ok boot /pci@8100/pci@4/pci@0/pci@8/usb@0/cdrom@6/disk
```

- Exemple de spécification de lecteur DVD USB (USB3.0) connecté sur le panneau arrière dans le SPARC M12-1

```
{0} ok boot /pci@8100/pci@4/pci@0/pci@8/usb@0/hub@1/cdrom@1/disk
```

- Exemple de spécification de lecteur DVD USB (USB2.0/1.1) connecté sur le panneau arrière dans le SPARC M12-1

```
{0} ok boot /pci@8100/pci@4/pci@0/pci@8/usb@0/hub@5/cdrom@1/disk
```

- Exemple de spécification de lecteur DVD USB connecté sur le panneau avant dans le SPARC M12-2/M12-2S lorsque deux processeurs sont installés

```
{0} ok boot /pci@8100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk
```

- Exemple de spécification de lecteur DVD USB (USB3.0) connecté sur le panneau arrière dans le SPARC M12-2/M12-2S lorsque deux processeurs sont installés

```
{0} ok boot /pci@8100/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk
```

- Exemple de spécification de lecteur DVD USB (USB2.0/1.1) connecté sur le panneau arrière dans le SPARC M12-2/M12-2S lorsque deux processeurs sont installés

```
{0} ok boot /pci@8100/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk
```

- Exemple de spécification de lecteur DVD USB connecté sur le panneau avant dans le SPARC M10-1

```
{0} ok boot /pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/cdrom@2/disk
```

- Exemple de spécification de lecteur DVD USB connecté sur le panneau arrière dans le SPARC M10-1

```
{0} ok boot /pci@8100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk
```

- Exemple de spécification de lecteur DVD USB connecté sur le panneau avant dans le SPARC M10-4/M10-4S

```
{0} ok boot /pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk
```

- Exemple de spécification de lecteur DVD USB connecté sur le panneau arrière dans le SPARC M10-4/M10-4S

```
{0} ok boot /pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/cdrom@1/disk
```

Remarque : selon le type de lecteur CD / DVD utilisé, « /cdrom@x » peut être remplacé par « /storage@x ».

Remarque : supposons que seul un lecteur DVD USB sur le panneau avant est connecté avec le SPARC M10-4/M10-4S et que vous spécifiez le chemin d'accès du lecteur vers un lecteur DVD USB sur le panneau arrière pour exécuter la commande boot. Même si le chemin d'accès du lecteur spécifié est incorrect, le démarrage est effectué depuis le DVD USB connecté au panneau avant. Lors de l'exécution de la commande boot, vérifiez toujours que l'appareil spécifié est correct.

4.6 Utilisation du stockage à distance

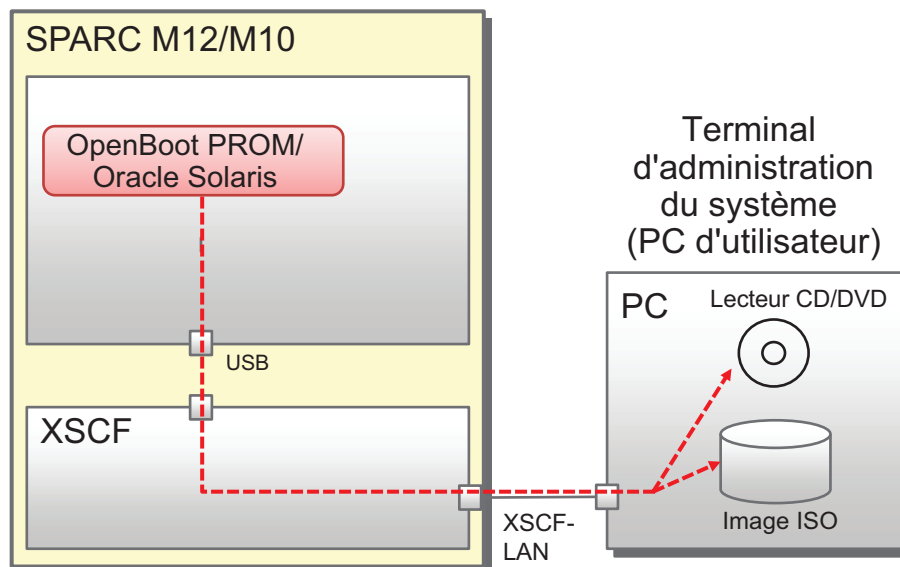
Cette section décrit le stockage à distance qui autorise l'accès au stockage monté

(supports) dans les terminaux. Pour le stockage à distance, utilisez l'Ethernet de l'interface du réseau XSCF (XSCF-LAN).

4.6.1 Qu'est-ce que le stockage à distance ?

Le stockage à distance est une fonction permettant d'accéder au stockage des terminaux, tels que le terminal de gestion du système ou un PC utilisateur, via le XSCF-LAN. Le stockage à distance prend uniquement en charge la lecture depuis le stockage vers un système SPARC M12/M10. [Figure 4-6](#) est un schéma conceptuel présentant comment la fonction de stockage à distance est utilisée depuis OpenBoot PROM ou Oracle Solaris pour accéder à un support dans un terminal.

Figure 4-6 Schéma conceptuel du stockage à distance



Le stockage à distance autorise des connexions depuis des domaines logiques vers les supports suivants :

- Supports insérés dans le lecteur CD/DVD monté sur/connecté à un terminal
- Image ISO sur un terminal

De plus, si tous les environnements suivants sont en place, vous pouvez utiliser le stockage à distance par l'intermédiaire des paramètres requis avec le XSCF :

- Environnement requis pour le système SPARC M12/M10
 - Le réseau XSCF-LAN peut être utilisé.
 - Le service HTTPS est activé et XSCF Web peut être utilisé.
- Environnement requis pour les terminaux
 - Le logiciel Java Runtime Environment peut être utilisé.

Pour plus de détails sur les paramètres du réseau XSCF, consultez « [3.9 Configuration du réseau XSCF](#) ». Pour plus de détails sur la configuration d'exploitation requise par XSCF Web et la procédure permettant d'activer le service XSCF HTTPS, consultez « [3.8 Configuration du service HTTPS pour la connexion à XSCF](#) ». De plus, pour

plus de détails sur la configuration d'exploitation requise par le logiciel Java Runtime Environment sur les terminaux, consultez « [4.6.4 Configuration d'exploitation requise des terminaux et des navigateurs](#) ».

Du point de vue d'Oracle Solaris

Lorsque les supports dans les terminaux sont accessibles depuis les domaines logiques à l'aide du stockage à distance, les dispositifs de stockage à distance sont reconnus en tant qu'appareils USB depuis OpenBoot PROM et Oracle Solaris, comme indiqué ci-dessous.

- Un exemple d'Oracle Solaris

```
# cfmadm -al
Ap_Id Type Receptacle Occupant Condition
...
usb1/3 usb-storage connected configured ok
```

- Un exemple d'OpenBoot PROM

```
{0} ok show-disks
a) /pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk
b) /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk
...
Enter Selection, q to quit:
```

Pour plus de détails sur la façon de connecter des supports, consultez « [4.6.12 Connexion aux supports en utilisant le stockage à distance](#) ». Pour plus de détails sur la façon d'accéder aux supports, consultez « [4.6.13 Utilisation du stockage à distance depuis Oracle Solaris](#) ».

4.6.2 Configuration réseau du stockage à distance

Configuration réseau

Le stockage à distance utilise le réseau XSCF-LAN du châssis du SPARC M12/M10 pour mettre en place un accès aux supports dans les terminaux.

[Figure 4-7](#) montre la configuration réseau lors de l'utilisation du stockage à distance, où le système est configuré seulement avec un SPARC M12/M10.

Figure 4-7 Système configuré avec seulement un SPARC M12/M10

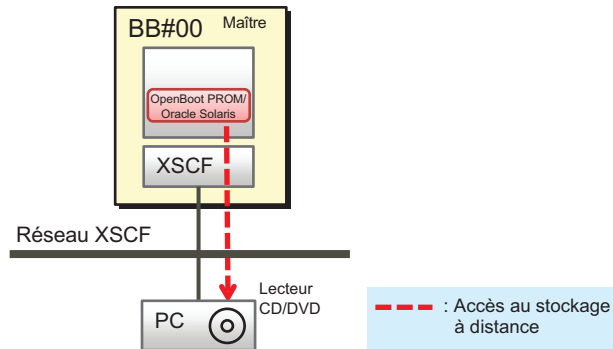
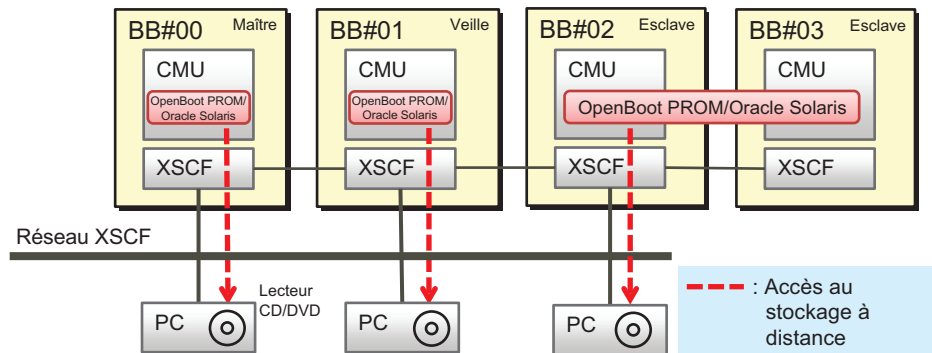


Figure 4-8 montre la configuration réseau lors de l'utilisation du stockage à distance dans le système dans une configuration de bloc de construction (sans boîtier à barre transversale). Le LAN du XSCF maître et le terminal de gestion du système, le XSCF-LAN utilisé via le stockage à distance, et le LAN des terminaux sont connectés dans le même sous-réseau.

Figure 4-8 Configuration réseau du stockage à distance (sans boîtier à barre transversale)

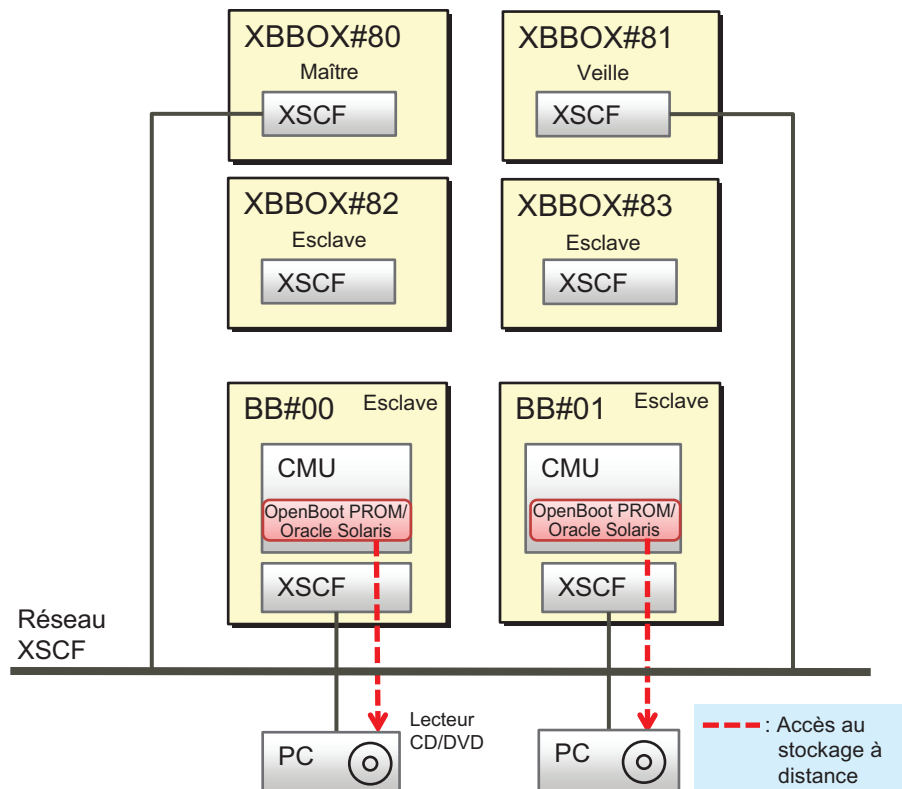


Remarque : s'il n'y a qu'un PC, vous pouvez même utiliser le stockage à distance depuis chaque SPARC M12/M10 en commutant le châssis du système SPARC M12/M10 se connectant à chaque fois.

Figure 4-9 montre la configuration réseau lors de l'utilisation du stockage à distance, où le système dans une configuration de bloc de construction est connecté à un boîtier à barre transversale. Lors de l'utilisation du stockage à distance, n'utilisez pas le XSCF-LAN du châssis de boîtier à barre transversale pour vous connecter aux supports. Utilisez le XSCF-LAN du châssis du système SPARC M12/M10, qui est un châssis esclave.

Dans Figure 4-9, le LAN du XSCF maître et le terminal de gestion du système, le XSCF-LAN utilisé via le stockage à distance, et le LAN des terminaux sont connectés dans le même sous-réseau.

Figure 4-9 Configuration réseau du stockage à distance (en cas de connexion à un boîtier à barre transversale)



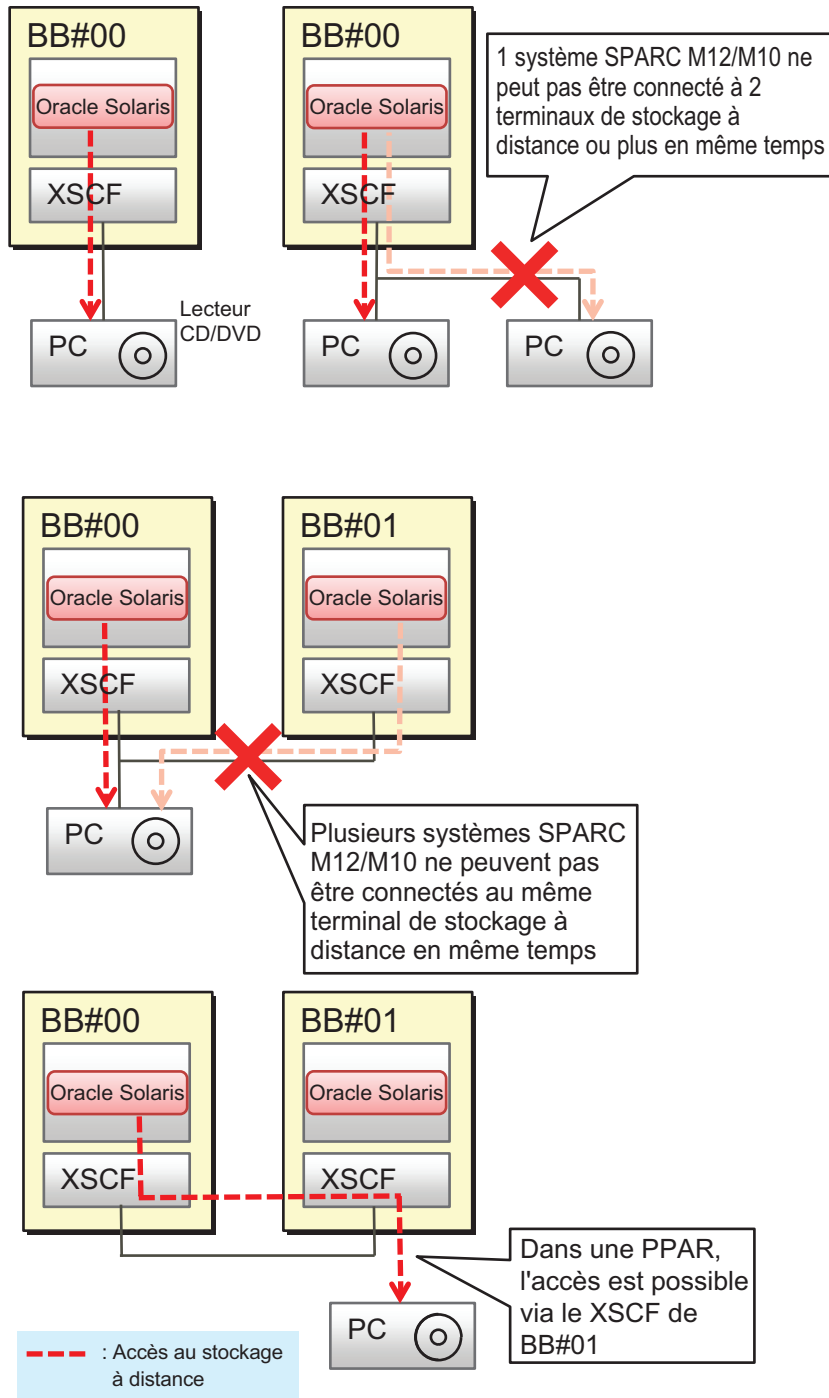
Remarque : s'il n'y a qu'un PC, vous pouvez même utiliser le stockage à distance depuis chaque SPARC M12/M10 en commutant le châssis du système SPARC M12/M10 se connectant à chaque fois.

Règles pour une connexion 1 à 1 entre un SPARC M12/M10 et un PC

Comme indiqué dans [Figure 4-10](#), le châssis du SPARC M12/M10 est connecté au support du terminal (PC) selon une configuration 1 à 1. Le même châssis de SPARC M12/M10 ne peut pas être connecté à deux terminaux ou plus et plusieurs châssis de SPARC M12/M10 ne peuvent pas être connectés au même terminal en même temps.

Pour une connexion depuis le domaine logique BB#00 vers un support dans un terminal via le XSCF de BB#01, veuillez noter que BB#00 et BB#01 doivent appartenir à la même partition physique.

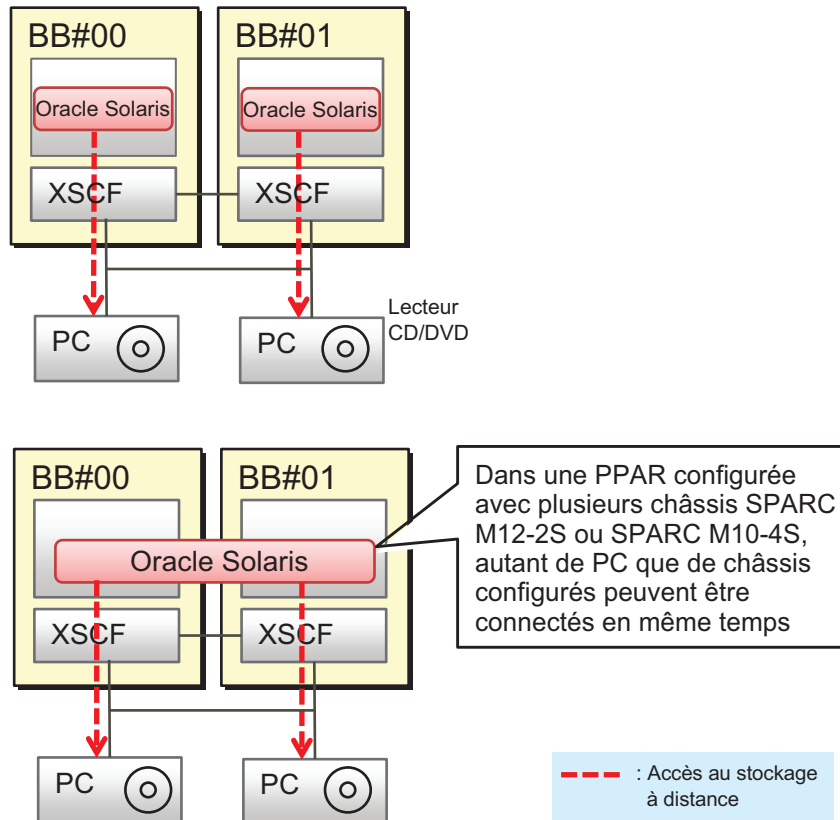
Figure 4-10 Règles pour une connexion avec un châssis de SPARC M12/M10



Comme indiqué dans [Figure 4-11](#), dans une configuration système avec plusieurs systèmes SPARC M12-2S ou plusieurs systèmes SPARC M10-4S, un terminal peut

être installé pour chaque système SPARC M12-2S/M10-4S selon une configuration 1 à 1. Parmi ces terminaux installés, plusieurs terminaux peuvent être connectés en même temps. De même, dans une configuration de partitions physiques avec plusieurs systèmes SPARC M12-2S ou plusieurs systèmes SPARC M10-4S, autant de terminaux que de châssis configurés peuvent être connectés en même temps.

Figure 4-11 Formes de connexion simultanée pour plusieurs systèmes SPARC M12-2S ou plusieurs systèmes SPARC M10-4S



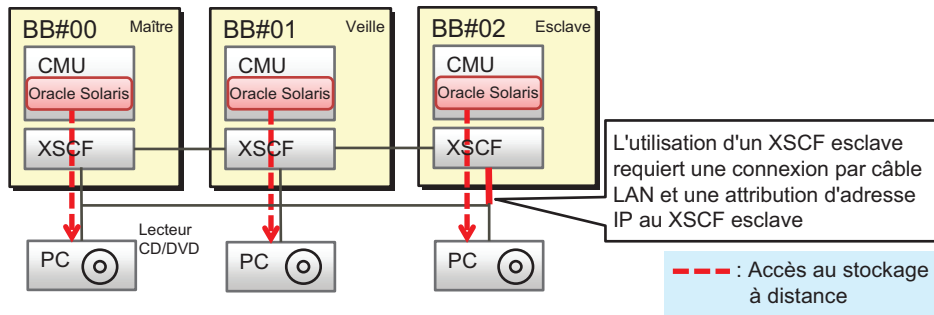
Connexion via un XSCF esclave

Comme indiqué dans [Figure 4-12](#), le stockage à distance de SPARC M12/M10 peut même être connecté via un XSCF esclave.

Remarque : le XSCF-LAN du XSCF esclave ne peut être utilisé que pour le stockage à distance. Il ne peut pas être utilisé pour des services tels que Telnet, SSH, XSCF Web et SNMP.

Remarque : le XSCF-LAN du boîtier à barre transversale esclave ne peut pas être utilisé pour le stockage à distance.

Figure 4-12 Connexion au stockage à distance via un XSCF esclave



Remarque : s'il n'y a qu'un PC, vous pouvez même utiliser le stockage à distance depuis chaque SPARC M12/M10 en commutant le châssis du système SPARC M12/M10 se connectant à chaque fois.

Avant de commencer la configuration du stockage à distance

Avant de commencer la configuration du stockage à distance avec XSCF Web, vous devez avoir effectué les réglages réseau du XSCF maître/de veille. Cela est dû au fait que le XSCF doit être redémarré lorsque le réseau XSCF maître/de veille a été configuré. De plus, pour activer le service HTTPS afin que XSCF Web puisse être utilisé, les réglages réseau du XSCF maître et les réglages du service HTTPS doivent avoir été effectués.

Pour établir une connexion via un XSCF esclave, vous devez connecter un câble XSCF-LAN et définir au préalable l'adresse IP du XSCF-LAN. De plus, pour les réglages réseau du XSCF esclave, configurez le stockage à distance depuis XSCF Web ou le shell XSCF, et non pas avec la commande `setnetwork` ou le menu [Réseau] sur le XSCF Web.

Si le boîtier à barre transversale est connecté, l'adresse IP du XSCF-LAN du châssis du SPARC M12/M10 (châssis esclave) connecté au boîtier à barre transversale doit être définie pour empêcher le XSCF-LAN du boîtier à barre transversale d'être utilisé pour un stockage à distance.

Tableau 4-2 répertorie les différences de réglages réseau de XSCF entre une utilisation du stockage à distance via le XSCF maître/de veille et une utilisation via un XSCF esclave.

Tableau 4-2 Différences de réglages réseau de XSCF pour l'utilisation du stockage à distance

XSCF	Paramètres du réseau XSCF-LAN
Châssis du SPARC M12/M10 d'un XSCF maître/de veille	Page [Réseau] de XSCF Web Ou bien, commandes setnetwork, setroute et applynetwork Remarque : un redémarrage du XSCF est nécessaire.
Châssis du SPARC M12/M10 du XSCF esclave	Page [Stockage à distance] de XSCF Web Ou bien, Commandes setremotestorage et showremotestorage Remarque : un redémarrage du XSCF n'est pas nécessaire.

Remarque : si aucune passerelle n'est définie dans les paramètres d'acheminement, le terminal et le XSCF-LAN doivent être connectés dans le même sous-réseau.

Dans une configuration système avec plusieurs systèmes SPARC M12-2S ou plusieurs systèmes SPARC M10-4S, l'adresse IP physique est utilisée comme adresse IP du XSCF-LAN pour accéder aux supports d'un terminal avec stockage à distance. L'adresse IP de prise de contrôle (adresse virtuelle) n'est pas utilisée. Pour plus de détails sur les paramètres du réseau XSCF, consultez « [4.6.10 Configuration du XSCF-LAN utilisé avec le stockage à distance](#) ».

4.6.3 Moyens d'utilisation du stockage à distance

Deux types d'écrans sont utilisés pour les réglages et les opérations pour l'utilisation du stockage à distance : l'un est la console XSCF Web et l'autre est [Serveur de stockage à distance XSCF] sur le terminal.

[Figure 4-13](#) montre la page [Stockage à distance] de XSCF Web. Sur la page, vous pouvez configurer le stockage à distance. Lorsque vous cliquez sur le bouton [Lancer], le serveur de stockage à distance XSCF pour la sélection/le démarrage du support démarre depuis le logiciel Java Runtime Environment sur le terminal. Puis l'écran [Serveur de stockage à distance XSCF] s'ouvre, comme présenté dans [Figure 4-14](#). Le support peut être connecté/arrêté plusieurs fois lorsque le serveur de stockage à distance XSCF fonctionne.

Figure 4-13 Page [Stockage à distance] de XSCF Web

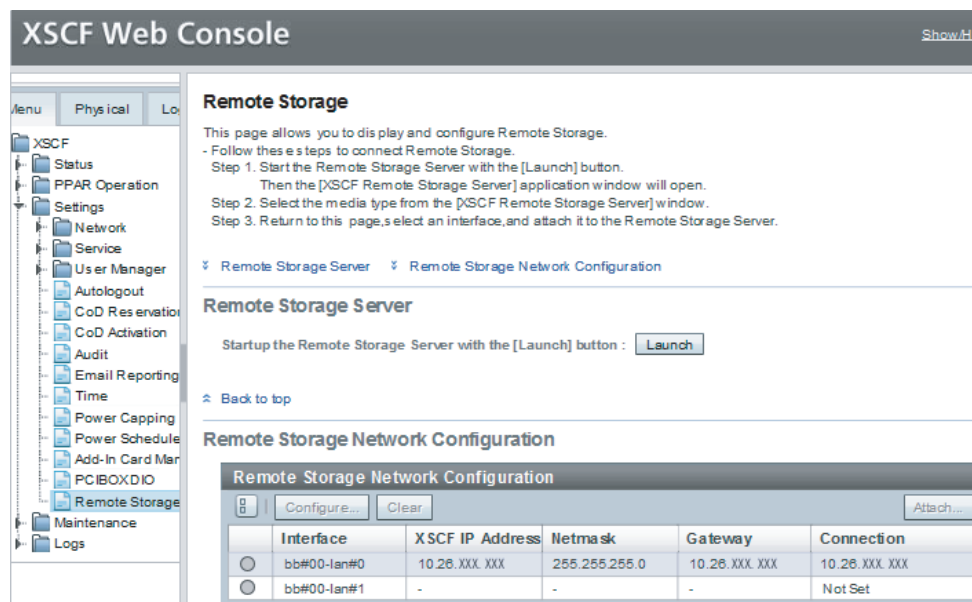
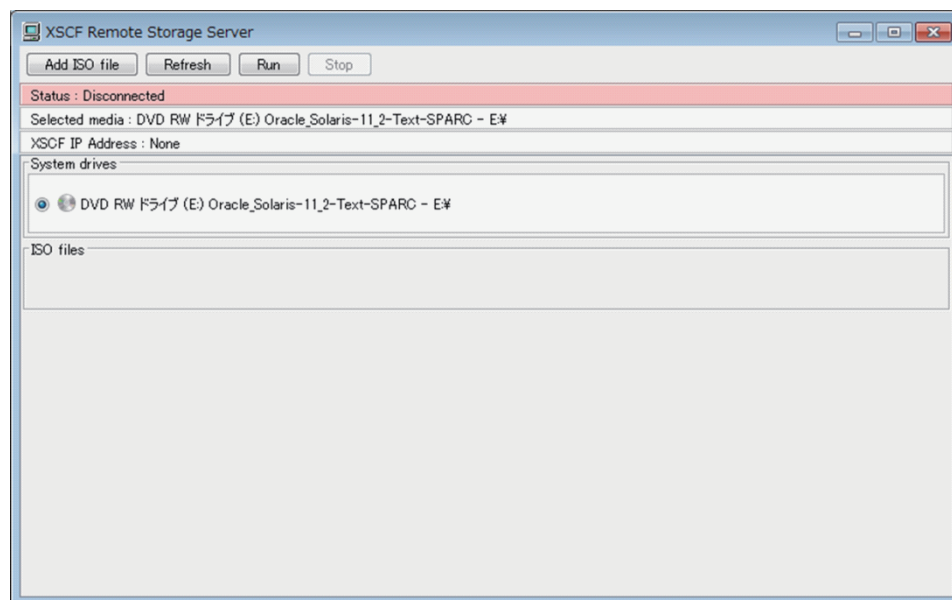


Figure 4-14 Écran [Serveur de stockage à distance XSCF]



4.6.4 Configuration d'exploitation requise des terminaux et des navigateurs

Cette section décrit la configuration d'exploitation requise et différents réglages pour utiliser le stockage à distance.

Configuration d'exploitation requise des terminaux et des navigateurs

Tableau 4-3 répertorie la configuration d'exploitation requise pour le système d'exploitation Windows sur les terminaux, prenant en charge le stockage à distance.

Tableau 4-3 Configuration d'exploitation requise des terminaux

Type	Configuration d'exploitation requise
Systèmes d'exploitation Windows	Windows 7, Windows 8, Windows 8.1, ou Windows 10

La version de Java Runtime Environment installée sur le terminal doit être la version correspondant au navigateur utilisé avec XSCF Web. Tableau 4-4 répertorie les combinaisons de Java Runtime Environment et d'un navigateur.

Tableau 4-4 Combinaisons de Java Runtime Environment et d'un navigateur utilisées avec XSCF Web

Navigateur	Java Runtime Environment
Microsoft Internet Explorer 8 ou 9, version 32 bits	Java Runtime Environment 8, version 32 bits
Microsoft Internet Explorer 8 ou 9, version 64 bits	Java Runtime Environment 8, version 64 bits
Microsoft Internet Explorer 10 ou 11	Java Runtime Environment 8, version 32 bits
Mozilla Firefox 10.0 à ESR 52, version 32 bits	Java Runtime Environment 8, version 32 bits

Remarque : téléchargez Java Runtime Environment depuis le site Web d'Oracle.

Pour plus de détails sur les systèmes d'exploitation du terminal, les dernières versions prises en charge de Java Runtime Environment et les navigateurs pris en charge par XSCF Web, consultez les dernières *Notes de produit* pour votre serveur.

Paramètres de répertoire de la variable d'environnement TMP du système d'exploitation Windows

Le fonctionnement du serveur de stockage à distance XSCF génère les trois fichiers

suivants pour la maintenance et le contrôle. Les fichiers sont générés dans le dossier défini dans la variable d'environnement TMP du système d'exploitation Windows du terminal. Si ces fichiers ne peuvent pas être générés dans le dossier défini, le serveur de stockage à distance XSCF ne parvient pas à démarrer, désactivant le stockage à distance.

- Fichier de trace (Remote_Storage_Trace.txt, maximum 512 Ko)
- Fichier de trace compressé provenant de la génération précédente (Remote_Storage_Trace_1.txt.zip, taille maximale de 512 Ko)
- Fichier de verrouillage pour surveiller les démarrages multiples (RemoteStorageLockFile 0 o)

En cas d'utilisation du stockage à distance, assurez-vous de vérifier ce qui suit.

- Un répertoire est défini dans la variable d'environnement TMP du système d'exploitation Windows.
- Les privilèges d'accès au répertoire défini ne sont pas des privilèges d'administrateur.

Dans le système d'exploitation Windows, le dossier suivant est le paramétrage par défaut de la variable d'environnement TMP.

```
%USERPROFILE%\AppData\Local\Temp
```

Lorsque le stockage à distance est utilisé avec le paramétrage par défaut, le démarrage du serveur de stockage à distance XSCF génère les fichiers dans le dossier suivant. Nous vous recommandons d'utiliser le paramétrage par défaut.

```
C:\Users\UserName\AppData\Local\Temp\Remote_Storage\
```

Port utilisé et autorisation sur un terminal

Le terminal utilise le port tcp/3260 pour une communication bidirectionnelle entre le serveur de stockage à distance XSCF et le XSCF.

Par conséquent, effectuez les réglages suivants sur le terminal.

- Dans le système d'exploitation Windows, autorisez la connexion au port 3260.
- Dans le logiciel antivirus utilisé, autorisez la connexion au port 3260.
- En cas d'utilisation du pare-feu Windows, autorisez les programmes binaires Java Platform SE.

Cliquer sur le bouton [Lancer] dans XSCF Web lorsque le stockage à distance est utilisé génère le message d'avertissement présenté dans [Figure 4-15](#). Dans ce cas, effectuez l'étape suivante.

Figure 4-15 Message d'avertissement si le pare-feu Windows est utilisé



1. Cliquez sur le bouton **[Autoriser accès]**.

Cela ajoute « Java Platform SE binary » aux programmes autorisés du pare-feu Windows dans le Panneau de configuration.

Activation de Java et autorisation des modules complémentaires

Si Java est installé sur le terminal, effectuez la procédure suivante pour activer Java dans le navigateur Web utilisé avec XSCF Web et pour autoriser les modules complémentaires.

Pour Internet Explorer

1. Sélectionnez **[Outils] - [Options Internet] - onglet [Programmes] - [Gérer les modules complémentaires]**.
2. Activez « Java Plug-in XX.XX.X ».
3. Dans Internet Explorer 8.0, sélectionner le menu **[Stockage à distance]** dans XSCF Web lorsque le stockage à distance est utilisé ouvre une page et déclenche la génération d'un message. Le message demande d'autoriser l'exécution d'un module complémentaire Java Runtime Environment. Effectuez la sélection sur cet écran de message pour autoriser le module complémentaire.

Pour Firefox

1. Dans le menu **[Firefox]**, sélectionnez **[Modules complémentaires] - [Modules d'extension]**.
2. Sélectionnez « Java(TM) Platform » puis réglez-le sur **[Demander l'activation]** ou **[Toujours activer]**.
3. Cliquer sur le bouton **[Lancer]** dans XSCF Web pendant l'utilisation du

- stockage à distance déclenche la génération d'un message. Le message demande d'autoriser l'exécution d'un module d'extension. Sélectionnez [Autoriser].
4. Le message est à nouveau généré pour demander d'autoriser l'exécution du module d'extension. Sélectionnez [Autoriser maintenant] ou [Autoriser et se rappeler], puis cliquez sur le bouton [OK].

Remarques sur les terminaux

En cas d'utilisation du serveur de stockage à distance XSCF sur un PC connecté à un bureau à distance, vous ne pouvez pas accéder au support inséré dans un lecteur CD/DVD. Spécifiez un fichier ISO.

4.6.5 Réglages d'Oracle Solaris

Pour utiliser le stockage à distance, activez les services de gestion des supports amovibles dans Oracle Solaris. Avec les services de gestion des supports amovibles activés, Oracle Solaris monte automatiquement les supports amovibles lors de la connexion des supports dans le terminal.

- Pour Oracle Solaris 11 ou version ultérieure
Services de gestion des supports amovibles : `svc:/system/hal:default`
`svc:/system/filesystem/rmvolmgr:default`
`svc:/system/dbus:default`
- Pour Oracle Solaris 10
`volfs service: svc:/system/filesystem/volfs:default`

Pour savoir comment activer les services de gestion des supports amovibles, consultez « 2. Comment connecter/déconnecter un lecteur USB-DVD » dans le *Manuel d'utilisation du lecteur USB-DVD externe*.

4.6.6 Versions logicielles du stockage à distance

[Tableau 4-5](#) répertorie les versions logicielles avec lesquelles le stockage à distance fonctionne. Le stockage à distance ne fonctionne pas avec les versions non incluses dans [Tableau 4-5](#). Pour obtenir des informations détaillées sur XCP, Oracle Solaris et les SRU/correctifs essentiels, consultez les dernières *Notes de produit* pour votre serveur.

Tableau 4-5 XCP, Oracle Solaris et SRU/correctifs essentiels avec lesquels le stockage à distance fonctionne

XCP	Oracle Solaris	SRU essentiels (*1) Correctif essentiel (*2)
2260 ou version ultérieure	Oracle Solaris 11.2 ou version ultérieure	Aucun

Tableau 4-5 XCP, Oracle Solaris et SRU/correctifs essentiels avec lesquels le stockage à distance fonctionne (*suite*)

XCP	Oracle Solaris	SRU essentiels (*1) Correctif essentiel (*2)
	Oracle Solaris 11.1	SRU 2.5 ou version ultérieure (*3)
	Oracle Solaris 10 1/13	Aucun

*1 Pour Oracle Solaris 11

*2 Pour Oracle Solaris 10

*3 Si le stockage à distance est attribué en tant que disque virtuel à un domaine invité, il est nécessaire de l'appliquer à un domaine de service.

4.6.7 Chemins d'accès et alias des dispositifs de stockage à distance

Pour plus de détails sur les chemins d'accès de périphériques des modèles SPARC M12/M10, consultez « [Annexe A Listes des chemins d'accès de périphériques des systèmes SPARC M12/M10](#) ». Pour plus de détails sur les alias du lecteur DVD, consultez « [Annexe J Listes des alias des lecteurs DVD](#) ».

4.6.8 Remarques sur le stockage à distance

Remarques sur l'utilisation du stockage à distance

Notez les points suivants concernant l'utilisation du stockage à distance.

- N'effectuez pas d'opération de connexion ou d'arrêt du stockage à distance tant que le traitement de mise sous tension/hors tension d'une partition physique n'est pas terminé.
- Si aucune passerelle par défaut n'est définie dans les réglages réseau, le tableau de configuration réseau du stockage à distance dans la page [Stockage à distance] de XSCF Web et la commande showremotestorage affichent « - » pour la passerelle.
- Si vous utilisez le stockage à distance pour vous connecter à une image ISO sur le terminal, ne passez pas en lecture seule (R) un attribut de propriété de l'image ISO et du dossier contenant cette image ISO.
Si l'attribut de propriété lecture seule (R) est défini, le support ne peut pas démarrer (Exécuter).
- L'éjection ou la commutation d'un support via une opération sur le terminal pendant l'utilisation du stockage à distance ne sont pas pris en charge. Si cette opération accède au stockage à distance, une erreur d'accès se produit.
L'éjection d'un support via une opération sur le terminal signifie l'éjection sans utiliser la commande eject depuis Oracle Solaris. Les opérations suivantes sont présumées :

- Appuyer sur le bouton d'éjection sur le lecteur CD/DVD du terminal pour éjecter le support
- Utiliser Windows sur le terminal pour éjecter le support

Pour éjecter le support, effectuez la procédure dans « [4.6.14 Déconnexion du support/Fin du stockage à distance](#) » afin de terminer le stockage à distance, puis éjectez le support.

Pour changer de support, effectuez la procédure dans « [Commutation des supports](#) » dans « [4.6.13 Utilisation du stockage à distance depuis Oracle Solaris](#) ».

- Si vous cliquez sur le bouton [Arrêt] sur l'écran [Serveur de stockage à distance XSCF] et accédez au stockage à distance pendant l'utilisation du stockage à distance, une erreur d'accès se produit.
Si vous avez cliqué sur le bouton [Arrêt] pendant l'utilisation du stockage à distance, effectuez la procédure dans « [4.6.14 Déconnexion du support/Fin du stockage à distance](#) » pour terminer le stockage à distance. Pour utiliser à nouveau le stockage à distance, effectuez la procédure dans « [4.6.12 Connexion aux supports en utilisant le stockage à distance](#) ».
- N'utilisez pas la commande deleteboard pour déconnecter un SPARC M12/M10 avec le stockage à distance connecté.
- Pour effectuer une opération (dont une mise à niveau du microprogramme, etc.) qui redémarre le XSCF ou bascule entre les XSCF maître et de veille pendant l'utilisation du stockage à distance, le stockage à distance doit être déconnecté. Déconnectez-le en consultant « [4.6.14 Déconnexion du support/Fin du stockage à distance](#) ».
S'il n'est pas déconnecté, il peut causer la génération d'un message d'erreur ou d'un message d'avertissement à la console du domaine et l'enregistrement d'un journal d'erreur avec le XSCF.
- Une tentative de connexion de stockage à distance via un VPN ou un autre réseau auquel la traduction d'adresse est appliquée échoue avec un message d'erreur « iscsiadm: no records found! ».
Ne connectez pas le stockage à distance via un VPN ou un autre réseau auquel la traduction d'adresse est appliquée. Si plusieurs connexions réseau existent dans un terminal, il est possible que le stockage à distance ne puisse pas être connecté dans certains cas.
Dans ce cas, désactivez les périphériques réseau sur les terminaux différents de celui utilisé pour connecter le XSCF-LAN avant de procéder à la connexion.

Remarque sur l'utilisation d'un CD (disque compact) en tant que support de stockage à distance

En cas d'utilisation d'un CD (disque compact) en tant que support de stockage à distance, utilisez un CD qui a été écrit avec la méthode Disc at once (DAO). Si le support utilisé est un CD qui n'a pas été écrit avec la méthode Disc at once (DAO), une erreur peut se produire dans OpenBoot PROM ou le pilote sd lorsque le support est lu.

4.6.9 Flux pour l'utilisation du stockage à distance

Cette section décrit le flux pour l'utilisation du stockage à distance. Normalement, en utilisant le stockage à distance, utilisez XSCF Web.

Avant d'utiliser le stockage à distance

Pour utiliser le stockage à distance, les préparations préalables suivantes sont nécessaires.

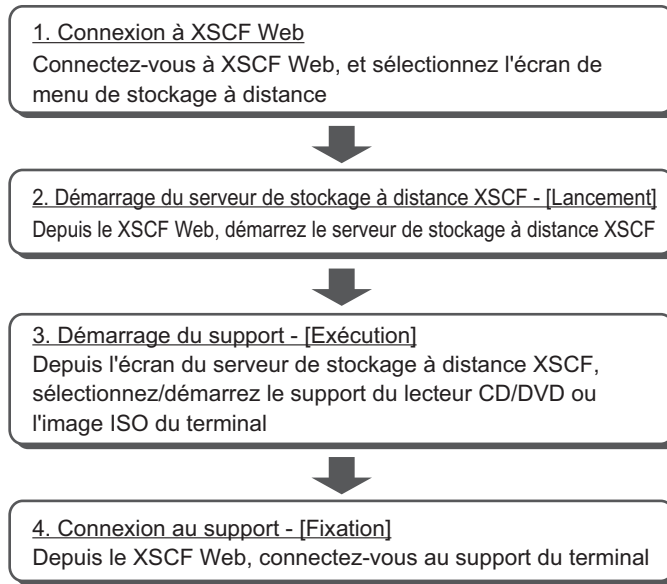
- En consultant « [4.6.2 Configuration réseau du stockage à distance](#) » et « [4.6.10 Configuration du XSCF-LAN utilisé avec le stockage à distance](#) », effectuez les réglages réseau XSCF du XSCF maître/de veille. Les réglages réseau du XSCF maître sont une nécessité pour utiliser XSCF Web.
- En consultant « [3.8 Configuration du service HTTPS pour la connexion à XSCF](#) », activez le service HTTPS.
- Répondre aux exigences de « [4.6.4 Configuration d'exploitation requise des terminaux et des navigateurs](#) ».
- En consultant « [4.6.5 Réglages d'Oracle Solaris](#) », effectuez les réglages nécessaires pour Oracle Solaris.

Une fois les préparations décrites ci-dessus terminées, effectuez les opérations de base.

Flux de fonctionnement de base

Pour utiliser le stockage à distance, effectuez les quatre opérations de base indiquées dans [Figure 4-16](#) à l'aide de XSCF Web depuis le terminal de gestion du système.

Figure 4-16 Opérations de stockage à distance de base



La vue d'ensemble suivante décrit les quatre opérations de base.

- 1. Connexion à XSCF Web**
Pour utiliser le stockage à distance, connectez-vous d'abord à XSCF Web. Sélectionnez le menu du stockage à distance et ouvrez la page Web de configuration du stockage à distance.
- 2. Démarrage du serveur de stockage à distance XSCF - [Lancement]**
Depuis XSCF Web, démarrez le serveur de stockage à distance XSCF (Lancement). Démarrer le serveur de stockage à distance XSCF ouvre l'écran [Serveur de stockage à distance XSCF] permettant de sélectionner/démarrer le support sur le terminal de gestion du système. Depuis cet écran, sélectionnez/démarrez le support et affichez le statut du support.

Remarque : Vous ne pouvez démarrer le serveur de stockage à distance XSCF que depuis XSCF Web. Aucune des commandes du Shell XSCF ne démarre le serveur de stockage à distance XSCF.

- 3. Démarrage du support - [Exécuter]**
Après avoir affiché l'écran [Serveur de stockage à distance XSCF], sélectionnez le lecteur CD/DVD ou une image ISO du terminal pour démarrer le support. Cette opération permet l'utilisation du port réseau utilisé avec le stockage à distance de ce terminal et définit l'état d'attente pour la connexion depuis XSCF.
- 4. Connexion au support - [Lier]**
Connectez-vous au support cible d'un terminal depuis XSCF Web ou le Shell XSCF. À ce moment-là, spécifiez l'interface XSCF-LAN et l'adresse IP du terminal. Ces opérations permettent d'utiliser le support cible depuis OpenBoot PROM et Oracle Solaris.

Ici, en cas d'accès à un support via un XSCF esclave, vous pouvez effectuer les réglages réseau de XSCF depuis XSCF Web et le Shell XSCF. Un redémarrage de XSCF n'est pas nécessaire à ce moment.

Vous pouvez utiliser les commandes `setremotestorage` ou `showremotestorage`, qui sont toutes les deux des commandes XSCF, pour vous connecter au support. Pour plus de détails sur chaque commande, consultez la page du manuel correspondant à la commande ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

Pour plus de détails sur chaque paramètre, consultez « [4.6.12 Connexion aux supports en utilisant le stockage à distance](#) ».

4.6.10 Configuration du XSCF-LAN utilisé avec le stockage à distance

Cette section décrit les paramètres du XSCF-LAN utilisés avec le stockage à distance. Pour utiliser le stockage à distance, le réseau d'interface du XSCF-LAN doit être configuré. Après avoir décidé d'utiliser XSCF-LAN#0 ou XSCF-LAN#1 du XSCF maître, de veille, ou esclave, configurez le réseau XSCF.

Configuration du XSCF maître/de veille pour utiliser XSCF Web

Avant de configurer le stockage à distance avec XSCF Web, vous devez avoir effectué les réglages réseau du XSCF maître/de veille. Cela permet d'utiliser XSCF Web, qui nécessite le service HTTPS activé. Un redémarrage de XSCF est nécessaire pour ces réglages.

Effectuez les réglages réseau de XSCF avec la commande `setnetwork` ou la page [Réseau] de XSCF Web. Ces réglages ne peuvent pas être effectués avec la commande `setremotestorage` ou la page [Stockage à distance] de XSCF Web.

Pour plus de détails sur les réglages réseau du XSCF maître/de veille et les réglages du service HTTPS, consultez « [3.9 Configuration du réseau XSCF](#) » et « [3.8 Configuration du service HTTPS pour la connexion à XSCF](#) ».

Utilisation du XSCF maître/de veille

Lorsque vous utilisez le stockage à distance via le XSCF-LAN sur tous les châssis maîtres/de veille, le réseau XSCF n'a pas besoin d'être configuré si les paramètres indiqués dans « [Configuration du XSCF maître/de veille pour utiliser XSCF Web](#) » ont été définis.

Remarque : si le XSCF maître/de veille est utilisé, l'adresse IP physique est utilisée comme adresse IP du XSCF-LAN lors de l'accès aux supports d'un terminal avec stockage à distance. L'adresse IP de prise de contrôle (adresse virtuelle) n'est pas utilisée.

Utilisation d'un XSCF esclave

Avant d'utiliser le stockage à distance via un XSCF esclave, vous devez avoir déjà effectué les réglages réseau du XSCF maître. Vous pouvez effectuer les réglages réseau du XSCF esclave avant ou pendant la configuration du stockage à distance. Effectuez les réglages réseau de XSCF avec la commande `setremotestorage` ou la page [Stockage à distance] de XSCF Web. Ces réglages ne peuvent pas être effectués avec la commande `setnetwork` ou la page [Réseau] de XSCF Web.

De plus, dans un système connecté à un boîtier à barre transversale, le stockage à distance est utilisé via un XSCF esclave qui est un SPARC M12/M10. Pour cette raison, le réseau du XSCF esclave doit être configuré.

La procédure permettant d'effectuer les réglages réseau d'un XSCF esclave avec XSCF Web est décrite ci-dessous. Pour plus de détails sur les paramètres avec le shell XSCF, consultez la page du manuel correspondant à la commande `setremotestorage` ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

1. **Connectez le câble XSCF LAN du XSCF esclave (XSCF-LAN#0 ou XSCF-LAN#1).**
2. **Exécutez la commande `sethttps` pour activer le service HTTPS.**
3. **Connectez-vous à XSCF Web sur le XSCF maître.**
4. **Sélectionnez [Menu] - [Paramètres] - [Stockage à distance].**
5. **À partir de la colonne Interface dans le tableau de configuration du réseau de stockage à distance, sélectionnez XSCF-LAN#0 ou XSCF-LAN#1 du XSCF esclave. Puis cliquez sur le bouton [Configurer].**
6. **Définissez l'adresse IP, le masque de réseau et la passerelle sur l'écran affiché, puis cliquez sur le bouton [OK].**
7. **En consultant le tableau de configuration réseau du stockage à distance, vérifiez que toutes ces données définies sont correctes.**

Un redémarrage de XSCF n'est pas nécessaire pour les réglages réseau du XSCF esclave.

4.6.11 Statut du serveur de stockage à distance XSCF

Cette section décrit l'affichage du Statut dans la partie supérieure de l'écran [Serveur de stockage à distance XSCF].

Les opérations de stockage à distance depuis l'écran [Serveur de stockage à distance XSCF] et XSCF Web actualisent l'affichage de Statut en haut de l'écran [Serveur de stockage à distance XSCF]. Vous pouvez utiliser les données de Statut pour vérifier le statut des connexions entre le XSCF et les supports dans les terminaux.

[Tableau 4-6](#) répertorie les transitions de statut sur l'écran [Serveur de stockage à distance XSCF] à partir des opérations de stockage à distance.

Tableau 4-6 Transitions de statut sur l'écran [Serveur de stockage à distance XSCF] à partir des opérations de stockage à distance

Opération	État
Connecter	
Immédiatement après le démarrage du Serveur de stockage à distance XSCF (Bouton [Lancer] cliqué sur le XSCF Web)	Déconnecté
Support cible sélectionné sur l'écran [Serveur de stockage à distance XSCF]	Déconnecté
Bouton [Exécuter] cliqué sur l'écran [Serveur de stockage à distance XSCF]	Attente de connexion provenant de XSCF
Bouton [Joindre] cliqué sur le XSCF Web	Connecté
Déconnecter	
Connecté en cliquant sur le bouton [Joindre]	Connecté
Bouton [Détacher] cliqué sur le XSCF Web	Attente de connexion provenant de XSCF
Bouton [Arrêt] cliqué sur l'écran [Serveur de stockage à distance XSCF]	Déconnecté
Éjecter	
Connecté en cliquant sur le bouton [Joindre]	Connecté
Éjection exécutée depuis Oracle Solaris	Éjecté
Bouton [Exécuter] cliqué sur l'écran [Serveur de stockage à distance XSCF]	Attente de connexion provenant de XSCF
Plusieurs secondes écoulées après avoir cliqué sur le bouton [Exécuter] ci-dessus	Connecté

[Tableau 4-7](#) répertorie les significations de l'affichage du Statut dans la partie supérieure de l'écran [Serveur de stockage à distance XSCF].

Tableau 4-7 Significations du statut du serveur de stockage à distance XSCF

État	Signification
Déconnecté	Le support dans un terminal a été déconnecté du XSCF.
Attente de connexion provenant de XSCF	Le support dans un terminal peut être connecté et attend la connexion provenant du XSCF.
Connecté	Le support dans un terminal est connecté au XSCF.
Éjecté	La commande eject a été exécutée depuis Oracle Solaris.

4.6.12 Connexion aux supports en utilisant le stockage à distance

Cette section décrit les opérations permettant de se connecter au support dans le terminal avec l'utilisation du stockage à distance. Veuillez noter que seule la lecture des supports est autorisée. L'écriture n'est pas autorisée.

Les descriptions sont réparties dans les trois cas suivants :

- Partition physique arrêtée
- Domaine de commande à l'invite ok
- Oracle Solaris en exécution sur le domaine de commande

Dans les trois cas ci-dessus, le fonctionnement de base pour se connecter au support est le même. Cependant, les opérations pour le domaine de commande une fois le support connecté sont différentes. Le fonctionnement de base pour chacun des cas ci-dessus est le même que dans le contenu « [Partition physique arrêtée](#) ».

Remarque : pour utiliser le stockage à distance dans un domaine invité, attribuez des ressources (ldm add-vdisk).

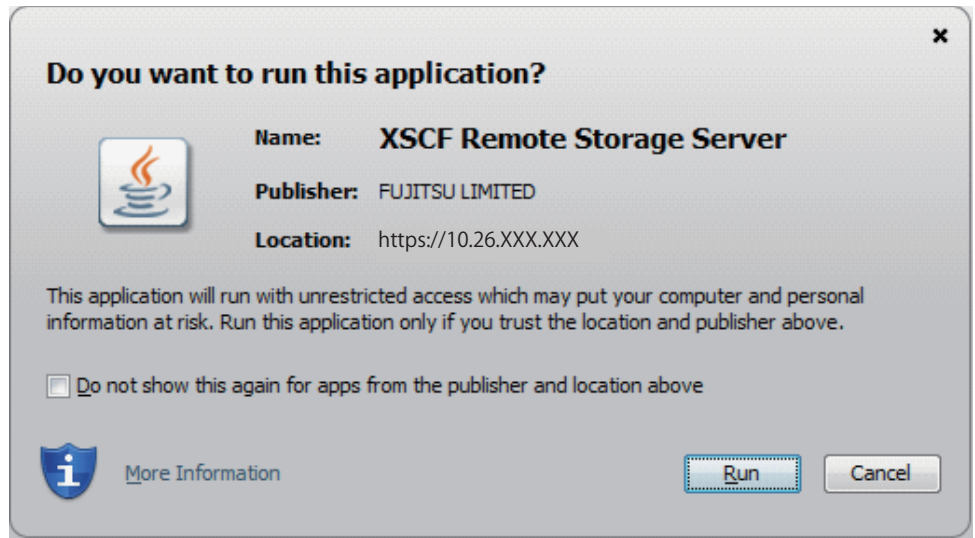
Remarque : lors de l'utilisation du stockage à distance, notre conseil est de n'effectuer aucune opération de connexion au support pendant la procédure de démarrage ou d'arrêt de la partition physique ou du domaine de commande. Cela permet d'éviter des temps de traitement plus longs dans les procédures de démarrage et d'arrêt de la partition physique et du domaine de commande. En fonction de la synchronisation, si le support est connecté pendant la procédure de démarrage de la partition physique ou du domaine de commande, OpenBoot PROM peut ne pas reconnaître le support cible. Par conséquent, le domaine de commande devra à nouveau être réinitialisé.

La procédure suivante présume que les opérations dans « [Avant d'utiliser le stockage à distance](#) » dans « [4.6.9 Flux pour l'utilisation du stockage à distance](#) » ont été effectuées.

Partition physique arrêtée

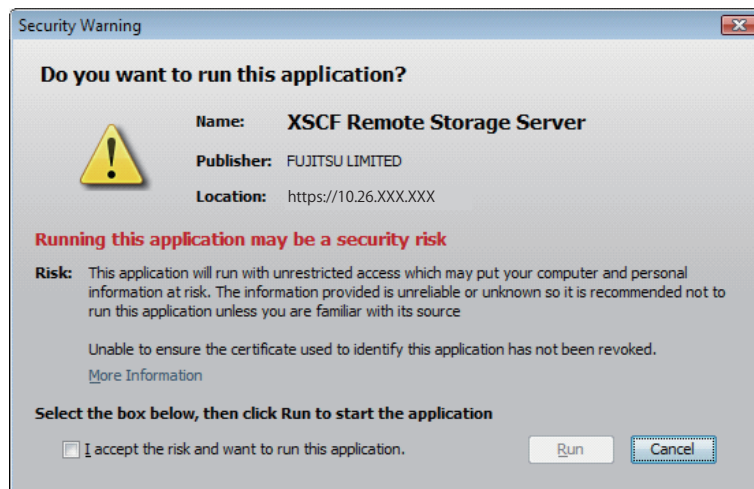
1. **Connectez-vous à XSCF Web depuis le terminal de gestion du système.**
2. **Sélectionnez [Menu] - [Paramètres] - [Stockage à distance].**
3. **Cliquez sur le bouton [Lancer] du serveur de stockage à distance.**
L'écran [Figure 4-17](#) apparaît. Cliquez sur le bouton [Exécuter] de l'écran pour afficher l'écran [Serveur de stockage à distance XSCF].

Figure 4-17 Message lorsque le bouton [Lancer] est cliqué



Si la validité du certificat signé pour le Serveur de stockage à distance XSCF ne peut pas être confirmée, un avertissement de sécurité tel que celui montré dans Figure 4-18 est généré. Cochez la case [J'accepte le risque et souhaite exécuter cette application], puis cliquez sur le bouton [Exécuter].

Figure 4-18 Message d'avertissement de sécurité



Si le pare-feu Windows est utilisé, le message d'avertissement montré dans « Figure 4-15 Message d'avertissement si le pare-feu Windows est utilisé » est généré. Suivez la procédure dans « Port utilisé et autorisation sur un terminal » dans « 4.6.4 Configuration d'exploitation requise des terminaux et des navigateurs ».

4. Sélectionnez le support du lecteur CD/DVD ou l'image ISO affichée sur l'écran

[Serveur de stockage à distance XSCF].

Si aucun support n'apparaît à l'écran, il se peut qu'aucun support n'ait été inséré dans le lecteur CD/DVD du terminal ou qu'aucune image ISO n'ait été ajoutée. Si aucun support n'est inséré dans le lecteur CD/DVD, insérez le support puis cliquez sur le bouton [Actualiser] en haut de l'écran. Vous pouvez également cliquer sur le bouton [Ajouter fichier ISO] pour afficher la liste des images ISO. Sélectionnez le support cible dans la liste affichée.

Chaque ligne de Statut, Support sélectionné et Adresse IP XSCF dans la partie supérieure de l'écran [Serveur de stockage à distance XSCF] est actualisée comme indiqué ci-dessous. Pour la signification du Statut, consultez « [4.6.11 Statut du serveur de stockage à distance XSCF](#) ».

Statut	Déconnecté
Support sélectionné	Chemin d'accès du support sélectionné
Adresse IP XCP	Aucune

5. Cliquez sur le bouton [Exécuter] de l'écran [Serveur de stockage à distance XSCF].

Cette opération permet d'utiliser le port réseau du terminal utilisé avec le stockage à distance. Le support cible sélectionné attend une connexion provenant du XSCF.

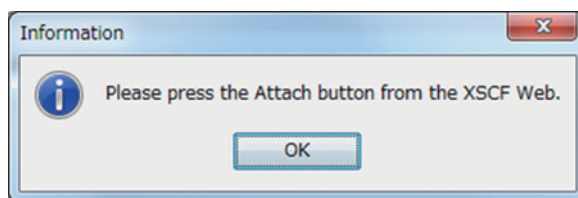
Chaque ligne de Statut, Support sélectionné et Adresse IP XSCF dans la partie supérieure de l'écran [Serveur de stockage à distance XSCF] est actualisée comme indiqué ci-dessous.

Statut	Attente de connexion provenant du XSCF
Support sélectionné	Chemin d'accès du support sélectionné
Adresse IP XCP	Aucune

Une fois effectuée, cette opération affiche l'écran [Information] pour effectuer l'opération « Joindre » depuis XSCF Web comme indiqué dans [Figure 4-19](#).

Cliquez sur le bouton [OK] pour retourner à la console XSCF Web.

Figure 4-19 Écran [Informations]



6. À partir de la colonne Interface dans le tableau de configuration du réseau de stockage à distance du XSCF Web, sélectionnez l'interface XSCF-LAN à connecter au support cible.

Si l'interface réseau XSCF-LAN n'est pas configurée, consultez « [4.6.10 Configuration du XSCF-LAN utilisé avec le stockage à distance](#) ». Puis configurez le réseau.

7. Cliquez sur le bouton [Joindre] pour vous connecter au support.

Un écran permettant de spécifier l'adresse IP du terminal apparaît. Après avoir vérifié que l'adresse IP est correcte, cliquez sur le bouton [OK].

La connexion dans le tableau de configuration réseau du stockage à distance affiche l'adresse IP du terminal. De cette façon, le XSCF et le support cible sont connectés.

Chaque ligne de Statut, Support sélectionné et Adresse IP XSCF dans la partie supérieure de l'écran [Serveur de stockage à distance XSCF] est actualisée comme indiqué ci-dessous.

Statut	Connecté
Support sélectionné	Chemin d'accès du support sélectionné
Adresse IP de XCP	Adresse IP physique du XSCF-LAN connecté

8. **Exécutez la commande poweron pour mettre la partition physique sous tension.**

Remarque : pour arrêter le domaine de commande à l'invite ok, utilisez la commande setenv pour changer la variable d'environnement auto-boot? d'OpenBoot PROM sur false.

[Exemple]

XSCF> setpparparam -p 0 -s bootscript "setenv auto-boot? false"

9. **Exécutez la commande cfgadm -al depuis Oracle Solaris et vérifiez que le chemin d'accès du dispositif de stockage à distance a été ajouté.**

# cfgadm -al				
Ap_Id	Type	Receptacle	Occupant	Condition
...				
usb1/3	usb-storage	connected	configured	ok

Remarque : Si le stockage à distance n'est pas utilisé dans le domaine de commande, l'étage 10 est inutile. Pour utiliser le stockage à distance dans un domaine invité, attribuez des ressources (ldm add-vdisk).

10. **Si le support cible n'a pas été ajouté, utilisez la commande mount d'Oracle Solaris pour le monter.**

L'exemple suivant montre un contrôle de l'état de montage du support cible. Vu que le dispositif de stockage à distance n'a pas été monté automatiquement, le support cible va être monté.

Pour plus de détails sur la commande mount, consultez *Oracle Solaris Reference Manual* de la version utilisée.

Remarque : pour savoir comment activer les services de gestion des supports amovibles, consultez « [4.6.5 Réglages d'Oracle Solaris](#) ».

# df	
/	(rpool/ROOT/solaris):425092886 blocks 425092886 files
/devices	(/devices): 0 blocks 0 files
...	
# mount -F hsfs /dev/dsk/c4t0d0s2 /media/xxxxx	

/dev/dsk/c4t0d0s2 spécifie le chemin d'accès de l'appareil du stockage à distance. Pour plus de détails sur la commande mount, consultez *Oracle Solaris Reference Manual* de la version utilisée.

Vous pouvez à présent installer des logiciels, lire des fichiers et effectuer d'autres opérations depuis le support cible. Veuillez noter que vous ne pouvez pas écrire sur le support cible.

Remarque : si le domaine de commande est à l'invite ok, exécutez la commande show-disks et vérifiez que le chemin d'accès du dispositif de stockage à distance a été ajouté.

```
{0} ok show-disks
a) /pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk
b) /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk
...
Enter Selection, q to quit:
```

Domaine de commande à l'invite ok

1. **Effectuez les étapes 1 à 7 dans « [Partition physique arrêtée](#) ».**
2. **Exécutez la commande console depuis le Shell XSCF pour passer à la console du domaine de commande qui se trouve à l'invite ok.**
L'exemple suivant montre la commutation vers la console du domaine de commande de la partition physique #0.

```
XSCF> console -p 0
```

3. **Exécutez la commande reset-all pour réinitialiser le domaine de commande qui est à l'invite ok.**

```
{0} ok reset-all
```

Remarque : Pour réinitialiser le domaine de commande en l'arrêtant à nouveau à l'invite ok, passez la valeur de la variable d'environnement OpenBoot PROM auto-boot? à faux avec la commande setenv.

4. **À l'invite ok du domaine de commande de réinitialisation, exécutez la commande show-disks et vérifiez que le chemin d'accès du dispositif de stockage à distance a été ajouté.**

```
{0} ok show-disks
a) /pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk
b) /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk
...
```

```
Enter Selection, q to quit:
```

Vous pouvez définir un alias du dispositif de stockage à distance, installer Oracle Solaris depuis le support cible et effectuer d'autres opérations.

Oracle Solaris en exécution sur le domaine de commande

1. **Effectuez les étapes 1 à 7 dans « [Partition physique arrêtée](#) ».**
2. **Exécutez la commande console depuis le shell XSCF pour passer à la console du domaine de commande où Oracle Solaris est en exécution.**
L'exemple suivant montre la commutation vers la console du domaine de commande de la partition physique #0.

```
XSCF> console -p 0
```

3. **Exécutez la commande `df` ou `cfgadm -al` depuis Oracle Solaris et vérifiez que le chemin d'accès du dispositif de stockage à distance a été ajouté.**

Remarque : si les services de gestion des supports amovibles sont activés (set pour activer), le dispositif de stockage distant est automatiquement monté lorsque le XSCF est connecté au stockage à distance. Pour savoir comment activer les services de gestion des supports amovibles, consultez « [4.6.5 Réglages d'Oracle Solaris](#) ».

L'exemple suivant exécute la commande `df` et montre que ce /support sur le dispositif de stockage à distance a été monté automatiquement.

```
# df
/                (rpool/ROOT/solaris):425092886 blocks 425092886 files
/devices        (/devices          ):          0 blocks 0 files
...
/media/DISC-LABEL(/dev/dsk/c4t0d0s2 ):          0 blocks 0 files
```

L'exemple suivant exécute la commande `cfgadm` et montre qu'un dispositif de stockage à distance (usb1/3) de type stockage usb a été ajouté.

#	cfgadm				
Ap_Id	Type	Receptacle	Occupant	Condition	
...					
usb1/3	usb-storage	connected	configured	ok	

Remarque : Si le stockage à distance n'est pas utilisé dans le domaine de commande, l'étape 4 est inutile. Pour utiliser le stockage à distance dans un domaine invité, attribuez des ressources (`ldm add-vdisk`).

4. **Si le dispositif de stockage à distance n'est pas monté, utilisez la commande mount pour le monter.**

L'exemple suivant montre que le dispositif de stockage à distance n'a pas été monté automatiquement, il va donc être monté.

```
# df
/                (rpool/ROOT/solaris):425092886 blocks 425092886 files
/devices         (/devices          ):          0 blocks 0 files
...
# mount -F hsfs /dev/dsk/c4t0d0s2 /media/xxxxx
```

/dev/dsk/c4t0d0s2 spécifie le chemin d'accès de l'appareil du stockage à distance. Pour plus de détails sur la commande mount, consultez *Oracle Solaris Reference Manual* de la version utilisée.

Vous pouvez à présent installer des logiciels, lire des fichiers et effectuer d'autres opérations depuis le support cible. Veuillez noter que vous ne pouvez pas écrire sur le support cible.

4.6.13 Utilisation du stockage à distance depuis Oracle Solaris

Cette section décrit des exemples d'utilisation du stockage à distance. La description des deux exemples suivants concerne le SPARC M10-1 :

- Installer Oracle Solaris
- Commuter les supports

Installer Oracle Solaris

Comme décrit ci-dessous, cet exemple installe Oracle Solaris dans le domaine de commande SPARC M10-1.

1. **Exécutez la commande console depuis le Shell XSCF pour passer à la console du domaine de commande qui se trouve à l'invite ok.**

L'exemple suivant montre la commutation vers la console du domaine de commande de la partition physique #0.

```
XSCF> console -p 0
```

2. **Installez Oracle Solaris depuis le support cible dans le lecteur CD/DVD.**

L'exemple suivant montre un contrôle des alias des périphériques actuellement définis et la spécification d'un alias de périphérique contrôlé. Si le nombre d'alias est omis, le nombre inférieur de LSB est utilisé depuis le stockage.

```
{0} ok devalias
{0} ok boot redrom
```

L'exemple suivant montre un chemin d'accès au périphérique spécifié.

```
{0} ok boot /pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/storage@3/disk@0
```

Remarque : pour plus de détails sur les chemins d'accès de périphériques des modèles SPARC M12/M10, consultez « [Annexe A Listes des chemins d'accès de périphériques des systèmes SPARC M12/M10](#) ». Pour plus de détails sur les alias des périphériques, consultez « [Annexe J Listes des alias des lecteurs DVD](#) ».

Commutation des supports

La procédure décrite ici exécute la commande eject depuis Oracle Solaris pour commuter le support du lecteur CD/DVD ou l'image ISO utilisée avec le stockage à distance.

Remarque : pour commuter les supports, exécutez la commande eject depuis Oracle Solaris. Le stockage à distance ne prend pas en charge la commutation de supports qui utilise le bouton Éjecter sur le lecteur CD/DVD d'un terminal. Si le support est commuté avec le bouton Éjecter, les modifications de taille des données peuvent ne pas être reconnues et un message d'avertissement peut être généré. Dans ce cas, exécutez la commande eject. Vous devrez ensuite cliquer à nouveau sur le bouton [Exécuter] depuis le Serveur de stockage à distance XSCF.

1. **Exécutez la commande console depuis le shell XSCF pour passer à la console du domaine de commande où Oracle Solaris est en exécution.**

L'exemple suivant montre la commutation vers la console du domaine de commande de la partition physique #0.

```
XSCF> console -p 0
```

2. **Utilisez la commande eject pour retirer le support cible.**

Avec la commande eject, vous pouvez afficher les noms des périphériques et une liste correspondante de pseudonymes en spécifiant une option. L'exemple suivant montre l'option -l spécifiée dans la commande eject en utilisant Oracle Solaris 11.

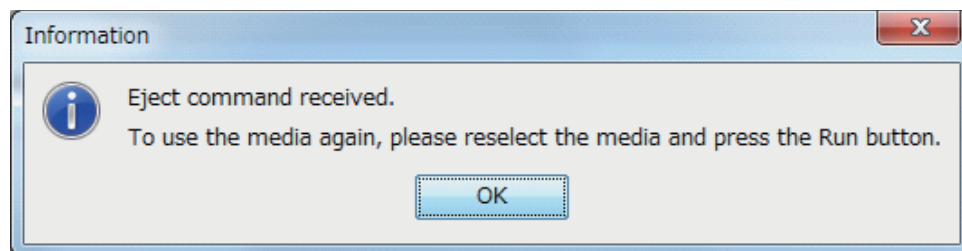
```
# eject -l  
/dev/dsk/c4t0d0s2      cdrom,cdrom0,cd,cd0,DISC-LABEL,/media/DISC-LABEL
```

L'exemple suivant montre le /support spécifié sur le dispositif de stockage à distance.

```
# eject /media/DISC-LABEL
```

Une fois effectuée, cette opération affiche l'écran [Information] pour le Serveur de stockage à distance XSCF comme indiqué dans [Figure 4-20](#). Cliquez sur le bouton [OK] pour retourner à l'écran [Serveur de stockage à distance XSCF].

Figure 4-20 Écran [Informations]



Chaque ligne de Statut, Support sélectionné et Adresse IP XSCF dans la partie supérieure de l'écran [Serveur de stockage à distance XSCF] est actualisée comme indiqué ci-dessous. Pour la signification du Statut, consultez « [4.6.11 Statut du serveur de stockage à distance XSCF](#) ».

Statut	Éjecté
Support sélectionné	Aucun
Adresse IP XCP	Aucune

Remarque : pour plus de détails sur les chemins d'accès de périphériques et les alias des périphériques de chaque modèle SPARC M12/M10, consultez « [Annexe A Listes des chemins d'accès de périphériques des systèmes SPARC M12/M10](#) » et « [Annexe J Listes des alias des lecteurs DVD](#) » respectivement.

3. **Passez le support dans le lecteur CD/DVD ou sélectionnez à nouveau l'image ISO.**
4. **Cliquez sur le bouton [Actualiser] de l'écran [Serveur de stockage à distance XSCF], puis sélectionnez le lecteur CD/DVD.**

Cliquer sur le bouton [Actualiser] actualise les informations des lecteurs système à l'écran. L'information à l'écran du support sélectionné est actualisée lorsqu'un lecteur CD/DVD est à nouveau sélectionné.

Chaque ligne de Statut, Support sélectionné et Adresse IP XSCF dans la partie supérieure de l'écran [Serveur de stockage à distance XSCF] est actualisée comme indiqué ci-dessous.

Statut	Éjecté
Support sélectionné	Chemin d'accès du support sélectionné
Adresse IP XCP	Aucune

5. **Cliquez sur le bouton [Exécuter] de l'écran [Serveur de stockage à distance XSCF].**

Cette opération permet d'utiliser le support cible du terminal utilisé avec le stockage à distance.

Chaque ligne de Statut, Support sélectionné et Adresse IP XSCF dans la partie supérieure de l'écran [Serveur de stockage à distance XSCF] est actualisée

comme indiqué ci-dessous.

Statut	Connecté
Support sélectionné	Chemin d'accès du support sélectionné
Adresse IP de XCP	Adresse IP physique du XSCF-LAN spécifié

Remarque : Pour commuter le support à l'invite ok, effectuez la procédure suivante.

1. Effectuez les étapes 1 à 6 dans « [Partition physique arrêtée](#) » dans « [4.6.14 Déconnexion du support/Fin du stockage à distance](#) ». Puis effectuez les étapes 2 à 4 dans « [Domaine de commande à l'invite ok](#) ».
 2. Passez le support dans le lecteur CD/DVD ou sélectionnez à nouveau l'image ISO.
 3. Effectuez les étapes 4 à 7 dans « [Partition physique arrêtée](#) » dans « [4.6.12 Connexion aux supports en utilisant le stockage à distance](#) ». Puis effectuez les étapes 2 à 4 dans « [Domaine de commande à l'invite ok](#) ».
-

4.6.14 Déconnexion du support/Fin du stockage à distance

Cette section décrit les opérations permettant de se déconnecter du support dans le terminal utilisé et de terminer le stockage à distance.

Les descriptions sont réparties dans les trois cas suivants :

- Partition physique arrêtée
- Domaine de commande à l'invite ok
- Oracle Solaris en exécution sur le domaine de commande

Dans les trois cas ci-dessus, le fonctionnement de base pour se déconnecter du support/terminer le stockage à distance est le même. Cependant, les opérations pour le domaine de commande avant et après que le support est déconnecté/le stockage à distance est terminé sont différentes. Le fonctionnement de base pour chacun des cas ci-dessus est le même que dans le contenu « [Partition physique arrêtée](#) ».

Partition physique arrêtée

1. **Le Serveur de stockage à distance XSCF fonctionne. Vérifiez que le statut de chaque ligne de Statut, Support sélectionné et Adresse IP XSCF en haut de l'écran sont comme suit.**

Statut	Connecté
Support sélectionné	Chemin d'accès du support sélectionné
Adresse IP de XCP	Adresse IP physique du XSCF-LAN spécifié

2. **Connectez-vous à XSCF Web depuis le terminal de gestion du système.**
3. **Sélectionnez [Menu] - [Paramètres] - [Stockage à distance].**
4. **À partir de la colonne Interface dans le tableau de configuration du réseau de stockage à distance, sélectionnez l'interface XSCF-LAN pour déconnecter le support cible du terminal.**
5. **Cliquez sur le bouton [Détacher].**
La connexion dans le tableau de configuration réseau du stockage à distance

affiche « Disponible ». Cette opération déconnecte le XSCF du support cible. Pendant que le Serveur de stockage à distance XSCF fonctionne, vous pouvez reconnecter le support en cliquant sur le bouton [Joindre].

Chaque ligne de Statut, Support sélectionné et Adresse IP XSCF dans la partie supérieure de l'écran [Serveur de stockage à distance XSCF] est actualisée comme indiqué ci-dessous.

Statut	Attente de connexion provenant du XSCF
Support sélectionné	Chemin d'accès du support sélectionné
Adresse IP XCP	Aucune

6. **Pour déconnecter le support cible, cliquez sur le bouton [Arrêt] de l'écran [Serveur de stockage à distance XSCF].**

Un message de confirmation apparaît. Cliquez sur le bouton [OK].

Cette opération déconnecte le support cible. Cependant, même après avoir effectué cette opération, le port réseau du terminal utilisé avec le stockage à distance peut toujours être utilisé. Cliquer à nouveau sur le bouton [Exécuter] va entraîner l'attente par le support cible d'une connexion provenant du XSCF.

Chaque ligne de Statut, Support sélectionné et Adresse IP XSCF dans la partie supérieure de l'écran [Serveur de stockage à distance XSCF] est actualisée comme indiqué ci-dessous.

Statut	Déconnecté
Support sélectionné	Chemin d'accès du support sélectionné
Adresse IP XCP	Aucune

7. **Pour terminer le stockage à distance, cliquez sur [x] dans le coin supérieur droit de l'écran [Serveur de stockage à distance XSCF].**

L'écran se ferme et se termine.

Domaine de commande à l'invite ok

1. **Effectuez les étapes 1 à 7 dans « [Partition physique arrêtée](#) ».**
2. **Exécutez la commande console depuis le Shell XSCF pour passer à la console du domaine de commande qui se trouve à l'invite ok.**

L'exemple suivant montre la commutation vers la console du domaine de commande de la partition physique #0.

```
XSCF> console -p 0
```

3. **Exécutez la commande reset-all pour réinitialiser le domaine de commande qui est à l'invite ok.**

```
{0} ok reset-all
```

Remarque : Pour réinitialiser le domaine de commande en l'arrêtant à nouveau à l'invite ok, passez la valeur de la variable d'environnement OpenBoot PROM auto-boot? à faux avec la commande setenv.

4. **À l'invite ok du domaine de commande de réinitialisation, exécutez la commande show-disks et vérifiez que le chemin d'accès du dispositif de stockage à distance a été supprimé.**

```
{0} ok show-disks
a) /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk
...
Enter Selection, q to quit:
```

Oracle Solaris en exécution sur le domaine de commande

1. **Exécutez la commande console depuis le shell XSCF pour passer à la console du domaine de commande où Oracle Solaris est en exécution.**
L'exemple suivant montre la commutation vers la console du domaine de commande de la partition physique #0.

```
XSCF> console -p 0
```

2. **Vérifiez qu'Oracle Solaris n'accède pas au support cible. Si nécessaire, démontez le dispositif de stockage à distance.**
L'exemple suivant démonte le dispositif de stockage à distance.

```
# cd /
# umount /media/xxxxx
```

3. **Arrêtez le service de gestion des supports amovibles.**
L'exemple suivant exécute la commande svcadm pour arrêter le service de gestion des supports amovibles.
 - Pour Oracle Solaris 11 ou version ultérieure

```
# svcadm disable hal
```

- Pour Oracle Solaris 10

```
# svcadm disable volfs
```

Remarque : pour utiliser le stockage à distance dans un domaine invité, arrêtez le service de gestion des supports amovibles du domaine invité.

4. **Exécutez la commande cfgadm -c unconfigure depuis Oracle Solaris pour arrêter un chemin d'accès particulier du dispositif de stockage à distance.**
L'exemple suivant exécute la commande cfgadm et montre que usb1/3 est un

dispositif de stockage à distance.

# cfgadm				
Ap_Id	Type	Receptacle	Occupant	Condition
...				
usb1/3	usb-storage	connected	configured	ok

L'exemple suivant exécute la commande `cfgadm -c unconfigure` et montre que le dispositif de stockage à distance est arrêté.

Remarque : Si la ressource du stockage à distance (`vdisk`) a été attribuée à un domaine invité, déconnectez la ressource (`ldm remove-vdisk`) puis exécutez `cfgadm -c unconfigure` depuis le domaine de commande.

```
# cfgadm -c unconfigure usb1/3
```

L'exemple suivant exécute la commande `cfgadm` et vérifie que l'`usb1/3` est arrêté.

# cfgadm				
Ap_Id	Type	Receptacle	Occupant	Condition
...				
usb1/3	usb-storage	connected	unconfigured	ok

- 5. **Effectuez les étapes 1 à 7 dans « [Partition physique arrêtée](#) ».**
- 6. **Exécutez la commande `df` ou `cfgadm` depuis Oracle Solaris et vérifiez que le chemin d'accès du dispositif de stockage à distance a été supprimé.**
L'exemple suivant exécute la commande `df` et montre que ce `/support` du dispositif de stockage à distance a été supprimé.

```
# df  
/ (rpool/ROOT/solaris):425092886 blocks 425092886 files  
/devices (/devices ): 0 blocks 0 files  
...
```

L'exemple suivant exécute la commande `cfgadm` et montre que le dispositif de stockage à distance (`usb1/3`) est arrêté.

# cfgadm				
Ap_Id	Type	Receptacle	Occupant	Condition
...				
usb1/3	unkown	empty	unconfigured	ok

4.6.15 Autres points à noter et opérations

Cette section décrit les points à noter et les méthodes de fonctionnement lorsque le stockage à distance est utilisé.

Points à noter concernant des erreurs se produisant lorsque le stockage à distance est utilisé

Un événement anormal, tel qu'un redémarrage du XSCF, une commutation du XSCF maître/de veille, une déconnexion du XSCF-LAN, et l'arrêt du terminal peut se produire lors de l'utilisation du stockage à distance à partir de l'invite ok ou d'Oracle Solaris. Les résultats seraient la génération d'un message d'erreur ou d'avertissement sur la console du domaine et l'enregistrement d'un journal d'erreur sur le XSCF. L'exemple suivant montre la génération d'un message d'erreur une fois Oracle Solaris installé depuis l'invite ok.

```
{0} ok boot rcdrom
Boot device: /pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@
3/disk@0,0:a File and args:
|
read failed
FCode aborted.
$boot failed
The file just loaded does not appear to be executable.
```

Si une erreur se produit lors de l'accès au stockage à distance sur Oracle Solaris, l'erreur est détectée depuis le pilote sd et un message d'avertissement est généré. L'exemple suivant montre un message d'avertissement généré par le pilote sd.

```
WARNING: /pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0 (sd5):
Error for Command: read(10)                      Error Level: Retryable
Requested Block: 39665                            Error Block: 39665
Vendor: Fujitsu                                    Serial Number:
Sense Key: Media_Error
ASC: 0x11 (unrecovered read error), ASCQ: 0x0, FRU: 0x0
```

```
WARNING: /pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0 (sd5):
SCSI transport failed: reason 'timeout': giving up
```

Après un rétablissement suite à une erreur qui s'est produite, vous pouvez restaurer la connexion au stockage à distance en effectuant les opérations correspondantes sur le XSCF et le terminal. Consultez « [Opérations de restauration pour une erreur qui s'est produite pendant l'utilisation du stockage à distance](#) ».

Opérations de restauration pour une erreur qui s'est produite pendant l'utilisation du stockage à distance

Cette section décrit les opérations de restauration pour une erreur qui s'est produite pendant l'utilisation du stockage à distance.

1. **Connectez-vous à XSCF Web depuis le terminal de gestion du système.**
2. **Sélectionnez [Menu] - [Paramètres] - [Stockage à distance].**
3. **Vérifiez la connexion dans le tableau de configuration réseau du stockage à distance.**
 - Si une adresse IP est affichée, effectuez les opérations des étapes 4 et suivantes.
 - Si « Disponible » est affiché, effectuez les opérations des étapes 6 et suivantes.
 - Si « Indisponible » est affiché, un redémarrage du XSCF est en cours. Après l'entrée dans l'état « Disponible », effectuez les opérations des étapes 6 et suivantes.
4. **À partir de la colonne Interface dans le tableau de configuration du réseau de stockage à distance, sélectionnez l'interface XSCF-LAN à connecter au support cible.**
5. **Cliquez sur le bouton [Détacher].**
6. **Vérifiez le statut sur l'écran [Serveur de stockage à distance XSCF].**
 - Si « Attente d'une connexion provenant du XSCF » est affiché, effectuez les opérations des étapes 8 et suivantes.
 - Si « Connecté » est affiché, cliquez sur le bouton [Arrêt]. Un message de confirmation apparaît. Cliquez sur le bouton [OK].

Remarque : Si l'écran [Serveur de stockage à distance XSCF] est déjà affiché, l'opération de Lancement de l'écran [Serveur de stockage à distance XSCF] dans XSCF Web n'est pas nécessaire.

Remarque : Si la connexion dans le tableau de configuration réseau du stockage à distance est « Disponible », « Connecté » est affiché en Statut sur l'écran [Serveur de stockage à distance XSCF]. Par conséquent, cliquez sur le bouton [Arrêt] pour passer le Statut à « Déconnecté ».

7. **Cliquez à nouveau sur le bouton [Exécuter] de l'écran [Serveur de stockage à distance XSCF].**
 - Le support cible attend une connexion provenant du XSCF.
8. **À partir de la colonne Interface dans le tableau de configuration du réseau de stockage à distance du XSCF Web, sélectionnez l'interface XSCF-LAN à connecter au support cible.**
9. **Cliquez sur le bouton [Joindre].**
 - À ce stade, un écran permettant de spécifier l'adresse IP du terminal apparaît. Vérifiez que l'adresse IP est correcte, puis cliquez sur le bouton [OK].
 - La connexion dans le tableau de configuration réseau du stockage à distance

affiche l'adresse IP du terminal. Cette opération connecte le XSCF au support cible.

Chaque ligne de Statut, Support sélectionné et Adresse IP XSCF dans la partie supérieure de l'écran [Serveur de stockage à distance XSCF] est actualisée comme indiqué ci-dessous.

Statut	Connecté
Support sélectionné	Chemin d'accès du support sélectionné
Adresse IP du XSCF	Adresse IP physique du XSCF-LAN connecté

10. **Pendant qu'Oracle Solaris est en exécution, connectez-vous au domaine à l'aide du stockage à distance. Exécutez ensuite les commandes `cfgadm` et `df`, puis vérifiez que le stockage à distance peut être utilisé. À l'invite `ok`, exécutez la commande `show-disks` et vérifiez que le chemin d'accès du dispositif de stockage à distance a été ajouté.**

L'exemple suivant exécute la commande `cfgadm` sur Oracle Solaris.

# cfgadm				
Ap_Id	Type	Receptacle	Occupant	Condition
...				
usb1/3	usb-storage	connected	configured	ok

L'exemple suivant exécute la commande `show-disks` à l'invite `ok`.

```
{0} ok show-disks
a) /pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk
b) /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk
...

Enter Selection, q to quit:
```


Activation de processeur

Les cœurs du processeur doivent être activés pour être en mesure d'utiliser les ressources de processeur du SPARC M12/M10. Ce chapitre fournit un aperçu de la gestion des cœurs du processeur. Afin de répondre au mieux à la charge de travail, vous pouvez ajouter ou supprimer dynamiquement des cœurs de processeur en cours de fonctionnement de votre SPARC M12/M10.

- [Concepts de base d'une activation de processeur](#)
- [Clé d'activation de processeur](#)
- [Ajout des ressources du cœur du processeur](#)
- [Suppression des ressources du cœur du processeur](#)
- [Déplacement des ressources du cœur du processeur](#)
- [Affichage des informations d'activation de processeur](#)
- [Sauvegarde/restauration des clés d'activation de processeur](#)
- [Dépannage des erreurs d'activation de processeur](#)
- [Remarques importantes au sujet de l'activation de processeur](#)

5.1 Concepts de base d'une activation de processeur

Afin de répondre au mieux à la charge de travail, vous pouvez agrandir ou réduire dynamiquement les ressources de cœur de processeur du SPARC M12/M10 sans interrompre le fonctionnement du système. Cette fonctionnalité permet une flexibilité de ressources de cœur de processeur, pour que vous puissiez agrandir autant de ressources de cœur de processeur que nécessaire, lorsque cela est nécessaire, tout en diminuant le coût initial du serveur.

Le coût des processeurs représentait une grande partie de l'investissement des anciens serveurs, car les ressources de cœur de processeur étaient achetées par unité de puce. Les coûts des logiciels étaient en sus directement liés au nombre de cœurs dont le serveur était équipé. En effet, les licences de nombreux logiciels étaient basées

sur le nombre de cœurs présents dans le système.

Dans le SPARC M12/M10, la fonction d'activation du processeur vous permet d'acheter des cœurs de processeur avec une granularité plus fine qu'une puce de processeur.

Remarque : le SPARC M12/M10 nécessite un minimum de cœurs de processeur activés pour fonctionner. L'activation du processeur SPARC M12/M10 désolidarise, à l'achat, les cœurs de processeur de la mémoire et de l'E/S (emplacements PCI Express, ports et périphériques embarqués et stockages internes). Même si aucun cœur n'est activé pour une puce de processeur donné, la mémoire et les E/S restent disponibles. Vous pouvez utiliser tous les emplacements DIMM, PCI Express et les périphériques et ports embarqués indépendamment du nombre de cœurs du processeur activés.

Pour activer les cœurs de processeur, vous devez acheter une activation de processeur, un droit permettant d'utiliser les cœurs de processeur. Lorsque vous achetez une activation de processeur, vous pouvez obtenir une clé d'activation de processeur pour rendre des ressources de cœur de processeur disponibles. L'unité d'achat d'activation de processeur pour chaque serveur est la suivante.

Tableau 5-1 Unité d'achat d'activation de processeur

Serveur	Nombre minimal de cœurs requis	Unité d'achat
SPARC M12-1	1 cœur	1 cœur (1 ensemble)
SPARC M12-2	2 cœurs	1 cœur (1 ensemble)
SPARC M12-2S	2 cœurs	1 cœur (1 ensemble)
SPARC M10-1	2 cœurs	2 cœurs (1 ensemble)
SPARC M10-4	4 cœurs	2 cœurs (1 ensemble)
SPARC M10-4S	4 cœurs	2 cœurs (1 ensemble)

Une clé d'activation de processeur est enregistrée en usine sur le XSCF, avant l'installation initiale du serveur. Une clé d'activation de processeur supplémentaire peut être activée non seulement lors de l'installation initiale du serveur, mais également lorsque le système de production est en cours d'exécution. Après avoir enregistré une clé d'activation de processeur sur le XSCF, vous devez attribuer les ressources de cœur de processeur à une partition physique. Les numéros et l'état des licences de certains types de logiciels varient selon le nombre de cœurs de processeur utilisés. Confirmez les conditions de la licence du logiciel lors de l'ajout de cœurs de processeur à utiliser.

Remarque : dans le SPARC M12/SPARC M10, un cœur de processeur possède plusieurs threads. Oracle Solaris reconnaît un processeur virtuel (vCPU) pour chaque thread matériel. Dans le SPARC M12, un ensemble d'activation de processeur est utilisé pour activer un cœur de processeur, soit huit processeurs virtuels disponibles au total pour Oracle Solaris. Dans le SPARC M10, un ensemble d'activation de processeur est utilisé pour activer deux cœurs de processeur, soit quatre processeurs virtuels disponibles au total pour Oracle Solaris.

Une clé d'activation de processeur peut être déplacée entre les unités du même modèle. Une clé d'activation de processeur enregistrée sur un serveur peut être

supprimée et enregistrée sur un serveur différent.

Vous pouvez déplacer une activation de processeur des manières suivantes :

- SPARC M12-1 ==> SPARC M12-1
- SPARC M12-2 ==> SPARC M12-2
- SPARC M12-2S ==> SPARC M12-2S
- SPARC M10-1 ==> SPARC M10-1
- SPARC M10-4 ==> SPARC M10-4
- SPARC M10-4S ==> SPARC M10-4S

Vous ne pouvez pas déplacer une activation de processeur entre des modèles différents de ceux indiqués ci-dessus :

5.2 Clé d'activation de processeur

Une clé d'activation de processeur peut être obtenue avec l'achat d'une activation de processeur. La clé est fournie sur CD-ROM. Chaque clé d'activation de processeur comprend une chaîne de caractères représentant des informations d'activation de processeur codées.

Le CD-ROM contient les éléments suivants :

/readme_ja.txt : Fichier lisez-moi en japonais
/readme_en.txt : Fichier lisez-moi en anglais
/Activation_key/ : Répertoire contenant les fichiers d'activation
/Activation_key/\$KEY_FILES (plusieurs fichiers)
: Chaque fichier contient un ensemble d'activation de processeur.
/Activation_key/\$CONSOLIDATED_KEY_FILES
: Un unique fichier contient les informations de toutes les clés
d'activation de processeur de chaque \$KEY_FILES.
/Certificate/Certificate.pdf
: Certificat d'activation du matériel

Les fichiers \$KEY_FILES et \$CONSOLIDATED_KEY_FILES sont des fichiers texte en clair. Leur nom de fichier est au format suivant :

\$KEY_FILES : AK11111_01_001.txt
\$CONSOLIDATED_KEY_FILES
: AK11111_01.txt

L'exemple suivant montre le contenu des fichiers d'activation d'un ensemble de clés

d'activation de processeur (2 cœurs) dans le SPARC M10.

```
Product: SPARC M10-1
SequenceNumber: 1234567890123456
Cpu: noExpiration 2
Text-Signature-SHA256-RSA2048:
U1VOVyXTUEFSQy1FbnRlcnByaXNlAA.....
```

Les informations de chaque clé d'activation du processeur sont divisées en plusieurs lignes. Chaque ligne possède un nom et sa valeur est suivie de « : » comme séparateur. Un exemple est donné ci-dessous. Dans cet exemple, le nom de l'élément est « Cpu » et sa valeur « noExpiration 2 ». Notez qu'une clé contient deux activations de processeur.

```
Cpu: noExpiration 2
```

Tableau 5-2 Éléments de clés d'activation du processeur et valeurs possibles

Élément	Valeur
Product	SPARC M12-2, SPARC M12-2S, SPARC M10-1, SPARC M10-4 ou SPARC M10-4S
SequenceNumber	Valeur numérique entre 1 et 16 chiffres
Cpu	Capacité du processeur (unité : cœur) noExpiration + valeur numérique comprenant jusqu'à 4 chiffres
Text-Signature-xxxxxx-xxxxxx	Signature

Les données de la clé d'activation de processeur sont stockées dans le XSCF. Les informations de clé sont automatiquement sauvegardées dans l'unité de fond de panier PSU (PSUBP). Si le XSCF échoue et est remplacé, les informations de la clé sont restaurées sur le nouveau XSCF à partir de la PSUBP.



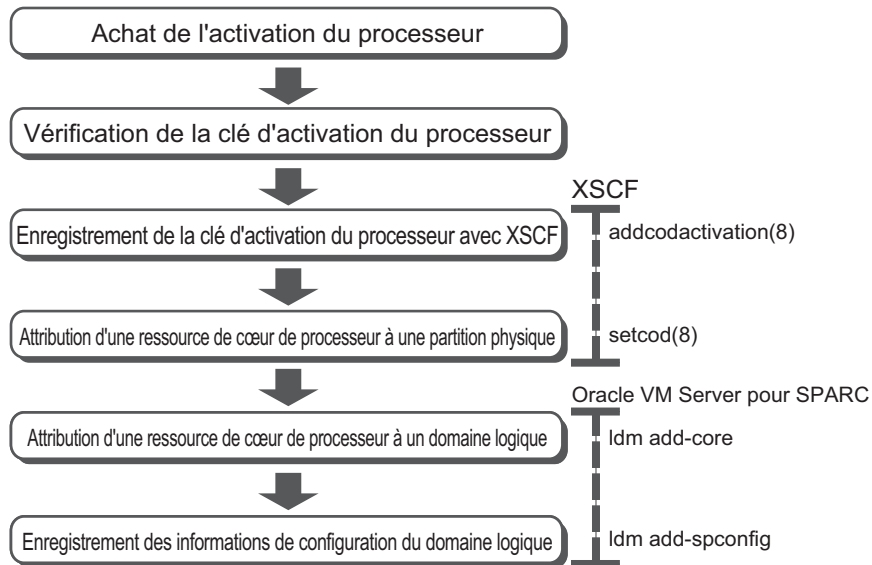
5.3 Ajout des ressources du cœur du processeur

Cette section indique comment ajouter des ressources de cœur de processeur à une partition physique et un domaine logique après avoir acheté une activation de processeur.

5.3.1 Processus jusqu'à l'ajout d'un cœur de processeur à une partition physique et un domaine logique

Figure 5-1 montre les étapes depuis l'achat d'une activation de processeur au démarrage de l'utilisation des ressources de cœur de processeur ajoutées à une partition physique et un domaine logique.

Figure 5-1 Processus jusqu'à l'ajout d'un cœur de processeur à un domaine logique



5.3.2 Achat d'activation de processeur supplémentaire

Lorsque la charge du SPARC M12/M10 augmente, vérifiez si des ressources de cœur de processeur peuvent être ajoutées. Vous pouvez utiliser la commande `showcodusage` sur le shell XSCF pour vérifier le nombre de cœurs utilisés dans une partition physique, le nombre de cœurs de processeur installés et le nombre d'activations de processeur attribuées à la partition physique. Si le nombre d'activations de processeur défini pour la partition physique est inférieur à celui des cœurs de processeurs installés, des ressources de cœur de processeur peuvent être ajoutées. Pour plus de détails, consultez « [5.6.4 Affichage de l'utilisation des ressources de cœur de processeur activées](#) ». Pour acheter des activations de processeur supplémentaires, contactez votre distributeur local. Pour soutenir la charge requise, vous pouvez utiliser un cœur de processeur temporairement jusqu'à ce que l'activation du processeur soit réalisée. Pour plus de détails, consultez « [Annexe K Permis temporaire d'activation de processeur](#) ».

5.3.3 Vérification de la clé d'activation du processeur

À l'obtention des activations de processeur commandées, vérifiez que le champ « Product » de chaque fichier de clé d'activation de processeur reçue correspond au nom de votre modèle. Sinon, la clé d'activation de processeur ne peut pas être enregistrée.

5.3.4 Enregistrement d'une clé d'activation du processeur

Pour enregistrer une clé d'activation de processeur reçue avec le XSCF, utilisez la commande `addcodactivation` du shell XSCF ou XSCF Web. Cette section décrit les procédures d'utilisation du shell XSCF.

Vous devez avoir un compte d'utilisateur bénéficiant d'un privilège `platadm` pour exécuter cette commande.

```
XSCF> addcodactivation key-signature
```

Spécifiez la clé d'activation du processeur reçue dans `key-signature`. Pour ce faire, spécifiez la clé USB avec l'option `-F` ou copiez et collez le contenu de la clé d'activation de processeur. La syntaxe de commande suivante montre comment sélectionner le support USB.

```
XSCF> addcodactivation -F file:///media/usb_msd/filename
```

Pour enregistrer toutes les clés d'activation de processeur sur le CD-ROM, spécifiez `$CONSOLIDATED_KEY_FILES` dans le nom de fichier.

Remarque : dans les versions antérieures à XCP 2041, vous ne pouvez pas spécifier `$CONSOLIDATED_KEY_FILES`.

Procédure de fonctionnement

1. **Connectez-vous à XSCF avec un compte d'utilisateur bénéficiant du privilège `platadm`.**
Pour plus de détails, consultez « [2.2 Connexion au Shell XSCF](#) ».
2. **Exécutez la commande `addcodactivation` pour enregistrer une clé d'activation de processeur avec le XSCF.**
Pour saisir la clé d'activation du processeur, spécifiez le contenu de la clé d'activation lors de l'exécution de la commande `addcodactivation`. Copiez et collez tout le contenu de la clé d'activation ou lisez-le depuis un fichier en spécifiant la fonction `-F`.
Répondez « `y` » au message de confirmation.

Dans l'exemple suivant, une clé d'activation de processeur est ajoutée à SPARC M10-1.

```
XSCF> addcodactivation "Product: SPARC M10-1
SequenceNumber: 1
Cpu: noExpiration 2
Text-Signature-SHA256-RSA2048: U1VOVyxTUEFSQy1FbnRlcnByaXNlAA....."
Above Key will be added, Continue?[y|n]: y
XSCF>
```

3. **Exécutez la commande `showcodactivation` pour confirmer que la clé d'activation de processeur a été ajoutée à XSCF.**

Avec l'option `-r` spécifiée, la commande affiche la clé d'activation de processeur recommandée.

L'exemple suivant montre les résultats obtenus à l'aide de la `showcodactivation`.

```
XSCF> showcodactivation -r
Product: SPARC M10-1
SequenceNumber: 1
Cpu: noExpiration 2
Text-Signature-SHA256-RSA2048:
U1VOVyxTUEFSQy1FbnRlcnByaXNlAA.....
```

À ce stade, les ressources de cœur de processeur ne sont pas prêtes pour une utilisation sur Oracle Solaris.

Pour rendre les ressources de cœur de processeur prêtes à être utilisées, allez dans « [5.3.5 Attribution de ressources de cœur de processeur à une partition physique](#) » pour les attribuer à une partition physique.

4. **Exécutez la commande `exit` pour vous déconnecter du shell XSCF.**

Si vous n'avez plus besoin d'utiliser le shell XSCF, vous pouvez vous déconnecter du XSCF.

Remarque : si les informations de la clé d'activation de processeur sont corrompues en raison d'une opération inattendue, la clé d'activation de processeur peut être exigée par le XSCF. Assurez-vous de stocker en sécurité les clés d'activation de processeur pour une réutilisation ultérieure.

Remarque : ajouter la même clé d'activation de processeur à plusieurs unités SPARC M12/M10 n'est pas permis.

5.3.5 Attribution de ressources de cœur de processeur à une partition physique

Pour attribuer une ressource de cœur de processeur à une partition physique, exécutez la commande `setcod` avec une opération interactive depuis le shell XSCF.

Vous devez bénéficier du privilège platadm pour exécuter cette commande.

```
XSCF> setcod [-p ppar_id] -s cpu
PROC Permits installed: XX cores
PROC Permits assigned for PPAR 0 (X MAX)
  [Permanent Xcores]
Permanent [X]: permits
PROC Permits assigned for PPAR 1 (X MAX)
  [Permanent Xcores]
Permanent [X]: permits
: Omis
```

Pour -p ppar_id, spécifiez l'identifiant de la partition physique à laquelle attribuer la ressource du cœur du processeur. Si l'opérande permits n'est pas spécifiée, la commande démarre une session interactive pour attribuer la ressource de cœur de processeur.

Si le microprogramme XSCF appliqué est XCP 2260 ou version ultérieure, vous pouvez également exécuter la commande suivante.

La valeur permits spécifie le nombre d'activations de processeur pour les cœurs de processeur utilisables.

Les activations de processeur peuvent être spécifiées en unités d'un cœur de processeur unique.

```
XSCF> setcod [[-q] -{y|n}] -p ppar_id -s cpu -c {set|add|del} permits
```

Remarque : Nous ne recommandons pas d'utiliser la commande setcod spécifiée de la façon suivante.

```
XSCF> setcod -p ppar_id -s cpu permits
```

Pour exécuter la commande setcod lorsque le microprogramme XCP est XCP 2260 ou version ultérieure, spécifiez l'option -c ou utilisez le fonctionnement interactif. Utilisez également le fonctionnement interactif pour XCP 2250 ou version précédente.

Les raisons sont les suivantes.

- À l'exécution de la commande, aucun message de confirmation ([o/n]) n'est généré concernant la mise en place des modifications avec les réglages effectués.
- Aucun message d'avertissement n'est généré lorsque le nombre d'attributions d'activations de processeur pour une partition physique en fonctionnement a été réduit. Toute carence dans le nombre d'activations de processeur, telle que celle due à des autorisations spécifiées de manière erronée, peut causer l'arrêt du système.

À l'aide de la commande setcod, vous pouvez spécifier jusqu'au nombre des activations de processeur enregistrées à l'aide de la commande addcodactivation.

Procédure de fonctionnement

1. **Connectez-vous à XSCF avec un compte d'utilisateur bénéficiant du privilège platadm.**

Pour plus de détails, consultez « [2.2 Connexion au Shell XSCF](#) ».

2. Attribuez la ressource de cœur de processeur à la partition physique à l'aide de la commande setcod.

Remarque : pour utiliser -c défini ou ne pas utiliser l'option -c, ne spécifiez pas seulement la quantité à ajouter ou à supprimer dans l'opérande permits. À la place, spécifiez la quantité actuellement définie plus le nombre d'attributions ajoutées, ou spécifiez la quantité actuellement définie moins le nombre d'attributions supprimées. Si vous indiquez par mégarde uniquement la quantité à ajouter ou supprimer, le nombre d'activations de processeur peut diminuer, ce qui peut provoquer un arrêt du système.

Dans l'exemple suivant, quatre ressources de cœur de processeur sont attribuées à la partition physique 1.

```
XSCF> setcod -p 1 -s cpu -c set 4
PROC Permits assigned for PPAR 1 : 0 -> 4

PROC Permits assigned for PPAR will be changed.
Continue? [y|n] :y

Completed.
```

L'exemple suivant montre l'attribution interactive des ressources de cœur de processeur à une partition physique.

```
XSCF> setcod -s cpu
PROC Permits installed: 5 cores
PROC Permits assigned for PPAR 0 (5 MAX) [Permanent 2cores]
Permanent [2]:1
PROC Permits assigned for PPAR 1 (4 MAX) [Permanent 0cores]
Permanent [0]:4
PROC Permits assigned for PPAR 2 (0 MAX) [Permanent 0cores]
Permanent [0]:
PROC Permits assigned for PPAR 3 (0 MAX) [Permanent 0cores]
Permanent [0]:
PROC Permits assigned for PPAR 4 (0 MAX) [Permanent 0cores]
Permanent [0]:
PROC Permits assigned for PPAR 5 (0 MAX) [Permanent 0cores]
Permanent [0]:
PROC Permits assigned for PPAR 6 (0 MAX) [Permanent 0cores]
Permanent [0]:
PROC Permits assigned for PPAR 7 (0 MAX) [Permanent 0cores]
Permanent [0]:
PROC Permits assigned for PPAR 8 (0 MAX) [Permanent 0cores]
Permanent [0]:
PROC Permits assigned for PPAR 9 (0 MAX) [Permanent 0cores]
Permanent [0]:
PROC Permits assigned for PPAR 10 (0 MAX) [Permanent 0cores]
Permanent [0]:
PROC Permits assigned for PPAR 11 (0 MAX) [Permanent 0cores]
Permanent [0]:
PROC Permits assigned for PPAR 12 (0 MAX) [Permanent 0cores]
Permanent [0]:
```

```
PROC Permits assigned for PPAR 13 (0 MAX) [Permanent 0cores]
Permanent [0]:
PROC Permits assigned for PPAR 14 (0 MAX) [Permanent 0cores]
Permanent [0]:
PROC Permits assigned for PPAR 15 (0 MAX) [Permanent 0cores]
Permanent [0]:
```

Dans l'exemple suivant, deux ressources de cœur de processeur sont ajoutées à la partition physique 0.

```
XSCF> showcod -p 0
PROC Permits assigned for PPAR 0: 10
XSCF> setcod -p 0 -s cpu -c add 2
PROC Permits assigned for PPAR 0 : 10 -> 12

PROC Permits assigned for PPAR will be changed.
Continue? [y|n] :y

Completed.
XSCF> showcod -p 0
PROC Permits assigned for PPAR 0: 12
```

Remarque : Avec **setcod -p 0 -s cpu -c set 12** spécifié, la commande donne les mêmes résultats.

Remarque : le microprogramme du XSCF de XCP 2250 ou versions précédentes ne prend pas en charge les options -c add, -c delete et -c set. Spécifiez les options de la commande setcod comme suit pour ajouter et supprimer interactivement des attributions.

XSCF> **setcod -s cpu**

3. **Exécutez la commande exit pour vous déconnecter du shell XSCF.**
Si vous n'avez plus besoin d'utiliser le shell XSCF, vous pouvez vous déconnecter du XSCF.

5.3.6 Ajout de cœurs de processeurs à un domaine logique

Pour attribuer un cœur de processeur à un domaine logique, utilisez add-core ou set-core, chacune d'elles étant une sous-commande ldm d'Oracle VM Server pour SPARC.

Pour plus de détails, consultez « Chapitre 3 Opérations pour la configuration de domaine » dans le *Guide de configuration du domaine Fujitsu SPARC M12 et Fujitsu M10/SPARCM10*.

5.3.7 Enregistrement des informations de configuration du domaine logique

Exécutez la commande `ldm` d'Oracle VM Server pour SPARC avec la sous-commande `spconfig` spécifiée pour enregistrer les informations de configuration du domaine logique.

```
primary# ldm add-spconfig config_name
```

Pour `config_name`, spécifiez le nom du fichier utilisé pour sauvegarder les informations de configuration du domaine logique vers le XSCF.

Remarque : la sous-commande `add-spconfig` ne peut pas substituer les informations de configuration dans un fichier existant. Avant de spécifier le nom d'un fichier existant pour `config_name`, vous devez supprimer le fichier présent en utilisant la sous-commande `remove-spconfig`.

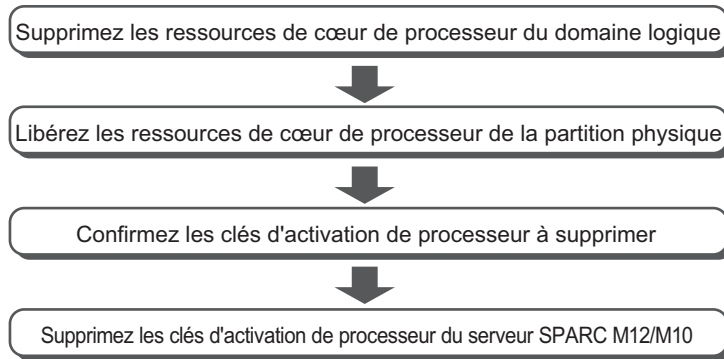
5.4 Suppression des ressources du cœur du processeur

Cette section explique comment supprimer une activation de processeur du SPARC M12/M10. En général, il n'est pas nécessaire de supprimer une activation de processeur. Lorsque vous déplacez une activation de processeur sur un autre serveur, vous devez la supprimer de votre SPARC M12/M10. Pour les procédures de déplacement, consultez « [5.5 Déplacement des ressources du cœur du processeur](#) ».

5.4.1 Processus de suppression d'une activation de processeur

[Figure 5-2](#) montre les étapes de suppression d'une activation de processeur.

Figure 5-2 Processus de suppression d'une activation de processeur



5.4.2 Suppression des cœurs de processeurs de domaines logiques

Pour retirer un cœur de processeur d'un domaine logique, utilisez `add-core` ou `set-core`, chacune d'elles étant une sous-commande `ldm` d'Oracle VM Server pour SPARC.

Pour plus de détails, consultez « Chapitre 3 Opérations pour la configuration de domaine » dans le *Guide de configuration du domaine Fujitsu SPARC M12 et Fujitsu M10/SPARCM10*.

5.4.3 Déconnexion de ressources de cœur du processeur d'une partition physique

Pour déconnecter une ressource de cœur de processeur à partir d'une partition physique, utilisez la commande `setcod` sur le shell XSCF. Vous pouvez déconnecter des ressources de cœur de processeur en spécifiant un nombre inférieur d'activations de processeur que la quantité actuellement définie.

Exécutez la commande `setcod` avec le fonctionnement interactif depuis le shell XSCF. Vous devez bénéficier du privilège `platadm` pour exécuter cette commande.

```
XSCF> setcod [-p ppar_id] -s cpu
```

Si le microprogramme XSCF appliqué est XCP 2260 ou version ultérieure, vous pouvez également exécuter la commande suivante.

La valeur `permits` spécifie le nombre d'activations de processeur pour les cœurs de processeur utilisables.

Les activations de processeur peuvent être spécifiées en unités d'un cœur de processeur unique.

```
XSCF> setcod [[-q] -{y|n}] -p ppar_id -s cpu -c {set|add|del} permits
```

Pour plus de détails, consultez « [5.3.5 Attribution de ressources de cœur de processeur à une partition physique](#) ».

5.4.4 Vérification de la clé d'activation de processeur à supprimer

Pour identifier la clé d'activation de processeur à supprimer, utilisez la commande `showcodactivation` sur le shell XSCF. Vous pouvez sélectionner n'importe quelle clé d'activation de processeur.

La commande `showcodactivation` vous permet de répertorier les clés d'activation de processeur à l'aide d'un index.

```
XSCF> showcodactivation
Index      Description Count
-----
      1  PROC           2
      2  PROC           2
```

Puis, trouvez le numéro d'index de la clé d'activation de processeur à supprimer. Utilisez enfin la commande `showcodactivation` pour confirmer les informations de clé d'activation de processeur identifiées par l'index. Supposons, par exemple, que vous allez supprimer la clé d'activation de processeur d'index=1. Saisissez la commande suivante pour identifier les informations de la clé d'activation de processeur à supprimer.

```
XSCF> showcodactivation -r -i 1
*Index1
Product: SPARC M10-1
SequenceNumber: 116
Cpu noExpiration 2
Text-Signature-SHA256-RSA2048:
SBxYBSmB32E1ctOidgWV09nGFnWKNtCJ5N3WSlowbRUYlVVySvjncfOrDNteFLzo
.
.
1TSgrjnee9FyEYITT+ddJQ==
```

Pour enregistrer les informations de la clé d'activation du processeur à supprimer, nous vous suggérons de copier et coller ou notez l'intégralité du contenu de la clé pour vos archives.

5.4.5 Suppression des clés d'activation de processeur

Pour supprimer une clé d'activation du processeur reçue à partir du XSCF du SPARC M12/M10, utilisez la commande `deletecodactivation` du shell XSCF. Vous devez bénéficier du privilège `platadm` pour exécuter cette commande.

```
XSCF> deletecodactivation -i key-index
```

Spécifiez le numéro d'index de la clé d'activation de processeur à supprimer. La commande `deletecodactivation` ne vous permet pas de supprimer des clés d'activation de processeur de sorte que la quantité devienne inférieure au nombre total d'activations de processeur définies pour la PPAR par la commande `setcod`. Réduisez le nombre d'activations de processeur définies pour la PPAR à l'avance.

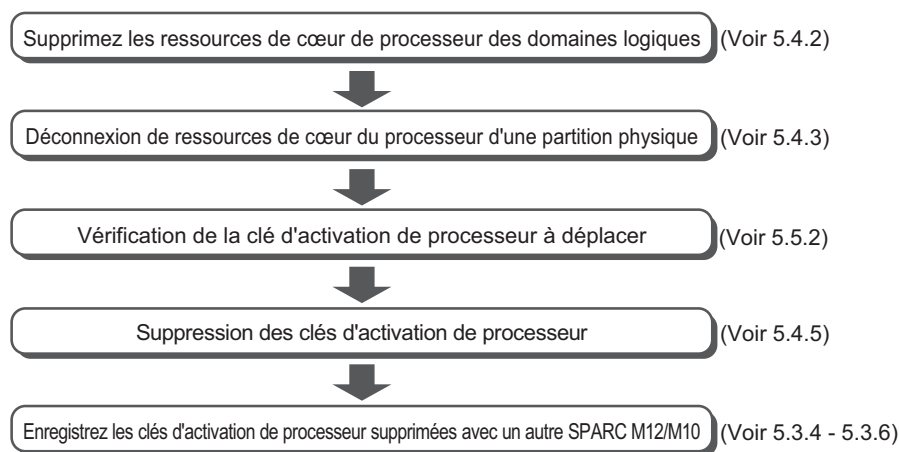
5.5 Déplacement des ressources du cœur du processeur

Lorsque vous utilisez plusieurs unités SPARC M12/M10, vous pouvez uniquement déplacer une activation de processeur entre les mêmes modèles.

5.5.1 Processus de déplacement d'une activation de processeur

Figure 5-3 montre les étapes de déplacement d'une activation de processeur.

Figure 5-3 Processus de déplacement d'une activation de processeur



Remarque : si le système SPARC M12/M10 est défaillant, une clé d'activation de processeur sur le système SPARC M12/M10 défectueux peut être enregistrée avec un autre système SPARC M12/M10. Vous n'avez pas besoin de supprimer la clé du système défectueux.

5.5.2 Vérification de la clé d'activation de processeur à déplacer

Pour identifier la clé d'activation du cœur de processeur à déplacer, utilisez la commande `addcodactivation` du shell XSCF. Vous pouvez sélectionner n'importe quelle clé d'activation de processeur pour vérifier ses informations.

La commande `showcodactivation` vous permet de répertorier les clés d'activation de processeur à l'aide d'un index.

```
XSCF> showcodactivation
Index      Description Count
-----
          1  PROC           2
          2  PROC           2
```

Puis, trouvez le numéro d'index de la clé d'activation de processeur à déplacer.

Utilisez enfin la commande `showcodactivation` pour confirmer les informations de clé d'activation de processeur identifiées par l'index.

Supposons, par exemple, que vous allez déplacer la clé d'activation de processeur d'index=1. Saisissez la commande suivante pour identifier les informations de la clé d'activation de processeur à déplacer.

```
XSCF> showcodactivation -r -i 1
*Index1
Product: SPARC M10-1
SequenceNumber: 116
Cpu noExpiration 2
Text-Signature-SHA256-RSA2048:
SBxYBSmB32E1ctOidgWV09nGFnWKNtCJ5N3WSlowbRUY1VVySvjncfOrDNteFLzo
.
.
1TSgrjnee9FyEYITT+ddJQ==
```

Puis ajoutez exactement la même clé à un autre M12/M10 du même modèle en copiant tout le contenu de cette clé, en commençant par la ligne `Produit`, puis en collant le contenu ou en le saisissant.

5.6 Affichage des informations d'activation de processeur

5.6.1 Vérification des informations de réglage et d'enregistrement de l'activation du processeur

L'affichage des informations des activations de processeur enregistrées et définies dans votre SPARC M12/M10 requiert l'utilisation de la commande `showcod` sur le shell XSCF. Vous devez bénéficier du privilège `platadm` ou `platop` pour exécuter cette commande. Vous pouvez également utiliser un compte d'utilisateur bénéficiant d'un privilège `pparadm`, `pparmgr` ou `pparop` pour la partition cible physique.

```
XSCF> showcod [-p ppar_id]
```

Pour l'option `ppar_id-p`, précisez l'identifiant de la partition physique dont vous souhaitez afficher les informations. Si cette option n'est pas spécifiée, la commande affiche les informations de toutes les partitions physiques accessibles.

Les informations suivantes sont affichées lorsque la commande `showcod` est exécutée.

- Nombre d'activations de processeur enregistrées dans le système
- Nombre d'activations de processeur définies pour une partition physique

Procédure de fonctionnement

1. **Connectez-vous à XSCF avec un compte d'utilisateur bénéficiant du privilège d'utilisateur approprié.**

Pour plus de détails, consultez « [2.2 Connexion au Shell XSCF](#) ».

2. **Exécutez la commande `showcod` pour afficher les informations d'activation de processeur.**

L'exemple suivant montre des informations détaillées sur toutes les activations de processeur.

```
XSCF> showcod -v -s cpu
PROC Permits installed : 8 cores
PROC Permits assigned for PPAR 0: 4 [Permanent 4cores]
:
PROC Permits assigned for PPAR 15: 0 [Permanent 0cores]
```

3. **Exécutez la commande `exit` pour vous déconnecter du shell XSCF.**

Si vous n'avez plus besoin d'utiliser le shell XSCF, vous pouvez vous déconnecter du XSCF.

5.6.2 Consultation du journal de COD

Pour afficher un journal d'événements (ajout/suppression d'une clé d'activation de processeur, par exemple), utilisez la commande `showcodactivationhistory` sur le shell XSCF.

Vous devez bénéficier du privilège `platadm`, `platop` ou `fieldeng` pour exécuter cette commande.

```
XSCF> showcodactivationhistory [target_url]
```

Spécifiez le nom de fichier pour le fichier de sortie sous le format suivant : `target_url`.

Procédure de fonctionnement

1. **Connectez-vous à XSCF avec un compte d'utilisateur bénéficiant du privilège `platadm`, `platop` ou `fieldeng`.**
Pour plus de détails, consultez « [2.2 Connexion au Shell XSCF](#) ».
2. **Exécutez la commande `showcodactivationhistory` pour afficher le journal de COD de la clé d'activation de processeur.**

```
XSCF> showcodactivationhistory
11/30/2012 01:42:41PM PST: Report Generated SPARC M10-1 SN: 843a996d
10/02/2012 02:08:49PM PST: Activation history initialized: PROC 0
cores
10/15/2012 01:36:13PM PST: Capacity added: PROC 2 cores
10/15/2012 01:46:13PM PST: Capacity added: PROC 2 cores
11/07/2012 01:36:23PM PST: Capacity deleted: PROC 2 cores
11/07/2012 01:46:23PM PST: Capacity deleted: PROC 2 cores
11/28/2012 01:37:12PM PST: Capacity added: PROC 2 cores
11/28/2012 01:47:12PM PST: Capacity added: PROC 2 cores
11/30/2012 01:37:19PM PST: Capacity added: PROC 2 cores
11/30/2012 01:41:19PM PST: Capacity added: PROC 2 cores
11/30/2011 01:42:41PM PST: Summary: PROC 8 cores
Signature: 9138HVZQ0zFJh8EoRy7i1A
```

3. **Exécutez la commande `exit` pour vous déconnecter du shell XSCF.**
Si vous n'avez plus besoin d'utiliser le shell XSCF, vous pouvez vous déconnecter du XSCF.

5.6.3 Affichage des informations de la clé d'activation de processeur

L'affichage des clés d'activation de processeur enregistrées sur votre système requiert l'utilisation de la commande `showcodactivation` sur le shell XSCF. Vous devez bénéficier du privilège `platadm` ou `platop` pour exécuter cette commande. La

commande `showcodactivation` sans spécifier d'options vous permet de répertorier les clés d'activation de processeur à l'aide d'un index.

```
XSCF> showcodactivation [-r] [-v] [-y key-index] [-M]
```

Spécifiez le numéro d'index de la clé d'activation dont vous souhaitez afficher les informations.

Vous pouvez consulter la clé d'activation de processeur de l'index spécifié sous forme de données brutes en spécifiant les options `-i` et `-r` et en exécutant la commande `showcodactivation`.

Utilisez l'option `-M` pour afficher un écran à la fois.

Procédure de fonctionnement

1. **Connectez-vous à XSCF avec un compte d'utilisateur bénéficiant du privilège `platadm` ou `platop`.**

Pour plus de détails, consultez « [2.2 Connexion au Shell XSCF](#) ».

2. **Exécutez la commande `showcodactivation` sans spécifier d'options pour répertorier les clés d'activation de processeur à l'aide d'un index.**

```
XSCF> showcodactivation
Index  Description Count
-----
1      PROC        2
2      PROC        2
```

3. **Exécutez la commande `showcodactivation` pour afficher des informations sur les clés d'activation du processeur de votre système.**

L'exemple suivant affiche les informations de la clé d'activation de processeur de l'index 2 sous forme de données brutes.

```
XSCF> showcodactivation -r -i 2
*Index2
Product: SPARC M10-1
SequenceNumber: 1
Cpu: noExpiration 2
Text-Signature-SHA256-RSA2048:
U1VOVyxTUEFSQy1FbnRlcnByaXNlAA.....
```

4. **Exécutez la commande `exit` pour vous déconnecter du shell XSCF.**

Si vous n'avez plus besoin d'utiliser le shell XSCF, vous pouvez vous déconnecter du XSCF.

5.6.4

Affichage de l'utilisation des ressources de cœur de processeur activées

L'utilisation des ressources de cœur de processeur comprend les éléments suivants :

- Ressources de cœur de processeur utilisées
- Nombre de cœurs de processeurs montés
- Nombre d'activations de processeur définies pour une partition physique
- Toute violation d'activation de processeur

Utilisez la commande `showcodusage` sur le shell XSCF pour afficher l'utilisation des ressources de cœur de processeur.

Vous devez bénéficier du privilège `platadm`, `platop` ou `fieldeng` pour exécuter cette commande. Vous pouvez également utiliser un compte d'utilisateur bénéficiant d'un privilège `pparadm`, `pparmgr` ou `pparop` pour la partition cible physique.

```
XSCF> showcodusage [-v] [-M] [-p {resource|ppar|all}]
```

Utilisez l'option `-M` pour afficher un écran à la fois.

Utilisez l'option `-p all` pour afficher l'utilisation des ressources de cœur de processeur pour toutes les partitions physiques.

Utilisez l'option `-p ppar` pour afficher l'utilisation des ressources de cœur de processeur de chaque partition physique.

Utilisez l'option `-p resource` pour chaque ressource de cœur de processeur.

Procédure de fonctionnement

1. **Connectez-vous à XSCF avec un compte d'utilisateur bénéficiant du privilège d'utilisateur approprié.**

Pour plus de détails, consultez « [2.2 Connexion au Shell XSCF](#) ».

2. **Exécutez la commande `showcodusage` pour afficher les informations d'activation de processeur.**

L'exemple suivant montre les informations d'activation du processeur.

L'exemple montre que le système dispose de 16 ressources de cœur de processeur installées et de 4 activations de processeur enregistrées, que 4 des ressources de cœur de processeur sont utilisées et que le nombre d'activations de processeur actuellement non utilisées est de 0.

```
XSCF> showcodusage -p resource
Resource In Use Installed CoD Permitted Status
-----
PROC          4         16          4 OK: 0 cores available

Note:
  Please confirm the value of the "In Use" by the ldm command of
  Oracle VM Server for SPARC.
```

The XSCF may take up to 20 minutes to reflect the "In Use" of logical domains.

Remarque : la valeur « In Use » affichée par la commande `showcodusage` peut être obsolète. Cela dépend du moment où XSCF est mis à jour. Jusqu'à 20 minutes peuvent être nécessaires pour que la valeur « In Use » soit mise à jour pour la dernière version disponible. Si la valeur « In Use » diffère de votre prévision, réexécutez la commande `showcodusage` pour vérifier la valeur.

3. **Exécutez la commande `exit` pour vous déconnecter du shell XSCF.**
Si vous n'avez plus besoin d'utiliser le shell XSCF, vous pouvez vous déconnecter du XSCF.

5.7 Sauvegarde/restauration des clés d'activation de processeur

Il arrive qu'un opérateur puisse accidentellement exécuter la commande de suppression d'une clé d'activation de processeur. Sauvegarder les clés d'activation de processeur pour les récupérer en cas d'incident est considéré comme une bonne pratique. Cette section décrit comment sauvegarder et restaurer les clés d'activation de processeur.

5.7.1 Sauvegarde des clés d'activation de processeur

Pour enregistrer les clés d'activation de processeur de votre système, utilisez la commande `addcodactivation` sur le shell XSCF. Vous devez avoir un compte d'utilisateur bénéficiant d'un privilège `platadm`, `platop` ou `fieldeng` pour exécuter cette commande.

Spécifiez l'URL de l'emplacement de stockage pour la clé d'activation de processeur. La syntaxe de commande suivante montre comment sélectionner le support USB.

```
XSCF> dumpcodactivation file:///media/usb_msd/filename
```

Cette commande enregistre toutes les clés d'activation de processeur stockées sur le XSCF.

Les clés d'activation de processeur sont stockées en clair par défaut.

Avec l'option `-e` spécifiée, la commande crypte et enregistre les clés d'activation de processeur.

5.7.2 Restauration des clés d'activation de processeur

Pour restaurer des clés d'activation de processeur sur votre système, utilisez la commande `restorecodactivation` du shell XSCF.

Vous devez avoir un compte d'utilisateur bénéficiant d'un privilège `platadm`, `platop` ou `fieldeng` pour exécuter cette commande.

Spécifiez l'URL de l'emplacement des clés d'activation du processeur stockées par la commande `dumpcodactivation`.

La syntaxe de commande suivante montre comment sélectionner le support USB.

```
XSCF> restorecodactivation file:///media/usb_msd/filename
```

Avant d'exécuter cette commande, vous devez mettre hors tension toutes les partitions physiques.

La commande restaure toutes les clés d'activation de processeur stockées à l'URL spécifiée.

5.8 Dépannage des erreurs d'activation de processeur

5.8.1 Le nombre de cœurs de processeurs dépasse le nombre de cœurs de processeurs activés

Si le nombre de cœurs de processeurs utilisés dépasse le nombre de cœurs de processeurs activés, l'erreur suivant est enregistrée dans le journal du service OVM (`/var/svc/log/ldoms-ldmd:default.log`).

Exemple :

CPU permits-violation detection. executing permits-violation clearance

Si l'enregistrement du journal de ce service se produit, une action doit être menée, telle que l'arrêt de l'utilisation des cœurs de processeurs.

Si le problème n'est pas résolu, les cœurs de processeurs dépassant le nombre de cœurs de processeurs activés sont automatiquement supprimés des domaines logiques. Cette suppression des cœurs de processeurs s'applique à tous les domaines logiques. Si la suppression de cœurs de processeurs ne parvient pas à satisfaire la condition du nombre de cœurs de processeurs activés, le système arrête les domaines logiques.

5.8.2 Le nombre de cœurs de processeurs en fonctionnement passe sous la barre du nombre d'activations de processeur en raison d'un échec

Si le nombre de cœurs de processeur en fonctionnement passe sous la barre du nombre d'activations de processeur en raison d'un échec, toutes les ressources de cœur de processeur non attribuées au sein de la partition physique sont ajoutées dynamiquement au domaine logique pour atteindre le nombre de cœurs de processeur ajoutés au domaine logique.

Les cœurs de processeurs en échec sont supprimés du domaine logique.

Durant cette opération, le nombre total de cœurs de processeurs en fonctionnement ne dépasse pas le nombre d'activations de processeur. Par conséquent, vous n'avez pas à préparer (acheter) des activations de processeur supplémentaires pour que cette fonction soit disponible.

Cette fonction est nommée « remplacement automatique des processeurs en échec ».

La fonction est activée par défaut.

Pour plus de détails, consultez « [10.7 Configuration d'une substitution automatique de cœurs du processeur en panne](#) » et la commande `ldm` d'Oracle VM Server pour SPARC.

5.9 Remarques importantes au sujet de l'activation de processeur

Cette section fournit les remarques suivantes sur la gestion de l'activation de processeur :

- [Ajout/Suppression dynamique de cœurs de processeur](#)
- [Migration en direct](#)
- [Ajout/Retrait d'un SPARC M12-2S/M10-4S dans une configuration de bloc de construction](#)
- [Enregistrement des informations de configuration du domaine logique](#)

Ajout/Suppression dynamique de cœurs de processeur

Vous pouvez ajouter ou supprimer dynamiquement des cœurs de processeurs à l'aide de la commande `ldm` ou par le remplacement automatique des processeurs en échec.

Cette fonctionnalité utilise la reconfiguration dynamique logique d'Oracle VM Server pour SPARC.

Des configurations spécifiques peuvent toutefois forcer à redémarrer les domaines logiques pour ajouter/supprimer des cœurs de processeur, et non d'utiliser la reconfiguration dynamique logique.

Cette situation se produit lorsque les cœurs de processeurs sont attribués en tant que

ressources physiques.

Pour plus d'informations, consultez « Assigning Physical Resources to Domains » dans le *Oracle VM Server for SPARC Administration Guide* pour la version utilisée.

Remarque : le SPARC M12/M10 possède les deux types de reconfiguration dynamique (DR) suivants :

- Une fonction DR qui (ré)attribue dynamiquement les ressources de cœur de processeur/mémoire de/à votre domaine logique en cours d'utilisation. Cette fonction est fournie par le logiciel Oracle VM Server pour SPARC.
 - Une fonction DR qui (ré)attribue dynamiquement un bloc de construction (soit un SPARC M12-2S ou SPARC M10-4S) de/à votre partition physique en cours d'utilisation. Cette fonction est fournie par le logiciel Oracle VM Server pour SPARC et le microprogramme XSOF.
-

Migration en direct

La partition physique destinée à recevoir la migration d'un domaine invité doit posséder suffisamment de ressources de cœur de processeur activées non attribuées à des domaines physiques. Si le nombre d'activations de processeur activées non utilisées est insuffisant, il est possible que deviez ajouter des activations de processeur. Même pour une migration à chaud entre des SPARC M12/M10 du même modèle, il est possible que les activations de processeur doivent être ajoutées à la destination. Cela est nécessaire car il est impossible de déplacer des activations de processeur entre deux systèmes (même s'ils ne forment pratiquement qu'un système.)

Pour plus de détails sur la migration à chaud, consultez « Chapitre 7 Migration d'un domaine invité » dans le *Guide de configuration du domaine Fujitsu SPARC M12 et Fujitsu M10/SPARCM10*.

Ajout/Retrait d'un SPARC M12-2S/M10-4S dans une configuration de bloc de construction

Lors de l'ajout d'un SPARC M12-2S/M10-4S dans une configuration de bloc de construction, vérifiez que le nombre d'activations de processeur est suffisant et ajoutez des unités si nécessaire.

Enregistrement des informations de configuration du domaine logique

Si vous modifiez la configuration d'un domaine logique, enregistrez les informations du domaine logique en exécutant la commande `ldm add-spconfig`.

Par exemple, supposons que vous avez déplacé un domaine logique vers un autre système grâce à la migration à chaud et réduit le nombre d'activations de processeur sur le système source. Dans ce cas, enregistrez les informations de configuration du domaine logique en utilisant la commande `ldm add-spconfig` une fois la migration à chaud terminée.

Si vous n'avez pas enregistré les informations de configuration du domaine logique, le domaine démarrera avec les informations de configuration précédente lors du prochain démarrage de la partition physique. Dans ce cas, le nombre d'activations de processeur peut être insuffisant et le démarrage peut donc échouer.

Remarque : même avec un système n'ayant que le domaine de commande dans sa

configuration, sauvegardez les informations de configuration de domaine logique lorsque vous modifiez la configuration des ressources avec la commande `ldm` d'Oracle Solaris.

Démarrage/Arrêt du système

Ce chapitre décrit les étapes pour démarrer et arrêter les systèmes SPARC M12/M10 ainsi que leurs procédures d'utilisation.

- Démarrage du système
- Arrêt du système
- Redémarrage du système
- Empêcher le démarrage d'Oracle Solaris lors de la mise sous tension

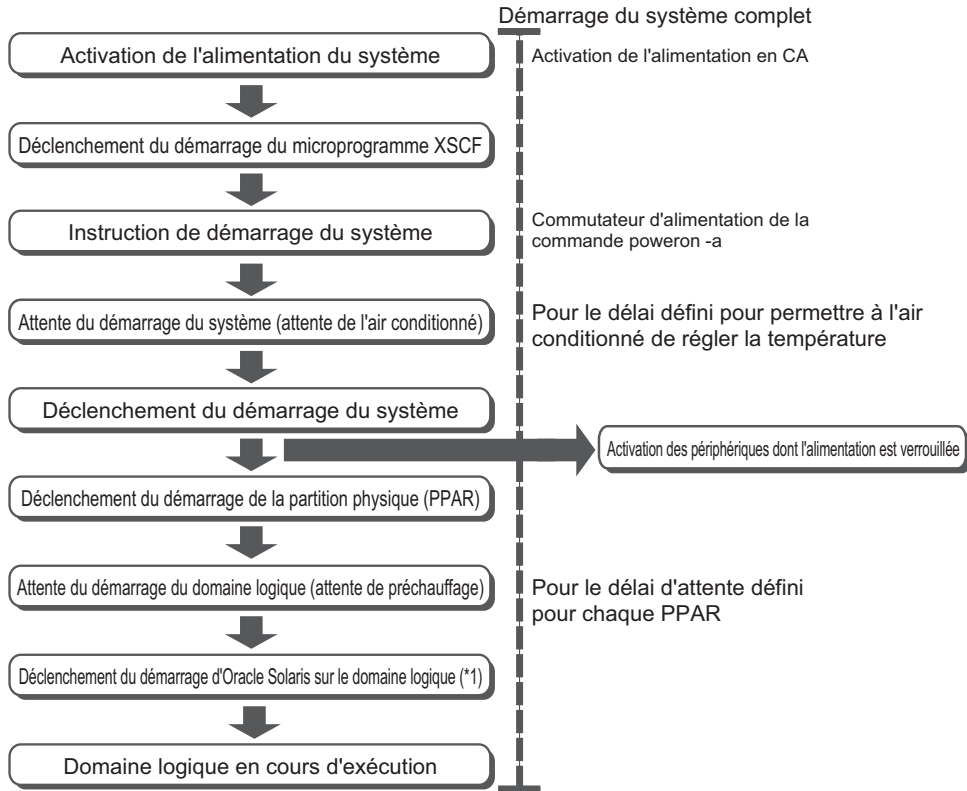
6.1 Démarrage du système

Ce chapitre décrit les étapes jusqu'au démarrage du système ainsi que les procédures d'utilisation.

6.1.1 Étapes à suivre depuis la mise sous tension jusqu'au démarrage du système

Cette section décrit les étapes à suivre depuis la mise sous tension jusqu'au démarrage du domaine logique.

Figure 6-1 Étapes à suivre depuis la mise sous tension jusqu'au démarrage du système



*1 Pour empêcher le démarrage d'Oracle Solaris, consultez « [6.4 Empêcher le démarrage d'Oracle Solaris lors de la mise sous tension](#) ».

Les deux méthodes pour spécifier l'instruction de démarrage du système sont indiquées ci-dessous. Pour les deux méthodes, effectuez les opérations sur le châssis disposant du XSCF maître.

- Utilisez le commutateur ALIMENTATION du panneau de commande.
- Utilisez la commande poweron du microprogramme XSCF.

6.1.2 Utilisation du commutateur ALIMENTATION

Appuyez sur le commutateur ALIMENTATION sur le panneau de commande du châssis disposant du XSCF maître. Appuyer sur le commutateur ALIMENTATION active l'alimentation de toutes les partitions physiques du système dans l'ordre approprié. Ensuite, tous les domaines logiques de chaque partition physique sont démarrés dans l'ordre approprié.

Remarque : seul le commutateur ALIMENTATION du châssis sur lequel se trouve le XSCF

maître fonctionne. Les commutateurs ALIMENTATION des autres châssis ne peuvent pas mettre le système sous tension.

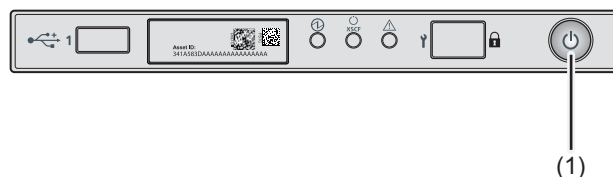
Remarque : si la commande setpparparam du microprogramme XSCF a supprimé le démarrage automatique d'un domaine de commande, le domaine de commande supprimé n'est pas démarré. En outre, si la commande setpparmode a supprimé le démarrage automatique d'une partition physique et de domaines logiques, les domaines logiques supprimés ne sont pas démarrés. Pour plus de détails sur les commandes setpparparam et setpparmode, consultez les pages du manuel correspondant aux commandes setpparparam (8) et setpparmode(8) ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

Le châssis disposant du XSCF maître varie selon le modèle.

- SPARC M12-1
Commutateur ALIMENTATION sur le SPARC M12-1
- SPARC M12-2
Commutateur ALIMENTATION sur le SPARC M12-2
- SPARC M12-2S (sans boîtier à barre transversale)
Commutateur ALIMENTATION BB#00 ou BB#01 (châssis dont la DEL MAÎTRE est sous tension) du SPARC M12-2S
- SPARC M12-2S (avec boîtier à barre transversale)
Commutateur ALIMENTATION sur le boîtier à barre transversale XBBOX#80 ou XBBOX#81 (châssis dont la LED MAÎTRESSE est sous tension)
- SPARC M10-1
Commutateur ALIMENTATION sur le SPARC M10-1
- SPARC M10-4
Commutateur ALIMENTATION sur le SPARC M10-4
- SPARC M10-4S (sans boîtier à barre transversale)
Commutateur ALIMENTATION BB#00 ou BB#01 (châssis dont la LED MAÎTRESSE est sous tension) du SPARC M10-4S
- SPARC M10-4S (avec boîtiers à barre transversale)
Commutateur ALIMENTATION sur le boîtier à barre transversale XBBOX#80 ou XBBOX#81 (châssis dont la LED MAÎTRESSE est sous tension)

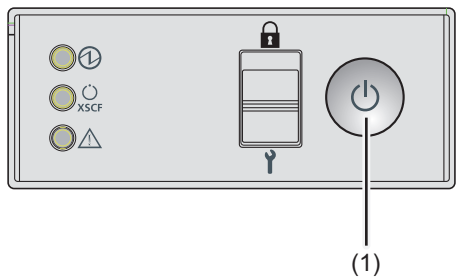
Pour plus de détails sur les commutateurs et les DEL du panneau de commande, consultez le *Service Manual* pour votre serveur.

Figure 6-2 Panneau de commande (SPARC M12-1/M10-1)



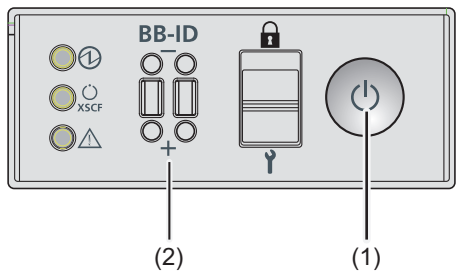
N°	Composant
1	Commutateur ALIMENTATION

Figure 6-3 Panneau de commande (SPARC M12-2/M10-4)



N°	Composant
1	Commutateur ALIMENTATION

Figure 6-4 Panneau de commande (Boîtier à barre transversale SPARC M12-2S/M10-4S)



N°	Composant
1	Commutateur ALIMENTATION
2	Commutateur BB-ID

Procédure de fonctionnement

1. **Appuyez sur le commutateur ALIMENTATION du panneau de commande du châssis disposant du XSCF maître.**
Toutes les partitions physiques du système démarrent. Ensuite, tous les domaines logiques de chaque partition physique sont démarrés.

6.1.3 Utilisation de la commande poweron

Utilisez la commande `poweroff` du microprogramme XSCF pour démarrer le système complet.

Exécutez la commande avec un compte d'utilisateur disposant du privilège `platadm` ou `fieldeng`.

```
XSCF> poweron -a
```

Pour démarrer le système complet, exécutez la commande `poweron` en spécifiant l'option `-a`. L'exécution de la commande affiche un message de confirmation.

Saisissez « y ».

Une fois la commande exécutée, toutes les partitions physiques du système sont activées dans l'ordre approprié. Ensuite, tous les domaines logiques de chaque partition physique sont démarrés dans l'ordre approprié.

Remarque : si la commande `setpparparam` du microprogramme XSCF a supprimé le démarrage automatique d'un domaine de commande, le domaine de commande supprimé n'est pas démarré. En outre, si la commande `setpparmode` a supprimé le démarrage automatique d'une partition physique et de domaines logiques, les domaines logiques supprimés ne sont pas démarrés. Pour plus de détails sur les commandes `setpparparam` et `setpparmode`, consultez les pages du manuel correspondant aux commandes `setpparparam` (8) et `setpparmode` (8) ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

Procédure de fonctionnement

1. **Exécutez la commande `poweron -a` pour mettre tout le système sous tension. Répondez « y » au message de confirmation.**

```
XSCF> poweron -a
PPAR-IDs to power on:00,01,02,03
Continue? [y|n] :y
00 :Powering on
01 :Powering on
02 :Powering on
03 :Powering on

*Note*
This command only issues the instruction to power-on.
The result of the instruction can be checked by the "showpparprogress".
XSCF>
```

Toutes les partitions physiques du système sont mises sous tension. Ensuite, tous les domaines logiques de chaque partition physique sont démarrés.

2. **Exécutez la commande `showpparstatus` et vérifiez que l'alimentation de toutes les partitions physiques du système sont mises sous tension.**

```
XSCF> showpparstatus -a
PPAR-ID      PPAR Status
00           Running
01           Running
02           Running
03           Running
```

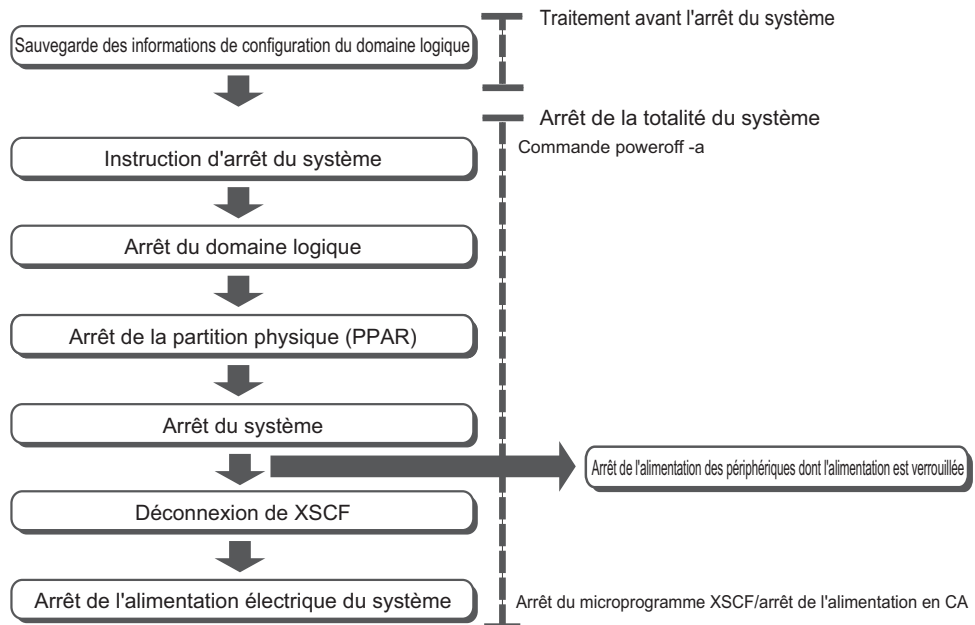
6.2 Arrêt du système

Ce chapitre décrit les étapes jusqu'à l'arrêt du système ainsi que les procédures d'utilisation.

6.2.1 Étapes à suivre depuis l'arrêt du système jusqu'à la mise hors tension

Cette section décrit les étapes à suivre depuis l'arrêt du système jusqu'à sa mise hors tension.

Figure 6-5 Étapes à suivre depuis l'instruction d'arrêt du système jusqu'à la mise hors tension



Pour arrêter le système, tous les domaines logiques des partitions physiques cibles

doivent être arrêtés. L'arrêt des domaines logiques dispose d'un ordre spécifique : les domaines autres que le domaine de commande doivent être arrêtés en premier et le domaine de commande doit être arrêté en dernier.

Les systèmes SPARC M12/M10 prennent en charge une technique nommée Arrêt commandé qui permet d'arrêter les domaines dans l'ordre approprié et d'arrêter les partitions physiques pour permettre à l'utilisateur de ne pas s'inquiéter de l'ordre de l'arrêt des domaines logiques.

Avec la fonction Arrêt commandé, les numéros qui représentent l'ordre des groupes devant être arrêtés sont définis à l'avance pour les domaines logiques. L'ordre défini est enregistré dans XSCF afin de permettre l'arrêt dans l'ordre approprié avec cette technique, même pour la gestion par XSCF.

Si un domaine invité non actif est inclus dans le groupe pour lequel un arrêt commandé est défini, l'arrêt du groupe prend environ 10 minutes.

Pour plus d'informations sur l'Arrêt commandé, consultez « [8.7 Arrêt commandé des domaines logiques](#) ».

6.2.2 Sauvegarde des informations de configuration du domaine logique avant l'arrêt du système

Dans le cas d'une configuration du domaine logique, exécutez la commande `ldm add-spconfig` d'Oracle VM Server pour SPARC dans le domaine de commande pour sauvegarder les informations de configuration les plus récentes dans le XSCF avant l'arrêt de la partition physique.

Pour plus de détails, consultez « [10.11.1 Sauvegarde/Affichage des informations de réglage du domaine logique](#) ».

Si les informations de configuration les plus récentes n'ont pas été sauvegardées dans le XSCF avant l'arrêt de la partition physique, les problèmes suivants peuvent survenir.

- Après avoir modifié la configuration du domaine logique, si la partition physique est arrêtée puis redémarrée sans que les informations de configuration du domaine logique soient sauvegardées, elle redémarre avec la même configuration du domaine logique qu'avant la modification.
- Même si la sauvegarde des informations de configuration les plus récentes dans XSCF a lieu après la modification de la configuration du domaine logique, et si la dernière sauvegarde de la configuration du domaine logique remonte à longtemps, l'heure du domaine logique peut être déviée quand la partition physique a été arrêtée puis redémarrée.

6.2.3 Arrêt du système complet

Utilisez la commande `poweroff` du microprogramme XCSF pour arrêter le système complet.

Exécutez la commande avec un compte d'utilisateur disposant du privilège `platadm` ou `fieldeng`.

Remarque : en mode Verrouillée, la mise hors tension n'est pas possible à partir du

commutateur ALIMENTATION sur le panneau de commande du châssis disposant du XSCF maître. Pour plus de détails sur le mode Verrouillé, consultez « [Chapitre 13 Passer en mode Verrouillé / Service](#) ».

```
XSCF> poweroff -a
```

Pour arrêter le système complet, exécutez la commande `poweroff` en spécifiant l'option `-a`. L'exécution de la commande affiche un message de confirmation. Saisissez « `y` ».

Une fois la commande exécutée, les domaines logiques de chaque partition physique sont arrêtés selon la règle de l'Arrêt commandé. Ensuite, la partition physique même est mise hors tension.

Procédure de fonctionnement

1. **Exécutez la commande `poweroff -a` pour mettre tout le système hors tension. Répondez « `y` » au message de confirmation.**

```
XSCF> poweroff -a
PPAR-IDs to power off:00,01,02,03
Continue? [y|n] :y
00 : Powering off
01 : Powering off
02 : Powering off
03 : Powering off
```

Note

```
This command only issues the instruction to power-off.
The result of the instruction can be checked by the "showpparprogress".
XSCF>
```

Tous les domaines logiques sont arrêtés pour toutes les partitions physiques, qui sont ensuite mises hors tension.

2. **Exécutez la commande `showpparstatus` et vérifiez que l'alimentation de toutes les partitions physiques du système sont mises hors tension.**

```
XSCF> showpparstatus -a
PPAR-ID      PPAR Status
00           Powered Off
01           Powered Off
02           Powered Off
03           Powered Off
```


6.3 Redémarrage du système

Cette section décrit comment redémarrer le système.

Utilisez la commande `rebootxscf` du microprogramme XSCF pour redémarrer le XSCF. Exécutez la commande avec un compte d'utilisateur disposant du privilège `platadm` ou `fieldeng`.

Après que les éléments de XSCF suivants sont configurés, un redémarrage de XSCF active les paramètres :

- Application du réseau XSCF configuré au XSCF (`applynetwork`)
- Altitude du système (`setaltitude`)
- Paramètres liés au NTP (`setntp`)

```
XSCF> rebootxscf -a | -b bb_id | -s
```

Pour redémarrer tous les XSCF du système, spécifiez `-a`. Pour redémarrer le XSCF du SPARC M12-2S/M10-4S spécifié, spécifiez `-b bb_id`. Seul le XSCF maître peut exécuter les options `-a` et `-b`. Afin de redémarrer le XSCF en cours de fonctionnement, spécifiez `-s`.

Le redémarrage de XSCF déconnecte les connexions SSH, Telnet et autres connexions de XSCF. Établir de nouveau la connexion.

Remarque : si le redémarrage effectué par la commande `setdate` du microprogramme XSCF est annulé, même le redémarrage du XSCF par la commande `rebootxscf` n'applique pas les paramètres. La commande `setdate` doit être exécutée à nouveau.

Procédure de fonctionnement

1. **Exécutez la commande `rebootxscf` pour redémarrer le XSCF. Répondez « y » au message de confirmation.**

L'exemple suivant redémarre tous les XSCF.

```
XSCF> rebootxscf -a  
The XSCF will be reset. Continue? [y|n] : y
```

6.4 Empêcher le démarrage d'Oracle Solaris lors de la mise sous tension

Cette section explique comment empêcher le démarrage d'Oracle Solaris lors de la mise sous tension du SPARC M12/M10.

Remarque : dans le SPARC M12/M10, même si vous réglez le commutateur de mode du panneau de commande sur « Service », vous ne pouvez pas empêcher le démarrage d'Oracle Solaris.

La méthode permettant d'empêcher le démarrage d'Oracle Solaris lors de la mise sous tension du SPARC M12/M10 est décrite ci-dessous.

- Empêcher le démarrage d'Oracle Solaris dans le domaine de commande
Exécutez l'une des opérations suivantes. Après cette opération, Oracle Solaris s'arrête dans OpenBoot PROM.
 - Réglez la valeur de la variable d'environnement auto-boot? OpenBoot PROM sur false à l'aide de la commande setpparparam du microprogramme XSCF.
[Exemple]XSCF> **setpparparam -p 0 -s bootscript "setenv auto-boot? false"**
 - Réglez la valeur de la variable d'environnement auto-boot? OpenBoot PROM sur false à l'aide de la commande eeprom d'Oracle Solaris.

Pour plus de détails sur la commande setpparparam, consultez la page du manuel correspondant à la commande setpparparam(8) ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

Pour plus de détails sur le changement des variables d'environnement d'OpenBoot PROM avec le microprogramme XSCF, consultez « [8.9.1 Variables d'environnement OpenBoot PROM pouvant être réglées avec le microprogramme XSCF](#) ».

- Empêcher le démarrage d'Oracle Solaris dans le domaine invité
Définissez guestboot=off avec la commande setpparmode du microprogramme XSCF.

[Exemple] XSCF> **setpparmode -p 0 -m guestboot=off**

Pour plus de détails sur la commande setpparmode, consultez la page du manuel correspondant à la commande setpparmode(8) ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

Contrôle des partitions physiques

Ce chapitre décrit les éléments nécessaires au contrôle des partitions physiques.

- Configuration d'une partition physique
- Réglage des modes de fonctionnement de la partition physique
- Mise sous tension de la partition physique
- Mise hors tension de la partition physique
- Modification de la configuration d'une partition physique

7.1 Configuration d'une partition physique

Cette section résume la configuration des partitions physiques.

Pour configurer un système SPARC M12-2S ou SPARC M10-4S, configurez une partition physique (PPAR) en combinant un ou plusieurs blocs de construction dans un serveur du même modèle. La configuration des partitions physiques s'appelle partitionnement, et l'objet configuré qui en résulte s'appelle partition physique (PPAR). Dans le SPARC M12-2S/M10-4S, jusqu'à 16 partitions physiques peuvent être configurées.

Il importe de relever que le SPARC M12-2/M10-1/M10-4 est un modèle constitué d'un seul châssis, qui peut être configuré à l'aide d'une seule partition physique.

Dans le microprogramme XSOF, lors de la configuration d'une partition physique, un bloc de construction est traité comme une carte système (PSB).

Les partitions physiques sont configurées avec la commande `addboard` du microprogramme XSOF. Pour plus de détails, consultez « Chapitre 3 Opérations pour la configuration de domaine » dans le *Guide de configuration du domaine Fujitsu SPARC M12 et Fujitsu M10/SPARCM10*.

7.2 Réglage des modes de fonctionnement de la partition physique

Cette section résume le mode de fonctionnement de la partition physique.

Dans le SPARC M12/M10, les modes de fonctionnement suivants peuvent être définis pour chaque partition physique :

- Niveau de diagnostic du test d'auto-diagnostic
- Niveau d'auto-diagnostic des messages de la console de test d'auto-diagnostic
- Vérification de l'activité (surveillance entre XSCF et le superviseur)
- Fonctionnement lorsque Host Watchdog (surveillance entre le superviseur et le domaine de commande) expire
- Suppression du signal d'arrêt
- Démarrage automatique de domaines invités
- Opération d'économie de l'énergie
- Reconfiguration bus E/S
- Fonction PPAR DR
- Mode de fonctionnement du processeur

La configuration d'un mode de fonctionnement permet de contrôler une partition physique donnée pour qu'elle ne reçoive pas de signaux ni d'instructions inutiles lors de l'exécution ou en cours de maintenance.

Le mode de fonctionnement de la partition physique est réglé par la commande `setpparmode` du microprogramme de XSCF. Pour plus de détails, consultez « Chapitre 3 Opérations pour la configuration de domaine » dans le *Guide de configuration du domaine Fujitsu SPARC M12 et Fujitsu M10/SPARCM10*.

Remarque : le démarrage automatique pour le domaine de commande est défini par la commande `setpparparam`. Pour plus de détails, consultez « [8.9.1 Variables d'environnement OpenBoot PROM pouvant être réglées avec le microprogramme XSCF](#) ».

7.2.1 Processeur installé sur une partition physique et mode de fonctionnement du processeur

Dans le SPARC M10-4S, vous pouvez configurer le système comme une partition physique qui possède à la fois un SPARC M10-4S avec le processeur SPARC64 X+ et un SPARC M10-4S avec le processeur SPARC64 X.

Lorsque le mode de fonctionnement du processeur de la commande `setpparmode` du microprogramme XSCF est réglé et que le type d'opération du processeur est spécifié par partition physique, lors de la prochaine activation d'Oracle Solaris, le système détermine automatiquement s'il doit fonctionner avec la fonction d'un processeur SPARC64X+ ou processeur SPARC64X.

Types de fonctionnement du processeur

Il existe deux types de fonctionnement du processeur comme suit :

- **Exploitation avec la fonction SPARC64 X+**
Tous les processeurs sur la partition physique fonctionnent avec la fonction améliorée du processeur SPARC64 X+.
Ceci s'applique uniquement lorsque le mode de fonctionnement du processeur (cpumode) est réglé sur « auto » avec la commande setpparmode, et tous les processeurs sur la partition physique sont configurés avec le processeur SPARC64 X+.
- **Exploitation avec la fonction SPARC64 X**
Tous les processeurs sur la partition physique fonctionnent avec la fonction de processeur de SPARC64 X.
Lorsque le mode de fonctionnement du processeur (cpumode) est réglé sur « compatible » avec la commande setpparmode, tous les processeurs installés sur la partition physique sont configurés avec la fonction du processeur SPARC64 X+.
En outre, lorsque le mode de fonctionnement du processeur est réglé sur « auto » avec la commande setpparmode, tous les processeurs fonctionnent avec la fonction du processeur SPARC64 X si le processeur SPARC64 X est installé sur la partition physique.

Remarque : pour que le microprogramme XCP puisse prendre en charge le paramétrage du mode de fonctionnement du processeur et la version Oracle Solaris, voir *Notes de produit des systèmes Fujitsu M10/SPARC M10* pour la dernière version de XCP (XCP 2210 ou version ultérieure).

Configuration du processeur et mode de fonctionnement des partitions physiques

Comme indiqué dans PPAR#2 dans [Figure 7-1](#), vous pouvez configurer une partition physique dotée du processeur SPARC64 X+ et du processeur SPARC64 X dans un système SPARC M10-4S.

Figure 7-1 Exemple de configuration des processeurs et des partitions physiques installés sur un système SPARC M10-4S

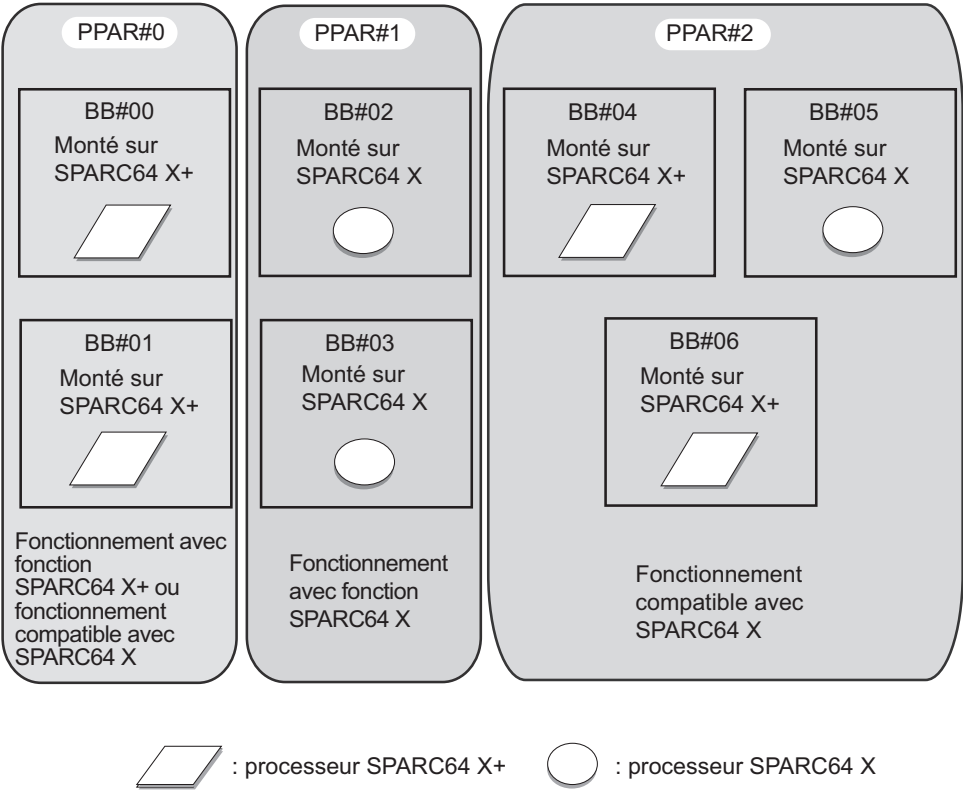


Tableau 7-1 recense les configurations de processeur des partitions physiques, les valeurs de configuration du mode de fonctionnement du processeur et les types de fonctionnement du processeur sur Oracle Solaris.

Tableau 7-1 Configuration du processeur et mode de fonctionnement des partitions physiques

Configuration du processeur de la PPAR	Valeur du mode de fonctionnement (mode CPU) de la commande setpparmode	Type de fonctionnement du processeur d'Oracle Solaris
SPARC64 X+	auto	Fonctionnement avec la fonction SPARC64 X+
SPARC64 X+	compatible	Fonctionnement avec SPARC64 X compatible
SPARC64 X+/X	« auto » ou « compatible »	Fonctionnement SPARC64 X+ avec SPARC64 X compatible Fonctionnement SPARC64 X avec SPARC64 X compatible
SPARC64 X	« auto » ou « compatible »	Fonctionnement de la fonction SPARC64 X

Pour plus de détails sur la configuration du processeur des partitions physiques au moment de l'opération PPAR DR et les types de fonctionnement de processeur sur Oracle Solaris, consultez « 2.6 Considérations à prendre en compte sur l'utilisation du processeur SPARC64 X+ » dans le *Guide de configuration du domaine Fujitsu SPARC M12 et Fujitsu M10/SPARCM10*.

Vérification du type de fonctionnement du processeur appliqué

Pour vérifier le type de fonctionnement du processeur actuellement appliqué, exécutez la commande `prtdiag` ou la commande `psrinfo` d'Oracle Solaris. Lorsque le processeur de la partition physique fonctionne avec la fonction SPARC64 X+, « SPARC64-X+ » sort sur la ligne du mode du processeur système. D'un autre côté, lorsque le processeur de la partition physique fonctionne avec la fonction SPARC64 X+, « SPARC64-X » s'affiche sur la ligne du mode du processeur système.

1. **Sur la partition physique ciblée, exécutez la commande `prtdiag` ou `psrinfo` d'Oracle Solaris avec l'option `-pv` pour vérifier le type de fonctionnement du processeur actuellement appliqué.**

Dans ce cas, la fonction de SPARC64 X+ est utilisée pour le fonctionnement.

L'exemple suivant illustre les résultats d'exécution d'une commande `prtdiag`.

```
primary# prtdiag
System Configuration: Oracle Corporation sun4v SPARC M10-4S
Memory size: 391168 Megabytes

===== Virtual CPUs =====

CPU ID Frequency Implementation      Status
-----
0      3700 MHz  SPARC64-X+                          on-line
```

L'exemple suivant illustre les résultats d'exécution de `psrinfo -pv`.

```
primary# psrinfo -pv
The physical processor has 12 cores and 24 virtual processors (0-23)
  The core has 2 virtual processors (0 1)
  The core has 2 virtual processors (2 3)
  The core has 2 virtual processors (4 5)
  The core has 2 virtual processors (6 7)
  The core has 2 virtual processors (8 9)
  The core has 2 virtual processors (10 11)
  The core has 2 virtual processors (12 13)
  The core has 2 virtual processors (14 15)
  The core has 2 virtual processors (16 17)
  The core has 2 virtual processors (18 19)
  The core has 2 virtual processors (20 21)
  The core has 2 virtual processors (22 23)
  SPARC64-X+ (chipid 0, clock 3700 MHz)
```

Vérification de l'état de réglage du mode de fonctionnement du processeur

Utilisez la commande `showpparmode` du microprogramme XSCF pour vérifier l'état

de configuration du mode de fonctionnement du processeur. Exécutez la commande avec un compte d'utilisateur disposant du privilège platadm ou fieldeng. Vous pouvez également l'exécuter avec un compte d'utilisateur disposant du privilège de pparadm de la partition physique cible.

Remarque : avec la commande de showpparmode, les dernières informations sur les paramètres définis par la commande setpparmode s'affiche. Il existe des cas qui ne correspondent pas au type de fonctionnement du processeur actuellement appliqué. Cette situation s'explique dans la mesure où les informations de paramétrage défini avec la commande setpparmode sont appliquées lors du redémarrage de la partition physique. À titre d'exemple, le mode de fonctionnement du processeur est réglé sur « auto » et le mode de fonctionnement du processeur est réglé sur « compatible » pour une partition physique qui fonctionne avec la fonction SPARC64 X+ en utilisant la commande setpparmode, « compatible » est sorti avec la commande showpparmode. Elle fonctionne toutefois avec la fonction SPARC64 X+ jusqu'à ce que la partition physique redémarre.

```
XSCF> showpparmode -p ppar_id
```

Pour ppar_id, indiquez l'ID de PPAR de la partition physique. Vous pouvez spécifier une valeur numérique comprise entre 0 et 15.

1. **Dans la partition physique cible, exécutez la commande showpparmode du microprogramme XSCF et vérifiez le mode de fonctionnement du processeur défini avec la commande setpparmode.**

Dans ce cas, il est vérifié par rapport à PPAR-ID 00.

```
XSCF> showpparmode -p 0
Host-ID                :0f010f10
Diagnostic Level        :min
Message Level          :normal
Alive Check            :on
Watchdog Reaction      :reset
Break Signal           :on
Autoboot (Guest Domain) :on
Elastic Mode           :off
IOreconfigure          :true
CPU Mode               :auto
PPAR DR (Current)      :off
PPAR DR (Next)         :off
```

Changement du mode de fonctionnement du processeur

Le mode de fonctionnement du processeur par défaut de la commande setpparmode est réglé sur « auto ». Lorsqu'il est configuré sur « auto », chaque fois qu'une partition physique est démarrée, le type de fonctionnement du processeur sur Oracle Solaris est automatiquement sélectionné en fonction du processeur installé sur la partition physique.

Lorsque le mode de fonctionnement du processeur passe de « auto » à « compatible » avec la commande setpparmode, quel que soit le type du processeur installé, à la prochaine activation de la partition physique, le processeur fonctionne avec la

fonction de SPARC64 X.

Changez le mode de fonctionnement du processeur avec la commande `showpparmode` du microprogramme XSCF. Exécutez la commande avec un compte d'utilisateur qui a le privilège `platadm`. Vous pouvez également l'exécuter avec un compte d'utilisateur disposant du privilège de `pparadm` de la partition physique cible.

```
XSCF> setpparmode -p ppar_id -m cpumode=mode
```

Pour `ppar_id`, indiquez l'ID de PPAR de la partition physique. Vous pouvez spécifier une valeur numérique comprise entre 0 et 15. Pour le mode, indiquez le mode de fonctionnement du processeur. Vous pouvez indiquer « auto » lorsque le processeur est utilisé avec la fonction SPARC64 X+, et « compatible » lorsqu'il est utilisé avec la fonction SPARC64 X. La valeur par défaut est « auto ».

Remarque : pour modifier le mode de fonctionnement du processeur, il est nécessaire de mettre la partition physique cible hors tension.

1. **Exécutez la commande `poweroff` pour mettre la partition physique cible hors tension.**

Les exemples suivants mettent PPAR-ID 00 hors tension.

```
XSCF> poweroff -p 0
PPAR-IDs to power off:00
Continue? [y|n] :y
00 : Powering off
```

```
*Note*
This command only issues the instruction to power-off.
The result of the instruction can be checked by the "showpparprogress".
XSCF>
```

2. **Exécutez la commande `showpparmode` pour confirmer la configuration actuelle du mode de fonctionnement du processeur (mode CPU).**

Dans l'exemple suivant, le mode de fonctionnement du processeur est réglé sur « auto ».

```
XSCF> showpparmode -p 0
Host-ID                :0f010f10
Diagnostic Level        :min
Message Level           :normal
Alive Check             :on
Watchdog Reaction       :reset
Break Signal            :on
Autoboot (Guest Domain) :on
Elastic Mode            :off
IOreconfigure           :true
CPU Mode                :compatible
PPAR DR (Current)       :off
PPAR DR (Next)         :off
```

3. **Exécutez la commande setpparmode pour modifier le mode de fonctionnement du processeur.**

Dans l'exemple suivant, le mode de fonctionnement du processeur passe de « auto » à « compatible ».

```
XSCF> setpparmode -p 0 -m cpumode=compatible
Diagnostic Level      :max      -> -
Message Level        :normal   -> -
Alive Check          :on       -> -
Watchdog Reaction    :reset    -> -
Break Signal         :on       -> -
Autoboot(Guest Domain) :on      -> -
Elastic Mode         :off      -> -
IOreconfigure        :true     -> -
CPU Mode             :auto     -> compatible
PPAR DR              :off      -> -
The specified modes will be changed.
Continue? [y|n] :y
configured.
Diagnostic Level      :max
Message Level        :normal
Alive Check          :on (alive check:available)
Watchdog Reaction    :reset (watchdog reaction:reset)
Break Signal         :on (break signal:non-send)
Autoboot(Guest Domain) :on
Elastic Mode         :on
IOreconfigure        :false
CPU Mode             :compatible
PPAR DR              :off
```

4. **Exécutez la commande showpparmode pour confirmer la configuration actuelle du mode de fonctionnement du processeur (mode CPU).**

Dans l'exemple suivant, le mode de fonctionnement du processeur est réglé sur « compatible ».

```
XSCF> showpparmode -p 0
Host-ID              :0f010f10
Diagnostic Level      :min
Message Level        :normal
Alive Check          :on
Watchdog Reaction    :reset
Break Signal         :on
Autoboot(Guest Domain) :on
Elastic Mode         :off
IOreconfigure        :true
CPU Mode             :compatible
PPAR DR(Current)     :off
PPAR DR(Next)        :off
```

5. **Exécutez la commande poweron pour mettre la partition physique cible sous tension.**

L'exemple suivant met PPAR-ID 00 sous tension.

```

XSCF> poweron -p 0
PPAR-IDs to power on:00
Continue? [y|n] :y
00 :Powering on

*Note*
This command only issues the instruction to power-on.
The result of the instruction can be checked by the "showpparprogress".
XSCF>

```

7.2.2 Vérification du fonctionnement de l'alimentation lors du rétablissement du courant/définition de la mise sous tension automatique

Cette section décrit comment vérifier et définir si ce qui suit est fait automatiquement lors du rétablissement du courant après une panne électrique : mise sous tension des partitions physiques et démarrage d'Oracle Solaris sur les domaines logiques.

Vérification des opérations d'alimentation lors du rétablissement du courant

Utilisez la commande `showpowerschedule` pour vérifier si une partition physique peut être mise sous tension automatiquement lors du rétablissement du courant. Utilisez la commande `showpparparam` ou `showpparmode` pour vérifier si Oracle Solaris sur un domaine logique peut être démarré automatiquement lors du rétablissement du courant. Pour toutes ces commandes, un résultat de sortie qui est la valeur par défaut signifie que la partition physique est sous tension et Oracle Solaris démarre sur le domaine logique lors du rétablissement du courant.

Procédure de fonctionnement

1. **Exécutez la commande `showpowerschedule`, et vérifiez les opérations d'alimentation électrique des partitions physiques lors du rétablissement du courant.**

```

XSCF> showpowerschedule -a -m state
PPAR-ID schedule member recover mode
-----
0         disable -      on
1         enable  1      auto

```

Si [mode de récupération] est "en marche" (par défaut) ou si [planification] est "activer" et [mode de récupération] est "auto," la partition physique est automatiquement mise sous tension lors du rétablissement du courant. [planification] a les significations suivantes.

- désactiver : les opérations d'alimentation planifiées sont désactivées. (Par défaut)
 - activer : les opérations d'alimentation planifiées sont activées.
- [mode de récupération] a les significations suivantes.
- en marche : Restaure l'alimentation lors du rétablissement du courant au même statut qu'avant la panne électrique.
En cas de statut sous tension avant la panne électrique, la mise sous tension sera effectuée. (Par défaut)
 - arrêt : Ne pas mettre sous tension lors du rétablissement du courant.
 - auto : Mettre sous tension dans la période planifiée de fonctionnement de l'alimentation lors du rétablissement du courant.

2. Exécutez la commande `showpparparam` et vérifiez le réglage du démarrage automatique du domaine de commande.

L'exemple suivant affiche la valeur définie la variable d'environnement OpenBoot PROM [auto-boot?] pour le domaine de commande de PPAR-ID 0. Le réglage est "vrai" (par défaut), ainsi Oracle Solaris démarre automatiquement lors du rétablissement du courant.

```
XSCF> showpparparam -p 0 -c auto-boot
auto-boot? :true
```

3. Exécutez la commande `showpparmode` et vérifiez le réglage du démarrage automatique du domaine invité.

L'exemple suivant affiche la valeur du paramètre de démarrage automatique [Autoboot(Guest Domain)] du domaine invité défini pour PPAR-ID 0. Le réglage est "en marche" (par défaut), ainsi Oracle Solaris démarre automatiquement lors du rétablissement du courant.

```
XSCF> showpparmode -p 0
Host-ID                :9007002b
Diagnostic Level        :min
Message Level          :normal
Alive Check            :on
Watchdog Reaction      :reset
Break Signal           :on
Autoboot(Guest Domain) :on
Elastic Mode           :off
IOreconfigure          :false
CPU Mode               :auto
PPAR DR(Current)       :-
PPAR DR(Next)          :off
```

Définir la mise sous tension automatique lors du rétablissement du courant

Utilisez la commande `setpowerschedule` pour définir le fonctionnement de

l'alimentation d'une partition physique lors du rétablissement du courant. Utilisez la commande `setpparparam` ou `setpparmode` pour définir le démarrage automatique d'un domaine logique. Définir le fonctionnement de l'alimentation d'une partition physique permet la mise sous tension automatique de la partition physique lors du rétablissement du courant. Activer la fonction de démarrage automatique d'un domaine logique permet le démarrage automatique d'Oracle Solaris lors du rétablissement du courant.

1. **Exécutez la commande `setpowerschedule` pour définir les opérations d'alimentation d'une partition physique lors du rétablissement du courant.**

Les deux types de réglages sont les suivants.

- Pour restaurer l'alimentation au même statut qu'avant la panne électrique (Par défaut)

```
XSCF> setpowerschedule -p ppar_id -c recover=on
```

- Pour suivre les opérations d'alimentation planifiées lors du rétablissement du courant

Utilisez-le lorsque la planification de l'alimentation de la partition physique a été définie par la commande `addpowerschedule`. À un moment donné couvert par la planification de l'alimentation, la partition est mise sous tension lors du rétablissement du courant, quel que soit le statut de l'alimentation de la partition physique au moment de la coupure de courant.

```
XSCF> setpowerschedule -p ppar_id -c control=enable
XSCF> setpowerschedule -p ppar_id -c recover=auto
```

2. **Exécutez la commande `setpparparam` pour définir la variable d'environnement `OpenBoot PROM` qui empêche le domaine de commande de s'arrêter à l'invite `ok`.**

```
XSCF> setpparparam -p ppar_id -s bootscript "setenv auto-boot? true"
```

3. **Pour démarrer automatiquement le domaine invité d'une partition physique, exécutez la commande `setpparmode`.**

```
XSCF> setpparmode -y -p ppar_id -m guestboot=on
```

Pour démarrer automatiquement un domaine lors du rétablissement du courant, vous devez utiliser la commande `ldm add-spconfig` sur le domaine de commande pour enregistrer les informations de configuration du domaine logique une fois domaine passé à l'état actif. Pour plus d'informations, consultez le *Oracle VM Server for SPARC Administration Guide* de la version utilisée.

Indépendamment du réglage ci-dessus, la mise sous tension lors du rétablissement du courant est supprimée lorsque le commutateur de mode est réglé sur « Service ».

Pour plus de détails sur les commandes `setpowerschedule`, `addpowerschedule`, `setpparparam` et `setpparmode`, consultez la page du manuel correspondant à chaque

7.3 Mise sous tension de la partition physique

Mettez des partitions physiques individuellement sous tension avec la commande `poweron` du microprogramme XSCF.

Exécutez la commande avec un compte d'utilisateur disposant du privilège `platadm` ou `fieldeng`. Vous pouvez également l'exécuter avec un compte d'utilisateur disposant du privilège de `pparadm` ou `pparmgr` pour la partition physique cible.

```
XSCF> poweron -p ppar_id
```

Pour spécifier une partition physique, spécifiez l'option `-p ppar_id`. Vous pouvez spécifier une valeur numérique de 0 à 15 pour `ppar_id`, qui est le PPAR-ID de la partition physique à démarrer.

L'exécution de la commande affiche un message de confirmation. Saisissez « `y` ».

Remarque : le SPARC M12-2/M10-1/M10-4 n'a qu'une seule partition physique, en conséquence, seul 0 peut être spécifié pour son PPAR-ID.

Une fois la commande exécutée, la partition physique spécifiée est mise sous tension. Ensuite, tous les domaines logiques de la partition physique sont démarrés. Le domaine de commande est démarré en premier, puis les autres domaines démarrent dans n'importe quel ordre.

Remarque : si la commande `setpparparam` du microprogramme XSCF a supprimé le démarrage automatique d'un domaine de commande, le domaine de commande supprimé n'est pas démarré. En outre, si la commande `setpparmode` a supprimé le démarrage automatique d'une partition physique et de domaines logiques, les domaines logiques supprimés ne sont pas démarrés. Pour plus de détails sur les commandes `setpparparam` et `setpparmode`, consultez les pages du manuel correspondant aux commandes `setpparparam` (8) et `setpparmode` (8) ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

Procédure de fonctionnement

1. **Exécutez la commande `poweron` pour mettre sous tension la partition physique spécifiée.**

L'exemple suivant met PPAR-ID 00 sous tension.

```

XSCF> poweron -p 0
PPAR-IDs to power on:00
Continue? [y|n] :y
00 :Powering on

*Note*
This command only issues the instruction to power-on.
The result of the instruction can be checked by the "showpparprogress".
XSCF>

```

La partition physique de PPAR-ID 00 est mise sous tension. Tous les domaines logiques de la partition physique sont démarrés.

2. **Exécutez la commande `showpparprogress` et confirmez que la partition physique spécifiée est mise sous tension.**

```

XSCF> showpparprogress -p 0
PPAR Power On Preprocessing PPAR#0 [ 1/12]
PPAR Power On                PPAR#0 [ 2/12]
XBBOX Reset                  PPAR#0 [ 3/12]
PSU On                       PPAR#0 [ 4/12]
CMU Reset Start              PPAR#0 [ 5/12]
XB Reset 1                   PPAR#0 [ 6/12]
XB Reset 2                   PPAR#0 [ 7/12]
XB Reset 3                   PPAR#0 [ 8/12]
CPU Reset 1                  PPAR#0 [ 9/12]
CPU Reset 2                  PPAR#0 [10/12]
Reset released                PPAR#0 [11/12]
CPU Start                    PPAR#0 [12/12]
The sequence of power control is completed.
XSCF>

```

7.4 Mise hors tension de la partition physique

Dans le cas d'une configuration du domaine logique, exécutez la commande `ldm add-sponfig` d'Oracle VM Server pour SPARC dans le domaine de commande pour sauvegarder les informations de configuration les plus récentes dans le XSCF avant d'arrêter la partition physique.

Pour plus de détails, consultez « [6.2.2 Sauvegarde des informations de configuration du domaine logique avant l'arrêt du système](#) » et « [10.11.1 Sauvegarde/Affichage des informations de réglage du domaine logique](#) ».

Avec la commande `poweroff` du microprogramme XSCF, mettez des partitions physiques individuellement sous tension.

Exécutez la commande avec un compte d'utilisateur disposant du privilège `platadm` ou `fieldeng`. Vous pouvez également l'exécuter avec un compte d'utilisateur

disposant du privilège de pparadm ou pparmgr pour la partition physique cible.

```
XSCF> poweroff -p ppar_id
```

Pour spécifier une partition physique, spécifiez -p ppar_id. Vous pouvez spécifier une valeur numérique de 0 à 15 pour ppar_id, qui est le PPAR-ID de la partition physique à arrêter. Cette valeur dépend de la configuration du système.

L'exécution de la commande affiche un message de confirmation. Saisissez « y ».

Une fois la commande exécutée, les domaines logiques de chaque partition physique sont arrêtés selon la règle de l'Arrêt commandé. Ensuite, la partition physique même est mise hors tension.

Procédure de fonctionnement

1. **Exécutez la commande poweroff pour mettre la partition physique spécifiée hors tension.**

Les exemples suivants mettent PPAR-ID 00 hors tension.

```
XSCF> poweroff -p 0  
PPAR-IDs to power off:00  
Continue? [y|n] :y  
00 : Powering off
```

Note

This command only issues the instruction to power-off.
The result of the instruction can be checked by the "showpparprogress".
XSCF>

Une fois que tous les domaines logiques de la partition physique avec PPAR-ID 00 sont arrêtés, la partition physique est mise hors tension.

2. **Exécutez la commande showpparprogress et vérifiez l'état en marche/arrêt de la partition physique spécifiée.**

```
XSCF> showpparprogress -p 0  
PPAR Power Off          PPAR#0 [ 1/ 3]  
CPU Stop                PPAR#0 [ 2/ 3]  
PSU Off                 PPAR#0 [ 3/ 3]  
The sequence of power control is completed.  
XSCF>
```

7.5 Modification de la configuration d'une partition physique

Cette section résume la procédure de modification de la configuration d'une partition

physique.

Après avoir configuré une partition physique dans le système SPARC M12/M10, vous pouvez en modifier la configuration en ajoutant ou en retirant une carte système physique (PSB).

Utilisez la commande `addboard` ou `deleteboard` du microprogramme XSCF pour modifier la configuration d'une partition physique. Pour plus de détails, consultez « Chapitre 3 Opérations pour la configuration de domaine » dans le *Guide de configuration du domaine Fujitsu SPARC M12 et Fujitsu M10/SPARCM10*.

Contrôle des domaines logiques

Ce chapitre décrit le contrôle des domaines logiques ainsi que la procédure de contrôle des domaines logiques.

- Configuration d'un domaine logique
- Configuration de la zone noyau d'Oracle Solaris
- Passage à la console du domaine de commande depuis le shell XSCF
- Retour au shell XSCF depuis la console du domaine de commande
- Démarrage d'un domaine logique
- Arrêt d'un domaine logique
- Arrêt commandé des domaines logiques
- Vérification des informations d'activation de processeur
- Réglage des variables d'environnement d'OpenBoot PROM du domaine de commande
- Fonction de connexion de la console du domaine
- Modification de la configuration d'un domaine logique
- Réglage de l'heure des domaines logiques
- Collecte d'un fichier de vidage du superviseur
- Gestion des ressources des domaines logiques associées aux sockets de processeur
- Réglage de la stratégie de reconfiguration dynamique de la partition physique
- Configuration de la taille de page maximale d'un domaine logique

8.1 Configuration d'un domaine logique

Un domaine logique correspond à l'environnement matériel virtuel fourni par Oracle VM Server pour SPARC. Vous pouvez diviser une plate-forme en plusieurs environnements matériels virtuels (domaines logiques). Oracle Solaris peut fonctionner indépendamment sur chaque domaine logique. Un SPARC M12/M10 peut avoir une configuration de plusieurs domaines logiques capable d'intégrer

plusieurs serveurs pour optimiser la disponibilité du système. En outre, les processeurs, la mémoire, les périphériques d'E/S et les autres ressources matérielles installées sur la plate-forme peuvent être répartis de manière flexible parmi les domaines logiques pour accroître l'utilisation des ressources.

Dans les systèmes SPARC M12/M10, après la configuration d'une partition physique, les domaines logiques sont configurés comme environnements de réseau indépendants (plateformes virtuelles) dans le partitionnement physique (PPAR).

Pour plus de détails sur la configuration des domaines logiques, consultez le *Guide de configuration du domaine Fujitsu SPARC M12 et Fujitsu M10/SPARCM10*.

8.2 Configuration de la zone noyau d'Oracle Solaris

La zone noyau d'Oracle Solaris est une fonction fournie avec Oracle Solaris les versions 11.2 et ultérieures d'Oracle Solaris. Une zone peut fonctionner en tant que système d'exploitation indépendant de la zone globale. La zone noyau d'Oracle Solaris est différente d'une zone non globale et fonctionne par noyaux séparés qui ne reposent pas sur une zone globale. Ceci améliore l'indépendance du système d'exploitation et des applications, et améliore la sécurité.

Pour plus d'informations sur la procédure de configuration de la zone noyau d'Oracle Solaris, consultez *Creating and Using Oracle Solaris Kernel Zones* de la version utilisée. D'autre part, pour les problèmes connus sur les zones noyau, consultez « Kernel Zone Issues » dans les *Oracle Solaris Release Notes* de la version utilisée.

8.2.1 Conditions matérielles et logicielles des zones noyau d'Oracle Solaris

Ce qui suit montre le XCP et les versions d'Oracle Solaris, et le SRU essentiel pour exécuter les zones noyau d'Oracle Solaris.

- SPARC M12 XCP 3021 ou ultérieur, Oracle Solaris 11.2 SRU11.2.4.6.0 ou ultérieur
- SPARC M10 XCP 2230 ou ultérieur, Oracle Solaris 11.2 SRU11.2.4.6.0 ou ultérieur

Ce qui suit montre le XCP et les versions d'Oracle Solaris, et le SRU essentiel pour exécuter la migration à chaud d'une zone noyau d'Oracle Solaris.

- SPARC M12 XCP 3021 ou ultérieur, Oracle Solaris 11.3 ou ultérieur
- SPARC M10 XCP 2280 ou ultérieur, Oracle Solaris 11.3 ou ultérieur

La zone noyau d'Oracle Solaris peut fonctionner sur un domaine logique. Il existe cependant une limite au nombre de zones noyau pouvant fonctionner simultanément sur un domaine logique. La limite est de 512 pour les systèmes SPARC M12 et de 256 pour les systèmes SPARC M10.

8.2.2 Gestion du processeur dans les zones noyau d'Oracle Solaris

Lorsque les zones noyau d'Oracle Solaris sont configurées sur des SPARC M10, nous recommandons d'exécuter la commande `zonecfg` avec la propriété « `dedicated-cpu` » pour attribuer un processeur dédié à la zone noyau d'Oracle Solaris dans les unités du cœur. Ceci peut maximiser les performances du processeur. Pour plus de détails sur la commande `zonecfg`, consultez les *Oracle Solaris Reference Manuals*.

8.2.3 Notes sur les zones noyau d'Oracle Solaris

- Si la zone noyau d'Oracle Solaris est en cours d'exécution sur un des domaines de la partition physique, vous ne pouvez pas effectuer la reconfiguration dynamique de la partition physique (PPAR DR). Arrêtez la zone noyau d'Oracle Solaris, puis effectuez la reconfiguration dynamique de la partition physique.
- Si vous exécutez la migration à chaud ou la PPAR DR (commande `deleteboard`) pendant que la zone de noyau est en cours d'utilisation sur un domaine invité, redémarrez le domaine invité avant de démarrer la zone de noyau.
- Avant d'exécuter la migration à chaud d'une zone noyau d'Oracle Solaris sur laquelle `cpu_arch=sparc64-class1` est défini entre les systèmes SPARC M12 et SPARC M10, réalisez les actions suivantes.

1. Ajoutez les lignes suivantes à `/etc/system` de la zone noyau cible de migration sur laquelle Oracle Solaris 11.3 ou ultérieur est installé.

```
set enable_lghz_stick = 1
set uhrt_enable=0x0
```

2. Redémarrez la zone noyau sur laquelle les lignes suivantes ont été ajoutées.

- Avant d'exécuter la migration à chaud d'une zone noyau d'Oracle Solaris entre un système SPARC M10 et un système autre que le SPARC M10, ou entre des systèmes SPARC M10, réalisez les actions suivantes.

Les domaines logiques/zones noyau d'Oracle Solaris requérant les actions sont les suivants.

- Tous les domaines logiques et les zones noyau d'Oracle Solaris où est installé Oracle Solaris 11.3 ou ultérieur et qui sont exécutés sur le SPARC M10 de la destination/source de migration
- Les zones noyau d'Oracle Solaris où est installé Oracle Solaris 11.3 ou ultérieur et qui sont migrées depuis un système autre que le SPARC M10

1. Ajoutez la ligne suivante au fichier `/etc/system` des domaines logiques/zones

noyau qui remplissent la condition ci-dessus.

```
set uhrt_enable = 0x0
```

2. Redémarrez les domaines logiques/zones noyau où les lignes suivantes ont été ajoutées.

8.3 Passage à la console du domaine de commande depuis le shell XSCF

Après avoir établi la connexion au Shell XSCF à partir du terminal Shell XSCF et exécuté la commande de la console, vous pouvez utiliser la console du domaine de contrôle.

Une fonction appelée redirection de console XSCF utilise une commande pour passer du Shell XSCF à la console du domaine de commande. Dans les systèmes SPARC M12/M10, le XSCF dispose d'une connexion série directe au châssis SPARC M12/M10. Lorsque l'utilisateur exécute la commande console, le XSCF sélectionne automatiquement le chemin d'un domaine de commande valide et passe à la console du domaine de commande.

8.3.1 Passage du shell XSCF à la console du domaine de commande

Lorsqu'un PC bénéficie d'une connexion XSCF-LAN ou série, vous pouvez utiliser le Shell XSCF et la console du domaine de commande sur un seul écran. Cette section décrit la procédure de permutation.

1. **Exécutez la commande console sur le terminal Shell XSCF pour passer à la console du domaine de commande.**

L'exemple suivant permet de spécifier une partition physique 0.

```
XSCF> console -p 0
```

2. **Assurez-vous que la fenêtre est bien passée à la console du domaine de commande.**

```
#
```

Seule une console RW peut être connectée par partition physique. Si une autre console RW est connectée de force par un utilisateur, avec le privilège d'utilisateur platadm ou pparadm pour la partition physique, la console RW connectée est déconnectée.

8.3.2 Connexion à la console du domaine de commande dans des circonstances appropriées

Il est impossible de passer à la console du domaine de commande lorsque la partition physique cible est hors tension.

Cette section décrit la procédure de mise sous tension de la partition physique et de connexion à la console du domaine de commande.

1. **Sur le terminal du Shell XSCF, spécifiez la partition physique et exécutez la commande `poweron` afin de mettre la partition physique sous tension.**
2. **En vous reportant à « [2.2 Connexion au Shell XSCF](#) », configurez et connectez-vous à un autre terminal shell XSCF pour afficher la console du domaine de commande dans une autre fenêtre.**
3. **Exécutez la commande `console`.**
4. **Confirmez la permutation à la console du domaine de commande spécifiée.**

8.4 Retour au shell XSCF depuis la console du domaine de commande

Une fois les opérations sur la console du domaine de commande terminées, vous pouvez revenir au Shell XSCF en appuyant sur certaines touches.

8.4.1 Passage de la console du domaine de commande au shell XSCF

Cette section décrit la procédure de retour depuis la console du domaine de commande vers le Shell XSCF.

1. **Pour repasser de la console du domaine de commande au shell XSCF, appuyez sur les touches [Entrée], [#] (valeur par défaut du caractère d'échappement) et [.] (point) respectivement.**
Pour définir un autre caractère d'échappement, différent de celui défini par défaut, spécifiez l'option et exécutez la commande `console`. Les caractères d'échappement autres que ceux par défaut ne sont valides que pour la session en cours. L'exemple suivant change le caractère d'échappement à [!].

```
XSCF> console -p 0 -s "|"
Console contents may be logged.
Connect to DomainID 0?[y|n] :y
```

Pour les types de caractères d'échappement, consultez la page de manuel

correspondant à la commande console(8) ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

2. **Assurez-vous que l'invite du Shell XSCF (XSCF>) s'affiche sur le terminal.**

8.4.2 Déconnexion de la console du domaine de commande

Lorsque vous revenez au Shell XSCF depuis la console du domaine sans vous déconnecter du domaine, vous êtes automatiquement déconnecté du domaine. Il en est de même lorsque vous quittez Shell XSCF sans vous déconnecter du domaine, vous êtes automatiquement déconnecté du domaine. À ce moment-là, des signaux de déconnexion peuvent être envoyés au programme d'arrière-plan démarré depuis la console de domaine.

Pour de plus amples informations sur le réglage de l'heure de déconnexion de la session, lorsque la console de domaine n'est pas utilisée, consultez l'explication ttymon dans le manuel de référence d'Oracle Solaris.

8.5 Démarrage d'un domaine logique

Utilisez la commande `ldm start-domain` d'Oracle VM Server pour SPARC pour démarrer les domaines logiques individuellement.

Seul un utilisateur racine ou un utilisateur ayant le rôle `ldomadm` est en droit d'exécuter cette commande.

```
primary# ldm start-domain ldom
```

Pour `ldom`, spécifiez le nom du domaine logique à démarrer.

Pour plus de détails sur la commande `ldm`, consultez le *Oracle VM Server for SPARC Reference Manual* de la version utilisée.

Procédure de fonctionnement

1. **Passez de la console XSCF à la console du domaine de commande à laquelle appartient le domaine logique cible.**

Pour plus d'informations sur le passage à la console du domaine de commande, consultez « [8.3 Passage à la console du domaine de commande depuis le shell XSCF](#) ».

Si vous êtes déjà passé à la console du domaine de commande cible, passez à l'étape suivante.

2. **Exécutez la commande `ldm list-domain` pour vérifier l'état de démarrage des domaines.**

L'exemple suivant effectue une vérification de l'état des domaines logiques `primary`, `ldom1`, `ldom2` et `ldom3`.


```
primary# ldm list-domain
NAME          STATE      FLAGS    CONS    VCPU  MEMORY  UTIL  UPTIME
primary       active    -n-cv-   SP      8      4G      3.1%  1d 36m
ldom1         active    -n----   5001    24     2G      34%   1m
ldom2         bound     ------  5002    16     1G      17%   17h 48m
ldom3         active    -n----   5003    16     4G      17%   17h 48m
```

3. **Exécutez la commande `ldm start-domain` pour démarrer le domaine spécifié.**
L'exemple suivant démarre ldom2.

```
primary# ldm start-domain ldom2
```

4. **Exécutez la commande `ldm list-domain` pour vérifier l'état de démarrage des domaines.**
L'exemple suivant effectue une vérification de l'état des domaines logiques primary, ldom1, ldom2 et ldom3.

```
primary# ldm list-domain
NAME          STATE      FLAGS    CONS    VCPU  MEMORY  UTIL  UPTIME
primary       active    -n-cv-   SP      8      4G      3.1%  1d 36m
ldom1         active    -n----   5001    24     2G      34%   1m
ldom2         active    -n----   5002    16     1G      34%   17h 48m
ldom3         active    -n----   5003    16     4G      17%   17h 48m
```

Vous pouvez constater que le domaine logique ldom2 a démarré correctement.

8.6 Arrêt d'un domaine logique

Utilisez la commande `ldm stop-domain` d'Oracle VM Server pour SPARC pour arrêter individuellement les domaines logiques.

Seul un utilisateur racine ou un utilisateur ayant le rôle `ldomadm` est en droit d'exécuter cette commande.

```
primary# ldm stop-domain ldom
```

Pour ldom, spécifiez le nom du domaine logique à arrêter.

Pour plus de détails sur la commande `ldm`, consultez le *Oracle VM Server for SPARC Reference Manual* de la version utilisée.

Procédure de fonctionnement

1. **Passez de la console XSCF à la console du domaine de commande à laquelle appartient la partition physique du domaine logique cible.**
Pour plus d'informations sur le passage à la console du domaine de commande,

consultez « [8.3 Passage à la console du domaine de commande depuis le shell XSCF](#) ».

Si vous êtes déjà passé à la console du domaine de commande cible, passez à l'étape suivante.

2. **Exécutez la commande `ldm list-domain` pour vérifier l'état de démarrage des domaines.**

L'exemple suivant effectue une vérification de l'état des domaines logiques `primary`, `ldom1`, `ldom2` et `ldom3`.

```
primary# ldm list-domain
```

NAME	STATE	FLAGS	CONS	VCPU	MEMORY	UTIL	UPTIME
primary	active	-n-cv-	SP	8	4G	3.1%	1d 36m
ldom1	active	-n----	5001	24	2G	34%	1m
ldom2	active	-n----	5002	16	1G	34%	17h 48m
ldom3	active	-n----	5003	16	4G 1	7%	17h 48m

3. **Exécutez la commande `ldm stop-domain` pour arrêter le domaine spécifié.**

L'exemple suivant arrête `ldom2`.

```
primary# ldm stop-domain ldom2
```

4. **Exécutez la commande `ldm list-domain` pour vérifier l'état de démarrage des domaines.**

L'exemple suivant effectue une vérification de l'état des domaines logiques `primary`, `ldom1`, `ldom2` et `ldom3`.

```
primary# ldm list-domain
```

NAME	STATE	FLAGS	CONS	VCPU	MEMORY	UTIL	UPTIME
primary	active	-n-cv-	SP	8	4G	3.1%	1d 36m
ldom1	active	-n----	5001	24	2G	34%	1m
ldom2	bound	-----	5002	16	1G		
ldom3	active	-n----	5003	16	4G 1	7%	17h 48m

Une fois que le domaine est arrêté, `STATE` devient l'état lié de la ressource (`bound`).



8.7 Arrêt commandé des domaines logiques

Dans les systèmes SPARC M12/M10, vous pouvez effectuer un arrêt commandé de tous les domaines logiques depuis le XSCF. Pour plus de détails sur la manière de démarrer un arrêt commandé, consultez le *Guide de configuration du domaine Fujitsu SPARC M12 et Fujitsu M10/SPARCM10*.

Vous pouvez changer les priorités de l'arrêt en définissant le nombre de groupes d'arrêt pour les domaines logiques avec la commande `ldm`.

Les domaines logiques sont arrêtés dans l'ordre décroissant de leur numéro de groupe d'arrêt. En d'autres termes, le domaine ayant le plus grand numéro est arrêté en premier. Le domaine ayant le numéro le plus bas est arrêté en dernier. Si plusieurs domaines partagent une priorité commune, ils sont arrêtés en même temps, sauf dans le cas d'une relation maître-esclave. Dans ce cas, un domaine esclave est arrêté avant un domaine maître.

Pour plus de détails sur comment définir le maître et l'esclave, consultez le *Oracle VM Server for SPARC Administration Guide*.

Les valeurs efficaces sont entre 1 et 15. Le numéro de groupe d'arrêt du domaine de commande est égal à 0 et ne peut être modifié. La valeur par défaut de tout autre domaine est 15.

```
# ldm set-domain shutdown-group=8 secondary
```

Supposons que tous les autres domaines invités possèdent le numéro de groupe d'arrêt par défaut. Dans ce cas, un arrêt commandé fermerait d'abord tous les autres domaines invités, puis le domaine secondaire et enfin le domaine de commande.

À titre d'exemple, le numéro de groupe d'arrêt défini pour un domaine nommé « secondary » n'est pas la valeur par défaut.

Remarque : vous pouvez définir la propriété `shutdown-group` lorsqu'un domaine logique est dans un des états inactifs, liés, et actifs. En outre, lors de la création d'un domaine logique, vous pouvez également définir ses propriétés. Toutefois, pour permettre une priorité d'arrêt mise à jour, le XSCF doit reconnaître les nouvelles valeurs de propriété.

Pour que le XSCF puisse reconnaître les valeurs des propriétés réglées, définissez chaque domaine à l'état lié ou actif et utilisez ensuite la commande `ldm add-spconfig` pour enregistrer les informations de configuration du domaine logique. Remettez ensuite le serveur sous tension pour permettre au XSCF de reconnaître les valeurs.

8.7.1 Tableau des domaines (IdomTable)

La propriété `IdomShutdownGroup` a été ajoutée à `IdomTable` qui est utilisé pour représenter les domaines individuels du système, et ses informations peuvent être obtenues à partir d'Oracle VM Server pour SPARC MIB.

Tableau 8-1 Tableau des domaines (IdomTable)

Nom	Type de données	Accès	Description
IdomShutdownGroup	Entier	Lecture seule	Arrêtez le numéro du groupe d'un domaine invité. Dans les systèmes SPARC M12/M10, lorsque le XSCF commence un arrêt commandé, les domaines sont arrêtés dans l'ordre décroissant des numéros de groupe d'arrêt (dans l'ordre de 15 à 0). La valeur par défaut est 15.

8.7.2 Ressources d'informations sur le domaine (Idom_info)

La propriété shutdown-group a été ajoutée aux propriétés d'option dans les ressources Idom_info.

```
<Envelope>
  <References/>
  <Content xsi:type="ovf:VirtualSystem_Type" id="primary">
    <Section xsi:type="ovf:ResourceAllocationSection_type">
      <Item>
        <rasd:OtherResourceType>Idom_info</rasd:OtherResourceType>
        :
        :
        <gprop:GenericProperty key="shutdown-group">0</gprop:GenericProperty>
        :
        :
      </Item>
    </Section>
  </Content>
</Envelope>
```

Les ressources Idom_info sont toujours contenues dans une section <Content>. Utilisez la balise avec la clé suivante dans les ressources Idom_info.

- shutdown-group

Cette propriété indique la priorité d'arrêt utilisée lors d'un arrêt commandé. Les demandes d'arrêt sont émises aux domaines dans l'ordre décroissant du groupe d'arrêt, de 15 à 0. Le domaine de commande est toujours un groupe d'arrêt 0. Les valeurs efficaces pour les groupes d'arrêt de tout autre domaine sont comprises entre 1 et 15.

Pour de plus amples informations sur les propriétés des ressources Idom_info, consultez le *Oracle VM Server for SPARC Administration Guide* de la version que vous utilisez.

8.8

Vérification des informations d'activation de processeur

Vous pouvez afficher une liste d'information sur l'activation du processeur en utilisant la commande `ldm`. Pour plus de détails sur l'activation du processeur, consultez « [Chapitre 5 Activation de processeur](#) ».

1. **Exécutez la sous-commande suivante pour afficher une liste des informations d'activation du processeur.**

```
# ldm list-permits
```

Les informations suivantes sont affichées lorsque la commande `ldm list-permits` est exécutée.

Tableau 8-2 Contenu affiché avec la commande `ldm list-permits`

Élément	Description
PERMITS	Affiche le nombre d'activations de processeur attribuées à la partition physique.
IN USE	Affiche le nombre d'activations de processeur utilisées dans les domaines logiques.
REST	Affiche le nombre d'activations de processeur non utilisées dans les domaines logiques.

Dans l'exemple suivant, la colonne PERMITS montre que 15 activations de processeur (nombre d'autorisations) ont été attribuées à la partition physique au total. La colonne IN USE montre que 14 cœurs de processeurs parmi tous ceux autorisés sont en cours d'utilisation. La colonne REST montre qu'un cœur de processeur supplémentaire peut être utilisé.

```
#ldm list-permits
CPU CORE
PERMITS (PERMANENT)  IN USE      REST
15      (15)         14         1
```

Pour de plus amples informations sur l'affichage des autres listes de ressources de domaine, consultez le *Oracle VM Server for SPARC Administration Guide* de la version que vous utilisez.

8.9

Réglage des variables d'environnement d'OpenBoot PROM du domaine de commande

Cette section décrit les éléments réglables avec le microprogramme XSCF parmi les variables d'environnement OpenBoot PROM pouvant être définies pour le domaine de contrôle.

Pour plus de détails sur les variables d'environnement OpenBoot PROM et OpenBoot PROM, consultez l'explication eeprom dans le manuel de référence d'Oracle Solaris et le *OpenBoot 4.x Command Reference Manual* d'Oracle Corporation.

Pour plus de détails sur les informations spécifiques au système SPARC M12/M10 pour les commandes OpenBoot PROM et les variables d'environnement d'OpenBoot PROM, consultez « [Annexe H Variables d'environnement et commandes d'OpenBoot PROM](#) ».

8.9.1

Variables d'environnement OpenBoot PROM pouvant être réglées avec le microprogramme XSCF

Parmi les variables d'environnement OpenBoot PROM destinées au domaine de commande, les variables d'environnement suivantes sont définies avec le microprogramme XSCF.

Tableau 8-3 Variables d'environnement OpenBoot PROM du domaine de commande telles que définies par le microprogramme XSCF

Variable d'environnement OpenBoot PROM	Description	Méthode de paramétrage
auto-boot?	Démarre automatiquement le domaine de commande à la mise sous tension (la valeur par défaut est true). Pour configurer le microprogramme XSCF de manière à ce qu'il ne démarre pas automatiquement le système d'exploitation (arrêt à {0}ok) avant de démarrer une partition physique, définissez cette variable.	Script de démarrage

Tableau 8-3 Variables d'environnement OpenBoot PROM du domaine de commande telles que définies par le microprogramme XSCF (*suite*)

Variable d'environnement OpenBoot PROM	Description	Méthode de paramétrage
input-device	Définit le périphérique d'entrée de la console du domaine de commande (par défaut console virtuelle). Si OpenBoot PROM ne peut pas démarrer, définissez cette variable de manière à ce que le microprogramme XSCF puisse mettre à jour la variable d'environnement OpenBoot PROM et démarrer OpenBoot PROM.	Script de démarrage
output-device	Définit le périphérique de sortie de la console du domaine de commande (la valeur par défaut est la console virtuelle). Si OpenBoot PROM ne peut pas démarrer, définissez cette variable de manière à ce que le microprogramme XSCF puisse mettre à jour la variable d'environnement OpenBoot PROM et démarrer OpenBoot PROM.	Script de démarrage
use-nvramrc?	Définit l'exécution du contenu nvramrc au démarrage du domaine de commande (la valeur par défaut est false). Si OpenBoot PROM ne peut pas démarrer, définissez cette variable de manière à ce que le microprogramme XSCF puisse mettre à jour la variable d'environnement OpenBoot PROM et démarrer OpenBoot PROM.	Opérande use-nvramrc
security-mode	Définit le mode de sécurité du microprogramme (la valeur par défaut est none). Si OpenBoot PROM ne peut pas démarrer, définissez cette variable de manière à ce que le microprogramme XSCF puisse mettre à jour la variable d'environnement OpenBoot PROM et démarrer OpenBoot PROM.	Opérande security-mode

Les opérations suivantes désignent les méthodes de paramétrage avec la commande setpparparam pour les variables d'environnement d'OpenBoot PROM ci-dessus, selon chaque type.

- Réglage des variables d'environnement dans le script de démarrage
Les variables d'environnement d'OpenBoot PROM auto-boot?, input-device et output-device sont définies par le script de démarrage pour la commande setpparparam. Le script de démarrage est une série de commandes OpenBoot PROM exécutées lors du démarrage d'OpenBoot PROM. Vous pouvez le définir à l'aide de la commande setpparparam avec l'option -s bootscript spécifiée. Le script

de démarrage qui est défini par la commande `setpparparam` est utilisé uniquement lors du démarrage du domaine de commande. Le contenu du script sont effacés après le démarrage. Vous pouvez écrire plusieurs commandes OpenBoot PROM avec 254 caractères maximum dans le script de démarrage. Si le script de démarrage a été défini incorrectement, ou si vous voulez supprimer un script de démarrage qui a été défini, spécifiez l'option- `r` avec le script `-s bootscript`.

- Réglage des variables d'environnement comme opérandes de la commande `setpparparam`
Certaines variables d'environnement d'OpenBoot PROM `user-nvramrc?` et `security-mode` sont définies avec les opérandes de la commande `setpparparam`. Ces variables d'environnement ne peuvent pas être définies dans le script de démarrage.

8.9.2 Réglage des variables d'environnement d'OpenBoot PROM pour le domaine de commande

Définissez les variables d'environnement OpenBoot PROM du domaine de contrôle avec la commande `setpparparam` du microprogramme XSCF.

Exécutez la commande avec un compte d'utilisateur disposant du privilège `platadm` ou `fieldeng`. Vous pouvez également l'exécuter avec un compte d'utilisateur disposant du privilège de `ppradm` de la partition physique cible.

Configuration du script de démarrage

```
XSCF> setpparparam -p ppar_id -s bootscript value
```

Pour `ppar_id`, définissez la partition physique pour laquelle les variables d'environnement doivent être enregistrées dans le script de démarrage. Vous pouvez spécifier un nombre entier entre 0 et 15, en fonction de la configuration du système.

Pour la valeur, définissez la commande OpenBoot PROM qui doit être enregistrée dans le script de démarrage pour modifier les variables d'environnement OpenBoot PROM. Spécifiez une valeur en la plaçant entre guillemets (« »).

Définition de `use-nvramrc ?` sur `false`

```
XSCF> setpparparam -p ppar_id use-nvramrc
```

Pour `ppar_id`, définissez la partition physique pour laquelle les variables d'environnement doivent être enregistrées. Vous pouvez spécifier un nombre entier entre 0 et 15, en fonction de la configuration du système.

Définition de `security-mode` sur `none`

```
XSCF> setpparparam -p ppar_id security-mode
```


Pour `ppar_id`, définissez la partition physique pour laquelle les variables d'environnement doivent être enregistrées. Vous pouvez spécifier un nombre entier entre 0 et 15, en fonction de la configuration du système.

Procédure de fonctionnement

1. Définissez les variables d'environnement d'OpenBoot PROM pour le domaine de commande.

L'exemple suivant autorise le démarrage automatique du domaine de commande PPAR-ID 0.

```
XSCF> setpparparam -p 0 -s bootscript "setenv auto-boot? true"
PPAR-ID of PPARs that will be affected:0
OpenBoot PROM variable bootscript will be changed.
Continue? [y|n]: y
```

L'exemple suivant définit `use-nvramrc?`, une variable d'environnement OpenBoot PROM, pour PPAR-ID 0 à faux.

```
XSCF> setpparparam -p 0 use-nvramrc
PPAR-ID of PPARs that will be affected:0
OpenBoot PROM variable use-nvramrc will be set to false.
Continue? [y|n]: y
```

L'exemple suivant définit `security-mode`, une variable d'environnement OpenBoot PROM, pour PPAR-ID 0 sur none.

```
XSCF> setpparparam -p 0 security-mode
PPAR-ID of PPARs that will be affected:0
OpenBoot PROM variable security-mode will be set to none.
Continue? [y|n]: y
```

8.9.3 Affichage des variables d'environnement d'OpenBoot PROM définies du domaine de commande

Affichez les variables d'environnement OpenBoot PROM pour le domaine de commande définies par la commande `setpparparam` avec la commande `showpparparam` du microprogramme XSCF.

Exécutez la commande avec un compte d'utilisateur qui a l'un des privilèges : `useradm`, `platadm`, `platop` ou `fieldeng`. Vous pouvez également l'exécuter avec un compte d'utilisateur disposant de `pparadm`, `pparmgr`, ou du privilège `pparop` pour la partition physique cible.

```
XSCF> showpparparam -p ppar_id
```

Pour `-ppar_id`, définissez la partition physique pour laquelle les variables d'environnement doivent être affichées. Vous pouvez spécifier un nombre entier entre 0 et 15, en fonction de la configuration du système.

Procédure de fonctionnement

1. **Affichez des variables d'environnement d'OpenBoot PROM définies et le script de démarrage du domaine de commande.**

L'exemple suivant affiche les variables d'environnement pour le domaine de commande PPAR-ID 0.

```
XSCF> showpparparam -p 0
use-nvramrc      :false
security-mode    :none
bootscript       :
setenv auto-boot? true
```

L'exemple suivant affiche la définition actuelle de `l'auto-boot?`, une variable d'environnement OpenBoot PROM pour le domaine de commande de PPAR-ID 0.

```
XSCF> showpparparam -p 0 -c auto-boot
auto-boot?      :true
```

8.9.4 Initialisation des variables d'environnement d'OpenBoot PROM définies du domaine de commande

Effacez les variables d'environnement OpenBoot du domaine de commande de l'environnement avec la commande et restaurez leur état de l'expédition de l'usine avec la commande `setpparparam` du microprogramme XSCF.

Exécutez la commande avec un compte d'utilisateur disposant du privilège `platadm` ou `fieldeng`. Vous pouvez également l'exécuter avec un compte d'utilisateur disposant du privilège de `pparadm` de la partition physique cible.

```
XSCF> setpparparam -p ppar_id set-defaults
```

Pour `ppar_id`, définissez la partition physique pour laquelle les variables d'environnement doivent être initialisées. Vous pouvez spécifier un nombre entier entre 0 et 15, en fonction de la configuration du système.

Procédure de fonctionnement

1. **Effacez les variables d'environnement d'OpenBoot PROM définies pour le domaine de commande.**

Dans l'exemple suivant, les variables d'environnement OpenBoot PROM définies

pour le domaine de commande PPAR-ID 0 sont effacées, et l'état de sortie d'usine est restauré.

```
XSCF> setpparparam -p 0 set-defaults
PPAR-ID of PPARs that will be affected:0
All OpenBoot PROM variables will be reset to original default
values.
Continue? [y|n]: y
```

8.10 Fonction de connexion de la console du domaine

Dans un environnement de domaine logique, la destination de sortie de la console du domaine de commande est XSCF. La destination de sortie de la console de tous les autres domaines logiques est le domaine de service ayant démarré la collecte du terminal de console virtuelle et l'unité de distribution (vcc).

Dans Oracle Solaris 11.1 et les versions ultérieures, les domaines de service prennent en charge la fonction de connexion de la console des domaines logiques autres que les domaines de commande.

Les données du journal sont enregistrées dans un fichier nommé `/var/log/vntsd/domain-name/console-log` placé dans le domaine de services qui fournit la collecte du terminal de console virtuelle et l'unité de distribution. Le fichier journal de la console tourne lorsque la commande `logadm` est exécutée. Pour plus de détails, consultez les pages du manuel de la commande `logadm` et du fichier `logadm.conf`.

Le logiciel Oracle VM Server pour SPARC vous permet d'activer et de désactiver la fonction de connexion de la console pour tous les domaines logiques sauf pour les domaines de commande. La fonction de connexion de la console est activée par défaut.

8.10.1 Méthode de désactivation de la fonction de connexion de la console

1. **Affichez les paramètres actuels de la console d'un domaine.**

```
# ldm list -o console domain
```

2. **Désactivez la fonction de journalisation de la console.**

```
# ldm set-vcons log=off domain
```

Remarque : pour modifier les paramètres de la fonction de connexion de la console avec la commande `ldm set-vcons`, vous devez définir le domaine invité à l'état délié, c'est-à-dire, l'état inactif.

Remarque : vous devez activer (on) ou désactiver (off) la fonction de connexion de la console pour chaque domaine invité.

8.10.2 Méthode de d'activation de la fonction de connexion de la console

1. **Affichez les paramètres actuels de la console d'un domaine.**

```
# ldm list -o console domain
```

2. **Activez la fonction de connexion de la console.**

```
# ldm set-vcons log=on domain
```

8.10.3 Exigences pour le domaine de service

Pour utiliser la fonction de connexion de la console, le domaine de service doit être démarré dans Oracle Solaris 11.1 ou une version ultérieure.

Remarque : vous devez activer (on) ou désactiver (off) la fonction de connexion de la console pour chaque domaine invité.

8.10.4 Tableau de groupe de la console virtuelle (ldmVconsTable)

La propriété `ldmVconsLog` est ajoutée à `ldmVconsTable`, en tant qu'information sur la MIB de Oracle VM Server pour SPARC. `ldmVconsTable` décrit tous les groupes de la console virtuelle pour les services de la console virtuelle.

Tableau 8-4 Tableau de groupe de la console virtuelle (ldomVconsTable)

Nom	Type de données	Accès	Description
ldomVconsLog	Chaîne de caractères affichée	Lecture seule	Statut de connexion de la console. La valeur de la propriété est la chaîne « on » ou « off » spécifiée par la commande ldm set-vcons.

Remarque : si un groupe comprend plusieurs domaines, la propriété ldomVconsLog indique l'état de la connexion de la console modifiée par la dernière commande ldm set-vcons exécutée.

8.10.5 Ressources de la console

La propriété enable-log a été ajoutée aux ressources de la console en tant qu'interface XML.

```
<Envelope>
  <References/>
  <Content xsi:type="ovf:VirtualSystem_Type" id="ldg1">
    <Section xsi:type="ovf:VirtualHardwareSection_Type">
      <Item>
        <rasd:OtherResourceType>console</rasd:OtherResourceType>
        :
        :
        <gprop:GenericProperty key="enable-log">on</gprop:GenericProperty>
      </Item>
    </Section>
  </Content>
</Envelope>
```

Les ressources de la console sont toujours présentes dans la section <Content>. Vous pouvez utiliser les balises avec les clés suivantes.

- enable-log
Cette clé permet d'activer ou de désactiver la connexion de la console virtuelle d'une console cible.

Pour plus de détails sur les propriétés des ressources de la console, consultez le *Oracle VM Server for SPARC Administration Guide* ou le *Oracle VM Server for SPARC Management Information Base User Guide* de la version que vous utilisez.

8.11 Modification de la configuration d'un domaine logique

Pour un domaine logique, vous pouvez facilement attribuer les processeurs, la mémoire, les périphériques d'E/S et d'autres ressources matérielles installés à la partition physique. En outre, le système peut reconfigurer dynamiquement les processeurs et la mémoire pour le domaine logique en cours d'exécution, de manière à gérer les augmentations de charge temporaires sans interrompre l'activité. Dans la mesure où les ressources peuvent être ajoutées et supprimées selon l'état de fonctionnement du domaine, les ressources matérielles dans un seul serveur peuvent être utilisées efficacement avec une meilleure utilisation.

Les ressources de cœur de processeur peuvent également être ajoutées dynamiquement à un domaine logique grâce à une combinaison de modifications de la configuration du domaine logique et d'activations de processeur. L'extension des ressources sans devoir retirer des ressources d'autres domaines pour la prise en charge d'une demande est possible en attribuant des ressources de cœurs du processeur non utilisées.

Oracle VM Server pour SPARC est utilisé pour la reconfiguration dynamique des processeurs et de la mémoire.

Pour la méthode de modification de la configuration des domaines logiques, consultez « Chapitre 3 Opérations pour la configuration de domaine » dans le *Guide de configuration du domaine Fujitsu SPARC M12 et Fujitsu M10/SPARCM10*.

8.12 Réglage de l'heure des domaines logiques

Cette section décrit les connaissances nécessaires et les normes de réglage de l'heure des domaines logiques.

Les systèmes SPARC M12/M10 gèrent les heures suivantes.

- Heure sur XSCF
Le XSCF gère le temps du système standard. Gérée par le XSCF maître, la même heure est réglée sur tous les XSCF. Ils gèrent l'heure même en cas de coupure de courant.
- Heure sur une partition physique
Le superviseur gère le temps pour chaque partition physique.
- Heure sur un domaine logique
L'heure est gérée pour chaque domaine logique. Une autre heure peut être gérée pour chaque domaine logique.

Pour plus de détails sur la relation entre l'heure de XSCF et les heures des domaines logiques, consultez « [3.6 Réglage de l'heure/date du XSCF](#) ».

8.13 Collecte d'un fichier de vidage du superviseur

Cette section décrit la procédure de paramétrage pour la collecte d'un fichier de vidage du superviseur.

8.13.1 Bases du vidage du superviseur

Le superviseur peut être interrompu en cas de panne matérielle ou d'erreur logicielle. Lorsque le superviseur est interrompu, une fois tous les domaines logiques réinitialisés, seul le domaine de commande démarre dans une configuration par défaut spéciale pour collecter un vidage du superviseur et les informations du superviseur sont enregistrées sous forme de fichier de vidage. Cela correspond à la fonction de vidage du superviseur.

Le fichier de vidage collecté peut contenir des informations importantes pour diagnostiquer le problème.

Remarque : si le vidage du superviseur est activé, un vidage du superviseur également collecté lorsque la commande de réinitialisation du microprogramme XSCF avec xir spécifié est exécuté pour réinitialiser une partition physique. Pour plus de détails sur la réinitialisation d'une partition physique, consultez « [10.17 Reconfiguration d'une partition physique](#) ».

Remarque : pour revenir à la configuration d'origine depuis la configuration par défaut spéciale pour collecter un vidage du superviseur, vous devez redémarrer la partition physique.

Un fichier de vidage avec le nom de fichier suivant est collecté dans le domaine de commande. Il est possible de collecter jusqu'à huit fichiers.

- Répertoire de stockage :
/var/opt/SUNWldm
- Nom du fichier :
hvdump.x.gz
x : un nombre entier compris entre 0 et 7 est attribué automatiquement.

La section suivante décrit les commandes utilisées pour la fonction de vidage du superviseur.

8.13.2 Commandes utilisées pour la fonction de vidage du superviseur

Activation/Désactivation du vidage du superviseur

Définissez le vidage du superviseur avec la commande `ldm set-hvdump` d'Oracle VM

```
primary# ldm set-hvdump [hvdump=on|off] [hvdump-reboot=on|off]
```

Pour hvdump, indiquez s'il faut activer la fonction de vidage du superviseur. Pour l'activer, spécifiez On. Pour la désactiver, spécifiez Off. Par défaut, cette fonction est activée (on).

Pour hvdump-reboot, spécifiez s'il faut redémarrer automatiquement la partition physique après la collecte du fichier de vidage. Pour redémarrer la partition physique, spécifiez on. Pour ne pas le redémarrer, spécifiez Off. La valeur par défaut est off. Si la valeur est réglée sur off, même après la collecte d'un fichier de vidage, le domaine de commande reste dans la configuration par défaut spéciale pour collecter un vidage de superviseur.

Si vous changer les réglages hvdump et hvdump-reboot grâce à la commande ldm set-hvdump, utilisez la commande ldm add-spconfig pour enregistrer les informations de configuration.

```
primary# ldm add-spconfig file
```

Remarque : même si vous redémarrez le domaine de commande démarré en configuration par défaut spéciale pour collecter un vidage de superviseur, le système ne revient pas à la configuration d'origine. Pour démarrer le système dans la configuration d'origine, vous devez redémarrer la partition physique. Après avoir exécuté la commande poweroff du XSCF ou la commande shutdown-i5 d'Oracle Solaris, exécutez la commande poweron de XSCF pour redémarrer le système.

Remarque : même lorsque le réglage hvdump-reboot est on, si un fichier de vidage n'est pas collecté car huit fichiers de vidage sont déjà collectés ou que l'espace sur le disque est insuffisant, la partition physique ne peut pas être redémarrée. Dans ce cas, déplacez ou supprimez d'abord un fichier de vidage collecté. Utilisez ensuite la commande ldm start-hvdump pour collecter un fichier de vidage. Une fois la collecte de fichier de vidage terminée, redémarrez la partition physique.

Affichage du contenu des paramètres du vidage du superviseur

Affichez les paramètres du vidage du superviseur avec la commande ldm list-hvdump.

```
primary# ldm list-hvdump
```

Les informations suivantes sont affichées lorsque la commande ldm list-hvdump est exécutée.

Tableau 8-5 Contenu affiché avec la commande ldm list-hvdump

Élément	Description

Tableau 8-5 Contenu affiché avec la commande `ldm list-hvdump` (suite)

<code>hvdump</code>	Indique si la fonction de vidage du superviseur est activée. Si elle est activée, « on » s'affiche. Si elle est désactivée, « off » s'affiche.
<code>hvdump-reboot</code>	Indique si le système est redémarré après la création du fichier de vidage. S'il doit redémarrer, le message on s'affiche. S'il ne doit pas redémarrer, le message off s'affiche.

Remarque : si la collecte d'un fichier de vidage ne s'est pas terminée comme prévu, le message « Pending hvdump exists » s'affiche.

Procédure de fonctionnement

1. **Passez de la console XSCF à la console du domaine de commande cible.**
Pour plus de détails sur le passage à la console du domaine de commande, consultez « [8.3 Passage à la console du domaine de commande depuis le shell XSCF](#) ».
Si vous êtes déjà passé à la console du domaine de commande ou au XSCF, passez à l'étape suivante.
2. **Configurer la fonction de vidage du superviseur.**
L'exemple suivant active la fonction de vidage du superviseur et définit le domaine de commande pour un redémarrage après la collecte du fichier de vidage.

```
primary# ldm set-hvdump hvdump=on hvdump-reboot=on
```

3. **Afficher les paramètres destinés à la fonction de vidage du superviseur.**
Dans l'exemple suivant, la fonction de vidage du superviseur est activée et le redémarrage après la collecte du fichier de vidage est activé.

```
primary# ldm list-hvdump
hvdump=on
hvdump-reboot=on
```

4. **Enregistrer les paramètres destinés à la fonction de vidage du superviseur.**
Dans l'exemple suivant, désignez et enregistrez un nom de fichier dans *config_name*.

```
primary# ldm add-spconfig config_name
```

8.13.3 Points à noter sur l'utilisation de la fonction de vidage du superviseur

Notez les informations suivantes sur l'utilisation de la fonction de vidage du superviseur.

- Même si une erreur se produit dans le superviseur, aucun fichier de vidage ne peut être collecté lorsque le répertoire pour l'enregistrement des fichiers de vidage a :

- Huit fichiers de vidage existants, ou
- Espace disque insuffisant pour le répertoire /var/opt/SUNWldm

Vérifiez régulièrement le nombre de fichiers de vidage ainsi que la capacité du disque du répertoire d'enregistrement des fichiers de vidage pour vous assurer que les exigences en matière de collecte de fichier de vidage sont remplies.

- S'il est impossible de collecter un fichier de vidage pour l'une des raisons indiquées ci-dessus, le processus de vidage s'arrête. Après avoir résolu le problème, exécutez la commande `ldm start-hvdump` pour collecter un fichier de vidage. Si le domaine de commande est redémarré sans que la commande `ldm start-hvdump` ne soit exécutée, aucun fichier de vidage n'est collecté et les informations du superviseur connecté sont effacées. Même lorsque le réglage `hvdump-reboot` est `on`, si un fichier de vidage n'est pas collecté, la partition physique ne peut pas être redémarrée. Dans ce cas, déplacez ou supprimez d'abord un fichier de vidage collecté. Utilisez ensuite la commande `ldm start-hvdump` pour collecter un fichier de vidage. Une fois la collecte de fichier de vidage terminée, redémarrez la partition physique.
- Même si le réglage `hvdump-reboot` est `on`, si la variable d'environnement `d'OpenBoot PROM auto-boot?` est `false`, le traitement s'arrête à l'invite `ok` sans redémarrer Oracle Solaris.
- Si le domaine de commande est involontairement démarré dans la configuration par défaut spéciale, il est possible que le processus de vidage du superviseur ne se termine pas correctement. Cela peut être dû au démarrage du domaine de commande dans une configuration par défaut spéciale pour collecter un vidage de superviseur. Exécutez la commande `ldm list-hvdump` pour vérifier si le fichier de vidage a été collecté.

L'exemple suivant montre que le fichier de vidage n'a pas pu être collecté.

```
primary# ldm list-hvdump
hvdump=on
hvdump-reboot=on
Pending hvdump exists
```

8.14 Gestion des ressources des domaines logiques associées aux sockets de processeur

8.14.1 Vue d'ensemble des contraintes des sockets de processeur

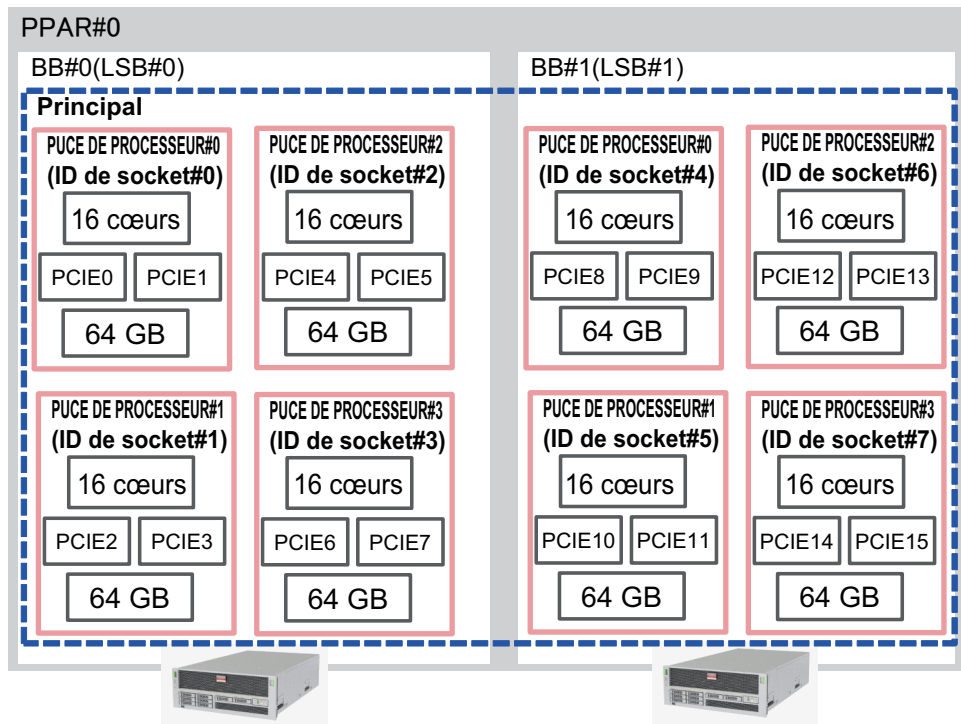
Les contraintes de socket de processeur vous permettent de créer et de configurer un domaine logique qui possède les processeurs, cœurs ou mémoire virtuels limités avec l'ID de socket de processeur spécifié. Dans la mesure où l'ID de socket de processeur est associé au numéro de LSB et au numéro d'emplacement du processeur, vous pouvez entièrement contrôler les ressources matérielles manuellement sans utiliser de liaisons physiques, telles que CID et PA.

L'ID de socket de processeur est déterminé par le numéro de LSB et le numéro d'emplacement du processeur comme suit.

$$\text{CPU socket ID} = \text{LSB number} \times 4 + \text{CPU location number}$$

Figure 8-1 montre les ressources physiques dans la partition physique configurée avec deux unités SPARC M10-4S (BB#0 et BB#1).

Figure 8-1 Ressources dans une partition physique



Pour plus de détails sur le numéro de LSB et le numéro d'emplacement du processeur, consultez « 2.4.1 Considération de la configuration de domaine logique » dans le *Guide de configuration du domaine Fujitsu SPARC M12 et Fujitsu M10/SPARCM10*.

Vous pouvez utiliser les contraintes des sockets de processeur pour effectuer des tâches telles que les suivantes.

- Créer un domaine extrêmement fiable en utilisant la mise en miroir de la mémoire, activée sur la puce de processeur spécifiée
- Avant d'exécuter la reconfiguration dynamique (PPAR DR) d'une partition physique, séparez les ressources du SPARC M12-2S et du SPARC M10-4S à supprimer à l'avance pour réduire la durée pendant laquelle un domaine invité, sur lequel la PPAR DR est exécutée, est arrêté.
- Réglez finement les performances en étendant les processeurs virtuels à chaque puce de processeur ou en consolidant les processeurs virtuels dans une puce de processeur.
- Configurez un domaine logique en utilisant uniquement le processeur SPARC64 X+ dans une partition physique possédant également un SPARC M10-4S avec un processeur SPARC64 X/SPARC64 X+.

Les commandes suivantes sont fournies en tant que commandes liées aux contraintes des sockets de processeur. Pour plus de détails sur chaque commande, consultez le *Oracle VM Server for SPARC Reference Manual* de la version utilisée.

- `ldm list-socket`

- ldm set-socket
- ldm grow-socket
- ldm shrink-socket

8.14.2 Exigences matérielles et logicielles des contraintes des sockets de processeur

Cette fonction est prise en charge sur les plateformes SPARC M12/M10. Cependant, puisque le SPARC M12-1/M10-1 dispose d'une configuration à un processeur, il n'a pas de sens dans cette fonctionnalité.

Pour utiliser les contraintes des sockets de processeur sur le SPARC M12/M10, le système doit répondre aux exigences suivantes.

- Exécute Oracle VM Server pour SPARC 3.3 ou version ultérieure
- Exécute XCP 2210 ou version ultérieure du microprogramme XCP pour SPARC M10
Pour activer l'option --remap des contraintes des sockets de processeur, le XCP 2260 ou une version ultérieure du microprogramme XCP est nécessaire.
Pour le SPARC M12, il n'y a pas d'exigences du microprogramme XCP.
- Utilise M12-2/M12-2S/M10-4/M10-4S(s)

8.14.3 Restrictions des contraintes des sockets de processeur

Les contraintes des sockets de processeur ont les restrictions suivantes.

- Si un domaine est migré, les contraintes du socket du processeur sont également effacées de la même manière qu'en attribuant physiquement un CID ou PA spécifié.
- Exécutez la commande ldm set-socket avec l'option --restore-degraded pour restaurer les contraintes des sockets de processeur.
- Le mode récupération ignore les contraintes du socket du processeur des puces de processeur en échec.
- La commande ldm init-system -f ignore les contraintes du socket du processeur du domaine de commande.
- Le remplacement automatique des processeurs en échec ne peut fonctionner que dans les ressources de socket spécifiées. S'il n'y a pas de processeur libre dans les sockets spécifiés, les processeurs en échec sont isolés mais ne sont pas remplacés.

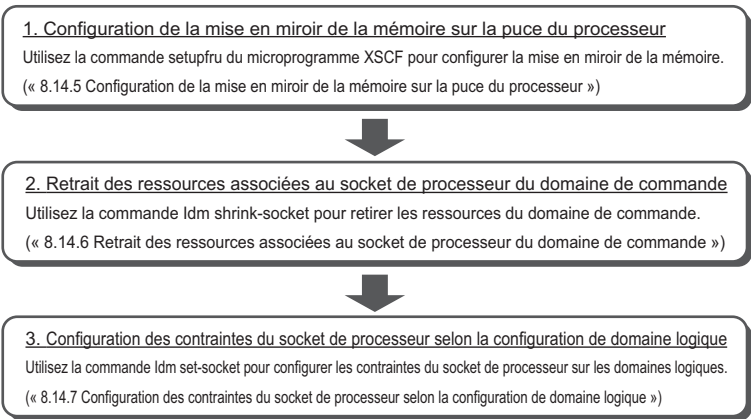
8.14.4 Création d'un domaine logique extrêmement fiable à l'aide des contraintes des sockets de processeur

Pour une meilleure compréhension des contraintes de socket de processeur, cette section décrit comment créer un domaine logique extrêmement fiable à l'aide des

contraintes de socket de processeur.

Figure 8-2 présente le flux de création d'un domaine logique extrêmement fiable.

Figure 8-2 Flux de création d'un domaine logique extrêmement fiable



Les sections suivantes 8.14.5 à 8.14.7 décrivent la procédure fournissant un exemple de création du domaine logique ldom1 en attribuant les ressources de la puce de processeur #0 dans BB#1 dans une partition physique configurée avec deux unités SPARC M10-4S (BB#0 et BB#1).

8.14.5 Configuration de la mise en miroir de la mémoire vers la puce de processeur

Utilisez la commande setupfru du microprogramme XSCF pour configurer la mise en miroir de la mémoire.

Pour plus de détails sur la configuration du mode de mise en miroir de la mémoire, consultez « 14.1 Configuration de la mise en miroir de la mémoire ». Pour plus de détails sur la commande setupfru, consultez la page du manuel correspondant à la commande setupfru(8) ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

Utilisez la commande ldm list-socket pour afficher la liste des ressources de chaque socket de processeur.

L'exemple suivant montre que la taille de la mémoire associée au socket de processeur #4 est réduite de moitié car le mode de mise en miroir de la mémoire a été réglé sur la puce de processeur #0 dans BB#1.

# ldm list-socket				
CONSTRAINTS				
SOCKET				
TENANT	VCPUS	CORES	SOCKET_ID	GROUP
primary	32	16	0	/BB0

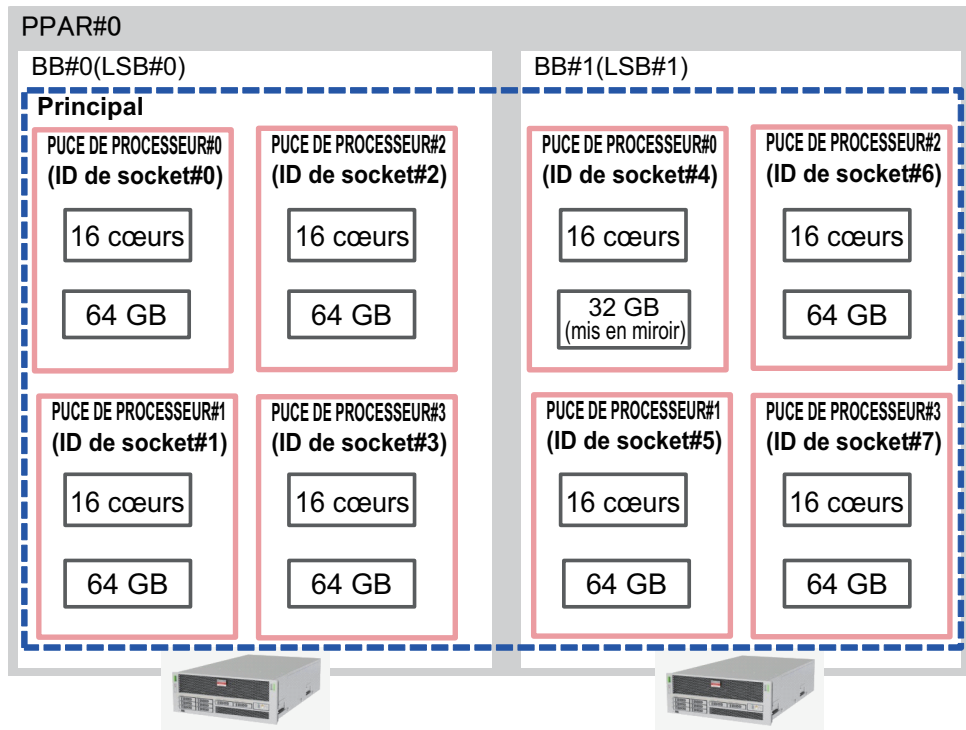
primary	32	16	1	/BB0
primary	32	16	2	/BB0
primary	32	16	3	/BB0
primary	32	16	4	/BB1
primary	32	16	5	/BB1
primary	32	16	6	/BB1
primary	32	16	7	/BB1

MEMORY				
PA		SIZE	SOCKET_ID	BOUND
0x700000000000		64G	7	primary
0x720000000000		64G	6	primary
0x740000000000		64G	5	primary
0x760050000000		31488M	4	primary
0x780000000000		64G	3	primary
0x7a0000000000		64G	2	primary
0x7c0000000000		64G	1	primary
0x7e0080000000		62G	0	primary

IO				
NAME	TYPE	BUS	SOCKET_ID	BOUND
PCIE0	BUS	PCIE0	0	primary
PCIE1	BUS	PCIE1	0	primary
PCIE2	BUS	PCIE2	1	primary
PCIE3	BUS	PCIE3	1	primary
PCIE4	BUS	PCIE4	2	primary
PCIE5	BUS	PCIE5	2	primary
PCIE6	BUS	PCIE6	3	primary
PCIE7	BUS	PCIE7	3	primary
PCIE8	BUS	PCIE8	4	primary
PCIE9	BUS	PCIE9	4	primary
PCIE10	BUS	PCIE10	5	primary
PCIE11	BUS	PCIE11	5	primary
PCIE12	BUS	PCIE12	6	primary
PCIE13	BUS	PCIE13	6	primary
PCIE14	BUS	PCIE14	7	primary
PCIE15	BUS	PCIE15	7	primary

Figure 8-3 montre un domaine de commande dans la partition physique qui possède toutes les ressources dans la partition physique configurée avec deux unités SPARC M10-4S (BB#0 et BB#1).

Figure 8-3 Cœurs de processeur et mémoire dans la partition physique



8.14.6 Retrait des ressources associées au socket de processeur depuis le domaine de commande

Utilisez la commande `ldm shrink-socket` pour supprimer les ressources dans le socket de processeur #4 depuis un domaine de commande.

L'exemple suivant montre le retrait de la mémoire et des processeurs virtuels dans le socket de processeur #4 depuis le domaine de commande.

```
# ldm shrink-socket cores=16 socket_id=4 primary
# ldm shrink-socket memory=31488M socket_id=4 primary
```

Remarque : la commande `ldm shrink-socket` peut échouer à supprimer la ressource cible car la ressource est occupée. Si tel est le cas, arrêtez le domaine logique et réessayez la commande `ldm shrink-socket`. Si le domaine est le domaine de commande, utilisez la reconfiguration retardée et réessayez.

Utilisez la commande `ldm list-socket` pour énumérer les ressources de chaque socket de processeur. Vous pouvez vérifier que la mémoire dans le socket de processeur #4 a été retirée du domaine de commande.


```
# ldm list-socket
CONSTRAINTS

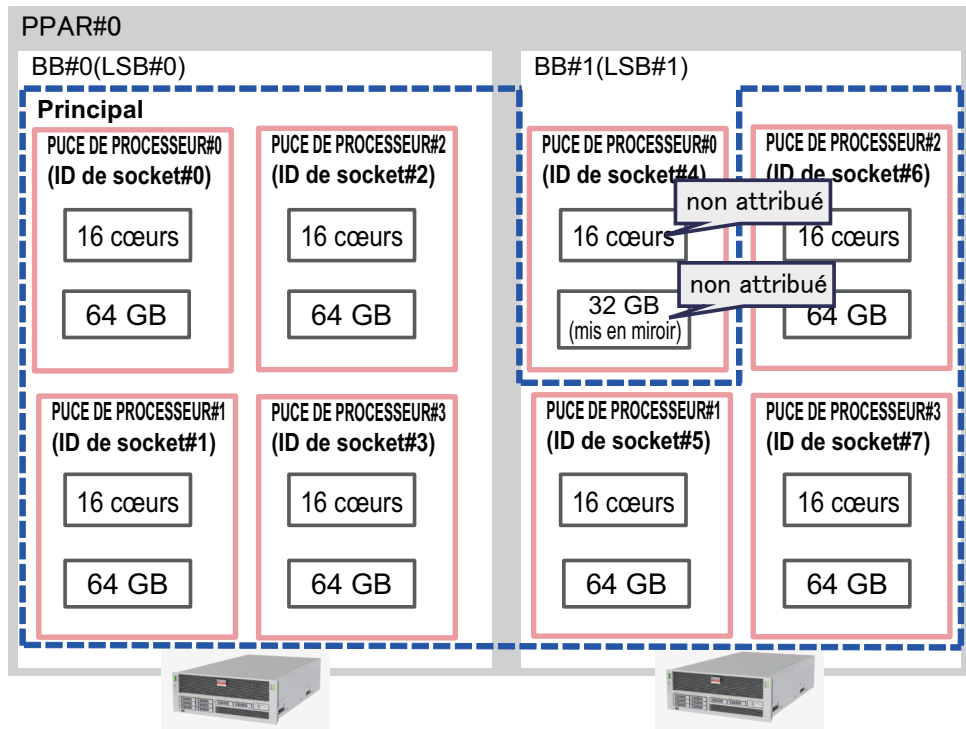
SOCKET
  TENANT      VCPUS  CORES  SOCKET_ID  GROUP
  primary     32     16     0           /BB0
  primary     32     16     1           /BB0
  primary     32     16     2           /BB0
  primary     32     16     3           /BB0
  primary     32     16     5           /BB1
  primary     32     16     6           /BB1
  primary     32     16     7           /BB1

  FREE        VCPUS  CORES  SOCKET_ID  GROUP
  -----
             32     16     4           /BB1

MEMORY
  PA          SIZE      SOCKET_ID  BOUND
  0x700000000000 64G      7         primary
  0x720000000000 64G      6         primary
  0x740000000000 64G      5         primary
  0x760050000000 31488M  4
  0x780000000000 64G      3         primary
  0x7a0000000000 64G      2         primary
  0x7c0000000000 64G      1         primary
  0x7e0080000000 62G      0         primary
--- Omis ---
```

Figure 8-4 montre la configuration de partition physique après l'exécution de la commande `ldm shrink-socket` dans la partition physique configurée avec deux unités SPARC M10-4S (BB#0 et BB#1).

Figure 8-4 Ressources après exécution de la commande ldm shrink-socket



8.14.7 Configuration des contraintes des socket de processeur par rapport à la configuration du domaine logique

L'exemple suivant décrit comment créer le domaine logique ldom1 doté de 16 Go de mémoire mise en miroir et de 8 cœurs de processeur associés au socket de processeur #4.

Utilisez la commande ldm add-domain pour créer le domaine logique ldom1.

```
primary# ldm add-domain ldom1
```

Utilisez la commande ldm set-socket pour contraindre ldom1 à utiliser les ressources associées au socket de processeur #4.

```
primary# ldm set-socket socket_id=4 ldom1
```

Attribuez 8 cœurs de processeur et 16 Go de mémoire à ldom1.

```
primary# ldm set-core 8 ldom1
primary# ldm set-memory 16G ldom1
```

Liez les ressources à ldom1 et démarrez ldom1.

```
primary# ldm bind-domain ldom1
primary# ldm start-domain ldom1
```

Remarque : pour lier et démarrer le domaine logique, vous devez préparer un concentrateur de la console virtuelle, un commutateur du réseau virtuel et un service de disque virtuel. Pour plus d'informations sur chaque élément, consultez le *Oracle VM Server for SPARC Administration Guide* de la version utilisée.

Utilisez la commande `ldm list-socket` pour afficher la liste des ressources de chaque socket de processeur.
Vous ne pouvez confirmer que les ressources associées au socket de processeur #4 et attribuées à ldom1.

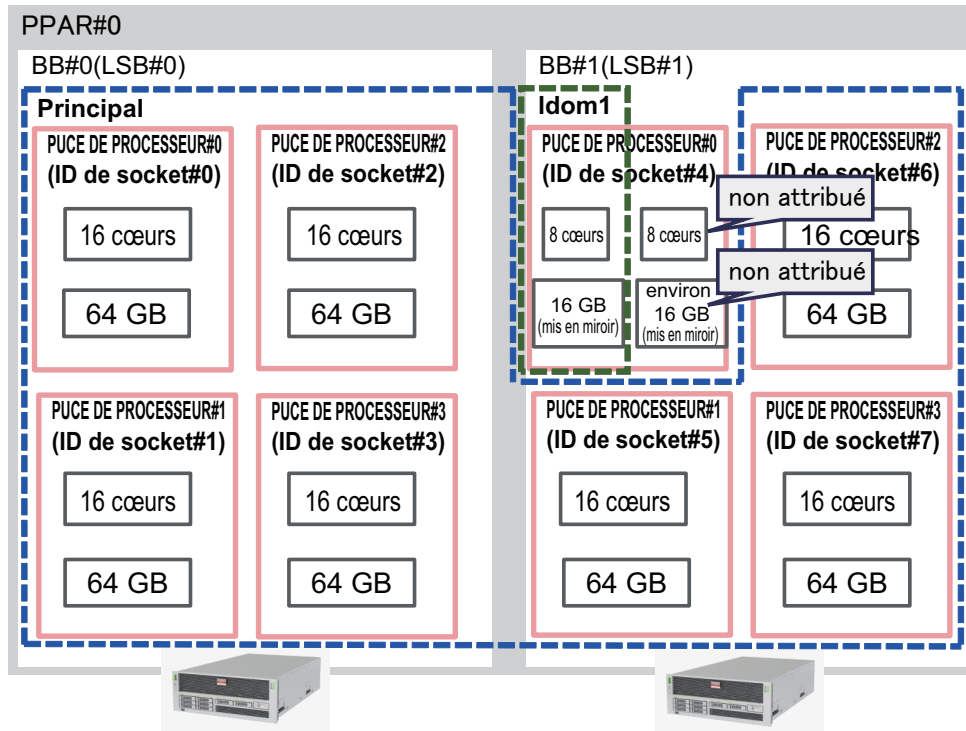
```
# ldm list-socket ldom1
CONSTRAINTS
  DOMAIN          SOCKET_ID    STATE
  ldom1           4             active

SOCKET
  TENANT          VCPUS  CORES  SOCKET_ID  GROUP
  ldom1           16     8     4             /BB1

MEMORY
  PA              SIZE          SOCKET_ID  BOUND
  0x760050000000  16G          4          ldom1

IO
```

Figure 8-5 montre la configuration de partition physique après l'exécution de la commande `ldm set-socket` dans la partition physique configurée avec deux unités SPARC M10-4S (BB#0 et BB#1).



8.15 Réglage de la stratégie de reconfiguration dynamique de la partition physique

Cette section décrit comment régler la stratégie de reconfiguration dynamique d'une partition physique.

8.15.1 Stratégie de reconfiguration dynamique de la partition physique

La stratégie de la reconfiguration dynamique de la partition physique (PPAR DR) est prise en charge dans la version 3.4 ou ultérieure d'Oracle VM Server pour SPARC. Avec la stratégie PPAR DR, vous pouvez modifier la stratégie de réduction des ressources qu'Oracle VM Server pour SPARC utilise lorsque l'opération PPAR DR est exécutée par la commande deleteboard.

La stratégie de réduction des ressources est définie sur la propriété ldmd/fj_ppar_dr_policy du service ldmd. La stratégie de réduction des ressources qui peut être

paramétrée est « auto », « ratio » ou « targeted ».

Pour plus de détails sur chaque stratégie de réduction des ressources, consultez
« [8.15.2 Détails sur la stratégie de réduction des ressources](#) ».

8.15.2 Détails sur la stratégie de réduction des ressources

Cette section décrit les détails de chaque stratégie de réduction des ressources.

fj_ppar_dr_policy = auto

Ce réglage de la stratégie PPAR DR est compatible pour l'utilisation automatique de la stratégie la plus récente. Lorsque « auto » est réglé pour le système avec Oracle VM Server pour SPARC 3.4, le système fonctionne comme lorsque « ratio » est réglé. Le réglage « auto » est la stratégie par défaut.

fj_ppar_dr_policy = ratio

Cette stratégie fonctionne sur les systèmes avec Oracle VM Server pour SPARC 3.4 ou une version ultérieure, lorsque tous les domaines logiques de la partition physique utilisent Oracle Solaris 11.3 ou une version ultérieure et quand XCP 2271 ou une version ultérieure est appliqué au système. Sinon, le système fonctionne comme avec le réglage « targeted ».

Exemple : vous configurez la stratégie de réduction des ressources sur « ratio » et effectuez l'opération deleteboard quand les ressources libres des blocs de construction restants ne suffisent pas pour déplacer les ressources du bloc de construction (carte système) à supprimer, et les ressources sont réduites par la libération automatique des ressources de tous les domaines existants.

Dans ce cas, les ressources sont automatiquement libérées selon la proportion des ressources attribuées aux domaines existants. Lorsque les ressources sont occupées ou pour d'autres raisons, la réduction proportionnelle exacte ne fonctionne pas toujours. La réduction proportionnelle se fait au mieux selon les possibilités.

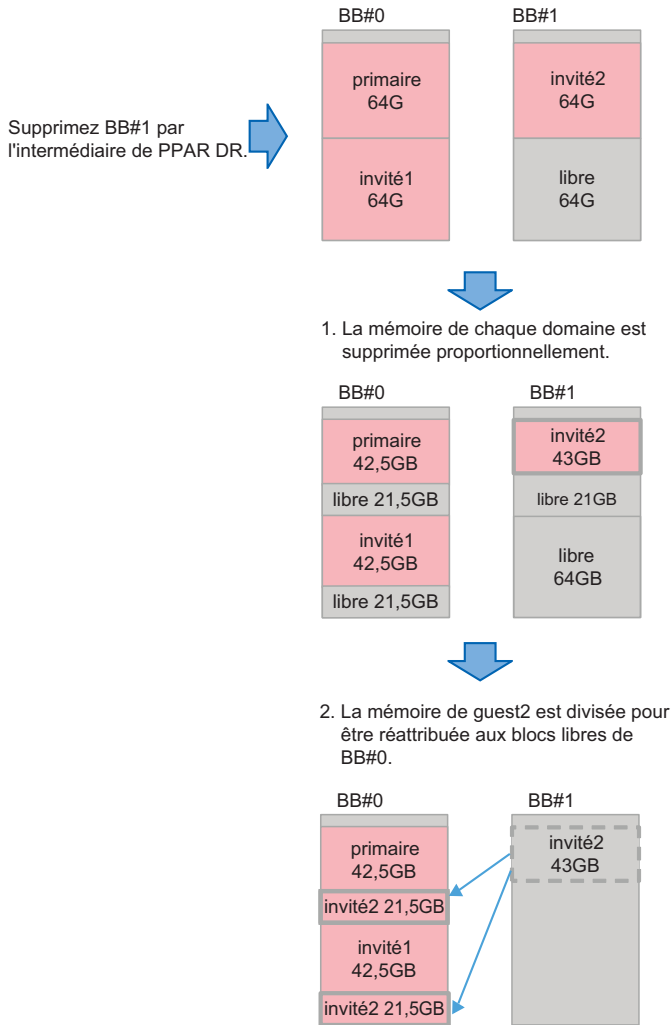
Cette stratégie est également compatible avec une fonction de division de bloc de mémoire qui divise automatiquement un grand bloc de mémoire en plus petits blocs. La division de bloc de mémoire élimine le besoin d'avoir des zones de mémoire contiguës libres suffisantes dans les blocs de construction de destination pour chaque bloc de mémoire relocalisé depuis le bloc de construction retiré par PPAR DR.

L'opération deleteboard divise les blocs de mémoire du domaine pour les adapter aux zones libres disponibles dans les blocs de construction restants.

Si vous ne pouvez pas garantir assez de ressources libres dans le bloc de construction de destination de déplacement parce que les ressources sont en cours d'utilisation ou pour d'autres raisons, la commande deleteboard échoue et un message d'erreur s'affiche. Dans ce cas, identifiez la cause de l'erreur grâce au message d'erreur émis par la commande deleteboard et le message Oracle Solaris, et prenez les mesures adéquates. Pour plus de détails sur les messages d'erreur émis par la commande deleteboard, consultez « [C.1.2 deleteboard](#) » dans le *Guide de configuration du domaine Fujitsu SPARC M12 et Fujitsu M10/SPARCM10*. Cela dit, il se peut que vous deviez couper ou redémarrer la partition physique en fonction des informations relatives à l'erreur qui s'est produite.

Le concept de suppression de mémoire lorsque « ratio » est décrit dans [Figure 8-6](#).

Figure 8-6 Mécanisme de la suppression de mémoire (lors de l'utilisation de `fj_ppar_dr_policy = ratio`)



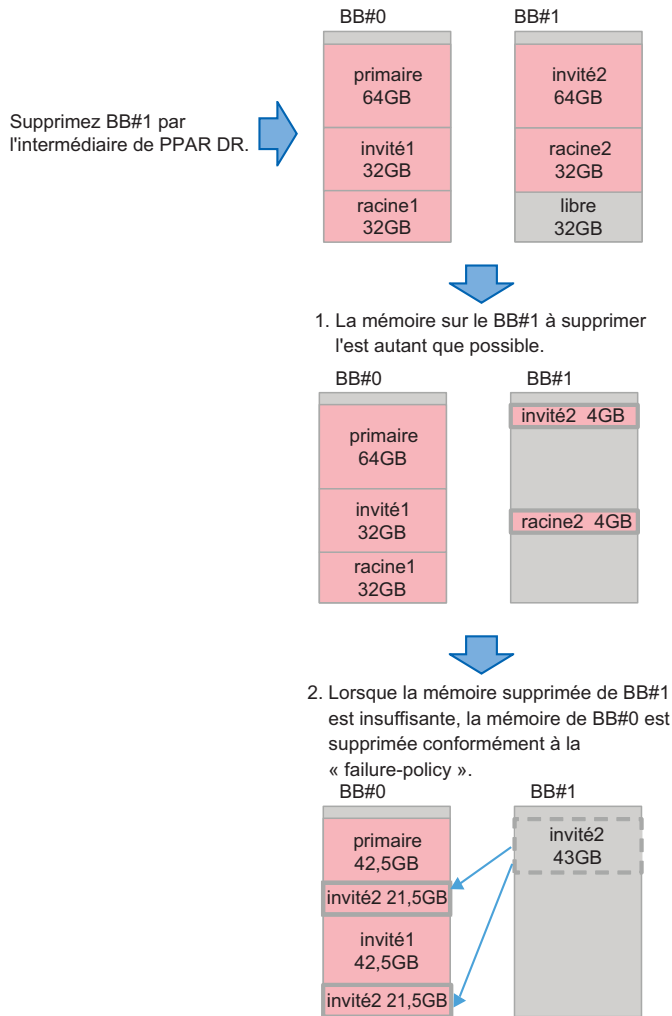
`fj_ppar_dr_policy = targeted`

La stratégie « Targeted » sera utilisée pour toutes les versions antérieures à Oracle VM Server pour SPARC 3.4. Si les ressources libres ne sont pas disponibles avec cette stratégie, les ressources sont libérées de chaque domaine logique ayant le processeur/la mémoire sur le bloc de construction devant être supprimé en premier.

Si les ressources libres ne sont pas suffisantes même après cette opération de suppression, les ressources sont libérées de chaque domaine logique ayant le processeur/la mémoire sur un bloc de construction restant. L'ordre des domaines logiques depuis lesquels les ressources sont libérées est défini par « failure-policy ». Avec cette stratégie, l'ordre est : domaine logique par défaut (pas de spécification), domaine logique spécifié comme maître, domaine I/O, domaine racine et domaine de commande. Pour les domaines ayant le même rôle, le classement se fait par ordre alphabétique.

Pour plus d'informations sur les domaines « failure-policy » et « master », consultez « Configuring Domain Dependencies » (configuration des dépendances de domaine) dans *Oracle VM Server for SPARC Administration Guide*. Si vous ne pouvez pas garantir de ressources libres dans la carte système de destination de déplacement, la commande deleteboard échoue et un message d'erreur s'affiche. Dans ce cas, identifiez la cause de l'erreur grâce au message d'erreur émis par la commande deleteboard et le message Oracle Solaris, et prenez les mesures adéquates. Cependant, il se peut que vous deviez couper ou redémarrer la partition physique en fonction des informations relatives à l'erreur qui s'est produite.

Figure 8-7 Mécanisme de la suppression de mémoire (lors de l'utilisation de `fj_ppar_dr_policy = targeted`)



8.15.3 Comment modifier la stratégie PPAR DR

Dans les versions 3.4 ou plus récentes d'Oracle VM Server pour SPARC la stratégie est modifiée en paramétrant la stratégie PPAR DR sur la propriété `fj_ppar_dr_policy` du service en utilisant la commande `svccfg`.

Pour plus de détails sur les stratégies PPAR DR pouvant être paramétrées, consultez « [8.15.2 Détails sur la stratégie de réduction des ressources](#) ».

La procédure de réglage est décrite ci-dessous.

1. **Connectez-vous au domaine de commande.**
2. **Devenez l'administrateur.**
Pour plus d'informations, consultez *Securing Users and Processes in Oracle Solaris 11.3*.
3. **Affichez la valeur de la propriété `fj_ppar_dr_policy`.**

```
# svccfg -s ldmd listprop ldmd/fj_ppar_dr_policy
```

4. **Arrêtez le service `ldmd`.**

```
# svcadm disable ldmd
```

5. **Changez la valeur de la propriété `fj_ppar_dr_policy`.**

```
# svccfg -s ldmd setprop ldmd/fj_ppar_dr_policy=value
```

6. **Rafraîchissez et redémarrez le service `ldmd`.**

```
# svcadm refresh ldmd
# svcadm enable ldmd
```

L'exemple suivant indique comment afficher la valeur de la propriété `fj_ppar_dr_policy` et comment la faire passer de « `auto` » à « `targeted` ».

```
# svccfg -s ldmd listprop ldmd/fj_ppar_dr_policy
ldmd/fj_ppar_dr_policy astring auto
# svcadm disable ldmd
# svccfg -s ldmd setprop ldmd/fj_ppar_dr_policy=targeted
# svcadm refresh ldmd
# svcadm enable ldmd
# svccfg -s ldmd listprop ldmd/fj_ppar_dr_policy
ldmd/fj_ppar_dr_policy astring targeted
```

8.16 Configuration de la taille de page maximale d'un domaine logique

Cette section décrit comment régler la taille de page maximale d'un domaine logique et l'effet que cela peut avoir.

Ce réglage s'applique à Oracle VM Server pour SPARC 3.5 ou version ultérieure.

8.16.1 Taille de page maximale d'un domaine logique

Trois paramètres de taille de page maximale (256 Mo, 2 Go et 16 Go) sont pris en charge par le SPARC M12. Pour plus de détails sur la façon de vérifier la taille de page maximale, consultez « [8.16.5 Vérification de la taille de page maximale d'un domaine logique](#) ».

Le SPARC M10 ne prend en charge que 256 Mo pour la taille de page maximale, et ce paramètre ne peut être modifié.

8.16.2 Avantages d'une taille de page maximale plus grande

Lorsqu'une grande valeur est définie pour la taille de page maximale, de grandes pages peuvent être utilisées par le domaine logique. En général, les applications utilisant une grande quantité de mémoire vont s'exécuter plus rapidement si la taille de page maximale est fixée à 2 Go ou 16 Go, contrairement à 256 Mo.

8.16.3 Inconvénients d'une taille de page maximale plus grande

Une valeur supérieure à la valeur standard pour la taille de page maximale peut affecter négativement le taux de réussite de la migration à chaud du domaine logique, de la migration à chaud d'une zone noyau d'Oracle Solaris sur un domaine logique, et de l'opération PPAR-DR exécutée par la commande `deleteboard`.

Nous vous recommandons de définir la taille de page maximale à 256 Mo pour garantir le taux de réussite le plus élevé pour la migration à chaud de domaines logiques et de zones noyau d'Oracle Solaris, ainsi que dans l'opération PPAR-DR exécutée par la commande `deleteboard`. Pour plus de détails, consultez les descriptions ci-dessous.

Taux de réussite de la migration à chaud et de l'opération PPAR-DR exécutée par la commande `deleteboard`

Le taux de réussite d'une migration à chaud et de l'opération PPAR-DR exécutée par la commande `deleteboard` dépend de l'utilisation de la mémoire à destination.

L'alignement en mémoire pour les domaines logiques est limité à des multiples de la taille de page maximale. Si les limites de la zone de mémoire contigüe libre à destination ne sont pas des multiples de la taille de page maximale, le transfert de mémoire échoue.

Exemples d'utilisation de la mémoire à destination et l'effet de grandes tailles de page maximales

Figure 8-8 présente un exemple de transfert de mémoire lorsque la taille de page maximale du domaine logique est définie à 2 Go. Bien qu'il y ait une zone de mémoire contigüe libre de 2 Go à destination, le transfert de mémoire échoue car les limites de la zone de mémoire contigüe libre ne sont pas des multiples de la taille de page maximale.

Figure 8-8 Quand la taille de page maximale d'un domaine logique est définie à 2 Go

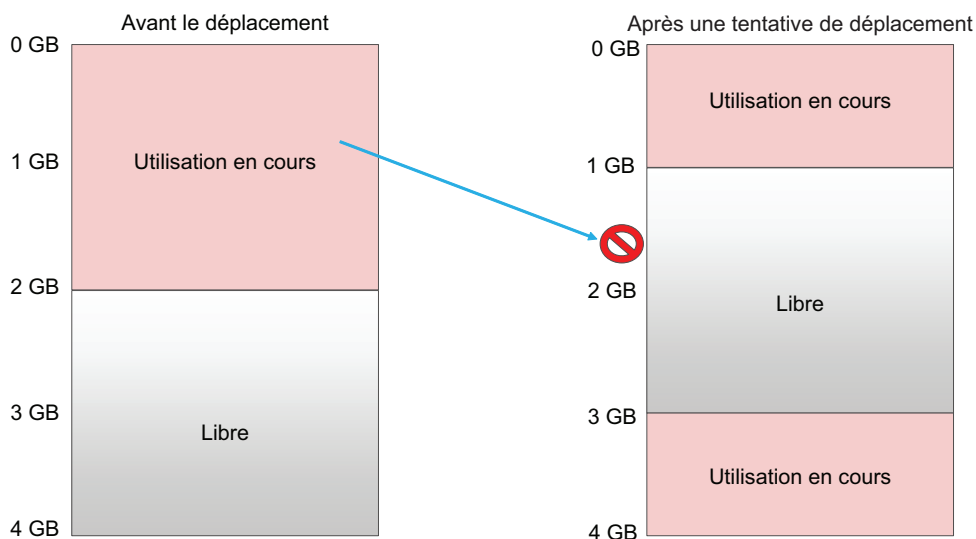
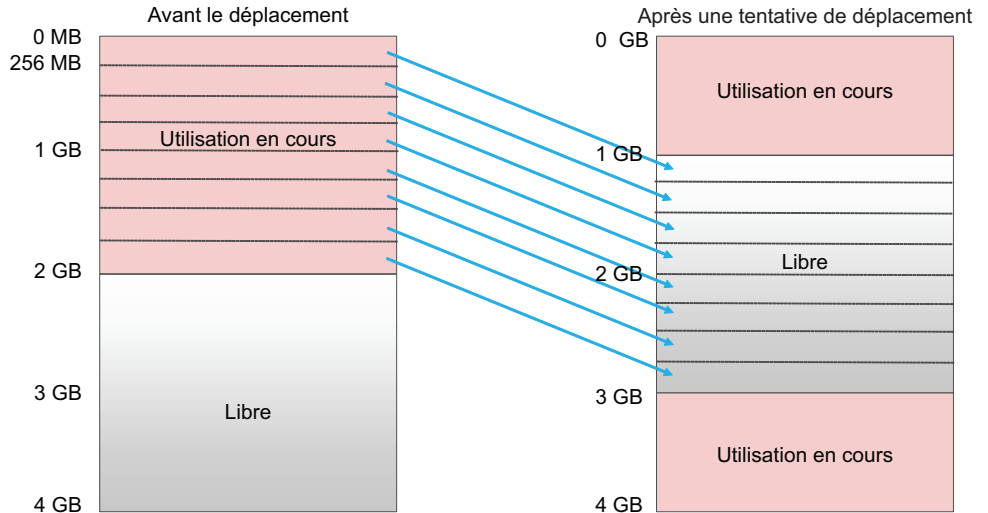


Figure 8-9 présente un exemple de transfert de mémoire lorsque la taille de page maximale du domaine logique est définie à 256 MB. Le transfert de mémoire réussit car les limites de la zone de mémoire contigüe libre à destination peuvent être définies sur des multiples de 256 Mo.

Figure 8-9 Quand la taille de page maximale d'un domaine logique est définie à 256 Mo



8.16.4 Définition et modification de la taille de page maximale d'un domaine logique

Les méthodes ci-dessous sont disponibles pour définir la taille de page maximale d'un domaine logique.

- [Définition de la propriété `fj\_dr\_sw\_limit\_pagesize` du service `ldmd`](#)
- [Définition et modification de `fj-software-limit-pagesize` avec les commandes `ldm add-domain/ldm set-domain`](#)

Définition de la propriété `fj_dr_sw_limit_pagesize` du service `ldmd`

Vous pouvez définir la valeur de la propriété `fj_dr_sw_limit_pagesize` sur « `true` » ou « `false` ».

- **`fj_dr_sw_limit_pagesize=false` [default]**
La taille de page maximale d'un domaine logique est définie automatiquement selon la taille de la mémoire allouée au domaine logique et la taille de page maximale prise en charge par le système.
Vous pouvez définir la taille de page maximale (`fj-software-limit-pagesize`) à l'aide des commandes `ldm add-domain` ou `ldm set-domain`.
- **`fj_dr_sw_limit_pagesize=true`**
La taille de page maximale est définie à 256 Mo pour les domaines logiques nouvellement créés.
Même lorsque cette propriété est définie sur « `true` », elle ne modifie pas la taille de page maximale actuelle du domaine de commande et des domaines logiques existants.

La procédure pour définir la propriété `fj_dr_sw_limit_pagesize` pour le service `ldmd` est décrite ci-dessous.

1. **Connectez-vous au domaine de commande.**
2. **Passer aux privilèges administrateur.**
Pour plus d'informations, consultez *Securing Users and Processes in Oracle Solaris 11.3*.
3. **Affichez la valeur de la propriété `fj_dr_sw_limit_pagesize`.**

```
primary# svccfg -s ldmd listprop ldmd/fj_dr_sw_limit_pagesize
```

4. **Arrêtez le service `ldmd`.**

```
primary# svcadm disable ldmd
```

5. **Modifiez la valeur de la propriété `fj_dr_sw_limit_pagesize`.**

```
primary# svccfg -s ldmd setprop ldmd/fj_dr_sw_limit_pagesize=value
```

6. **Rafraîchissez et redémarrez le service `ldmd`.**

```
primary# svcadm refresh ldmd
primary# svcadm enable ldmd
```

Dans l'exemple suivant, la valeur de la propriété `fj_dr_sw_limit_pagesize` est vérifiée puis passe de « `false` » à « `true` ».

```
primary# svccfg -s ldmd listprop ldmd/fj_dr_sw_limit_pagesize
ldmd/fj_dr_sw_limit_pagesize boolean false
primary# svcadm disable ldmd
primary# svccfg -s ldmd setprop ldmd/fj_dr_sw_limit_pagesize=true
primary# svcadm refresh ldmd
primary# svcadm enable ldmd
```

Dans l'exemple suivant, la valeur de la propriété `fj_dr_sw_limit_pagesize` est confirmée comme « `true` ».

```
primary# svccfg -s ldmd listprop ldmd/fj_dr_sw_limit_pagesize
ldmd/fj_dr_sw_limit_pagesize boolean true
```

Définition et modification de `fj-software-limit-pagesize` avec les commandes `ldm add-domain`/`ldm set-domain`

- **Pour définir `fj-software-limit-pagesize` avec la commande `ldm add-domain`**
La taille de page maximale d'un domaine logique peut être définie à l'aide de la

commande `ldm add-domain`.

Si la propriété `fj_dr_sw_limit_pagesize` est réglée sur « `true` », la taille de page maximale est définie à 256 Mo, et ne peut être modifiée.

Pour plus de détails sur les commandes `ldm`, consultez le *Oracle VM Server for SPARC 3.5 Reference Manual*.

L'exemple suivant définit la taille de page maximale à 256 Mo pour le domaine A, un domaine logique nouvellement créé.

```
primary# ldm add-domain fj-software-limit-pagesize=256MB domainA
```

- **Pour définir et modifier `fj-software-limit-pagesize` avec la commande `ldm set-domain`**

La taille de page maximale d'un domaine logique peut être définie et modifiée à l'aide de la commande `ldm set-domain`. La taille de page maximale peut être définie et modifiée uniquement lorsque le domaine logique est en reconfiguration retardée ou dans un état inactif.

Cependant, si la propriété `fj_dr_sw_limit_pagesize` est réglée sur « `true` », la taille de page maximale est définie à 256 Mo, et ne peut être modifiée.

Pour plus de détails sur les commandes `ldm`, consultez le *Oracle VM Server for SPARC 3.5 Reference Manual*.

L'exemple suivant définit la taille de page maximale du domaine de commande à 256 Mo.

```
primary# ldm start-reconf primary
primary# ldm set-domain fj-software-limit-pagesize=256MB primary
primary# shutdown -y -i6 -g0
```

L'exemple suivant définit la taille de page maximale à 2 Go pour le domaine B, un domaine logique.

```
primary# ldm stop-domain domainB
primary# ldm unbind-domain domainB
primary# ldm set-domain fj-software-limit-pagesize=2GB domainB
primary# ldm bind-domain domainB
primary# ldm start-domain domainB
```

8.16.5 Vérification de la taille de page maximale d'un domaine logique

La taille de page maximale (`fj-software-limit-pagesize`) de chaque domaine logique peut être vérifiée avec la commande `ldm list-domain`.

L'exemple suivant nous montre que la taille de page maximale du domaine C est de 2 Go.

```

primary# ldm list-domain -l domainC
NAME                STATE      FLAGS    CONS    VCPU    MEMORY    UTIL    NORM    UPTIME
domainC             active     -n----   5003     8       6G        0.1%    0.0%    58m
SOFTSTATE
Solaris running
UUID
    xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
MAC
    xx:xx:xx:xx:xx:xx
HOSTID
    0xxxxxxxxx
CONTROL
    failure-policy=ignore
    extended-mapin-space=on
    cpu-arch=native
    rc-add-policy=
    shutdown-group=15
    perf-counters=
    boot-policy=warning
    effective-max-pagesize=256MB
    hardware-max-pagesize=16GB
    fj-software-limit-pagesize=2GB

```

Gestion quotidienne des systèmes

Ce chapitre décrit les tâches quotidiennes nécessaires à la gestion du système SPARC M12/M10.

Copie de sauvegarde des informations des réglages de XSCF

Sauvegardez régulièrement les informations des réglages de XSCF enregistrées sur le XSCF maître. Après un remplacement d'une unité de champ remplaçable (FRU) causé par une panne du FRU contenant le XSCF maître, la restauration des informations des réglages de XSCF sauvegardées permet à l'opération système de fonctionner normalement, comme avant la panne.

Pour plus de détails, consultez « [10.10 Sauvegarde/restauration des informations des réglages de XSCF](#) ».

Copie de sauvegarde des informations de configuration du domaine logique

Sauvegardez régulièrement les informations de configuration du domaine logique configurées par Oracle VM Server pour SPARC. Effectuez une sauvegarde par domaine logique depuis le domaine de commande. Les informations de configuration du domaine logique peuvent être enregistrées grâce aux deux méthodes suivantes :

- Sauvegarde dans XCSF
- Sauvegarde en tant que fichier XML

Après avoir changé la configuration du domaine, assurez-vous que les informations de configurations les plus récentes ont bien été sauvegardées. Il est recommandé de sauvegarder des copies des fichiers de sauvegarde sur d'autres supports en cas de panne du disque.

Pour plus de détails, consultez « [10.11 Sauvegarde / restauration des informations de configuration du domaine logique dans le XSCF](#) » et « [10.12 Sauvegarde / restauration des informations de configuration du domaine logique dans un fichier XML](#) ».

Copie de sauvegarde des variables d'environnement d'OpenBoot PROM

Enregistrez et sauvegardez de manière périodique les variables d'environnement d'OpenBoot PROM définies dans le domaine de commande.

Si vous souhaitez modifier les domaines logiques à la configuration par défaut pour restaurer les informations de configuration du domaine logique depuis un fichier XML, les variables d'environnement d'OpenBoot PROM dans le domaine de commande sont initialisées et le démarrage d'Oracle Solaris ne peut pas être réalisé.

Pour empêcher ceci, enregistrez et sauvegardez les variables d'environnement d'OpenBoot PROM dans le domaine de commande avant de passer à la configuration par défaut. Après avoir changé la configuration des domaines logiques à la configuration par défaut, restaurez les variables d'environnement d'OpenBoot PROM dans le domaine de commande en utilisant les informations enregistrées.

Pour plus de détails, consultez « [10.13 Enregistrement/Restauration des variables d'environnement d'OpenBoot PROM](#) ».

Copie de sauvegarde des lecteurs de disque internes

Sauvegardez régulièrement les données des lecteurs de disque internes. La méthode de sauvegarde varie selon la configuration des lecteurs installés. Effectuez les sauvegardes conformément à la configuration du lecteur.

Mise à jour du microprogramme le plus récent

Le microprogramme XSCF pour la gestion du système SPARC M12/M10 est fourni dans le package XCP avec OpenBoot PROM, le superviseur et POST. Les dernières mises à jour du package XCP sont régulièrement publiées, elles contiennent de nouvelles fonctions et/ou des correctifs de bogues. Mettez toujours le package XCP à jour avec la version la plus récente immédiatement après sa publication.

Pour plus de détails sur la mise à jour vers le microprogramme le plus récent, consultez « [Chapitre 16 Mise à jour du microprogramme XCP](#) ».

Les nouvelles fonctions et modifications du package XCP sont mentionnées dans les *Notes de produit* de la version XCP correspondant à votre serveur. Il est recommandé de lire ces notes.

Surveillance de l'état du système

XSCF contrôle régulièrement le fonctionnement du système.

Vous pouvez avoir une idée de l'état du serveur en accédant au XSCF depuis le shell XSCF ou XSCF Web.

Utilisez la fonction d'agent SNMP du XSCF, la fonction de notification des informations de panne et divers messages et journaux pour surveiller les défaillances et les événements du système.

Pour plus de détails, consultez « [10.2 Réception de notifications par e-mail lorsqu'une panne se produit](#) », « [10.3 Surveillance/gestion de l'état du système avec l'agent SNMP](#) » et « [Chapitre 12 Consultation des journaux et des messages](#) ».

Se préparer et prendre des mesures en cas de pannes

Ce chapitre décrit les fonctions qui sont configurées à l'avance pour parer aux occurrences potentielles de panne dans les systèmes SPARC M12/M10. Ces systèmes disposent de diverses fonctions pour la préparation aux pannes potentielles. Afin d'identifier et d'agir au plus tôt, les utilisateurs doivent effectuer quelques préparations, telles que configurer les paramètres de surveillance du système, rendre le matériel redondant et enregistrer des données.

Ce chapitre décrit ces méthodes de gestion.

- Familiarisation avec les procédures de dépannage et les fonctions connexes
- Réception de notifications par e-mail lorsqu'une panne se produit
- Surveillance/Gestion de l'état du système avec l'agent SNMP
- Surveillance du système
- Comprendre le mécanisme de détérioration suite à une panne
- Vérification des ressources matérielles en panne
- Configuration d'une substitution automatique de cœurs du processeur en panne
- Configuration du mode de récupération
- Configuration de composants redondants
- Sauvegarde/restauration des informations des réglages de XSCF
- Sauvegarde / restauration des informations de configuration du domaine logique dans le XSCF
- Sauvegarde / restauration des informations de configuration du domaine logique dans un fichier XML
- Enregistrement/Restauration des variables d'environnement d'OpenBoot PROM
- Sauvegarde / Restauration du contenu d'un disque dur
- Réinitialisation d'un domaine logique
- Génération d'une panique dans un domaine logique
- Reconfiguration d'une partition physique
- Restauration de l'état du serveur aux valeurs par défaut en vigueur à l'expédition
- Récupération d'un fichier de vidage d'incident à l'aide du vidage différé

10.1 Familiarisation avec les procédures de dépannage et les fonctions connexes

Tableau 10-1 répertorie les actions et les fonctions utilisées pour se préparer aux occurrences potentielles de panne. Pour plus de détails sur des éléments individuels, consultez les sections suivantes.

Tableau 10-1 Dépannage et fonctions

Action	Fonction	Commande liée
Envoyer une information sur la panne aux utilisateurs dans les plus brefs délais	- Notification par e-mail	setsmtp(8), showsmtp(8), setemailreport(8), showemailreport(8)
	- Service de maintenance à distance	Consultez les dernières <i>Notes de produit</i> pour votre serveur.
Surveiller / gérer les pannes et les événements	- Surveillance du système à l'aide de la fonction de l'agent SNMP	setsnmp(8), showsnmp(8), setsnmpusm(8), showsnmpusm(8), setsnmpvacm(8), showsnmpvacm(8)
Identifier les pannes plus tôt pour déterminer les opérations du serveur	- Surveillance du système, pulsation, vérification d'activité	setpparmode(8), showpparmode(8), setpparparam(8), showpparparam(8)
	- Contrôle du fonctionnement du serveur	
Parer aux pannes pour qu'elles n'affectent pas d'autres parties ou utiliser une configuration redondante	- Détérioration suite à une panne	showstatus(8), showhardconf(8)
	- Configuration des composants	
Protéger les données de réglage actuelles pour qu'elles reviennent à leur état initial	- Sauvegarde / restauration des informations des réglages de XSCF	dumpconfig(8), restoreconfig(8), Commandes d'Oracle VM Server pour SPARC
	- Sauvegarde / restauration des informations du domaine logique	
	- Sauvegarde / restauration des disques durs	

Remarque : si le XSCF échoue, aucune notification n'est émise par la fonction de notification par e-mail du XSCF, les trap SNMP, ou le service de maintenance à distance (fonction ASR, REMCS, etc.). Pour surveiller les défaillances du XSCF, utilisez un logiciel de surveillance de serveur. Pour plus de détails, consultez les manuels des logiciels liés à la gestion du serveur utilisé.

10.2 Réception de notifications par e-mail lorsqu'une panne se produit

En prévision d'une panne ou d'un événement dans ce système, le XSCF peut être paramétré pour informer un utilisateur de l'état d'une panne par e-mail.

Il est fortement recommandé de configurer la notification par e-mail. Une fois la notification par e-mail de XSCF définie, un utilisateur spécifique (tel qu'un administrateur système ayant le privilège d'utilisateur platadm) peut recevoir immédiatement une notification sur les pannes du serveur ou de la partition physique.

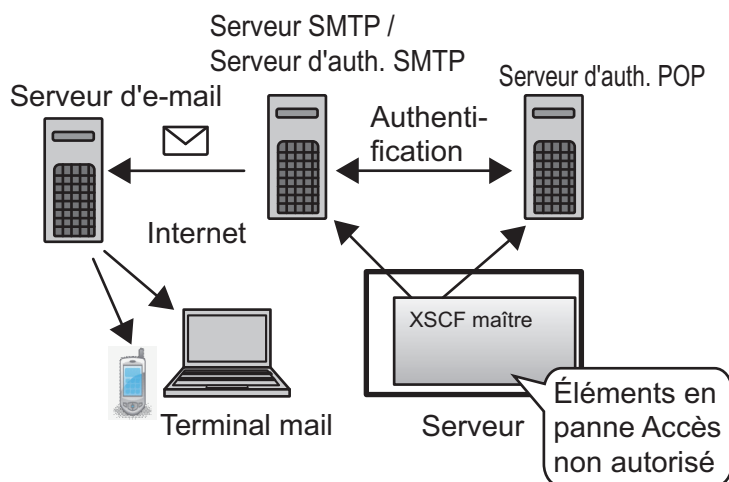
10.2.1 Caractéristiques de la fonction de notification par e-mail

La fonction de notification par e-mail a les caractéristiques suivantes :

- Notification par e-mail des pièces défaillantes dans le système contrôlé par le XSCF
L'e-mail peut être systématiquement envoyé, même si le système tombe en panne ou même en cas d'une erreur grave qui désactive le redémarrage.
- Autorisation des fonctions d'authentification POP et SMTP lors de la transmission de l'e-mail
Pour éviter une transmission illégale d'e-mail, l'authentification POP (POP avant SMTP) ou l'authentification SMTP (SMTP-AUTH) peut être effectuée avant que la transmission de l'e-mail soit acceptée par le serveur SMTP.

Figure 10-1 décrit un cas où le XSCF envoie un e-mail via chacun des serveurs.

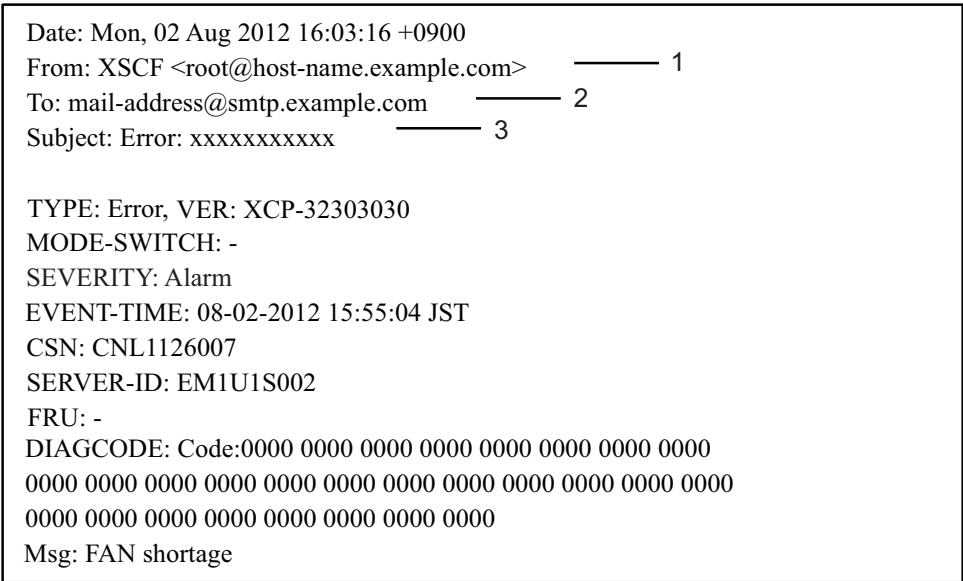
Figure 10-1 Présentation de la fonction d'e-mail de XSCF



10.2.2 Détails des notifications de panne

Figure 10-2 illustre un exemple de notification par e-mail.

Figure 10-2 Exemple d'un e-mail en cas de panne d'une pièce



- 1 « Reply e-mail address » qui est défini dans les paramètres d'e-mail

2 « Destination e-mail address » qui est défini dans les paramètres d'e-mail

3 En-tête de l'e-mail

Les éléments suivants apparaissent dans l'exemple d'e-mail.

Tableau 10-2 Contenu d'une notification par e-mail au moment de la panne

Élément	Description
TYPE	Type de notification
VER	Version
MODE	État du commutateur de mode
SEVERITY	Niveau d'erreur
EVENT-TIME	Heure à l'occurrence de l'événement (affichage en heure locale)
CSN	Numéro de série du châssis
SERVER-ID	ID du système
FRU	Pièce probablement en panne

Tableau 10-2 Contenu d'une notification par e-mail au moment de la panne (*suite*)

Élément	Description
DIAGCODE	Utilisé pour la résolution de panne par les techniciens sur site et les techniciens de maintenance. Les utilisateurs indiquent ce code à un technicien sur site ou à notre technicien de maintenance. Le code permet de trouver rapidement une solution au problème.
Msg	Message décrivant le problème

10.2.3 Vérification des éléments de réglage et des commandes liés aux notifications par e-mail

[Tableau 10-3](#) répertorie les éléments de réglage liés à la notification par e-mail de XSCF et les commandes du Shell XSCF associées.

Tableau 10-3 Éléments de réglage liés à la notification par e-mail

Élément de réglage	Paramétrage requis ou optionnel	Commande liée
Serveur SMTP - Nom d'hôte - Numéro de port - Adresse e-mail de destination des réponses	Optionnel	setsmtp(8), showsmtp(8)
Activation / désactivation de la fonction de notification par e-mail	Optionnel	setemailreport(8), showemailreport(8)
Adresse e-mail de destination	Optionnel	setemailreport(8), showemailreport(8)
Serveur d'authentification - Authentification POP/SMTP - Nom d'hôte - ID / mot de passe de l'utilisateur	Optionnel	setsmtp(8), showsmtp(8)

Seul un serveur SMTP est spécifié. Pour spécifier un serveur SMTP par son nom d'hôte, les serveurs DNS doivent être en mesure de résoudre le nom du serveur.

Le numéro de port par défaut du serveur SMTP est 25.

L'adresse e-mail de destination des réponses correspond à l'adresse utilisée pour transmettre un e-mail de l'erreur lorsqu'un problème survient sur le chemin de l'adresse e-mail de destination. L'e-mail est transmis par un serveur e-mail sur ce chemin.

10.2.4 Procédures de réglage pour configurer une notification par e-mail

Cette section décrit les opérations à effectuer pour configurer une notification par e-mail avec le XSCF.

1. **Connectez-vous au XSCF.**
2. **Spécifiez le nom d'hôte ou l'adresse IP du serveur SMTP (voir `setsmtp(8)`).**
3. **Sélectionnez l'authentification POP ou SMTP (voir `setsmtp(8)`).**
4. **Spécifiez l'e-mail de destination des réponses (de spécification) (voir `setsmtp(8)`).**
5. **Spécifiez l'adresse e-mail de destination pour la réponse de l'administrateur système (voir `setemailreport(8)`).**
6. **Activez la notification par e-mail de XSCF (voir `setemailreport(8)`).**
7. **Envoyez un e-mail test.**

Une fois les paramètres d'e-mail terminés, l'e-mail de test est automatiquement envoyé. Lorsque l'e-mail test envoyé arrive dans la messagerie de l'administrateur système, les réglages sont terminés. Si l'e-mail n'arrive pas, un e-mail d'erreur est envoyé à l'adresse e-mail de réponse (de spécification), ou cet événement est enregistré dans un journal d'erreur. Dans ce cas, après avoir identifié la cause et résolu le problème, répétez la procédure depuis l'étape 1. La fonction de notification par e-mail est activée lorsque le test se termine normalement.

10.2.5 Réglage du nom d'hôte, du numéro de port, de l'adresse e-mail des réponses et de la méthode d'authentification du serveur SMTP

1. **Exécutez la commande `showsmtp` pour afficher les informations de configuration du serveur SMTP.**

```
XSCF> showsmtp
Mail Server:
Port : 25
Authentication Mechanism: none
Reply address:
```

2. **Exécutez la commande `setsmtp` pour définir les informations du serveur SMTP.**
Dans l'exemple suivant, le nom d'hôte, le numéro de port, l'adresse e-mail de destination des réponses et l'authentification SMTP sont spécifiés.

```
XSCF> setsmtp -s mailserver=192.1.4.5 -s port=25 -s
replyaddress=yyyy@example.com -s auth=smtp-auth -s user=usr001 -s
password=xxxxxxxx
```

Dans l'exemple suivant, en mode interactif, le nom d'hôte, le numéro de port, l'adresse e-mail des réponses et l'authentification POP sont spécifiés.

```
XSCF> setsmtp
Mail Server [192.1.4.2]: 192.1.4.5
Port[25]:
Authentication Mechanism [none]:pop
POP Server [192.1.4.2]:
User Name []: usr001
Password []: xxxxxxxx
Reply Address [yyyy@example.com]:
```

3. **Exécutez la commande `showsmtp` pour vérifier les informations de réglage du serveur SMTP.**

```
XSCF> showsmtp
Mail Server: 192.1.4.5
Port: 25
Authentication Mechanism : pop
User Name: usr001
Password: *****
Reply Address: yyyy@example.com
```

10.2.6 Réglage de l'adresse e-mail de destination pour la notification et activation/désactivation de la fonction de notification par e-mail

Configurez le serveur SMTP à l'avance, tel que décrit dans « [10.2.5 Réglage du nom d'hôte, du numéro de port, de l'adresse e-mail des réponses et de la méthode d'authentification du serveur SMTP](#) ».

Une fois la fonction d'e-mail de XSCF configurée, vous pouvez envoyer un e-mail test pour confirmer le réglage. Le temps d'émission (indiqué en temps local) de l'e-mail test et des informations sur la source de l'e-mail sont affichés. En outre, le titre de l'e-mail test contient les caractères « Test Mail: ».

1. **Exécutez la commande `showemailreport` pour afficher les paramètres de la notification par e-mail.**

```
XSCF> showemailreport
E-Mail Reporting: disabled
```

2. **Exécutez la commande `setemailreport` pour définir les informations de notification par e-mail.**

L'exemple suivant spécifie, en mode interactif, l'activation de la notification par e-mail ainsi que l'adresse e-mail de destination.

```
XSCF> setemailreport  
Enable E-Mail Reporting? [no]: yes  
E-mail Recipient Address []: xxxxx@example.com  
Do you want to send a test mail now [no]?: yes  
... Sending test mail to 'xxxxx@example.com'
```

3. **Exécutez la commande `showemailreport` pour vérifier les paramètres de la notification par e-mail.**

```
XSCF> showemailreport  
E-Mail Reporting: enabled  
E-Mail Recipient Address: xxxxx@example.com'
```

4. **Vérifiez que l'e-mail test portant la mention « Test Mail » peut être reçu.**

10.3 Surveillance/Gestion de l'état du système avec l'agent SNMP

Cette section décrit la procédure de surveillance des pannes et des événements du système.

Une fois l'agent SNMP défini avec XSCF, un gestionnaire de serveur peut surveiller / gérer les pannes et les événements.

10.3.1 Bases de SNMP

Simple Network Management Protocol (SNMP) correspond à un protocole de gestion de réseau.

SNMP est décrit comme un protocole de requête, commande ou réponse, pour le test et la modification des paramètres de configuration d'un réseau LAN ou WAN auquel des ponts, routeurs, commutateurs ou d'autres appareils sont connectés.

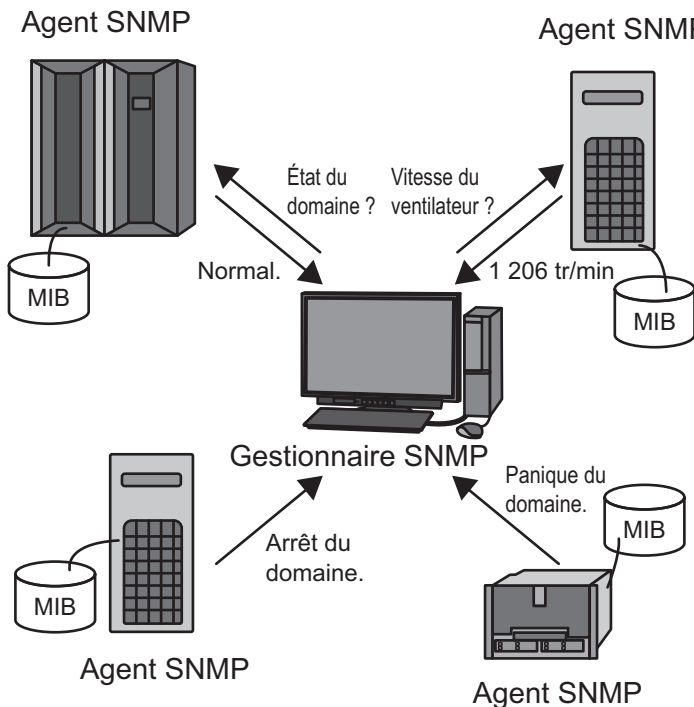
Les versions suivantes sont offertes à l'heure actuelle : SNMPv1, SNMPv2c, et SNMPv3. Contrairement à SNMPv1 et SNMPv2c, SNMPv3 dispose de fonctions de chiffrement et d'authentification supplémentaires.

Le gestionnaire SNMP gère de façon centrale l'état de fonctionnement et de panne des terminaux sur le réseau. L'agent SNMP renvoie les informations de gestion, appelées base d'informations de gestion (MIB), en réponse à une demande du gestionnaire. L'agent peut envoyer au gestionnaire une notification asynchrone avec des informations spécifiques à l'aide de la fonction Trap.

Figure 10-3 illustre un exemple d'un environnement de gestion de réseau avec le

protocole SNMP.

Figure 10-3 Exemple d'environnement de gestion de réseau



Numéros de port par défaut utilisés par SNMP

Les numéros de ports par défaut utilisés par SNMP sont les suivants.

- Pour l'agent SNMP : port 161
- Pour le trap : port 162

10.3.2 Termes liés à SNMP

Tableau 10-4 répertorie des termes liés à SNMP.

Tableau 10-4 Termes liés à SNMP

Terme	Description
USM	Abréviation pour User-based Security Model. Il s'agit d'un modèle de sécurité basé sur l'utilisateur défini dans SNMPv3.
VACM	Abréviation pour View-based Access Control Model. Il s'agit d'un modèle de contrôle d'accès basé sur l'affichage défini dans SNMPv3.
Groupe	Ensemble d'utilisateurs appartenant au modèle VACM. Un groupe est défini par les privilèges d'accès de tous les utilisateurs appartenant à ce groupe.

Tableau 10-4 Termes liés à SNMP (*suite*)

Terme	Description
OID	Abréviation de Object Identifier. Un OID est un numéro d'identification d'objet. En ce qui concerne les objets dans un fichier de définition de MIB, l'adresse numérique de la MIB est représentée par la concaténation des nombres entiers avec des points.
Affichage (Affichage MIB)	Un affichage est une méthode de référencement d'un fichier de définition MIB. L'affichage correspond à un sous-arbre de la MIB définie par un OID ou un masque d'OID. L'affichage du contrôle d'accès de la MIB peut être attribué au groupe.

10.3.3 Bases d'un fichier de définition de la MIB

La fonction de l'agent SNMP dispose des informations de gestion appelées MIB. Ces informations MIB sont renvoyées en réponse à une demande du gestionnaire.

MIB standard

Le XSCF prend en charge MIB-II (qui prend en charge SNMPv2 et v3) et MIB-I (qui prend en charge SNMPv1) qui sont définies comme des normes Internet pour gérer principalement les informations suivantes :

- Informations de base relatives à XSCF-LAN (par exemple, nom de l'administrateur)
- Informations relatives au traitement de la communication XSCF-LAN
- Informations relatives aux opérations de l'agent XSCF SNMP

Pour plus de détails sur les MIB standard prises en charge par XSCF, consultez « [Annexe D Informations sur la MIB de XSCF](#) ».

MIB étendue

En sus des MIB standard, ce système prend en charge les MIB étendues suivantes :

- MIB étendue XSCF : MIB étendue pour l'agent SNMP de XSCF

Cette MIB gère principalement les informations suivantes :

- Informations de base relatives au système (par exemple, le numéro de série)
- Diverses informations d'état relatives au système (par exemple, état de fonctionnement d'Oracle Solaris de haut niveau)
- Informations relatives aux partitions physiques dans le système
- Informations relatives aux pannes des pièces dans le système
- Informations relatives aux valeurs d'alimentation du système

L'exemple suivant indique des données d'information sur la gestion de la MIB étendue avec XSCF.

```
scfMachineType OBJECT-TYPE
SYNTAX DisplayString
ACCESS read-only
```

```

STATUS mandatory
DESCRIPTION "System model name and model type name."
::= { scfInfo 1 }
scfNumberOfCpu OBJECT-TYPE
SYNTAX INTEGER
ACCESS read-only
STATUS mandatory
DESCRIPTION "Number of CPUs"
::= { scfInfo 2 }
scfSysSerial OBJECT-TYPE
SYNTAX DisplayString
ACCESS read-only
STATUS mandatory
DESCRIPTION "System serial number"
::= { scfInfo 3 }

```

Pour plus de détails sur les MIB étendues de XSCF prises en charge par le XSCF, consultez « [Annexe D Informations sur la MIB de XSCF](#) ».

Installation du fichier de définition de la MIB étendue

Un fichier de définition MIB est défini en fonction de la notation standard ASN1. Le fichier de définition MIB étendue avec XSCF définit les informations de gestion de sorte que ces systèmes sont surveillés par le gestionnaire SNMP. Pour surveiller le serveur, installez le fichier de définition SNMP étendu avec XSCF pour le gestionnaire SNMP.

Pour plus de détails sur la procédure d'installation, consultez le manuel du gestionnaire SNMP utilisé. Pour savoir où obtenir le fichier de définition de la MIB étendue, consultez les dernières *Notes de produit* pour votre serveur ou les informations relatives au fichier de définition de la MIB situées sur le site de téléchargement du microprogramme.

10.3.4 Traps

Si vous activez la fonction d'agent SNMP, une notification appelée Trap est émise au gestionnaire SNMP. Les traps de XSCF couvrent les événements suivants :

- Notification de pulsation (XCP 2050 ou version supérieure)
- Basculement de XSCF
- Les changements de configuration résultant de l'ajout, du retrait, du remplacement, etc. des PSB et des composants
- Panne d'une pièce dans le système, ou remplacement de la pièce défectueuse dans le système suivie d'une reprise dans ces cas-là
- Changement d'une partition physique au démarrage, à la panique, à la mise hors tension, ou à tout autre état
- Incorporation ou libération d'un BB (PSB) dans une partition physique
- Hypervisor Abort

- Changements de configuration, tels que l'ajout et la suppression de pièces de l'unité d'extension PCI
- Changement de l'état de la DEL d'une pièce dans l'unité d'extension PCI
- Température anormale de l'unité d'extension PCI
- Changement du commutateur de mode
- Lorsque une panique ou tout autre changement d'état du domaine logique se produit
- Démarrage de la fonction d'agent SNMP de XSCF (trap standard)
- Accès non autorisé à l'agent SNMP de XSCF (trap standard)
- Émission d'un trap de démarrage à froid (trap standard) généré lorsqu'un changement dans la configuration de l'objet de gestion a eu lieu au démarrage de l'agent SNMP

Parmi les pièces contrôlées par l'unité XSCF dans le système, la pièce cible d'une trap peut être identifiée à partir de l'emplacement de la défaillance et du numéro de la pièce. Une trap est générée lorsqu'une notification d'événement XSCF est émise, même si la pièce ne peut pas être identifiée.

L'exemple suivant montre la SNMP-Trap pour la défaillance d'une pièce dans le système.

```
Aug 12 06:07:16 paplsv2 snmptrapd[11958]: 2012-08-12 06:07:16
A4U4S141 [10.26.147.50] (via UDP: [10.26.147.50]:38221) TRAP,
SNMP v1, community abccommunity XSCF-SP-MIB::scfMIBTraps
Enterprise Specific Trap (XSCF-SP-MIB::scfComponentStatusEvent)
Uptime: 6:27:33.28 XSCF-SP-MIB::scfComponentErrorStatus.bb.
0.cmuu.0.notApplicable.0 = INTEGER: deconfigured(4) XSCF-
SP-MIB::scfTrapStatusEventType.0 = INTEGER: alarm(1)
```

Cet exemple contient les informations suivantes :

- Adresse IP de XSCF ayant émis la trap (par ex. 10.26.147.50)
- Chaîne de communauté pour SNMPv1 (par ex. adcommunity)
- Type de trap (par ex. spécifique à l'entreprise ou au modèle)
- Trap heure d'émission (par ex. Uptime: 6:27:33:28)
- Informations supplémentaires sur la trap
Les informations peuvent comporter une pièce potentiellement défectueuse, un type d'événement, ou un niveau d'erreur.

Pour les versions de microprogramme XCP 2050 et ultérieures, si vous activez la fonction d'agent SNMP de XSCF, des trap de notification de pulsation XSCF (information d'existence) sont envoyées au système.

Les notifications de pulsation sont émises lorsque l'un des événements suivants se produit.

- Lorsque la fonction d'agent SNMP de XSCF est démarrée ou réactivée.
- Toutes les 12 heures après le démarrage de la fonction d'agent SNMP de XSCF
- Lorsque la commande rastest -c hb est exécutée

L'exemple suivant montre une trap SNMP concernant la notification de pulsation de XSCF.

Vous pouvez confirmer la notification de pulsation de XSCF lorsque le code de la trap est « FF010001 » et son message est « M10-Heartbeat ».

```
(solaris.4.1.1.12.2.1.13.100.0.254.0.254.0 [1 1 0] 1)
(solaris.4.1.2.1.2.0 [1 1 0] 4)
(solaris.4.1.1.4.3.0 [2 10 0] PZ31426015)
(solaris.4.1.1.4.2.0 [2 11 0] SPARC M10-1)
(solaris.4.1.1.4.1.0 [2 10 0] x-integ-ts)
(solaris.4.1.2.1.14.0 [2 8 0] FF010001)
(solaris.4.1.2.1.15.0 [2 28 0] Oct 23 03:06:04.367 JST 2014)
(solaris.4.1.2.1.16.0 [2 0 0] )
(solaris.4.1.2.1.17.0 [2 0 0] )

(solaris.4.1.2.1.18.0 [2 0 0] )
(solaris.4.1.2.1.19.0 [2 0 0] )
(solaris.4.1.2.1.20.0 [2 0 0] )
(solaris.4.1.2.1.21.0 [2 0 0] )
(solaris.4.1.2.1.22.0 [2 0 0] )
(solaris.4.1.2.1.23.0 [2 0 0] )
(solaris.4.1.2.1.24.0 [2 13 0] Fujitsu M10-1)
(solaris.4.1.2.1.25.0 [1 1 0] 1)
(solaris.4.1.2.1.26.0 [2 13 0] M10-Heartbeat)
```

Pour plus de détails sur les informations OID des notifications de pulsation de XSCF, consultez « Chapitre 5 XSCF Trap Type List » dans le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF MIB and Trap Lists*.

Informations des traps XSCF

Les trap XSCF signalent les pannes et les modifications de l'état du système. Pour envoyer les trap appropriées aux systèmes utilisés, effectuez les réglages de réception de trap nécessaires dans le gestionnaire SNMP.

Pour plus de détails sur les listes des traps XSCF SNMP MIB, consultez *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF MIB and Trap Lists*.

10.3.5 Vérification des éléments de réglage et des commandes liés à l'agent SNMP

Tableau 10-5 répertorie les éléments de réglage liés à l'agent SNMP de XSCF ainsi que les commandes du Shell XSCF correspondantes.

Tableau 10-5 Éléments de réglage liés à l'agent SNMP

Élément de réglage	Paramétrage requis ou optionnel	Commande liée
Informations de gestion du système - Emplacement d'installation du système de l'agent - Adresse e-mail de l'administrateur - Description du système de l'agent - Numéro de port de l'agent (numéro de port d'écoute)	Optionnel	setsnmp(8), showsnmp(8)
Activation / désactivation de l'agent	Optionnel Par défaut : désactivé	setsnmp(8), showsnmp(8)
Trap SNMPv3 - Nom d'utilisateur - Mot de passe d'authentification - Mot de passe de chiffrement - ID du moteur de l'agent local ou demande d'accusé de réception positif de la part d'un hôte de réception - Algorithme d'authentification - Protocole de chiffrement - Numéro du port de destination de la trap - Nom d'hôte de destination de la trap	Optionnel	setsnmp(8), showsnmp(8)
Désactivation des traps SNMPv3	Optionnel	setsnmp(8), showsnmp(8)
Activation / désactivation de la communication SNMPv1 et SNMPv2c	Optionnel	setsnmp(8), showsnmp(8)
Trap SNMPv1/SNMPv2c - Spécification du type de trap - Chaîne de communauté - Numéro du port de destination de la trap - Nom d'hôte de destination de la trap	Optionnel	setsnmp(8), showsnmp(8)
Désactivation des traps SNMPv1/SNMPv2c	Optionnel	setsnmp(8), showsnmp(8)
Initialisation paramètres SNMP	Optionnel	setsnmp(8), showsnmp(8)

Tableau 10-5 Éléments de réglage liés à l'agent SNMP (*suite*)

Élément de réglage	Paramétrage requis ou optionnel	Commande liée
Informations de gestion d'USM (paramètre pour SNMPv3) - Enregistrement d'un mot de passe d'authentification/chiffrement pour un utilisateur - Changement d'un mot de passe d'authentification/chiffrement d'un utilisateur - Spécification d'un algorithme d'authentification - Spécification d'un protocole de chiffrement - Copie d'un utilisateur - Suppression d'un utilisateur	Optionnel	setsnmpusm(8), showsnmpusm(8)
Informations de gestion de VACM (paramètre pour SNMPv3) - Enregistrement d'un groupe de commande d'accès pour un utilisateur - Suppression d'un groupe de commande d'accès d'un utilisateur - Création d'un affichage du contrôle d'accès de la MIB - Suppression d'un affichage du contrôle d'accès de la MIB - Affectation d'un affichage du contrôle d'accès de la MIB à un groupe - Suppression d'un groupe de tous les affichages de contrôle à l'accès d'une MIB	Optionnel	setsnmpvacm(8), showsnmpvacm(8)

10.3.6 Procédures de réglage de l'agent SNMP

Cette section décrit les opérations à effectuer pour configurer l'agent SNMP de XSCF.

Pour de plus amples informations sur chaque étape, consultez « [10.3.7 Réglage des informations de gestion du système sur l'agent SNMP et activation/désactivation de l'agent SNMP](#) » et les sections suivantes.

Il est impossible de dire que SNMPv1 et SNMPv2c sont sécurisés dans la mesure où ils ne fournissent pas de chiffrement des données de communication. Les données peuvent être envoyées et reçues en toute sécurité grâce à SNMPv3, en utilisant les paramètres d'authentification / chiffrement configurés à la fois du côté de l'agent et du côté du gestionnaire. Ces systèmes fournissent SNMPv3 comme agent SNMP par défaut.

Lancement de la transmission et de la réception

1. **Connectez-vous au XSCF.**
2. **Définissez les informations de gestion suivantes, communes aux protocoles d'agent SNMPv1, SNMPv2c et SNMPv3 (voir setsnmp(8)).**
 - Emplacement d'installation du système de l'agent
 - Adresse e-mail de l'administrateur
 - Description du système de l'agent
 - Numéro de port de l'agent (numéro de port d'écoute)
3. **Définissez les informations de gestion suivantes pour SNMPv3 ou pour SNMPv1 et SNMPv2c (voir setsnmp(8)).**
 - Paramétrage des informations de gestion de SNMPv3
 - Nom d'utilisateur
 - Mot de passe d'authentification
 - Mot de passe de chiffrement
 - Algorithme d'authentification
 - Protocole de chiffrement
 - Numéro du port de destination de la trap
 - Nom d'hôte de destination de la trap
 - Paramétrage des informations de gestion de SNMPv1 et SNMPv2c
 - Spécification du type de trap (sélection de v1, v2c, ou information à <v2c et réponse>)
 - Nom communautaire
 - Numéro du port de destination de la trap
 - Nom d'hôte de destination de la trap
4. **Activez la fonction de l'agent SNMP de XSCF. Activez la fonction selon l'une ou l'autre des méthodes suivantes, en fonction de l'environnement de l'utilisateur (voir setsnmp(8)).**
 - Activation de SNMPv1 et de SNMPv2c
 - Activation de SNMPv3

Remarque : si l'agent SNMP de XSCF a été activé, les informations de la MIB, autres que les éléments de réglage de l'étape 3, sont initialisées.

Arrêt ou désactivation de la transmission et de la réception

- **Désactivation de la fonction de l'agent SNMP de XSCF**
Désactivez la fonction selon l'une ou l'autre des méthodes suivantes, en fonction de l'environnement de l'utilisateur :
 - Invalidation de SNMPv1 et SNMPv2c
 - Invalidation de SNMPv3

- Désactivation de la transmission à l'hôte de destination de la trap cible de SNMPv3
Spécifiez les éléments suivants pour désactiver la transmission :
 - Nom d'utilisateur
 - Hôte de destination de la trap
- Désactivation de la transmission à l'hôte de destination de la trap cible pour SNMPv1 ou SNMPv2c
Spécifiez les éléments suivants pour désactiver la transmission :
 - Spécification du type de protocole (v1/v2c)
 - Hôte de destination de la trap

Gestion des utilisateurs (gestion USM) et gestion des affichages de contrôle d'accès des fichiers de définition MIB (gestion de VACM)

Gérez USM et VACM pour SNMPv3.

Lors de l'utilisation d'un agent SNMPv3, utilisez la commande `setsnmp` pour définir le protocole d'authentification ainsi que celui de chiffrement. Utilisez ensuite la commande `setsnmpusm` pour définir les informations de gestion pour le modèle de sécurité basé sur l'utilisateur (USM), puis la commande `setsnmpvacm` pour définir les informations de gestion pour le modèle de contrôle d'accès basé sur l'affichage (VACM). Lors du paramétrage de SNMPv3, la spécification d'un protocole d'authentification et d'un protocole de chiffrement est nécessaire. En outre, un mot de passe doit être saisi pour utiliser les commandes `setsnmp` et `setsnmpusm`.

1. **Connectez-vous au XSCF.**
2. **Enregistrez, modifiez ou supprimez les informations de gestion des utilisateurs suivantes (voir `setsnmpusm(8)` et `setsnmpvacm(8)`).**
 - Spécification d'un algorithme d'authentification d'utilisateur
 - Spécification d'un protocole de chiffrement d'utilisateur
 - Enregistrement d'un mot de passe d'authentification/chiffrement pour un utilisateur
 - Changement d'un mot de passe d'authentification/chiffrement d'un utilisateur
 - Copie d'un utilisateur
 - Suppression d'un utilisateur
3. **Enregistrez, attribuez ou supprimez le groupe de contrôle d'accès et l'affichage du contrôle d'accès (affichage MIB) pour un utilisateur comme suit :**
 - Enregistrement d'un groupe de commande d'accès pour un utilisateur
 - Suppression d'un groupe de commande d'accès d'un utilisateur
 - Création d'un affichage du contrôle d'accès de la MIB
 - Suppression d'un affichage du contrôle d'accès de la MIB
 - Affectation d'un affichage du contrôle d'accès de la MIB à un groupe
 - Suppression d'un groupe de tous les affichages de contrôle à l'accès d'une MIB

10.3.7 Réglage des informations de gestion du système sur l'agent SNMP et activation/désactivation de l'agent SNMP

L'agent SNMP est désactivé par défaut. Le numéro de port par défaut de l'agent est 161. Spécifiez une adresse e-mail comportant jusqu'à 128 caractères. Lorsque vous imposez des restrictions pour la réception sur l'adresse e-mail, vérifiez le paramètre.

1. **Exécutez la commande `shownmp` pour afficher les paramètres SNMP.**
Dans l'exemple suivant, l'état dans lequel aucune information de gestion n'est définie est affiché.

```
XSCF> shownmp
Agent Status:      Disabled
Agent port:        161
System Location:   Unknown
System Contact:    Unknown
System Description: Unknown
:
```

2. **Exécutez la commande `setsnmp` pour configurer SNMP.**
Dans l'exemple suivant, l'emplacement de l'installation et la description du système ainsi que l'adresse e-mail de l'administrateur sont indiqués.

```
XSCF> setsnmp -l MainTower21F -c foo@example.com -d DataBaseServer
```

3. **Exécutez la commande `setsnmp` pour activer l'agent SNMP.**
Dans l'exemple suivant, l'agent est activé.

```
XSCF> setsnmp enable
```

Dans l'exemple suivant, l'agent est désactivé.

```
XSCF> setsnmp disable
```

4. **Exécutez la commande `shownmp` pour vérifier le réglage de SNMP.**
Dans l'exemple suivant, l'agent SNMP est activé.

```
XSCF> shownmp
Agent Status:      Enabled
Agent port:        161
System Location:   MainTower21F
System Contact:    foo@example.com
System Description: DataBaseServer
```

10.3.8 Configuration des traps SNMPv3

Spécifiez le nom d'utilisateur SNMPv3 et le mot de passe d'authentification / chiffrement commun du côté de la transmission et du côté de la réception. L'ID du moteur doit commencer par « 0x » et être un nombre pair au format hexadécimal.

L'algorithme d'authentification est Secure Hash Algorithm 256 (SHA256) ou MD5.

Les protocoles de chiffrement sont Data Encryption Standard (DES) et Advanced Encryption Standard (AES).

Aucune valeur par défaut n'a été définie pour l'hôte de destination de la trap. Le numéro de port par défaut de la destination de la trap est 162.

1. **Exécutez la commande `showsnmp` pour afficher les paramètres SNMP.**
Dans l'exemple suivant, le paramétrage de l'état de SNMPv1 et SNMPv2c est illustré.

```
XSCF> showsnmp
Agent Status:      Enabled
Agent port:        161
System Location:   MainTower21F
System Contact:    foo@example.com
System Description: DataBaseServer
Trap Hosts:None
Hostname Port Type Community String Username Auth Encrypt
-----
host1      62  v1  public                n/a   n/a   n/a
host2     1162 v2  public                n/a   n/a   n/a
SNMP V1/V2c:
Status:          Enabled
Community String: public
```

2. **Exécutez la commande `setsnmp` pour configurer les traps SNMPv3.**
Dans l'exemple suivant, le nom d'utilisateur, l'ID du moteur, l'algorithme d'authentification, le mot de passe d'authentification, le mot de passe de chiffrement et le nom d'hôte de destination du trap ou son adresse IP s'affichent avec l'opérande `addv3traphost`.

```
XSCF> setsnmp addv3traphost -u yyyyyy -n 0x### -r SHA host3
Enter the trap authentication passphrase: xxxxxxxx
Enter the trap encryption passphrase: xxxxxxxx
```

3. **Exécutez la commande `showsnmp` et vérifiez le réglage du trap SNMPv3.**

```

XSCF> showsnmp
Agent Status:      Enabled
Agent port:        161
System Location:   MainTower21F
System Contact:    foo@example.com
System Description: DataBaseServer

Trap Hosts:

Hostname Port Type Community String Username Auth Encrypt
-----
host3     162   v3      n/a                yyyyyy SHA   DES
host1      62    v1      public             n/a    n/a   n/a
host2    1162   v2      public             n/a    n/a   n/a
SNMP V1/V2c:
Status:           Enabled
Community String: public

Enabled MIB Modules:
SP MIB

```

10.3.9 Désactivation des traps à l'hôte cible pour SNMPv3

1. Exécutez la commande **showsnmp** pour afficher les paramètres SNMP.

```
XSCF> showsnmp
```

2. Exécutez la commande **setsnmp** pour désactiver l'hôte de destination du trap cible de SNMPv3.
L'exemple suivant spécifie, avec l'opérande de **remv3traphost**, un nom d'utilisateur et un nom d'hôte.

```
XSCF> setsnmp remv3traphost -u yyyyyy host3
```

3. Exécutez la commande **showsnmp** et vérifiez si l'hôte de destination du trap cible est désactivé.

```
XSCF> showsnmp
```

10.3.10 Activation/Désactivation de la communication SNMPv1 et SNMPv2c

La chaîne de communauté utilisée pour l'activation de SNMPv1 et SNMPv2c est en

lecture seule.

1. **Exécutez la commande `showsnmp` pour afficher les paramètres SNMP.**

```
XSCF> showsnmp
```

2. **Exécutez la commande `setsnmp` pour activer la communication SNMPv1 et SNMPv2c.**

L'exemple suivant spécifie l'opérande `enablev1v2c` pour l'activation de SNMPv1 et SNMPv2c.

```
XSCF> setsnmp enablev1v2c public
```

L'exemple suivant spécifie l'opérande `disablev1v2c` pour la désactivation de SNMPv1 et SNMPv2c.

```
XSCF> setsnmp disablev1v2c
```

3. **Exécutez la commande `setsnmp` pour activer l'agent SNMP.**

```
XSCF> setsnmp enable
```

4. **Exécutez la commande `showsnmp` et vérifiez que l'agent est activé / désactivé.**

```
XSCF> showsnmp
```

10.3.11 Configuration des traps SNMPv1 et SNMPv2c

Sélectionnez un type de trap parmi les trois suivants :

- v1
- v2
- inform

Lorsque vous sélectionnez `inform`, `InformRequest` est envoyé à l'aide de l'agent SNMPv2c.

Le numéro de port par défaut de la destination de la trap est 162.

1. **Exécutez la commande `showsnmp` pour afficher les paramètres SNMP.**

```
XSCF> showsnmp
```

2. **Exécutez la commande `setsnmp` pour configurer le trap SNMPv1 ou SNMPv2c.**
Dans l'exemple suivant, le type SNMPv2c est spécifié avec l'opérande `addtraphost`.

```
XSCF> setsnmp addtraphost -t v2 -s public host2
```

L'exemple suivant indique le type de SNMPv1.

```
XSCF> setsnmp addtraphost -t v1 -s public host1
```

3. **Exécutez la commande `showsnmp` pour vérifier les paramètres des traps pour SNMPv1 et SNMPv2c.**

```
XSCF> showsnmp
```

10.3.12 Désactivation des traps à l'hôte cible pour SNMPv1 et SNMPv2c

1. **Exécutez la commande `showsnmp` pour afficher les paramètres SNMP.**

```
XSCF> showsnmp
```

2. **Exécutez la commande `setsnmp` pour désactiver l'hôte de destination de la trap cible pour SNMPv1 ou SNMPv2c.**

L'exemple suivant indique l'opérande `remtraphost` pour désactiver un hôte de type SNMPv2c.

```
XSCF> setsnmp remtraphost -t v2 host2
```

3. **Exécutez la commande `showsnmp` et vérifiez si l'hôte de destination de la trap est désactivé.**

```
XSCF> showsnmp
```

10.3.13 Restauration des valeurs par défaut pour les paramètres SNMP

Vous pouvez restaurer les valeurs par défaut aux données configurées en désactivant l'agent SNMP.

1. **Exécutez la commande `showsnmp` pour afficher les paramètres SNMP.**

```
XSCF> showsnmp
```

2. **Exécutez la commande `setsnmp` pour restaurer les valeurs par défaut des paramètres de SNMP.**

L'agent SNMP est désactivé pour l'instant.

```
XSCF> setsnmp default
```

3. **Exécutez la commande `showsnmp` et vérifiez que les valeurs par défaut des paramètres de SNMP ont été restaurées.**

```
XSCF> showsnmp
```

4. **Exécutez la commande `setsnmp` et reconfigurez SNMP. Activez ensuite l'agent SNMP.**

```
XSCF> setsnmp enable
```

5. **Exécutez la commande `showsnmp` pour vérifier le réglage de SNMP.**

```
XSCF> showsnmp
```

10.3.14 Réglage des informations de gestion d'USM

Les informations de gestion d'USM sont composées de réglage pour SNMPv3. Réglez ce qui suit :

- Algorithme d'authentification de l'utilisateur
- Protocole de chiffrement de l'utilisateur
- Mot de passe d'authentification / de chiffrement
- Copie / suppression d'un utilisateur

1. **Exécutez la commande `showsnmpusm` pour afficher les informations de gestion d'USM.**

```
XSCF> showsnmpusm

Username  Auth  Encrypt
-----  -
yyyyyy   SHA  DES
user2    SHA  DES
```

2. **Exécutez la commande `setsnmpusm` pour définir les informations de gestion d'USM.**

Dans l'exemple suivant, l'algorithme d'authentification, le mot de passe d'authentification et le mot de passe de chiffrement d'un nouvel utilisateur sont

enregistrés. Le mot de passe doit comporter huit caractères minimum.

```
XSCF> setsnmpusm create -a SHA yyyy  
Enter the user authentication passphrase: xxxxxxxx  
Enter the user encryption passphrase: xxxxxxxx
```

Dans l'exemple suivant, seul le mot de passe d'authentification est modifié.
(Si aucun mot de passe n'est saisi, le système vous demande de le saisir.)

```
XSCF> setsnmpusm passwd -c auth -o xxxxxxxx -n xxxxxxxx yyyy
```

Dans l'exemple suivant, un utilisateur existant est copié pour ajouter un utilisateur en tant que clone.

```
XSCF> setsnmpusm clone -u yyyy newuser
```

Dans l'exemple suivant, un utilisateur est supprimé.

```
XSCF> setsnmpusm delete yyyy
```

3. **Exécutez la commande `showsnmpusm` pour afficher les informations de gestion d'USM.**

```
XSCF> showsnmpusm  
  
Username  Auth  Encrypt  
-----  
yyyyy    SHA   DES  
user2    SHA   DES
```

10.3.15 Réglage des informations de gestion de VACM

Les informations de gestion de VACM sont composées de réglage pour SNMPv3.
Réglez ce qui suit :

- Enregistrement / suppression d'un utilisateur dans un groupe de contrôle d'accès
- Création / suppression d'un affichage du contrôle d'accès de la MIB
- Affectation d'un affichage du contrôle d'accès de la MIB à un groupe
- Suppression d'un groupe de tous les affichages de contrôle à l'accès d'une MIB

L'affichage en lecture seule est attribué lorsqu'un affichage de contrôle d'accès est attribué à un groupe.

1. **Exécutez la commande `showsnmpvacm` pour afficher les informations de gestion de VACM.**


```
XSCF> showsnmpvacm
```

```
Groups:
```

```
Groupname      Username
```

```
-----      -
```

```
xxxxx         user1, user2
```

```
Views
```

```
View           Subtree           Mask           Type
```

```
-----      -
```

```
all_view       .1                ff             include
```

```
Access
```

```
View Group
```

```
-----      -
```

```
all_view       xxxxx
```

2. Exécutez la commande `setsnmpvacm` pour définir les informations de gestion de VACM.

Dans l'exemple suivant, le groupe de contrôle d'accès xxxxx est ajouté à l'utilisateur yyyyy.

```
XSCF> setsnmpvacm creategroup -u yyyyy xxxxx
```

Dans l'exemple suivant, l'utilisateur yyyyy est supprimé du groupe de contrôle d'accès xxxxx.

```
XSCF> setsnmpvacm deletegroup -u yyyyy xxxxx
```

Dans l'exemple suivant, l'affichage du contrôle d'accès de la MIB est créé sans conditions.

```
XSCF> setsnmpvacm createview -s .1 all_view
```

Dans l'exemple suivant, l'affichage du contrôle d'accès de la MIB est créé à l'aide du masque OID.

```
XSCF> setsnmpvacm createview -s .1.3.6.1.2.1 -m fe excl_view
```

Dans l'exemple suivant, l'affichage du contrôle d'accès de la MIB est supprimé.

```
XSCF> setsnmpvacm deleteview -s .1.3.6.1.2.1 excl_view
```

Dans l'exemple suivant, l'affichage du contrôle d'accès de la MIB est attribué au groupe xxxxx.

```
XSCF> setsnmpvacm createaccess -r all_view xxxxx
```

Dans l'exemple suivant, le group1 est supprimé de tous les affichages du

contrôle d'accès de la MIB.

```
XSCF> setsnmpvacm deleteaccess group1
```

3. **Exécutez la commande `showsnmpvacm` et vérifiez les informations de gestion de VACM.**

```
XSCF> showsnmpvacm
```

10.4 Surveillance du système

Cette section décrit la surveillance d'Oracle Solaris et de chaque élément du microprogramme de ces systèmes.

10.4.1 Compréhension du mécanisme de la fonction Host watchdog / de vérification d'activité

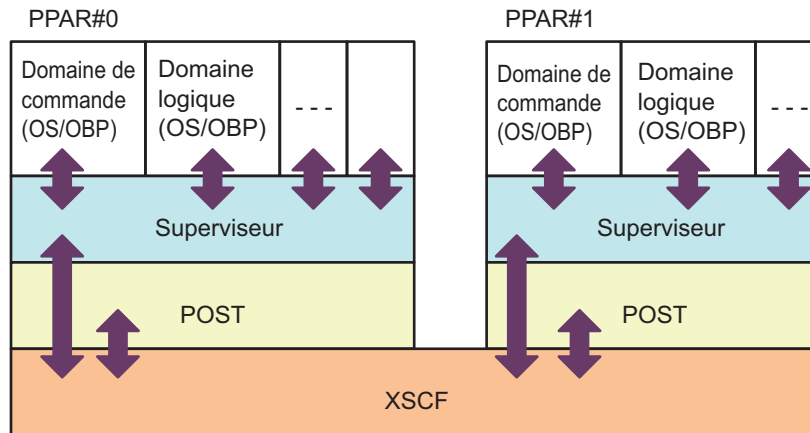
Un domaine logique d'Oracle Solaris, OpenBoot PROM, le superviseur, POST et XSCF établissent des communications et surveillent mutuellement leurs états d'activité. En cas de détection d'une panne, une panique est générée ou ils sont arrêtés individuellement pour parer à la propagation de la panne.

Dans ces systèmes, le superviseur surveille le domaine logique / OpenBoot PROM, et XSCF surveille POST.

Le mécanisme de surveillance entre le superviseur et le domaine logique et entre le superviseur et OpenBoot PROM est la fonction Host Watchdog. De plus, le mécanisme de surveillance entre XSCF et POST est la fonction de vérification d'activité.

[Figure 10-4](#) montre la surveillance des ressources respectives les unes sur les autres.

Figure 10-4 Caractéristiques de la surveillance du système



Remarque : OBP dans [Figure 10-4](#) correspond à OpenBoot PROM.

XSCF surveille POST et détermine si une erreur survient lorsqu'aucune réponse n'est reçue après une durée spécifique, puis il redémarre la partition physique ou désactive l'alimentation.

Le superviseur surveille régulièrement l'état fonctionnel des domaines logiques (Oracle Solaris/OpenBoot PROM) afin de déterminer une interruption d'Oracle Solaris. Lorsqu'une interruption d'Oracle Solaris est détectée, le superviseur génère une panique d'Oracle Solaris dans le domaine concerné.

Remarque : pour des informations complémentaires concernant la fonction de vérification d'activité entre le XSCF et le superviseur, qui est définie par la commande `setpparmode`, consultez les dernières *Notes de produit* pour votre serveur.

10.4.2

Contrôle de la surveillance et du fonctionnement du serveur

Si le système est en cours d'exécution ou de maintenance, vous pouvez avoir besoin de supprimer certaines fonctions pour chaque partition physique ou domaine logique. Supposons par exemples que vos préférences pour la maintenance du système n'inclue pas le démarrage automatique (la suppression de démarrage automatique est activée) ni de réception de signaux de rupture de la console (la suppression des interruptions de signal est activée).

Dans ces systèmes, le mode opérationnel spécifié pour chaque partition physique inclut la méthode de surveillance et le niveau de diagnostic. Il est ensuite possible de contrôler le fonctionnement des domaines logiques et de la partition physique.

Vous pouvez définir les paramètres suivants pour chaque partition physique spécifiée avec la commande `setpparmode` : niveau de diagnostic initial du matériel, niveau de message, fonction de vérification des activités, réaction en cas d'expiration de Host watchdog, activation / désactivation de la suppression de la transmission du signal d'arrêt, activation / désactivation du démarrage automatique des domaines invités, activation / désactivation de la fonction d'économie d'énergie, et activation / désactivation de la fonction de reconfiguration du bus d'E/S.

Vous pouvez également activer / désactiver le démarrage automatique du domaine de commande de chaque partition physique spécifié avec la commande `setpparparam`.

Pour plus de détails sur le contrôle des opérations du serveur avec la commande `setpparmode`, consultez « Chapitre 3 Opérations pour la configuration de domaine » dans le *Guide de configuration du domaine Fujitsu SPARC M12 et Fujitsu M10/SPARCM10*.

Remarque : pour plus de détails sur la commande `setpparmode` et des informations complémentaires sur chaque fonction de cette commande, consultez les dernières *Notes de produit* pour votre serveur.

10.5 Comprendre le mécanisme de détérioration suite à une panne

La libération d'un composant du système à cause d'une panne matérielle s'appelle une « détérioration ». Une détérioration a pour principe d'empêcher l'accès à ce composant pour ne pas propager le problème dans tout le système.

Les scénarios de détérioration sont décrits ci-dessous.

- **Détérioration réservée**
Si la détérioration est impossible immédiatement au redémarrage ou en cas d'erreur fatale, la détérioration est réservée dans le système pour générer la détérioration au redémarrage. Ce scénario peut être réalisé avec le XSCF en conservant l'emplacement de la détérioration dans la mémoire.
- **Détérioration pendant l'exécution d'Oracle Solaris**
Les processeurs, la mémoire, etc. sont détériorés quand ils peuvent être libérés pendant l'exécution d'Oracle Solaris. Seuls les composants autorisés à être libérés pendant l'exécution d'Oracle Solaris sont soumis à une détérioration.
- **Détérioration pendant l'exécution de POST**
Une partition physique est détériorée sans réinitialisation.
- **Détérioration réservée pendant l'exécution d'OpenBoot PROM**
La détérioration est réservée pendant l'exécution d'OpenBoot PROM est réalisée après une réinitialisation. Les erreurs de l'adaptateur PCI, erreurs de mémoire, etc. sont des cibles pour la détérioration.
- **Détérioration dynamique des chemins internes dans le matériel**

Une voie est détériorée de manière dynamique dans les chemins entre les châssis, tels que le châssis SPARC M12/M10, les unités à barres croisées, et les unités à barres croisées dans un boîtier à barre transversale et entre les composants, sans réinitialiser le système.

La commande `showstatus` permet d'afficher les informations de détérioration du composant. Pour plus détails sur la gestion de la détérioration résultant d'une panne, consultez « [11.1.4 Vérification des composants en panne/détériorés](#) ».

10.6 Vérification des ressources matérielles en panne

Les systèmes SPARC M12/M10 détectent et dégradent automatiquement les ressources de mémoire et de processeur défectueuses.

Vous pouvez afficher l'occurrence des pannes de ressources de mémoire et de processeur en spécifiant l'option `-S` pour les commandes `ldm list-domain` et `ldm list-devices`.

Pour de plus amples informations sur les commandes `ldm list-domain` et `ldm list-device`, consultez le *Oracle VM Server for SPARC Reference Manual* de la version utilisée. Consultez également « [10.7 Configuration d'une substitution automatique de cœurs du processeur en panne](#). » La section décrit les méthodes de configuration pour la substitution automatique d'un cœur de processeur défectueux.

10.6.1 Vérification d'une mémoire ou de processeurs en panne avec la commande `list-domain`

1. **Affichez les informations détaillées du domaine logique dans la partition physique ainsi que les informations concernant la panne ou l'absence de panne de la mémoire ou du processeur.**

```
primary# ldm list-domain -l -S
```

10.6.2 Vérification d'une mémoire ou de processeurs en panne avec la commande `list-device`

1. **Affichez les informations relatives aux ressources d'une mémoire ou de processeurs disponibles dans une partition physique avec les informations permettant de déterminer si la mémoire ou le processeur est effectivement en panne.**

10.7 Configuration d'une substitution automatique de cœurs du processeur en panne

Le SPARC M12/M10 peut utiliser des systèmes en continu sans réduire les ressources de processeur en utilisant la fonction de substitution automatique de processeur pour attribuer automatiquement un autre cœur de processeur, même si un cœur de processeur tombe en panne.

La fonction de substitution automatique de processeur est activée/désactivée en fonction de la politique de substitution automatique du service ldmd spécifié par la commande `svccfg` d'Oracle Solaris. Par défaut, cette fonction est activée.

Si la politique de substitution automatique est activée, le cœur de processeur en panne qui a été automatiquement substitué est contrôlé afin pour qu'il ne soit pas ensuite attribué à un domaine logique. Si le cœur de processeur en panne n'a pas été substitué automatiquement, le cœur de processeur reste à attribuer à un domaine logique.

Si la politique de substitution automatique est désactivée, le cœur de processeur en panne n'est pas substitué.

Pour plus de détails sur les procédures de changement de politique de substitution automatique, consultez « [10.7.2 Méthode de modification de la politique de substitution automatique](#) ».

10.7.1 Conditions requises pour la substitution automatique d'un cœur de processeur

Pour qu'un remplacement automatique de cœurs de processeur soit effectué, les conditions suivantes doivent être vérifiées.

- De tous les cœurs de processeur montés sur une partition physique, au moins un est garanti de ne pas être attribué à la PPAR.
Si vous allouez tous les cœurs de processeur montés sur la PPAR à la PPAR avec la commande `setcod(8)` du microprogramme XSCF, le remplacement automatique n'est pas disponible.

Pour le SPARC M10-4 (configuration à 4 processeurs x 16 cœurs), 64 cœurs de processeur sont montés sur la PPAR. Pour utiliser la fonction de remplacement automatique dans cette configuration, il est nécessaire de définir le nombre de cœurs de processeurs alloués sur la PPAR à 63 ou moins au moyen de la commande `setcod`.

Lorsque 56 cœurs de processeur sont alloués à PPAR-ID 0 comme suit et que 64

cœurs de processeur sont montés sur la PPAR, des cœurs peuvent être échangés automatiquement.

```
XSCF> setcod -p 0 -s cpu -c set 56
PROC Permits assigned for PPAR 0 : 0 -> 56

PROC Permits assigned for PPAR will be changed.
Continue? [y|n] :y

Completed.
```

Remarque : le microprogramme du XSCF de XCP 2250 ou versions précédentes ne prend pas en charge les options -c add, -c delete et -c set. Spécifiez les options de la commande setcod comme suit pour ajouter et supprimer interactivement des attributions.

```
XSCF> setcod -s cpu
```

Le nombre de cœurs de processeur disponibles pour être automatiquement remplacés n'est pas lié au nombre de cœurs de processeur enregistrés avec les clés d'activation du processeur. Par exemple, si 56 activations de processeur sont enregistrées dans l'exemple ci-dessus d'un SPARC M10-4, alors jusqu'à 8 cœurs de processeur disponibles peuvent être échangés avec la fonction de remplacement automatique même si 56 cœurs de processeur sont alloués avec la commande setcod(8). Dans ce cas, les 8 cœurs de processeur disponibles pour être échangés ne nécessitent pas les clés d'activation du processeur.

- Les cœurs de processeur peuvent être supprimés automatiquement.

Le remplacement automatique de cœurs de processeur est impossible dans les cas suivants.

- Des identifiants de cœur physique (option cid) sont spécifiés lorsque des cœurs de processeur sont attribués au domaine logique.
Le remplacement automatique de cœurs de processeur est impossible si les cœurs de processeur sont attribués au domaine logique avec l'option cid spécifiée comme ci-dessous.

```
# ldm set-core cid=20 ldom
# ldm add-core cid=20 ldom
```

Si vous avez attribué des cœurs de processeur avec l'option cid spécifiée, retirez-la. Pour la méthode d'annulation de la spécification cid, consultez la section « How to Remove the physical-bindings Constraint » dans le *Oracle VM Server for SPARC Administration Guide* de la version utilisée.

Remarque : pour utiliser la fonction de remplacement automatique de processeur, n'utilisez pas les zones noyau d'Oracle Solaris.

Quand les zones de noyau d'Oracle Solaris sont utilisées, les processeurs CPU assignés aux zones de noyau d'Oracle Solaris ne sont pas automatiquement remplacés de la bonne manière.

Les six restrictions suivantes sont supprimées sur Oracle VM Server pour SPARC 3.3 et versions ultérieures.

- Lorsqu'un seul cœur de processeur est alloué à un domaine logique
Utilisez la commande `ldm set-core` ou `ldm add-core` pour attribuer deux cœurs de processeur ou plus à un domaine. Vous pouvez vérifier les ressources de cœurs de processeur utilisées par le domaine logique avec la commande `ldm list-domain -o core`.
- Lorsque le processeur défini du pool de ressources ne répond pas aux conditions suivantes
[SPARC M12]

La propriété `pset.min` est définie à 9 ou plus, et la propriété `pset.max` est définie à `pset.min + 8` ou plus.
[SPARC M10]

La propriété `pset.min` est définie à 3 ou plus, et la propriété `pset.max` est définie à `pset.min + 2` ou plus.

Pour la méthode de configuration de l'ensemble de processeurs du pool de ressources, consultez le *System Administration Guide: Oracle Solaris Containers-Resource Management and Oracle Solaris Zones*.
- Lors de la spécification du nombre de processeurs pour la ressource de processeur dédié d'une zone d'Oracle Solaris
La spécification d'un nombre précis de processeurs lors de l'utilisation de la ressource de processeur dédié d'une zone d'Oracle Solaris est incompatible avec le remplacement automatique du cœur de processeur.
(par ex., `ncpu=5`)
- Lorsque l'ensemble des processeurs spécifiés pour la ressource de processeur dédié d'une zone d'Oracle Solaris ne répond pas aux conditions suivantes
[SPARC M12]

Neuf processeurs ou plus (deux cœurs) pour la valeur minimale et la valeur minimale + huit processeurs ou plus pour la valeur maximale
(par ex., `ncpus=9-17`)
[SPARC M10]

Trois processeurs ou plus (deux cœurs) pour la valeur minimale et la valeur minimale + deux processeurs ou plus pour la valeur maximale
(par ex., `ncpus=3-5`)
- Lorsque des processus sont liés au cœur de processeur avec la commande `pbind`
Vous devez vérifier/libérer les processus liés à des cœurs de processeur avec la commande `pbind` afin d'utiliser le cœur de processeur avec la fonction de remplacement automatique du cœur de processeur.
- Lorsque des processeurs sont liés à un cœur de processeur unique avec la commande `psrset`
Attribuez deux cœurs de processeur ou plus à l'ensemble de processeurs, ou supprimez l'ensemble de processeurs, libérant ainsi le cœur de processeur que vous voulez utiliser avec la fonction de remplacement automatique du cœur de processeur.

10.7.2 Méthode de modification de la politique de substitution automatique

La politique de substitution automatique peut être modifiée avec la commande `svccfg` d'Oracle VM Server pour SPARC.

La substitution automatique peut être activée / désactivée par la propriété `autoreplacement_policy_cpu` du service `ldmd`. Vous pouvez utiliser les valeurs suivantes pour la propriété `autoreplacement_policy_cpu`.

- `autoreplacement_policy_cpu=1`
Une ressource de processeur en panne est automatiquement substituée. Il s'agit de la stratégie par défaut.
- `autoreplacement_policy_cpu=0`
Si une panne se produit dans un processeur, il n'est pas automatiquement substitué.

La procédure de réglage est décrite ci-dessous.

1. **Connectez-vous au domaine de commande.**
2. **Devenez l'administrateur.**
3. **Affichez la valeur de la propriété `autoreplacement_policy_cpu`.**

```
# svccfg -s ldmd listprop ldmd/autoreplacement_policy_cpu
```

4. **Arrêtez le service `ldmd`.**

```
# svcadm disable ldmd
```

5. **Modifiez la valeur de la propriété `autoreplacement_policy_cpu`.**

```
# svccfg -s ldmd setprop ldmd/autoreplacement_policy_cpu=value
```

6. **Rafraîchissez et redémarrez le service `ldmd`.**

```
# svcadm refresh ldmd
# svcadm enable ldmd
```

L'exemple suivant montre comment afficher la valeur actuelle de la propriété `autoreplacement_policy_cpu` et la modifier pour obtenir une nouvelle valeur. La valeur initiale de cette propriété est 0. Dans ce cas, le processus de substitution automatique du processeur est désactivé. Arrêtez ou redémarrez le service `ldmd` avec la commande `svcadm`. Affichez ou configurez les valeurs de la propriété avec la commande `svccfg`.

```
# svccfg -s ldmd listprop ldmd/autoreplacement_policy_cpu
ldmd/autoreplacement_policy_cpu integer 0
# svcadm disable ldmd
# svccfg -s ldmd setprop ldmd/autoreplacement_policy_cpu=1
# svcadm refresh ldmd
# svcadm enable ldmd
```

10.7.3 Méthodes de modification du nombre de tentatives maximum et intervalle entre les tentatives

Vous pouvez non seulement modifier la politique de substitution automatique mais également définir le nombre maximal de tentatives ainsi que l'intervalle entre les tentatives pour le processus de substitution automatique du processeur.

- Pour spécifier le nombre maximum de tentatives, définissez la propriété `autoreplacement_retry_counter` du service `ldmd`. Si 0 est spécifié, il n'y a aucune limite sur le nombre de tentatives. La valeur par défaut est 5.
- Pour spécifier l'intervalle entre les tentatives, définissez la propriété `autoreplacement_retry_interval` du service `ldmd`. L'intervalle minimal est de 1 seconde. La valeur par défaut est 300 secondes.

Les procédures de modification de ces propriétés sont identiques à celles de modification de la valeur de la propriété `autoreplacement_policy_cpu`. Consultez « [10.7.2 Méthode de modification de la politique de substitution automatique](#) ».

10.8 Configuration du mode de récupération

Une configuration de domaine qui ne peut pas être démarrée à cause de problème de ressources, de ressources manquantes, etc. peut être récupérée automatiquement en définissant un mode de récupération, qui est proposé par Oracle VM Server pour SPARC 3.1 et versions supérieures.

Cette fonction est activée par défaut dans Oracle VM Server pour SPARC 3.3 ou version ultérieure.

Pour de plus amples informations sur le mode de reprise, voir « Handling Hardware Errors » dans le document *Oracle VM Server for SPARC Administration Guide* de la version utilisée. De plus, pour connaître les correctifs nécessaires pour le mode de récupération, consultez les *Oracle VM Server for SPARC Release Notes* de la version utilisée.

10.9 Configuration de composants redondants

Avec des composants dans une configuration redondante, si l'un des composants échoue, le système peut continuer à fonctionner avec les composants restants.

Pour plus de détails sur les configurations de composants redondants, consultez le *Service Manual* pour votre serveur.

La commande `showhardconf` permet d'afficher la configuration des composants. Pour plus de détails sur la façon de vérifier les composants, consultez « [11.1.2 Vérification des composants montés dans le système](#) ».

10.10 Sauvegarde/restauration des informations des réglages de XSCF

Pour enregistrer/restaurer les informations des réglages de XSCF, exécutez les commandes `dumpconfig` et `restoreconfig` du microprogramme XSCF. L'exécution de la commande avec des options spécifiées enregistre ou restaure toutes les informations des réglages XSCF à l'emplacement spécifié.

10.10.1 Compréhension de la sauvegarde/restauration des informations des réglages de XSCF

Cette section décrit les deux méthodes suivantes de sauvegarde / restauration des informations de paramétrage de XSCF.

- Enregistrez / restaurez les informations de réglage localement en connectant un périphérique USB au connecteur USB installé sur le panneau (arrière) de l'unité XSCF du XSCF maître.
- Transférez les données vers l'hôte du réseau via le réseau. Le transfert de données à ce moment-là utilise un protocole de chiffrement.

Remarque : lors de la substitution de l'unité XSCF du SPARC M12-2/M12-2S, l'information des réglages XSCF peut être prise en charge en échangeant également la carte SD. Lors du remplacement du boîtier à barre transversale (XBBOX) ou de l'unité de mémoire du processeur (inférieure) (CMUL) du SPARC M10-4/M10-4S, l'information des réglages XSCF peut être prise en charge en échangeant également la carte microSD.

Pour plus de détails, consultez la section « Replacing the SD card » ou « Replacing microSD card » dans le *Service Manual* pour votre serveur. Lorsque vous remplacez l'unité XSCF d'un boîtier à barre transversale, consultez « 8.5 Switching the microSD Card » dans le *Crossbar*

Intérêt de la sauvegarde

Les intérêts de la sauvegarde des informations des réglages de XSCF avec la commande `dumpconfig` sont les suivants.

- La sauvegarde des données de réglage permet de restaurer les données après une panne.
- La copie des informations des réglages XSCF maître permet aux XSCF des autres serveurs d'utiliser les mêmes informations de réglage.

Remarque sur la sauvegarde et la restauration

- Le périphérique USB doit être formaté avec le système de fichiers FAT32. Pour la capacité du périphérique USB utilisé pour sauvegarder / restaurer les informations de réglage au niveau local et pour les points à noter à propos de la manipulation, demandez à un technicien de maintenance.
- Les informations de réglage peuvent être restaurées sur un système du même modèle que celui sur lequel elles sont sauvegardées. Par exemple, les informations de réglage sauvegardées sur un système SPARC M10-1 ne peuvent être restaurées que sur un système SPARC M10-1. Pour restaurer les données, la cohérence entre le fichier de configuration du système actuel et celui à restaurer est vérifiée. Le fichier est restauré uniquement lorsque les versions des fichiers de configuration, les noms de système et d'autres informations peuvent être confirmés comme étant cohérentes. La version du fichier de configuration ne dépend toutefois pas de la version de XCP. Les versions des fichiers de configuration peuvent être différentes, même si les versions XCP sont les mêmes pour la sauvegarde / restauration.
- Les systèmes avec plusieurs XSCF sauvegardent / restaurent les données du côté XSCF maître.
- La commande `dumpconfig` peut être utilisée avec des options spécifiées pour chiffrer les données sauvegardées. Vous pouvez restaurer en toute sécurité les données chiffrées en saisissant la clé spécifiée lors de l'enregistrement et de l'exécution de la commande `restoreconfig`.
- Les informations d'identification suivantes sont ajoutées au début d'un fichier de configuration enregistré. Vous pouvez consulter les informations d'identification dans le texte.
 - Commentaire de l'utilisateur
 - Version des données
 - Si le chiffrement est activé ou désactivé
 - Temps d'enregistrement
 - Nom du système
 - Numéro de série
 - Version de XCP
- Les paramètres réseau de XSCF spécifient des options de restauration des données.

- Pour restaurer les informations de réglage, mettez hors tension toutes les partitions physiques. En outre, lorsque la commande de restauration est exécutée, les informations des réglages de XSCF sont chargées, de manière à pouvoir vérifier l'exactitude de son contenu. Une fois la confirmation terminée, le XSCF est redémarré et les données sont restaurées.

10.10.2 Sauvegarde des informations des réglages de XSCF

Cette section décrit la procédure de sauvegarde du fichier de configuration XSCF.

Remarque : avec la commande `dumpconfig`, l'information des réglages XSCF peut être cryptée et enregistrée. Pour plus de détails, consultez la page du manuel correspondant à la commande `dumpconfig(8)` ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

Enregistrement des informations de configuration vers le périphérique USB du XSCF maître

1. **Connectez le périphérique USB à un port USB sur le panneau (arrière) de l'unité XSCF du XSCF maître.**
2. **Indiquez le nom du fichier de sortie pour le périphérique USB local sur le XSCF puis exécutez la commande `dumpconfig`.**

```
XSCF> dumpconfig file:///media/usb_msd/backup-file.txt
```

3. **Retirez le périphérique USB du port USB lorsque le transfert de données est terminé.**
4. **Vérifiez les informations d'identification au début du fichier de configuration qui a été enregistré.**

Spécification du répertoire cible et enregistrement des informations de configuration via un réseau

1. **Spécifiez le répertoire cible et le nom du fichier de sortie, puis exécutez la commande `dumpconfig`.**

```
XSCF> dumpconfig ftp://server/backup/backup-sca-ff2-16.txt
:
```

2. **Vérifiez les informations d'identification au début du fichier de configuration enregistré une fois le transfert de données terminé.**

Format de fichier de configuration

Le fichier de configuration enregistré a le format suivant :

- Nom de fichier : nom choisi par l'utilisateur
- Format du fichier : texte encodé en base64

10.10.3 Restauration des informations des réglages de XSCF

Cette section décrit la procédure de restauration du fichier de configuration.

Remarque : la commande `restoreconfig` est capable de déchiffrer les fichiers qui ont été chiffrés à l'aide de la commande `dumpconfig`. Pour plus de détails, consultez la page du manuel correspondant à la commande `restoreconfig`(8) ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

Remarque : lorsque vous enregistrez des informations de configuration de domaine logique à l'aide de la commande `ldm add-spconfig` sur le domaine de commande après avoir exécuté la commande `dumpconfig`, restaurer les informations de configuration du domaine logique avec la commande `restoreconfig` peut ne pas fonctionner correctement. Par conséquent, avant de restaurer les informations des réglages de XSCF avec la commande `restoreconfig`, utilisez la commande `ldm remove-spconfig` sur tous les domaines de commande pour supprimer toutes les informations de configuration des domaines logiques à l'exception des réglages d'usine par défaut.

Pour vérifier les dates des fichiers d'informations de configuration qui ont été enregistrés en utilisant la commande `ldm add-spconfig`, exécutez la commande `showdomainconfig` pour toutes les partitions physiques.

Pour de plus amples informations sur la configuration du domaine logique, consultez la section « Managing Domain Configurations » dans le *Oracle VM Server for SPARC Administration Guide* de la version que vous utilisez.

Restauration des informations de réglage depuis le périphérique USB du XSCF maître

1. **Mettez hors tension toutes les partitions physiques.**
2. **Connectez le périphérique USB contenant le fichier de configuration au port USB du panneau (arrière) de l'unité XSCF du XSCF maître.**
3. **Spécifiez le périphérique USB local de l'unité XSCF comme fichier de saisie et exécutez la commande `restoreconfig`.**

```
XSCF> restoreconfig file:///media/usb_msd/backup-file.txt
Configuration backup created on Tue Jul 19 17:04:48 2011
:
*** You will need to power-cycle the entire system after this operation
is completed
*** Do you want to restore this configuration to your system? [y|n]:
```

Le message affiche les informations d'identification du fichier de configuration à restaurer.

4. **Si l'information est correcte, saisissez « y » pour restaurer le fichier.**
Le XSCF est redémarré.
5. **La session est déconnectée une fois. Reconnectez.**
6. **Retirez le périphérique USB du port USB lorsque la restauration est terminée.**

Spécification du répertoire cible et enregistrement des informations de réglage via un réseau

1. **Mettez hors tension tous les domaines.**
2. **Spécifiez le répertoire cible et exécutez la commande restoreconfig.**

```
XSCF> restoreconfig ftp://server/backup/backup-sca-ff2-16.txt
Configuration backup created on Tue Jul 19 17:04:48 2011
:
*** You will need to power-cycle the entire system after this operation
is completed
*** Do you want to restore this configuration to your system? [y|n]:
```

Le message affiche les informations d'identification du fichier de configuration à restaurer.

3. **Si l'information est correcte, saisissez « y » pour restaurer le fichier.**
Le XSCF est redémarré.
4. **La session est déconnectée une fois. Reconnectez.**

10.11 Sauvegarde / restauration des informations de configuration du domaine logique dans le XSCF

Cette section décrit la procédure de sauvegarde des informations de configuration du domaine logique dans XSCF et de restauration de la configuration enregistrée. Pour la méthode de sauvegarde/restauration des informations de configuration du domaine logique dans un fichier XML, consultez « [10.12 Sauvegarde / restauration des informations de configuration du domaine logique dans un fichier XML](#) ».

10.11.1 Sauvegarde/Affichage des informations de réglage du domaine logique

Vous pouvez enregistrer les informations de configuration du domaine logique pour les partitions physiques individuelles. Pour sauvegarder les informations de configuration, connectez-vous au domaine de commande de la partition physique cible. La destination de sauvegarde des informations de configuration enregistrées est le processeur de service dans la partition physique.

Vous pouvez enregistrer au maximum huit ensembles d'informations de configuration de domaine logique par partition physique. L'un des ensembles enregistrés reflète l'état lors de l'expédition de l'usine, et son nom est `factory-default`. Dans la mesure où `factory-default` est déjà sauvegardé, vous pouvez enregistrer jusqu'à sept ensembles d'informations de configuration. En sauvegardant différents schémas de configuration à l'avance, il est possible de spécifier la configuration de domaine logique adaptée à l'activité lors du redémarrage de la partition physique. Pour de plus amples informations sur la configuration du domaine logique, consultez la section « Managing Domain Configurations » dans le *Oracle VM Server for SPARC Administration Guide* de la version que vous utilisez.

Enregistrement des informations de configuration du domaine logique

Exécutez la commande `ldm` d'Oracle VM Server pour SPARC avec la sous-commande `spconfig` spécifiée pour enregistrer les informations de configuration du domaine logique.

```
primary# ldm add-spconfig config_name
```

Pour `config_name`, spécifiez le nom du fichier utilisé pour sauvegarder les informations de configuration du domaine logique vers le XSCF.

Remarque : la sous-commande `add-spconfig` ne peut pas substituer les informations de configuration dans un fichier existant. Avant de spécifier le nom d'un fichier existant pour `config_name`, vous devez supprimer le fichier présent en utilisant la sous-commande `remove-spconfig`.

Affichage des informations de configuration du domaine logique

Vous pouvez afficher les informations de configuration du domaine logique sur le domaine de commande d'une partition physique ou sur le XSCF maître.

- Affichage des informations sur le domaine de commande d'une partition physique
Exécutez la commande `ldm` d'Oracle VM Server pour SPARC avec la sous-commande `list-spconfig` spécifiée pour afficher les informations de configuration du domaine logique enregistrées sur le domaine de commande.

```
primary# ldm list-spconfig
```


- Affichage des informations sur le Shell XSCF
Affichez les informations de configuration de domaine logique enregistrée sur le Shell XSCF avec la commande `showdomainconfig` du microprogramme de XSCF.

```
XSCF> showdomainconfig -p ppar_id
```

Pour `ppar_id`, spécifiez le PPAR-ID de la partition physique pour les informations de configuration du domaine logique enregistré que vous souhaitez afficher. Vous pouvez spécifier uniquement un seul nombre entier entre 0 et 15, en fonction de la configuration du système.

Procédure de fonctionnement

1. **Passez du Shell XSCF à la console du domaine de commande de la partition physique cible.**
Pour plus de détails sur le passage à la console du domaine de commande, consultez « [8.3 Passage à la console du domaine de commande depuis le shell XSCF](#) ».
2. **Affichez les informations de configuration du domaine logique enregistrées avec la commande `ldm set-spconfig`.**

```
primary# ldm list-spconfig
```

3. **Exécutez la commande `ldm add-spconfig` pour sauvegarder l'état du domaine logique comme informations de configuration.**
L'exemple suivant montre que le fichier nommé `ldm_set1` est la destination de sauvegarde.

```
primary# ldm add-spconfig ldm_set1
```

4. **Exécutez la commande `ldm list-spconfig` et vérifiez que les informations de configuration ont été correctement sauvegardées.**

```
primary# ldm list-spconfig
```

10.11.2 Restauration des informations de configuration du domaine logique

Lors du redémarrage d'une partition physique, vous pouvez spécifier des informations de configuration du domaine logique à partir d'une liste de configurations enregistrées pour la partition physique. Cette fonction peut être utilisée lorsque vous souhaitez redémarrer avec une configuration de domaine logique différente de la configuration actuelle.

Remarque : pour restaurer des informations de configuration de domaine logique, les informations de configuration de domaine logique doivent avoir été enregistrées à l'avance. Pour plus de détails, consultez « [10.11.1 Sauvegarde/Affichage des informations de réglage du domaine logique](#) ».

Restauration des informations de configuration du domaine logique sauvegardées

Exécutez la commande `setdomainconfig` du microprogramme XSCF (voir ci-dessous) pour restaurer les informations de configuration du domaine logique enregistrée sur le domaine de commande.

```
XSCF> setdomainconfig -p ppar_id [-i index]
```

Pour `ppar_id`, indiquez le PPAR-ID de la partition physique. Vous pouvez spécifier uniquement un seul nombre entier entre 0 et 15, en fonction de la configuration du système. Pour l'`index`, indiquez le numéro de l'index des informations de configuration. En cas d'omission, vous pouvez indiquer un numéro d'index de façon interactive, tout en vérifiant la liste des informations de configuration sauvegardées.

Procédure de fonctionnement

1. **Exécutez la commande `setdomainconfig` et indiquez une configuration de domaine logique à utiliser lors du prochain démarrage de la partition physique.**
L'exemple suivant illustre la configuration du domaine logique de PPAR-ID 0 spécifiée de manière interactive lors d'une vérification de la liste des informations de configuration enregistrées.

```
XSCF> setdomainconfig -p 0
PPAR-ID      :0
Booting config
(Current)    :ldm-set2
(Next)       :ldm-set2
-----
Index        :1
config_name  :factory-default
domains      :1
date_created:-
-----
Index        :2
config_name  :ldm-set1
domains      :8
date_created:'2012-08-08 11:34:56'
-----
Index        :3
config_name  :ldm-set2
domains      :20
date_created:'2012-08-09 12:43:56'
-----
Select Index of Using config_name:2
PPAR-ID of PPARs that will be affected:00
```

```
Logical domain config_name will be set to "ldm-set1".
Continue? [y|n] :y
XSCF>
```

L'exemple suivant illustre le numéro d'index 1 indiqué pour PPAR-ID 0 pour spécifier des informations de configuration.

```
XSCF> setdomainconfig -p 0 -i 1
Index          :1
config_name    :factory-default
domains        :1
date_created:-
-----
PPAR-ID of PPARs that will be affected:00
Logical domain config_name will be set to "factory-default".
Continue? [y|n] : y
XSCF>
```

Restauration des domaines logiques à leur état lors de l'expédition de l'usine

Exécutez la commande `setdomainconfig` du microprogramme XSCF (voir ci-dessous) pour restaurer les informations de configuration du domaine logique enregistrée à leur état lors de l'expédition de l'usine.

```
XSCF> setdomainconfig -p ppar_id -c default
```

Pour `ppar_id`, indiquez le PPAR-ID de la partition physique. Vous pouvez spécifier uniquement un seul nombre entier entre 0 et 15, en fonction de la configuration du système. Pour restaurer l'état lors de l'expédition de l'usine, indiquez `-c default`.

Procédure de fonctionnement

1. **Exécutez la commande `setdomainconfig` et indiquez les informations de configuration à utiliser pour redémarrer le domaine logique.**
L'exemple suivant illustre la configuration du domaine logique de PPAR-ID 0 restaurée à son état lors de l'expédition de l'usine.

```
XSCF> setdomainconfig -p 0 -c default
PPAR-ID of PPARs that will be affected:00
Logical domain config_name will be set to "factory-default".
Continue? [y|n] : y
XSCF>
```

10.12 Sauvegarde / restauration des informations de configuration du domaine logique dans un fichier XML

Cette section décrit la procédure de sauvegarde des informations de configuration du domaine logique et de restauration de la configuration enregistrée dans un fichier XML.

Lorsque les informations enregistrées sur le XSCF sont perdues, restaurez le système avec un fichier XML.

10.12.1 Sauvegarde/Vérification des informations de configuration du domaine logique

Vous pouvez enregistrer les informations de configuration du domaine logique par partition physique dans un fichier XML. Pour sauvegarder les informations de configuration du domaine logique dans un fichier XML, connectez-vous au domaine de commande de la partition physique cible.

Pour de plus amples informations, consultez la section « Managing Domain Configurations » dans le *Oracle VM Server for SPARC Administration Guide* de la version que vous utilisez.

Enregistrement des informations de configuration du domaine logique

Exécutez la commande `ldm list-constraints -x` d'Oracle VM Server pour SPARC pour enregistrer les informations de configuration du domaine logique.

```
primary# ldm list-constraints -x > file_name.xml
```

Désignez un nom de fichier pour enregistrer les informations de configuration dans `file_name.xml`.

Procédure de fonctionnement

1. **Passez du Shell XSCF à la console du domaine de commande de la partition physique cible.**
Pour plus d'informations sur le passage à la console du domaine de commande, consultez « [8.3 Passage à la console du domaine de commande depuis le shell XSCF](#) ».
2. **Exécutez la commande `ldm list-spconfig` pour vérifier que les informations sur la configuration actuelle du domaine logique ont été enregistrées sur le XSCF.**

Remarque : la commande `ldm list-spconfig` liste les noms des informations de configuration

du domaine enregistré. Cela n'indique pas les heures de création, le nombre de domaines, ou si les informations de configuration enregistrées correspondent à la configuration actuelle du domaine. Un administrateur doit conserver un suivi des noms de fichiers de configuration enregistrés, des configurations qu'ils mappent et s'ils correspondent à la configuration actuelle du domaine logique. Vous pouvez aussi utiliser la commande `showdomainconfig` pour voir la date et l'heure de création et le nombre de domaines logiques dans chaque configuration enregistrée.

Dans l'exemple suivant, les informations sur la configuration actuelle sont définies sur `test1`.

Lorsque les informations sur la configuration actuelle ne sont pas stockées sur le XSCF, enregistrez les informations avec la commande `ldm add-spconfig`.

```
primary# ldm list-spconfig
factory-default
test1 [current]
test2
test3
```

3. **Exécutez `ldm list-constraints -x` et enregistrez les informations sur la configuration du domaine logique dans un fichier XML.**

L'exemple illustre la procédure d'enregistrement des informations dans `/ldm-set1.xml`.

```
primary# ldm list-constraints -x > /ldm-set1.xml
```

4. **Exécutez les commandes telles que `more` et vérifiez que les informations de configuration sont stockées dans le fichier XML.**

```
primary# more /ldm-set1.xml
<?xml version="1.0"?>
<LDM_interfaceversion="1.3" xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
```

Pour parer à la perte du fichier XML enregistré, sauvegardez le fichier sur un autre support.

Remarque : si une fonction virtuelle (VF) est attribuée à un domaine logique avec la fonction SR-IOV, exécutez la commande `ldm` pour enregistrer les informations définies pour chaque VF à l'avance.

10.12.2 Restauration des informations de configuration du domaine logique

Exécutez la commande `ldm init-system` pour refléter le réglage du fichier XML qui a été enregistré, et exécutez la commande `shutdown` pour redémarrer le domaine de

commande.

Restauration des informations de configuration du domaine logique sauvegardées

Pour restaurer les informations de configuration enregistrées dans le fichier XML, exécutez la commande `ldm init-system` command sur le domaine de commande telle qu'indiquée ci-dessous.

```
primary# ldm init-system -i file_name.xml
```

Procédure de fonctionnement

1. **Vérifiez que la configuration actuelle de domaine logique est la configuration par défaut.**

```
primary# ldm list-config | grep "factory-default"
factory-default [current]
```

Si [current] n'est pas affiché adjacent à factory-default, la configuration actuelle de domaine logique n'est pas la configuration par défaut. Dans ce cas, procédez comme suit pour modifier la configuration actuelle du domaine logique aux valeurs par défaut.

Spécifiez factory-default et exécutez la commande `ldm set-spconfig`.

```
primary# ldm set-spconfig factory-default
```

Exécutez la commande `poweroff` du microprogramme de XSCF pour mettre hors tension la partition physique.

```
XSCF> poweroff -p ppar_id
```

2. **Exécutez la commande `ldm init-system` pour refléter le réglage du fichier XML enregistré.**

Cet exemple affiche la procédure de restauration des informations sur la configuration enregistrées dans `/ldm-set1.xml`.

```
primary# ldm init-system -i /ldm-set1.xml
Initiating a delayed reconfiguration operation on the primary
domain.
All configuration changes for other domains are disabled until
the primary
domain reboots, at which time the new configuration for the
primary domain
will also take effect.
```

3. **Exécutez la commande `shutdown` pour redémarrer le domaine de commande.**

```
primary# shutdown -y -g0 -i6
```

4. **Liez la ressource à un domaine logique autre que le domaine de commande pour démarrer le domaine.**

Dans l'exemple suivant, la ressource est liée à ldom1 pour démarrer le domaine.

```
primary# ldm bind ldom1
primary# ldm start ldom1
```

10.13 Enregistrement/Restauration des variables d'environnement d'OpenBoot PROM

Pour restaurer les informations de configuration de domaine logique depuis un fichier XML, enregistrez et sauvegardez les variables d'environnement d'OpenBoot PROM dans le domaine de commande avant de passer les domaines logiques à la configuration par défaut.

Après être passé à la configuration par défaut, restaurez les variables d'environnement d'OpenBoot PROM en utilisant les informations enregistrées.

Lors de l'enregistrement/la restauration des variables d'environnement d'OpenBoot PROM, vérifiez les variables d'environnement d'OpenBoot PROM en exécutant la commande printenv d'OpenBoot PROM et enregistrez le contenu. Puis utilisez la commande setenv pour restaurer.

10.13.1 Sauvegarde des variables d'environnement d'OpenBoot PROM

Cette section décrit la procédure de sauvegarde des variables d'environnement d'OpenBoot PROM.

1. **Exécutez la commande printenv pour vérifier les variables d'environnement d'OpenBoot PROM.**

```
{0} ok printenv
Variable Name      Value      Default Value
ttya-rts-dtr-off   false     false
ttya-ignore-cd     true      true
keyboard-layout
reboot-command
security-mode       none      No default
security-password   No default
```

security-#badlogins	1	No default
diag-switch?	false	false
local-mac-address?	false	true
fcode-debug?	false	false
scsi-initiator-id	7	7
oem-logo		No default
oem-logo?	false	false
oem-banner		No default
oem-banner?	false	false
ansi-terminal?	true	true
screen-#columns	80	80
screen-#rows	34	34
ttya-mode	9600,8,n,1,-	9600,8,n,1,-
output-device	virtual-console	virtual-console
input-device	virtual-console	virtual-console
auto-boot-on-error?	false	false
load-base	16384	16384
auto-boot?	false	true
os-root-device		
network-boot-arguments	host-ip=192.168.123.100, ...	
boot-command	boot	boot
boot-file		
boot-device	mydisk1 mydisk2 mydisk3 ...	disk net
multipath-boot?	false	false
boot-device-index	0	0
use-nvramrc?	true	false
nvramrc	devalias mydisk1 /pci@80 ...	
error-reset-recovery	boot	boot
{0} ok		

2. **Sauvegardez le résultat de sortie dans un texte.**
3. **S'il existe une variable avec une valeur remplacée par « ... » dans l'étape 1, exécutez la commande `printenv` avec la variable correspondante spécifiée.**
L'exemple suivant vérifie la variable `boot-device`.

```
{0} ok printenv boot-device
boot-device = mydisk1 mydisk2 mydisk3 mynet
```

L'exemple suivant vérifie les réglages `nvramrc`.

```
{0} ok printenv nvramrc
nvramrc = devalias mydisk1 /pci@80000/pci@4/pci@0/pci@0/scsi@
0/disk@p3,0:a
devalias mydisk2 /pci@8100/pci@4/pci@0/pci@0/scsi@
0/disk@p0,0:a
devalias mydisk3 /pci@8100/pci@4/pci@0/pci@0/scsi@
0/disk@p1,0:a
devalias mynet /pci@8000/pci@4/pci@0/pci@9/network@0
h# 8 value video-mode
```

L'exemple suivant vérifie les réglages `network-boot-arguments`.


```
{0} ok printenv network-boot-arguments
network-boot-arguments = host-ip=192.168.123.100,subnet-mask=255.255.255.
0,iscsi-target-ip=192.168.100.10,iscsi-target-name=iqn.2016-12.com.fujitsu:02:
iscsiboot,iscsi-lun=0
```

4. **Sauvegardez le résultat de sortie à l'étape 3 dans un fichier texte.**

10.13.2 Restauration des variables d'environnement d'OpenBoot PROM

Cette section décrit la procédure de restauration des variables d'environnement d'OpenBoot PROM.

- Lors d'une restauration autre que nvramrc

1. **Vérifiez les variables d'environnement d'OpenBoot PROM sauvegardées dans un fichier texte.**
2. **Exécutez la commande `setenv` pour restaurer les valeurs et la commande `printenv` pour vérifier le contenu.**

Si vous comptez restaurer les informations du domaine logique à l'aide d'un fichier XML, réglez `auto-boot?` sur « `false` » et `security-mode` sur « `none` » avant de lancer le prochain redémarrage.

L'exemple suivant restaure `local-mac-address?` sur « `false` ».

```
{0} ok setenv local-mac-address? false
local-mac-address? = false
{0} ok printenv local-mac-address?
local-mac-address? = false
```

L'exemple suivant restaure `boot-device` sur « `mydisk1 mydisk2 mydisk3 mynet` ».

```
{0} ok setenv boot-device mydisk1 mydisk2 mydisk3 mynet
boot-device = mydisk1 mydisk2 mydisk3 mynet
{0} ok printenv boot-device
boot-device = mydisk1 mydisk2 mydisk3 mynet
```

L'exemple suivant restaure `use-nvramrc?` sur « `true` ».

```
{0} ok setenv use-nvramrc? true
use-nvramrc? = true
{0} ok printenv use-nvramrc?
use-nvramrc? = true
```

- Lors de la restauration de nvramrc

1. **Vérifiez les variables d'environnement d'OpenBoot PROM sauvegardées dans un fichier texte.**
2. **Exécutez la commande nvedit pour régler une valeur sur nvramrc.**
L'exemple suivant écrit le contenu vérifié à l'étape 1 sur nvramrc.

```
{0} ok nvedit
0: devalias mydisk1 /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p3,0:a
1: devalias mydisk2 /pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p0,0:a
2: devalias mydisk3 /pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p1,0:a
3: devalias mynet /pci@8000/pci@4/pci@0/pci@9/network@0
4: h# 8 value video-mode
5:
```

3. **Appuyez sur [Ctrl] et [C] pour quitter nvedit et retournez à l'invite ok.**
4. **Exécutez la commande nvstore pour enregistrer la modification.**

```
{0} ok nvstore
```

5. **Exécutez la commande printenv pour vérifier si nvramrc a été correctement écrit.**

```
{0} ok printenv nvramrc
nvramrc =                devalias mydisk1 /pci@8000/pci@4/pci@0/pci@0/scsi@
0/disk@p3,0:a            devalias mydisk2 /pci@8100/pci@4/pci@0/pci@0/scsi@
0/disk@p0,0:a            devalias mydisk3 /pci@8100/pci@4/pci@0/pci@0/scsi@
0/disk@p1,0:a            devalias mynet /pci@8000/pci@4/pci@0/pci@9/network@0
                          h# 8 value video-mode
```

6. **Si la variable d'environnement d'OpenBoot PROM auto-boot? est « true », exécutez la commande setenv pour la régler sur « false ».**

```
{0} ok setenv auto-boot? false
```

7. **Exécutez la commande reset-all pour redémarrer OpenBoot PROM.**

```
{0} ok reset-all
```

8. **Démarrez ensuite Oracle Solaris et restaurez les informations du domaine logique à l'aide d'un fichier XML.**
Ceci permet la restauration des variables d'environnement d'OpenBoot PROM dans tous les domaines logiques, sauf security-password, dans la partition

physique comprenant le domaine de commande.

Pour plus de détails sur la restauration des informations de configuration du domaine logique à l'aide d'un fichier XML, consultez « [10.12 Sauvegarde / restauration des informations de configuration du domaine logique dans un fichier XML](#) ».

Pour les domaines logiques avec security-mode réglé sur command ou full, demandez à l'administrateur du système de régler security-password.

10.14 Sauvegarde / Restauration du contenu d'un disque dur

Il est important d'effectuer des sauvegarde régulière du contenu d'un disque dur pour parer à une perte de données critiques, telles que d'une panne du disque dur.

Les systèmes SPARC M12/M10 prennent en charge les configurations redondantes de disque avec la fonction RAID matérielle. La configuration redondante de disque rend le fonctionnement du système beaucoup plus fiable.

Pour parer à une éventuelle perte des données résultant des défaillances de plusieurs disques de données, il est nécessaire d'effectuer des sauvegardes régulières du contenu des disques durs.

Étudiez les méthodes de sauvegarde appropriées au système et mettez-les en place. Les méthodes de sauvegarde et de restauration du contenu du disque dur peuvent varier en fonction de la méthode de sauvegarde en place. Utilisez une méthode qui convient à la méthode de sauvegarde mise en place.

10.15 Réinitialisation d'un domaine logique

Exécutez la commande reset du microprogramme XSCF pour réinitialiser le domaine logique spécifié.

Exécutez la commande avec un compte d'utilisateur disposant du privilège platadm ou fieldeng. Vous pouvez également l'exécuter avec un compte d'utilisateur disposant du privilège de pparadm ou pparmgr pour la partition physique à laquelle appartient le domaine logique cible.

Remarque : la commande de réinitialisation forçant la réinitialisation de la partition physique peut provoquer la défaillance d'un disque, etc. N'utilisez cette commande qu'en cas d'urgence, par exemple lors d'une restauration d'Oracle Solaris suite à une panne.

```
XSCF> reset -p ppar_id -g domainname sir | panic
```

Pour `ppar_id`, indiquez le PPAR-ID de la partition physique à laquelle le domaine logique à réinitialiser appartient. Vous pouvez spécifier uniquement un seul nombre entier entre 0 et 15, en fonction de la configuration du système.
Pour `domainname`, spécifiez le nom du domaine logique à réinitialiser.
Pour réinitialiser le domaine logique elle-même, précisez `sir`. Pour provoquer une panique dans Oracle Solaris sur le domaine logique, spécifiez `panic`.

Procédure de fonctionnement

1. **Exécutez la commande `reset` pour réinitialiser le domaine logique spécifié. Répondez « y » au message de confirmation.**

L'exemple suivant réinitialise le domaine invité `ldom1` de PPAR-ID 00.

```
XSCF> reset -p 0 -g ldom1 sir
PPAR-ID:00 GuestDomain to sir:ldom1
Continue? [y|n] : y
00 ldom1 :Resetting

*Note*
This command only issues the instruction to reset.
The result of the instruction can be checked by the
"showdomainstatus".
XSCF>
```

2. **Exécutez la commande `showdomainstatus` et vérifiez que le domaine logique spécifié a été réinitialisé.**

L'exemple suivant vérifie les états des domaines logiques de PPAR-ID 0.
`OpenBoot initializing` ou `OpenBoot Running` apparaît pour `Status`, qui affiche ensuite éventuellement `Solaris` en cours d'exécution.

```
XSCF> showdomainstatus -p 0
```

10.16 Génération d'une panique dans un domaine logique

Cette section décrit la procédure de génération d'une panique dans un domaine logique spécifié.

Après une panique dans le domaine logique cible lorsque le domaine logique a une augmentation de charge anormale, ou le domaine logique est en panne, un fichier de vidage est collecté.

10.16.1 Génération d'une panique dans un domaine invité

Exécutez la commande `ldm panic-domain` d'Oracle VM Server pour SPARC à partir du domaine de commande pour générer une panique dans le domaine invité spécifié. Pour plus de détails sur la commande `ldm`, consultez le *Oracle VM Server for SPARC Reference Manual* de la version utilisée.

Remarque : la commande `ldm panic-domain` forçant une panique dans le domaine invité spécifié peut provoquer la défaillance d'un disque, etc. N'utilisez cette commande qu'en cas d'urgence, etc.

```
primary# ldm panic-domain ldom
```

Pour `ldom`, spécifiez le nom du domaine invité où la panique s'est produite.

Remarque : vous pouvez également générer une panique dans un domaine invité à l'aide de la commande de réinitialisation du microprogramme XSCF. Pour plus de détails, consultez la page du manuel correspondant à la commande `reset(8)` ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

10.16.2 Génération d'une panique dans un domaine de commande

Exécutez la commande `reset` du microprogramme XSCF pour causer une panique dans le domaine de commande spécifié.

Exécutez la commande avec un compte d'utilisateur disposant du privilège `platadm` ou `fieldeng`. Vous pouvez également l'exécuter avec un compte d'utilisateur disposant du privilège de `pparadm` ou `pparmgr` pour la partition physique cible.

Remarque : la commande `reset` forçant une panique dans le domaine de commande spécifié peut provoquer la défaillance d'un disque, etc. N'utilisez cette commande qu'en cas d'urgence, etc.

```
XSCF> reset -p ppar_id -g primary panic
```

Pour `ppar_id`, indiquez l'ID de partition physique associée au domaine de commande (le domaine appartient à la partition) où la panique se produira. Vous pouvez spécifier un nombre entier entre 0 et 15, en fonction de la configuration du système.

La commande `reset` est ignorée lorsque la source d'alimentation est hors tension et tandis que le domaine de commande est arrêté.

Procédure de fonctionnement

1. **Exécutez la commande `reset` pour provoquer une panique dans le domaine de commande spécifié.**

L'exemple suivant entraîne une panique dans le domaine de commande de la partition physique ID 0.

```
XSCF> reset -p 0 -g primary panic
PPAR-ID:00
GuestDomain to panic:primary
Continue? [y|n] : y
00 primary :Resetting

*Note*
This command only issues the instruction to reset.
The result of the instruction can be checked by the
"showdomainstatus".
XSCF>
```

2. **Exécutez la commande `showdomainstatus` pour vérifier qu'une panique s'est produite dans le domaine de commande spécifié.**

```
XSCF> showdomainstatus -p 0
```

10.17 Reconfiguration d'une partition physique

Exécutez la commande `reset` du microprogramme XSCF pour réinitialiser la partition physique spécifiée.

Exécutez la commande avec un compte d'utilisateur disposant du privilège `platadm` ou `fieldeng`. Vous pouvez également l'exécuter avec un compte d'utilisateur disposant du privilège de `pparadm` ou `pparmgr` pour la partition physique cible.

Remarque : la commande de réinitialisation forçant la réinitialisation de la partition physique peut provoquer la défaillance d'un disque, etc. N'utilisez cette commande qu'en cas d'urgence, par exemple lors d'une restauration d'Oracle Solaris suite à une panne.

```
XSCF> reset -p ppar_id por | xir
```

Pour `ppar_id`, spécifiez le PPAR-ID de la partition physique à réinitialiser. Vous pouvez spécifier uniquement un seul nombre entier entre 0 et 15, en fonction de la configuration du système.

Pour réinitialiser la partition physique elle-même, indiquez por. Pour réinitialiser tous les processeurs de la partition physique, indiquez xir.

Remarque : si la partition physique est réinitialisée avec la commande xir spécifiée et que le vidage du superviseur est activée, un vidage du superviseur est collecté, et les domaines logiques démarrent avec la configuration par défaut après la réinitialisation. Pour restaurer la configuration de domaine logique avant la réinitialisation de la partition physique, mettez hors tension la partition physique puis remettez-le sous tension. Pour plus de détails sur la fonction de vidage du superviseur, consultez « [8.13 Collecte d'un fichier de vidage du superviseur](#) ».

Si la fonction de démarrage automatique pour le domaine de commande, telle que définie par la commande setpparparam est désactivée lorsque la commande de réinitialisation est exécutée, le traitement s'arrête avant le démarrage d'Oracle Solaris.

Procédure de fonctionnement

1. **Exécutez la commande reset pour réinitialiser la partition physique spécifiée. Répondez « y » au message de confirmation.**

L'exemple suivant réinitialise PPAR-ID 00.

```
XSCF> reset -p 0 por
PPAR-ID to reset:00 Continue? [y|n] : y
00 :Resetting

*Note*
This command only issues the instruction to reset.
The result of the instruction can be checked by the "showpparprogress".
XSCF>
```

2. **Exécutez la commande showpparprogress et vérifiez que le domaine physique spécifié a été réinitialisé.**

```
XSCF> showpparprogress -p 0
PPAR Power On Preprocessing PPAR#0 [ 1/12]
PPAR Power On                PPAR#0 [ 2/12]
XBBOX Reset                  PPAR#0 [ 3/12]
PSU On                       PPAR#0 [ 4/12]
CMU Reset Start              PPAR#0 [ 5/12]
XB Reset 1                   PPAR#0 [ 6/12]
XB Reset 2                   PPAR#0 [ 7/12]
XB Reset 3                   PPAR#0 [ 8/12]
CPU Reset 1                  PPAR#0 [ 9/12]
CPU Reset 2                  PPAR#0 [10/12]
Reset released               PPAR#0 [11/12]
CPU Start                    PPAR#0 [12/12]
The sequence of power control is completed.
XSCF>
```

10.18 Restauration de l'état du serveur aux valeurs par défaut en vigueur à l'expédition

Cette section décrit la procédure de réinitialisation de l'état du SPARC M12/M10 aux valeurs par défaut.

Afin de restaurer les données sauvegardées des informations des réglages de XSCF dans le châssis du SPARC M12/M10 ou afin de restaurer les informations des réglages de XSCF aux valeurs par défaut, exécutez la commande `initbb` ou `restoredefaults` du microprogramme XSCF.



Attention - L'exécution de la commande supprime les informations de réglage de l'unité XSCF définies par l'utilisateur ainsi que les informations d'erreur ou les informations de sauvegarde de XSCF placées sur chaque châssis.

10.18.1 Compréhension des commandes d'initialisation

Les commandes `initbb` et `restoredefaults` ont les rôles suivants.

- **Commande `restoredefaults`**

Cette commande initialise le châssis XSCF maître. Cette commande initialise les informations de réglage de l'unité XSCF et ses informations de sauvegarde, ou initialise seulement les informations de réglage de l'unité XSCF.

- **Commande `initbb`**

Depuis le XSCF maître, cette commande initialise les informations d'un châssis autre que le châssis maître. Cette commande ne peut pas être utilisée sur des systèmes ne disposant que d'un XSCF.

Remarque : la commande `restoredefaults` restaure les informations des réglages de XSCF et celles de sauvegarde à leur état en vigueur lors de l'expédition de l'usine.

Remarque : si une clé d'activation du processeur n'a pas été enregistrée et que la commande `restoredefaults` est exécutée, la clé d'activation du processeur devra être réenregistrée.

10.18.2 Initialisation du serveur

Dans les systèmes avec un XSCF

Utilisez la commande `restoredefaults` pour initialiser le serveur.

Procédure de fonctionnement

1. **Établir une connexion série avec le XSCF.**
2. **Connectez-vous au XSCF.**
3. **Exécutez la commande poweroff -a pour arrêter le système.**
4. **Exécutez la commande restoredefaults pour initialiser le châssis (les informations de réglage de l'unité XSCF et celles de sauvegarde) ou les informations de réglage de l'unité XSCF.**

Remarque : pour plus de détails sur la procédure de spécification des options de la commande restoredefaults et les notes qui s'y rapportent, consultez la page du manuel de la commande restoredefaults(8) ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

Dans les systèmes avec plusieurs XSCF

Les conditions suivantes doivent être satisfaites pour l'initialisation.

- Chaque châssis est relié au réseau de XSCF.
- Si le PPAR-ID d'une partition physique en cours est le même que le BB-ID du châssis à initialiser, cette partition physique doit être mise hors tension.
- La PSB du châssis à initialiser doit être dans l'état de pool de cartes système.
- La PSB du châssis à initialiser ne doit pas appartenir à une PPAR.
- Si un boîtier à barre transversale autre que le XSCF maître doit être initialisée, exécutez la commande poweroff -a pour mettre le système complet hors tension.

Procédure de fonctionnement

1. **Pour initialiser le maître XSCF, exécutez la commande poweroff avec l'option-a spécifiée pour arrêter le système.**
2. **Établissez une connexion série avec le XSCF maître.**
3. **Connectez-vous au XSCF maître.**
4. **Initialisez le châssis cible en spécifiant sa BB-ID et en exécutant la commande initbb.**
Effectuez cette étape pour une cible autre que le maître.
Ensuite, pour initialiser le châssis principal, procédez comme suit.
5. **Exécutez la commande restoredefaults pour initialiser le châssis (les informations de réglage de l'unité XSCF et celles de sauvegarde) ou les informations de réglage de l'unité XSCF.**

Remarque : pour plus de détails sur la procédure de spécification des options de la commande initbb(8) et de celle de restoredefaults(8) avec les notes qui s'y rapportent, consultez la page du manuel de chaque commande ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

Remarque : pour plus de détails sur la connexion de câbles, consultez « Chapitre 4 Réglage du SPARC M12-2S dans une configuration de bloc de construction » dans le *Guide d'installation Fujitsu SPARC M12-2S* ou « Chapitre 4 Configuration des connexions des blocs de construction » dans le *Guide d'installation Fujitsu M10-4S/SPARC M10-4S*.

Remarque : pour plus de détails sur les informations complémentaires pour cette commande, consultez les dernières *Notes de produit* pour votre serveur.

10.19 Récupération d'un fichier de vidage d'incident à l'aide du vidage différé

Sur les versions XCP 2290 ou plus récentes et Oracle Solaris 11.2 SRU11.2.8.4.0 ou plus récente, le fichier de vidage d'incident peut être enregistré dans la mémoire sur la mémoire jusqu'à ce que le système soit redémarré après un incident du système. Pendant le redémarrage du système, le fichier de vidage d'incident est extrait de la mémoire sur le fichier système défini par la configuration de vidage.

Après l'écriture de ces fichiers, le système est automatiquement redémarré sur la configuration multi-utilisateur normale.

Ce processus est appelé le vidage différé. Lorsque le vidage différé est utilisé, le système peut revenir à l'état fonctionnel peu après l'évènement « kernel panic ». Pour plus de détails sur les fonctions de vidage différé, consultez le *Managing Devices* in *Oracle Solaris* de votre version Solaris.

Vérifier l'état du système

Ce chapitre décrit comment vérifier la configuration matérielle et l'état du système, ainsi que la configuration et l'état de la partition physique lors de la configuration ou du fonctionnement du système.

- [Vérifier la configuration et l'état du système](#)
- [Vérification d'une partition physique](#)

11.1 Vérifier la configuration et l'état du système

11.1.1 Vérification des éléments et des commandes liés à la configuration et à l'état du système

[Tableau 11-1](#) répertorie les éléments et les commandes du Shell XSCF pour vérifier la configuration et l'état du système.

Pour plus de détails sur des éléments individuels, consultez les sections suivantes.

Tableau 11-1 Commandes permettant de vérifier la configuration et l'état

Vérifier l'élément	Commande liée
Vérification des composants montés	showhardconf(8)
- Toutes les pièces montées dans le système	
- État du commutateur de mode	
Vérification des composants en panne/détériorés	showstatus(8)

Tableau 11-1 Commandes permettant de vérifier la configuration et l'état (*suite*)

Vérifier l'élément	Commande liée
Vérification des informations de l'environnement du système - Température ambiante - Tension - Vitesse du ventilateur - Consommation électrique - Évacuation d'air	showenvironment(8)
Vérification des informations de réglage de l'unité d'extension PCI	ioxadm(8)

11.1.2 Vérification des composants montés dans le système

Vous pouvez vérifier tous les composants montés dans le système et leur état en utilisant la commande `showhardconf`. La commande affiche un astérisque (*) pour marquer une pièce ayant un problème. L'administrateur système peut connaître la configuration du composant, le nombre d'unités montées, l'état du commutateur de mode et les unités remplaçables sur site (FRU).

Informations sur les composants

Tableau 11-2 répertorie les informations relatives à chaque composant du SPARC M12. Vous pouvez vérifier les détails du composant dans une structure hiérarchique en exécutant la commande `showhardconf`.

Tableau 11-2 Informations relatives à chaque composant du SPARC M12

Composant	Description
Information du système	Numéro de série, état du commutateur de mode, état d'alimentation du système, phase d'alimentation du système, état de la partition physique
Informations sur le SPARC M12-2/M12-2S	Nombre d'unités, état, rôle, version, numéro de série, nombre de FRU, type de source d'alimentation, capacité de la mémoire Le rôle peut être maître, en veille ou esclave.
Mémoire CPU (inférieure) Informations (CMUL) (SPARC M12-2/M12-2S)	État, version, numéro de série, nombre de FRU, capacité de la mémoire, type
Mémoire CPU (supérieure) Informations (CMUU) (SPARC M12-2/M12-2S)	État, version, numéro de série, nombre de FRU, capacité de la mémoire, type
Unité de la carte mère Informations (MBU) (SPARC M12-1)	État, version, numéro de série, nombre de FRU, capacité de la mémoire, type

Tableau 11-2 Informations relatives à chaque composant du SPARC M12 (*suite*)

Composant	Description
Informations sur le processeur	Nombre d'unités, état, version, numéro de série, fréquence du processeur, type de processeur, nombre de cœurs de processeur, nombre de threads physiques du processeur
Informations sur la mémoire (MEM)	Nombre d'unités, état, code, type (ID unique), capacité
Informations sur la norme PCI	Nombre d'unités, état, propriété du nom, ID du fournisseur, ID du périphérique, ID du fournisseur du sous-système, ID du sous-système, nombre de VPD, connexion, informations sur l'unité d'extension PCI
Informations sur l'unité d'extension PCI (PCIBOX)	Nombre d'unités, état, version, numéro de série, nombre de FRU Informations sur la carte d'E/S (IOB) : état, numéro de série, type, nombre de FRU Informations sur le panneau de liaison : état, version, numéro de série, nombre de FRU Informations PCI : nombre d'unités, propriété du nom, ID du fournisseur, ID du périphérique, ID du fournisseur de sous-système, ID du sous-système, nombre de VPD Informations du backplane du ventilateur (FANBP) : nombre d'unités, état, numéro de série, nombre de FRU Informations sur le fond de panier PSU (PSUBP) : nombre d'unités, état, numéro de série, nombre de FRU Informations sur l'unité d'alimentation (PSU) : nombre d'unités, état, numéro de série, nombre de FRU Informations sur l'unité de ventilateur (FAN) : nombre d'unités, état
Informations sur l'unité à barre transversale (XBU) (SPARC M12-2/M12-2S)	Nombre d'unités, état, version, numéro de série, nombre de FRU, type
Informations sur le câble à barre transversale (CBL)	Nombre d'unités, état, ID du fournisseur, version, type de câble, longueur
Informations sur l'unité XSCF (XSCFU)	État, version, numéro de série, nombre de FRU, type
Informations sur le panneau de commande (OPNL)	État, version, numéro de série, nombre de FRU, type
Informations sur le fond de panier PSU (PSUBP)	État, version, numéro de série, nombre de FRU, type
Informations sur l'unité d'alimentation (PSU)	Nombre d'unités, état, numéro de série, nombre de FRU, état d'alimentation, type d'alimentation, tension, type Le type d'alimentation est CA (courant alternatif).
Informations sur l'unité de ventilation (FANU)	Nombre d'unités, état, type
Informations sur le fond de panier du disque dur (HDDBP)	Nombre d'unités, état, type

Tableau 11-2 Informations relatives à chaque composant du SPARC M12 (*suite*)

Composant	Description
Informations sur le boîtier à barre transversale (XBBOX) (SPARC M12-2S)	Nombre d'unités, état, rôle, version, numéro de série, nombre de FRU, type de source d'alimentation Informations sur l'unité à barre transversale (XBU) : nombre d'unités, état, version, numéro de série, nombre de FRU, type Informations sur le câble à barre transversale (CBL) : nombre d'unités, état, nombre de FRU, version, type de câble, longueur Informations sur l'unité XSCF (XSCFU) : état, version, numéro de série, nombre de FRU Informations sur le panneau de commande (OPNL) : état, version, numéro de série, nombre de FRU Informations sur le fond de panier à barre transversale (XBBPU) : état, version, numéro de série, nombre de FRU, type Informations sur l'unité d'interface XSCF (XSCFIFU) : état, version, numéro de série, nombre de FRU, type

Tableau 11-3 répertorie les informations relatives à chaque composant du SPARC M10. Vous pouvez vérifier les détails du composant dans une structure hiérarchique en exécutant la commande `showhardconf`.

Tableau 11-3 Informations relatives à chaque composant du SPARC M10

Composant	Description
Information du système	Numéro de série, état du commutateur de mode, état d'alimentation du système, phase d'alimentation du système, état de la partition physique
Informations sur le système SPARC M10-4/M10-4S	Nombre d'unités, état, rôle, version, numéro de série, nombre de FRU, type de source d'alimentation, capacité de la mémoire Le rôle peut être maître, en veille ou esclave.
Informations sur l'unité de mémoire du processeur (inférieure) (CMUL) (SPARC M10-4/M10-4S)	État, version, numéro de série, nombre de FRU, capacité de la mémoire, type
Informations sur l'unité de mémoire du processeur (supérieure) (CMUL) (SPARC M10-4/M10-4S)	État, version, numéro de série, nombre de FRU, capacité de la mémoire, type
Informations sur l'unité de carte mère (MBU) (SPARC M10-1)	État, version, numéro de série, nombre de FRU, capacité de la mémoire, type
Informations sur le processeur	Nombre d'unités, état, version, numéro de série. Fréquence du processeur, type de processeur, nombre de cœurs de processeur, nombre de threads physiques du processeur

Tableau 11-3 Informations relatives à chaque composant du SPARC M10 (*suite*)

Composant	Description
Informations sur la mémoire (MEM)	Nombre d'unités, état, code, type (ID unique), capacité
Informations sur la norme PCI	Nombre d'unités, état, propriété du nom, ID du fournisseur, ID du périphérique, ID du fournisseur du sous-système, ID du sous-système, nombre de VPD, connexion, informations sur l'unité d'extension PCI
Informations sur l'unité d'extension PCI (PCIBOX)	Nombre d'unités, état, version, numéro de série, nombre de FRU Informations sur la carte d'E/S (IOB) : état, numéro de série, type, nombre de FRU Informations sur le panneau de liaison : version, numéro de série, nombre de FRU Informations PCI : nombre d'unités, propriété du nom, ID du fournisseur, ID du périphérique, ID du fournisseur de sous-système, ID du sous-système, nombre de VPD Informations du backplane du ventilateur (FANBP) : nombre d'unités, état, numéro de série, nombre de FRU Informations sur le fond de panier PSU (PSUBP) : nombre d'unités, état, numéro de série, nombre de FRU Informations sur l'unité d'alimentation (PSU) : nombre d'unités, état, numéro de série, nombre de FRU Informations sur l'unité de ventilateur (FAN) : nombre d'unités, état
Informations sur l'unité à barre transversale (XBU) (SPARC M10-4/M10-4S)	Nombre d'unités, état, version, numéro de série, nombre de FRU, type
Informations sur le câble à barre transversale (CBL)	Nombre d'unités, état, nombre de FRU, version, type de câble, longueur
Informations sur le panneau de commande (OPNL)	État, version, numéro de série, nombre de FRU
Informations sur l'unité XSCF (XSCFU)	État, version, numéro de série, nombre de FRU
Informations sur le fond de panier PSU (PSUBP)	État, version, numéro de série, nombre de FRU, type
Informations sur l'unité d'alimentation (PSU)	Nombre d'unités, état, numéro de série, nombre de FRU, état d'alimentation, type d'alimentation, tension, type Le type d'alimentation affiché est CA (courant alternatif) ou CC (courant continu).
Informations sur l'unité de ventilation (FANU)	Nombre d'unités, état, type

Tableau 11-3 Informations relatives à chaque composant du SPARC M10 (suite)

Composant	Description
Informations sur le boîtier à barre transversale (XBBOX) (SPARC M10-4S)	Nombre d'unités, état, rôle, version, numéro de série, nombre de FRU, type de source d'alimentation Informations sur l'unité à barre transversale (XBU) : nombre d'unités, état, version, numéro de série, nombre de FRU, type Informations sur le câble à barre transversale (CBL) : nombre d'unités, état, nombre de FRU, version, type de câble, longueur Informations sur l'unité XSCF (XSCFU) : état, version, numéro de série, nombre de FRU Informations sur le panneau de commande (OPNL) : état, version, numéro de série, nombre de FRU Informations sur le fond de panier à barre transversale (XBBPU) : état, version, numéro de série, nombre de FRU, type Informations sur l'unité d'interface XSCF (XSCFIFU) : état, version, numéro de série, nombre de FRU, type

Procédure de fonctionnement

1. **Exécutez la commande `showhardconf` pour vérifier la configuration du composant et l'état du commutateur de mode.**

L'exemple suivant affiche le système SPARC M10-1.

```
XSCF> showhardconf
SPARC M10-1;
+ Serial:2101151008A; Operator_Panel_Switch:Locked;
+ System_Power:On; System_Phase:Cabinet Power On;
  Partition#0 PPAR_Status:Powered Off;
MBU Status:Normal; Ver:0101h; Serial:7867000297;
+ FRU-Part-Number:CA20393-B50X A2 ;
+ Power_Supply_System:Single;
+ Memory_Size:16 GB;
CPU#0 Status:Normal; Ver:0201h; Serial:PP0629L068
+ Freq:2.800 GHz; Type:32;
+ Core:16; Strand:2;
MEM#00A Status:Normal;
:
```

2. **Exécutez la commande `showhardconf` pour vérifier le nombre de FRU montés.**

Dans l'exemple suivant, l'option `-u` est spécifiée pour afficher le nombre de FRU montés dans le système SPARC M10-1.

```
XSCF> showhardconf -u
SPARC M10-1; Memory_Size:16 GB;
+-----+-----+
| FRU                                     | Quantity |
+-----+-----+
| MBU                                     |         1 |
|           CPU                         |         1 |
```


	Freq:2.800 GHz;		(1)	
	MEM		16	
	Type:01; Size:4 GB;		(16)	
	PCIBOX		1	
	IOB		1	
	PSU		2	
	FAN		2	
	OPNL		1	
	PSUBP		1	
	PSU		2	
	FAN_A		2	
	-----		-----	

11.1.3 Vérification de l'environnement du système

La commande `showenvironment` affiche toutes les valeurs des capteurs du système. En connaissant la température d'admission du système, la tension et la vitesse du ventilateur, l'administrateur système peut vérifier les anomalies dans l'environnement de fonctionnement du système. De même, en connaissant la consommation électrique et l'évacuation d'air du système, le responsable du site peut identifier les réductions de consommation d'énergie potentielles sur les parties du site d'installation du système.

Procédure de fonctionnement

1. **Exécutez la commande `showenvironment` pour vérifier les informations de l'environnement du système et les tensions.**

L'exemple suivant affiche les températures d'admission.

```
XSCF> showenvironment
BB#00
    Temperature:30.71C
BB#01
    Temperature:29.97C
```

L'exemple suivant spécifie l'opérande `temp` pour afficher les températures des composants.

```
XSCF> showenvironment temp
BB#00
    Temperature:30.71C
    CMUU
        CPU#0
            CPU#0:45.21C
            CPU#0:45.42C
            CPU#0:43.24C
            CPU#0:47.11C
        CPU#1
            CPU#1:45.21C
            CPU#1:45.42C
```

```
CPU#1:43.24C
CPU#1:47.11C
```

```
...
```

L'exemple suivant spécifie l'opérande volt pour afficher les tensions des composants.

```
XSCF> showenvironment volt
MBU
  0.89V Power Supply Group:0.891V
  0.90V#0 Power Supply Group:0.898V
  0.90V#1 Power Supply Group:0.894V
  0.90V#2 Power Supply Group:1.023V
  0.90V#3 Power Supply Group:1.024V
  1.0V#0 Power Supply Group:1.038V
  1.0V#1 Power Supply Group:1.041V
  1.35V#0 Power Supply Group:1.346V
  1.35V#1 Power Supply Group:1.348V
  1.5V#0 Power Supply Group:1.539V
  1.5V#1 Power Supply Group:1.506V
  1.8V#0 Power Supply Group:1.804V
PSUBP
  3.3V Power Supply Group:3.300V
  5.0V Power Supply Group:5.000V
XSCF>
```

Température ambiante et vitesse du ventilateur

Du fait de la définition de l'altitude de l'emplacement de l'installation, la vitesse du ventilateur varie en fonction de la température ambiante. Plus la valeur de la vitesse du ventilateur est élevée, plus la vitesse du ventilateur est rapide.

Tableau 11-4 répertorie les vitesses du ventilateur affichées par la commande `showenvironment`, pour les températures ambiantes et les altitudes définies correspondantes.

Tableau 11-4 Vitesse du ventilateur selon l'altitude et la température ambiante (Valeurs communes au SPARC M12/M10)

Vitesse du ventilateur	Température ambiante en fonction de l'altitude			
	500 m ou moins	Entre 501 et 1000 m	Entre 1001 et 1500 m	Entre 1501 et 3000 m
Vitesse élevée (niveau-3 ->niveau-4)	31 °C ou plus	29°C ou plus	27°C ou plus	25°C ou plus
Vitesse intermédiaire (niveau-4 ->niveau-3)	29°C ou moins	27°C ou moins	25°C ou moins	23°C ou moins
Vitesse intermédiaire (niveau-2 ->niveau-3)	26°C ou plus	24°C ou plus	22°C ou plus	20°C ou plus
Vitesse faible (niveau-3 ->niveau-2)	24°C ou moins	22°C ou moins	20°C ou moins	18°C ou moins

Tableau 11-4 Vitesse du ventilateur selon l'altitude et la température ambiante (Valeurs communes au SPARC M12/M10) *(suite)*

Vitesse du ventilateur	Température ambiante en fonction de l'altitude			
	500 m ou moins	Entre 501 et 1000 m	Entre 1001 et 1500 m	Entre 1501 et 3000 m
Vitesse faible (niveau-1 ->niveau-2)	22°C ou plus	20°C ou plus	18°C ou plus	16°C ou plus
Vitesse faible (niveau-2 ->niveau-1)	20°C ou moins	18°C ou moins	16°C ou moins	14°C ou moins

Procédure de fonctionnement

1. **Exécutez la commande `showenvironment Fan` pour vérifier la vitesse du ventilateur.**
L'exemple suivant spécifie l'opérande Ventilateur pour afficher la vitesse du ventilateur des unités de ventilation.

```
XSCF> showenvironment Fan
BB#00
  FANU#0: Middle speed (Level-3)
    FAN#0: 14323rpm
    FAN#1: 14285rpm
  FANU#1: Middle speed (Level-3)
    FAN#0: 14173rpm
    FAN#1: 14285rpm
  FANU#2: Middle speed (Level-3)
    FAN#0: 14248rpm
    FAN#1: 14136rpm
  FANU#3: Middle speed (Level-3)
    FAN#0: 14099rpm
    FAN#1: 14062rpm
  FANU#4: Middle speed (Level-3)
    FAN#0: 14323rpm
    FAN#1: 14099rpm
```

Consommation électrique et évacuation d'air

Utilisez la fonction de surveillance de l'alimentation et l'indicateur d'évacuation d'air pour afficher la consommation électrique et l'évacuation d'air du système. La fonction de surveillance de l'alimentation et l'indicateur d'évacuation d'air permettent des vérifications régulières de la consommation d'énergie réelle par le système en fonctionnement, ainsi que le volume d'air évacué.

Utilisez la commande `showenvironment power` pour afficher la consommation d'énergie. La commande affiche la valeur de la consommation électrique du système, la valeur de la consommation électrique maximale (consommation électrique en CA autorisée) et la valeur de la consommation électrique réelle (consommation électrique en CA réelle) dans le châssis, etc. Si le type d'alimentation est le CC, la mention « ...DC power... » s'affiche à la place.

Remarque : dans les systèmes SPARC M12, la consommation électrique nominale « Available AC power consumption » dans le châssis est affichée.

Utilisez la commande `showenvironment air` pour afficher l'évacuation d'air. La fonction d'agent SNMP peut également être utilisée pour acquérir les informations de consommation électrique et d'évacuation d'air.

Pour acquérir les informations de consommation électrique et d'évacuation d'air par la fonction d'agent SNMP, installez le dernier fichier de définition de la MIB étendue de XSCF pour le gestionnaire de SNMP. Pour savoir où obtenir le fichier de définition de la MIB étendue du XSCF, consultez les dernières *Notes de produit* pour votre serveur ou les informations relatives au fichier de définition de la MIB situées sur le site de téléchargement du microprogramme.

Remarque : dans les cas suivants, les valeurs de la consommation électrique et de l'évacuation d'air peuvent ne pas être affichées correctement par les informations de la MIB, les commandes `showenvironment power` et `showenvironment air` et XSCF Web. Vérifiez de nouveau les valeurs après une minute.

- Pendant la mise sous/hors tension du système ou pendant un court instant après la mise sous/hors tension
 - Pendant le remplacement actif d'une unité d'alimentation ou pendant un court instant après le remplacement actif
-

Remarque : l'unité d'extension PCI et les périphériques d'E/S ne sont pas compris dans les informations de consommation électrique et d'évacuation d'air.

Procédure de fonctionnement

1. Exécutez la commande `showenvironment air` pour vérifier l'évacuation d'air du système.

L'exemple suivant spécifie l'opérande `air` pour afficher l'évacuation d'air du système.

```
XSCF> showenvironment air
BB#00
    Air Flow:306CMH
```

Remarque : l'unité du flux d'évacuation (CMH = m³/h) indique combien de mètres cubes d'air sont générés par heure.

2. Exécutez la commande `showenvironment power` pour vérifier la consommation électrique du système.

L'exemple suivant spécifie l'opérande `power` pour afficher les informations de consommation électrique. Le contenu de l'affichage indique, en partant du haut, la valeur de l'alimentation électrique maximale de l'unité d'alimentation (PSU) pour l'ensemble du système, la valeur de la consommation électrique minimale et la valeur de la consommation électrique maximale du système, suivies des

valeurs de la consommation électrique maximale et réelle du châssis.

```
XSCF> showenvironment power
Power Supply Maximum :5000W
Installed Hardware Minimum:1268W
Peak Permitted :2322W
BB#00
Permitted AC power consumption:5000W
Actual AC power consumption :1719W
```

Remarque : les valeurs des mesures du moniteur de l'alimentation et de l'indicateur d'évacuation d'air sont les valeurs de référence. Leurs valeurs varient en fonction de la charge du système.

11.1.4 Vérification des composants en panne/détériorés

En utilisant la commande `showstatus`, vous pouvez vérifier les unités et les composants en panne ou dégradés parmi les FRU qui composent le système. Une unité ou un composant dont l'état est en panne sont indiqués par un astérisque (*).

Il existe cinq types d'états comme indiqué dans [Tableau 11-5](#).

Tableau 11-5 État du composant

Composant	Signification
Faulted	La pièce en question est en panne, l'unité ne fonctionne donc pas.
Degraded	L'unité présente une panne partielle, mais l'unité continue à fonctionner.
Deconfigured	Du fait d'une panne ou d'une détérioration dans une autre unité, l'unité, dont les composants de niveau inférieur, est en état de détérioration, même si elle fonctionne normalement.
Maintenance	L'unité est en maintenance. Les commandes <code>replacefru</code> , <code>addfru</code> ou <code>initbb</code> sont en cours d'exécution.
Normal	L'unité est normale.

Procédure de fonctionnement

1. Exécutez la commande `showstatus` pour vérifier l'état du composant.

Une unité dont l'état est en panne est indiquée par un astérisque (*).

L'exemple suivant indique qu'un processeur et une mémoire sur la mémoire CPU (inférieure) de BB#00 et la PSU de XBBOX#80, ont été détériorés en raison de pannes.

```
XSCF> showstatus
BB#00;
    CMUL Status:Normal;
*      CPU#0 Status:Faulted;
*      MEM#00A Status:Faulted;
    XBBOX#80;
*      PSU#0 Status:Faulted;
```

L'exemple suivant indique que la mémoire de l'unité de la carte-mère a été détériorée en raison d'une panne.

```
XSCF> showstatus
    MBU Status:Normal;
*      MEM#0A Status:Faulted;
```

L'exemple suivant indique qu'une mémoire CPU a été détériorée en raison de la détérioration de l'unité à barre transversale.

```
XSCF> showstatus
BB#00
    CMUU Status:Normal;
*      CPU#1 Status:Deconfigured;
*      XBU#0 Status:Degraded;
```

Dans l'exemple suivant, aucune unité n'est détériorée.

```
XSCF> showstatus
No failures found in System Initialization.
```

Remarque : les informations concernant la panne et la détérioration d'un composant en panne ou détérioré sont supprimées par le remplacement de la pièce concernée. Pour la procédure de remplacement d'éléments, contactez un technicien sur site.

11.1.5 Affichage de l'état de l'unité d'extension PCI

Cette section décrit comment vérifier l'unité d'extension PCI connectée au système, les pièces de l'unité d'extension PCI, une carte de liaison montée dans un emplacement PCI intégré du système et l'état de l'unité d'extension PCI.

Vous pouvez vérifier l'état et les paramètres de l'unité d'extension PCI en utilisant la commande `ioxadm`.

Remarque : pour plus de détails sur la configuration matérielle de l'unité d'extension PCI, consultez « Chapitre 2 Understanding the PCI Expansion Unit Components » dans le *PCI Expansion Unit for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Service Manual*. Pour plus

Informations affichées

Tableau 11-6 résume les informations affichées par la commande ioxadm exécutée.

Tableau 11-6 Informations sur l'unité d'extension PCI affichées

Élément d'affichage	Description
Affichage de listes (list)	- Liste des chemins d'accès (host_path) entre l'unité d'extension PCI et les cartes de liaison montées dans les emplacements du châssis - Informations détaillées sur l'unité d'extension PCI - Informations détaillées sur les FRU (carte d'E/S, unité d'alimentation électrique, etc.) de l'unité d'extension PCI Les informations affichées comprennent le type de FRU, la version du microprogramme, le numéro de série, le numéro de la pièce et l'état.
Affichage de l'environnement (env)	- Conditions environnementales selon les valeurs de mesure des capteurs de l'unité d'extension PCI ou de la carte de liaison spécifiées - Informations environnementales sur les FRU de l'unité d'extension PCI ou les cartes montées dans les emplacements PCI Les informations affichées comprennent les éléments suivants : - Courant (A) - Tension (V) - Vitesse du ventilateur (tr/min) - Température (C) - État DEL - COMMUTATEUR
Affichage de la DEL de localisation (locator)	- États de la DEL de localisation de l'unité d'extension PCI spécifiée et de chaque élément de l'unité d'extension PCI Les états de la DEL de localisation sont les suivants : - Clignotante - Activée - Désactivée
Résultat de la comparaison de version (versionlist)	Affiche la version du microprogramme de l'unité d'extension PCI, la version de microprogramme de la carte de liaison de la destination de la connexion, et le résultat de la comparaison de ces microprogrammes. Les résultats possibles de la comparaison sont les suivants. - equal - mismatch

Affichage de listes

La procédure pour afficher une liste de l'unité d'extension PCI, des cartes d'E/S, des cartes de liaison et des unités d'alimentation est décrite ci-dessous.

1. **Exécutez la commande ioxadm pour vérifier les cartes de liaison et l'unité d'extension PCI.**
Dans l'exemple suivant, une liste de toutes les unités d'extension PCI et toutes les cartes de liaison est affichée.

```
XSCF> ioxadm list
PCIBOX          Link
PCIBOX#0033 BB#00-PCI#1
PCIBOX#12B4 BB#01-PCI#0
```

L'exemple suivant affiche une seule unité d'extension PCI.

```
XSCF> ioxadm list PCIBOX#12B4
PCIBOX          Link
PCIBOX#12B4 BB#01-PCI#0
```

L'exemple suivant utilise `host_path` pour afficher les cartes en mode d'émission détaillé avec les en-têtes masqués.

```
XSCF> ioxadm -A -v list BB#00-PCI#1
BB#00-PCI#1 F20 - 000004 5111500-01 On
```

Affichage de l'environnement

La procédure pour afficher l'environnement en utilisant les valeurs de mesure des capteurs est décrite ci-dessous.

1. Exécutez la commande `ioxadm` pour vérifier les informations d'environnement.

L'exemple suivant affiche les valeurs mesurées par les capteurs pour la température, la tension, le courant, la vitesse du ventilateur, etc.

```
XSCF> ioxadm env -te PCIBOX#A3B4
Location Sensor Value Res Units

PCIBOX#A3B4/PSU#0 FAN 3224.324 - RPM
PCIBOX#A3B4/PSU#1 FAN 3224.324 - RPM
PCIBOX#A3B4/FAN#0 FAN 3522.314 - RPM
PCIBOX#A3B4/FAN#1 FAN 3522.314 - RPM
PCIBOX#A3B4/FAN#2 FAN 3522.314 - RPM
PCIBOX#A3B4/FAN#0 FAN 3522.314 - RPM
PCIBOX#A3B4/IOBT T_INTAKE 32.000 - C
PCIBOX#A3B4/IOBT T_PART_NO1 32.000 - C
PCIBOX#A3B4/IOBT T_PART_NO2 32.000 - C
PCIBOX#A3B4/IOBT T_PART_NO3 32.000 - C
PCIBOX#A3B4/IOBT V_12_0V 12.400 - V
PCIBOX#A3B4/IOBT V_3_3_NO0 3.320 - V
PCIBOX#A3B4/IOBT V_3_3_NO1 3.310 - V
PCIBOX#A3B4/IOBT V_3_3_NO2 3.310 - V
PCIBOX#A3B4/IOBT V_3_3_NO3 3.320 - V
PCIBOX#A3B4/IOBT V_1_8V 1.820 - V
PCIBOX#A3B4/IOBT V_0_9V 0.910 - V
```

L'exemple suivant affiche toutes les valeurs de mesure des capteurs relatives à une liaison.


```
XSCF> ioxadm -A env BB#00-PCI#1
BB#00-PCI#1 LINK On - LED
BB#00-PCI#1 MGMT On - LED
```

Affichage de l'emplacement

La procédure pour afficher les états de la DEL de localisation de l'unité d'extension PCI et des pièces spécifiées est décrite ci-dessous.

1. **Exécutez la commande ioxadm pour vérifier l'état de l'unité d'extension PCI.**
L'exemple suivant affiche l'état de la DEL de localisation de l'unité d'extension PCI.

```
XSCF> ioxadm locator PCIBOX#12B4
Location          Sensor      Value Resolution Units
PCIBOX#12B4       LOCATE    Blink -          LED
```

Résultat de la comparaison de version

La méthode d'affichage de la version du microprogramme de l'unité d'extension PCI, de la version de microprogramme de la carte de liaison de la destination de la connexion, et du résultat de la comparaison de ces microprogrammes, est la suivante.

1. **Exécutez la commande ioxadm pour confirmer la version de microprogramme de l'unité d'extension PCI, la version de microprogramme de la carte de liaison de la destination de la connexion, et le résultat de la comparaison.**
Dans l'exemple suivant, le résultat de la comparaison de toutes les unités d'extension PCI et toutes les cartes de liaison est affiché.

```
XSCF> ioxadm versionlist
PCIBOX      Ver. Link      Ver. Info
PCIBOX#0033 1010 BB#00-PCI#1 1010 equal
* PCIBOX#12B4 1010 BB#00-PCI#0 1011 mismatch
```

11.2 Vérification d'une partition physique

11.2.1 Vérification des éléments et des commandes liés à la configuration/à l'état des partitions physiques et des domaines logiques

Tableau 11-7 répertorie les éléments et les commandes du shell XSCF permettant de vérifier la configuration/l'état de la partition physique, l'état des blocs de construction

(PSB) et l'état du domaine logique. Pour plus de détails sur des éléments individuels, consultez les sections suivantes.

Tableau 11-7 Commandes permettant de vérifier la configuration et l'état

Vérifier l'élément	Commande liée
Vérification des informations de configuration de la partition physique - PPAR-ID - Numéro de LSB - Numéro de PSB - Stratégie de configuration - Disponibilité de l'E/S - Disponibilité de la mémoire	showpcl(8)
Vérification de l'état de fonctionnement de la partition physique	showpparstatus(8), showpcl(8)
Vérifier le réglage de la PSB - Emplacement (PSB, processeur) - Mode de mise en miroir de la mémoire	showfru(8)
Vérifier l'état de la PSB	showboards(8)
Vérification de l'état du domaine logique	showdomainstatus(8) Commandes d'Oracle VM Server pour SPARC

Remarque : pour plus de détails sur les paramètres/la configuration/l'état de la partition physique et la configuration de domaines logiques depuis une partition physique, consultez le *Guide de configuration du domaine Fujitsu SPARC M12 et Fujitsu M10/SPARCM10*.

11.2.2 Vérification de la configuration de la partition physique

La commande showpcl affiche les informations de configuration pour chaque partition physique ou chaque carte système logique composant la partition physique. L'administrateur système fait référence à une PCL (liste de configuration de la partition physique) lors de l'incorporation d'une carte système logique dans une partition physique.

Vous pouvez consulter la PCL de la partition physique spécifiée à l'aide de la commande showpcl.

Le mappage entre les cartes de système logique (LSB) sur la partition physique et les cartes de système physique (PSB) est déterminé par les informations de la PCL.

[Figure 11-1](#) illustre un exemple de mappage PCL.

PSB fait référence à la ressource matérielle pour configurer une partition physique. Spécifiez (ou affichez) une PSB en format xx-y. xx est BB-ID et y est fixé à 0.

Figure 11-1 Image du mappage entre des cartes de système logique et des cartes de système

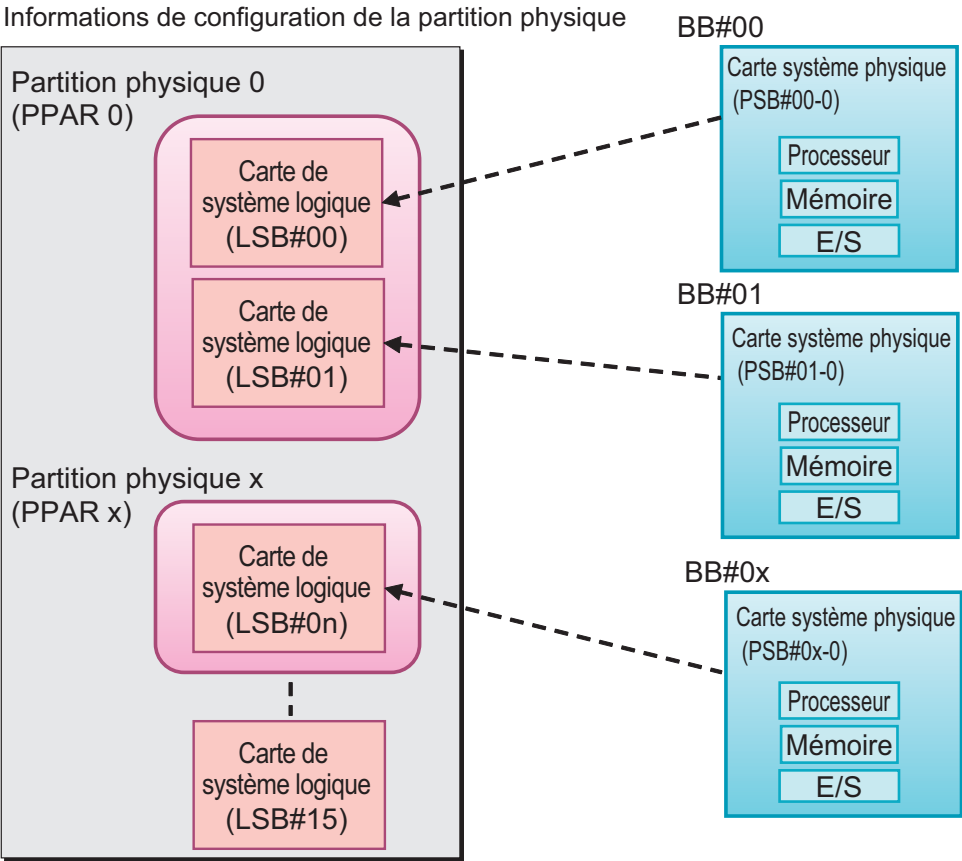


Tableau 11-8 décrit les termes liés aux partitions physiques.

Tableau 11-8 Termes liés aux partitions physiques

Terme	Description
Carte système physique (PSB)	PSB est l'acronyme de physical system board (carte système physique). La PSB est constituée de composants physiques (processeur, mémoire et E/S) montés dans un châssis SPARC M12/M10. Dans le SPARC M12-1/M10-1, une carte système physique est une unité de carte-mère. Dans le SPARC M12-2/M12-2S/M10-4/M10-4S, une carte système physique est une unité de mémoire de processeur (comprenant une unité inférieure (CMUL) et supérieure (CMUU)). Une carte système physique peut être utilisée en tant qu'unité représentant un châssis, en maintenance pour ajouter/supprimer/remplacer un châssis SPARC M12/M10. Pour un système dans une configuration de bloc de construction, une carte système physique fait référence à un bloc de construction (BB).

Tableau 11-8 Termes liés aux partitions physiques (*suite*)

Terme	Description
Carte de système logique (LSB)	LSB est l'acronyme de logical system board (carte de système logique). Les noms d'unités logiques sont attribués à une PSB. Un ensemble de cartes de système logique est attribué à chaque partition physique. Avec un numéro de PSB attribué aux cartes de système logique dans la partition physique, elles peuvent être reconnues dans le système. Les numéros de LSB sont utilisés pour contrôler l'attribution de ressources, telles que la mémoire, à la partition physique.
Configuration d'une partition physique	Ce terme correspond au partitionnement des ressources matérielles du système en unités indépendantes pour le fonctionnement du logiciel. Une partition physique est un cluster de PSB et le système est composé d'une ou plusieurs partitions physiques. Une partition physique est configurée à l'aide du XSCF comme suit. 1. Attribuez les numéros de LSB à la PSB. 2. Attribuez la PSB à une partition physique. 3. La partition physique fonctionne avec les ressources et les numéros de la LSB.
Informations de configuration de la partition physique	Ce terme correspond aux informations des ressources matérielles configurées pour chaque partition physique ou chaque LSB composant la partition physique. Les commandes setpcl et showpcl peuvent définir et afficher respectivement la PCL.
Stratégie de configuration	Cette stratégie peut spécifier l'unité des ressources logiques à détériorer pour chaque partition physique quand une erreur est détectée dans un diagnostic matériel initial. La stratégie de configuration spécifie une PSB ou des ressources distinctes en tant que plage de détérioration.
E/S désactivée (no-io)	Ce terme fait référence au moment où l'utilisation logique de l'unité d'E/S sur la PSB est désactivée dans la partition physique.
Mémoire désactivée (no-mem)	Ce terme fait référence au moment où l'utilisation logique de la mémoire sur la PSB est désactivée dans la partition physique.
État de la PSB	Cet état de chaque PSB indique l'état de l'alimentation (power), l'état du diagnostic (test), l'état de l'attribution (assignment), l'état de l'incorporation (connection), l'état de fonctionnement (configuration) et l'état de détérioration (fault). Vous pouvez être informé de l'avancement du changement de l'état de la PSB dans la partition physique. Vous pouvez consulter les informations d'état de la PSB à l'aide des commandes showpcl et showboards.
Pool de cartes système (SP)	Ce terme fait référence à l'état des BB (PSB) qui n'appartiennent pas à une partition physique. Dans le cas d'une partition physique ayant une importante charge de processeur ou de mémoire, un BB (PSB) peut être ajouté à cette partition physique. Lorsque la carte système n'est plus nécessaire, elle peut être retournée au pool de cartes système.

Une PCL est une liste de définition pour définir les informations pour une LSB. Vous pouvez définir les informations de la LSB pour 16 LSB au maximum par partition physique.

Tableau 11-9 répertorie les détails des informations de configuration de la partition physique. La stratégie de configuration peut uniquement être définie dans les systèmes SPARC M12-2/M10-1/M10-4.

Tableau 11-9 PCL

Terme	Description
PPAR-ID	ID d'une PPAR
Numéro de LSB	Numéro de LSB
Numéro de PSB	Numéro de PSB attribué à une LSB. Le même numéro de PSB ne peut pas être attribué à une autre LSB dans la même partition physique.
no-mem (Option d'invalidation de la mémoire)	True : la mémoire ne peut pas être utilisée False : la mémoire peut être utilisée (valeur par défaut)
no-io (Option d'invalidation de l'E/S)	True : E/S non incorporée False : E/S incorporée (valeur par défaut)
Stratégie de configuration	FRU : la détérioration est effectuée en unités pour les unités remplaçables sur site (FRU). (Par défaut) PSB : la détérioration est effectuée en unités de PSB. Système : les partitions physiques sont mises hors tension, dans les unités des partitions physiques, sans détérioration.
État de la partition physique	Ceci indique l'état de fonctionnement de la partition physique, par exemple si l'alimentation est désactivée ou si l'initialisation de POST est terminée. Pour des définitions plus détaillées, consultez la page du manuel correspondant à la commande showpcl(8) ou le <i>Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual</i> .

Procédure de fonctionnement

1. **Exécutez la commande showpcl pour vérifier les informations PCL.**
L'exemple suivant affiche les informations PCL définies pour PPAR-ID 00.

XSCF> showpcl -p 0			
PPAR-ID	LSB	PSB	Status
00			Running
	00	00-0	
	04	01-0	
	08	02-0	
	12	03-0	

L'exemple suivant affiche les informations PCL définies pour PPAR-ID 00 en détail.

XSCF> showpcl -v -p 0						
PPAR-ID	LSB	PSB	Status	No-Mem	No-IO	Cfg-policy
00			Running			System
	00	-				
	01	-				
	02	-				
	03	-				
	04	01-0		False	False	
	05	-				
	06	-				
	07	-				
	08	02-0		True	False	
	09	-				
	10	-				
	11	-				
	12	03-0		False	True	
	13	-				
	14	-				
	15	-				

Remarque : pour plus de détails sur les configurations de partition physique, consultez le *Guide de configuration du domaine Fujitsu SPARC M12 et Fujitsu M10/SPARCM10*.

11.2.3 Vérification de l'état de fonctionnement de la partition physique

Vous pouvez consulter l'état de fonctionnement de la partition physique, dont l'état de déconnexion ou d'initialisation de l'alimentation, à l'aide de la commande `showpparstatus`. Vous pouvez obtenir les mêmes informations en utilisant « `Status` » de la commande `showpcl`.

Remarque : pour plus de détails sur l'état de fonctionnement de la partition physique, consultez la page du manuel pour la commande `showpparstatus(8)` ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

Remarque : vous pouvez vérifier l'état des domaines logiques dans une partition physique à l'aide de la commande `showdomainstatus`. Pour plus de détails, consultez « [11.2.6 Vérification de l'état du domaine logique](#) ».

Remarque : pour plus de détails sur l'état de partition physique, consultez le *Guide de configuration du domaine Fujitsu SPARC M12 et Fujitsu M10/SPARCM10*.

Procédure de fonctionnement

La procédure pour consulter l'état de fonctionnement de la partition physique est

décrite ci-dessous.

1. **Exécutez la commande `showpparstatus` pour vérifier l'état de la partition physique.**

L'exemple suivant affiche l'état de fonctionnement de toutes les partitions physiques.

```
XSCF> showpparstatus -a
PPAR-ID PPAR Status
00      Powered Off
01      Initialization Phase
02      Initialization Phase
03      Running
```

11.2.4 Vérification des réglages du mode de mise en miroir de la mémoire

Utilisez la commande `showfru` pour vérifier les réglages du mode de mise en miroir de la mémoire. Vous pouvez consulter le contenu suivant en fonction d'une PSB utilisée pour configurer une partition physique.

- **Device**
sb : vous pouvez vérifier le BB (PSB).
Exemple : 00-0 : PSB du BB-ID 0
cpu : vous pouvez vérifier le processeur installé sur le BB.
Exemple : 00-0-2 : processeur#2 sur la PSB du BB-ID 0
- **Mode de mise en miroir de la mémoire**
Vous pouvez vérifier l'état des réglages du mode de mise en miroir de la mémoire, qui peut être défini pour chaque processeur.
yes : mode de mise en miroir de la mémoire
no : pas de mode de mise en miroir de la mémoire

Remarque : pour les paramètres/détails du mode de mise en miroir de la mémoire, consultez « [Chapitre 14 Configuration d'un système hautement fiable](#) ».

Procédure de fonctionnement

1. **Exécutez la commande `showfru` pour vérifier les informations du périphérique.**
L'exemple suivant affiche les informations définies pour tous les périphériques.

```
XSCF> showfru -a
Device    Location    Memory Mirror Mode
sb        00-0
  cpu     00-0-0    yes
  cpu     00-0-1    yes
```

	cpu	00-0-2	yes
	cpu	00-0-3	yes
sb		01-0	
	cpu	01-0-0	yes
	cpu	01-0-1	yes
	cpu	01-0-2	yes
	cpu	01-0-3	yes
sb		02-0	
	cpu	02-0-0	no
	cpu	02-0-1	no
	cpu	02-0-2	no
	cpu	02-0-3	no
sb		03-0	
	cpu	03-0-0	yes
	cpu	03-0-1	yes
	cpu	03-0-2	no
	cpu	03-0-3	no
:			

L'exemple suivant spécifie l'opérande sb pour afficher les informations définies pour la PSB spécifique.

XSCF> showfru sb 01-0			
Device	Location	Memory	Mirror Mode
sb	01-0		
	cpu	01-0-0	yes
	cpu	01-0-1	yes
	cpu	01-0-2	yes
	cpu	01-0-3	yes

L'exemple suivant spécifie l'opérande cpu pour afficher les informations définies pour le processeur spécifique.

XSCF> showfru cpu 01-0-3			
Device	Location	Memory	Mirror Mode
sb	01-0		
	cpu	01-0-3	yes

11.2.5 Vérification de l'état de la PSB

Une carte système (PSB) fait référence à un châssis SPARC M12/SPARC M10. Vous pouvez vérifier l'état d'alimentation de la PSB (power), l'état de diagnostic (test) et l'état de détérioration (fault) en exécutant la commande showboards. Dans une configuration de bloc de construction, après avoir exécuté la commande addboard ou deleteboard, respectivement pour configurer ou pour déconnecter une PSB dans une partition physique, vous pouvez être informé de l'avancement de cette opération, tel que le succès ou l'échec de l'opération, à l'aide de la commande showboards. L'avancement est un état tel que l'attribution de la PSB à la partition physique (assignment), l'état de configuration/déconnexion (connection) ou l'état de

fonctionnement (configuration).

En utilisant la commande `showboards`, vous pouvez vérifier l'état d'alimentation de la PSB (power), l'état du diagnostic (test), l'état d'attribution (assignment), l'état de configuration (connection), l'état de fonctionnement (configuration) et l'état de détérioration (fault).

Remarque : pour plus de détails sur l'état de la PSB, consultez le *Guide de configuration du domaine Fujitsu SPARC M12 et Fujitsu M10/SPARCM10*, la page du manuel pour la commande `showboards(8)` ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

Procédure de fonctionnement

La procédure pour consulter l'état de la PSB est décrite ci-dessous.

1. **Exécutez la commande `showboards` pour vérifier l'état de la PSB.**
L'exemple suivant affiche l'état de toutes les PSB.

```
XSCF> showboards -a
```

PSB	PPAR-ID(LSB)	Assignment	Pwr	Conn	Conf	Test	Fault
00-0	00(00)	Assigned	y	y	y	Passed	Normal
01-0	SP	Unavailable	n	n	n	Testing	Normal
02-0	Other	Assigned	y	y	n	Passed	Degraded
03-0	SP	Unavailable	n	n	n	Failed	Faulted

L'exemple suivant affiche les informations détaillées pour PSB 00-0.

```
XSCF> showboards 00-0
```

PSB	PPAR-ID(LSB)	Assignment	Pwr	Conn	Conf	Test	Fault
00-0	00(00)	Assigned	y	y	y	Passed	Normal

L'exemple suivant affiche la PSB qui se trouve dans le pool des cartes système et définie pour PPAR-ID 00.

```
XSCF> showboards -p 0 -c sp
```

PSB	PPAR-ID(LSB)	Assignment	Pwr	Conn	Conf	Test	Fault
01-0	SP	Available	n	n	n	Passed	Normal

11.2.6 Vérification de l'état du domaine logique

Vous pouvez consulter l'état de fonctionnement d'Oracle Solaris sur le domaine de commande dans une partition physique, l'état OpenBoot PROM sur le domaine de commande, etc. à l'aide de la commande `showdomainstatus`.

Remarque : pour des définitions détaillées de l'état de fonctionnement du domaine logique, consultez la page du manuel pour la commande `showdomainstatus(8)` ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*. Vous pouvez également consulter l'état du domaine logique avec la commande `ldm list-domain` d'Oracle VM Server pour SPARC. Pour plus de détails sur la commande `ldm`, consultez le *Oracle VM Server for SPARC Reference Manual* de la version utilisée.

Procédure de fonctionnement

La procédure pour consulter l'état de fonctionnement du domaine logique est décrite ci-dessous.

1. **Exécutez la commande `showdomainstatus` pour vérifier l'état de fonctionnement des domaines logiques appartenant à la partition physique spécifiée.**
L'exemple suivant affiche l'état de fonctionnement de tous les domaines logiques de PPAR-ID 0.

```
XSCF> showdomainstatus -p 0
Logical Domain Name  Status
primary              Solaris running
guest00              Solaris running
guest01              Solaris booting
guest02              Solaris powering down
guest03              Solaris panicking
guest04              Shutdown Started
guest05              OpenBoot initializing
guest06              OpenBoot Primary Boot Loader
```

L'exemple suivant affiche l'état de fonctionnement du domaine logique de PPAR-ID 0 nommé « `guest01` ».

```
XSCF> showdomainstatus -p 0 -g guest01
Logical Domain Name  Status
guest01              Solaris powering down
```

Chapitre 12

Consultation des journaux et des messages

Ce chapitre décrit les types de journaux et de messages affichés et stockés sur les systèmes, et les commandes pour référencer les journaux et les messages.

- [Consultation d'un journal enregistré par le XSCF](#)
- [Consultation des messages d'avertissement et de notification](#)

12.1 Consultation d'un journal enregistré par le XSCF

Cette section décrit comment consulter les informations du journal XSCF.

Les informations du journal XSCF servent à identifier les problèmes du système. L'administrateur système, les administrateurs de domaine et les techniciens sur site peuvent consulter les informations du journal. Ils peuvent être informés de l'état de fonctionnement et d'utilisation du serveur ainsi que des détails sur les anomalies qui se sont produites.

12.1.1 Vérification des types de journaux et commandes de référence

Les journaux collectés/gérés par le système comprennent les journaux liés aux informations sur les pannes, les journaux d'enregistrement des événements, les journaux liés à la sécurité et les journaux liés à l'environnement du serveur.

Cette section décrit les différents types de journaux.

Type de journal

Ces systèmes collectent les types suivants de journaux, qui peuvent être référencés par l'administrateur système.

- Journaux liés aux informations sur les pannes
 - Journal de gestion des pannes (journal FM) (*1)
 - Journal d'erreurs
 - Syslog (*1)
 - Journal de messages de surveillance

*1 Ce journal peut uniquement être référencé sur Oracle Solaris. Pour plus d'informations, consultez les manuels relatifs à Oracle Solaris.
- Journaux d'enregistrement d'événements
 - Journal d'alimentation
 - Journal des événements
 - Journal de la console
 - Journal de panique
 - Journal IPL
- Journaux liés à la sécurité et à l'authentification
 - Journal d'audit
 - Journal de CoD
 - Journal Active Directory
 - Journal LDAP sur SSL
- Journal lié à l'environnement du serveur
 - Journal de l'historique de la température

Présentations et méthodes de référence des journaux

Tableau 12-1 répertorie les types, les présentations et les méthodes de référence des journaux liés aux informations sur les pannes. Pour plus de détails sur les commandes XSCF, consultez la page du manuel correspondant à chaque commande ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*. Pour plus de détails sur chaque type de journal, consultez les sections suivantes.

Tableau 12-1 Journaux liés aux informations sur les pannes

Type de journal	Description	Taille (Taille de l'entrée)/ <Durée de stockage standard> Archivage	Destination de l'affichage de sortie/ Méthode de référence
Journal de gestion des pannes (journal FM)	Journal des erreurs, notifications et pannes s'étant produites dans le système.		Domaine/ fmdump
Journal d'erreur	Journal des erreurs, notifications et pannes s'étant produites dans le système. Le format d'affichage du journal est spécifique à la plate-forme.	Environ 1 024 générations (longueur variable) <Quantité pour environ 1 mois> Archivé	XSCF/ showlogs(8) XSCF Web

Tableau 12-1 Journaux liés aux informations sur les pannes (*suite*)

Type de journal	Description	Taille (Taille de l'entrée)/ <Durée de stockage standard> Archivage	Destination de l'affichage de sortie/ Méthode de référence
Syslog (SYSLOG)	Journal enregistrant les messages émis par Oracle Solaris. En cas de panne, une présentation de celle-ci est produite.		Domaine/ Utilisez une commande Oracle Solaris pour le consulter.
Journal des messages de surveillance (Journal des messages de surveillance)	Journal enregistrant les messages du XSCF signalant les anomalies	512 Ko, environ 10 000 lignes	XSCF/ showlogs(8) XSCF Web

Remarque : les journaux affichés par les commandes d'Oracle Solaris ne sont pas archivés.

Tableau 12-2 répertorie les types, les présentations et les méthodes de référence des journaux pour l'enregistrement des événements.

Tableau 12-2 Journaux d'enregistrement d'événements

Type de journal	Description	Taille (Taille de l'entrée)/ <Durée de stockage standard> Archivage	Méthode de référence
Journal d'alimentation (Journal d'alimentation)	Journal d'enregistrement des événements d'alimentation serveur	1 920 générations (x 16 o) <Quantité pour environ 1 mois> Archivé	showlogs(8) XSCF Web
Journal des événements (Journal des événements XSCF)	Journal enregistrant les opérations du système, du panneau de commande et les notifications d'événements émises à Oracle Solaris.	4 096 générations (x 48 o) <Quantité pour environ 1 mois> Archivé	showlogs(8) XSCF Web

Tableau 12-2 Journaux d'enregistrement d'événements *(suite)*

Type de journal	Description	Taille (Taille de l'entrée)/ <Durée de stockage standard> Archivage	Méthode de référence
Journal de la console (Journal de la console)	Journal enregistrant les messages de la console du domaine de commande. Mettre hors tension efface le journal.	512 Ko/PPAR, environ 10 000 lignes/PPAR <Quantité pour environ 1 semaine> Archivé	showlogs(8) XSCF Web
Journal de panique (Journal de panique)	Journal de la console en cas de panique	1 génération, 64 Ko/PPAR (environ 1 200 lignes) <Quantité pour 1 occurrence> Archivé	showlogs(8) XSCF Web
Journal IPL (Journal IPL)	Journal de la période comprise entre la mise sous tension et le démarrage effectif d'Oracle Solaris	1 génération, 32 Ko/PPAR, environ 600 lignes/PPAR <Quantité pour 1 occurrence> Archivé	showlogs(8) XSCF Web

Tableau 12-3 répertorie les types, les présentations et les méthodes de référence des journaux liés à la sécurité.

Tableau 12-3 Journaux liés à la sécurité

Type de journal	Description	Taille (Taille de l'entrée)/ <Durée de stockage standard> Archivage	Méthode de référence
Journal d'audit (Journal d'audit)	Journal lié aux audits XSCF	4 Mo <Quantité pour environ 1 mois> Archivé	viewaudit(8) XSCF Web
Journal CoD (Journal d'activation de CoD)	Journal des ajouts et des suppressions des activations de CPU	1 024 générations (x 32 Ko) Licence par cœur Archivé	showcodactivationhistory(8) XSCF Web

Tableau 12-3 Journaux liés à la sécurité (suite)

Type de journal	Description	Taille (Taille de l'entrée)/ <Durée de stockage standard> Archivage	Méthode de référence
Journal Active Directory	Un journal de messages pour diagnostiquer l'authentification et l'autorisation de l'Active Directory.	250 Ko (environ 3 000 lignes) Non archivé	showad(8) XSCF Web
Journal LDAP sur SSL (Journal LDAP sur SSL)	Un journal de messages pour diagnostiquer l'authentification et l'autorisation du LDAP sur SSL.	250 Ko (environ 3 000 lignes) Non archivé	showldapssl(8) XSCF Web

Tableau 12-4 répertorie les types, les présentations et les méthodes de référence des journaux liés à l'environnement du serveur.

Tableau 12-4 Journal lié à l'environnement du serveur

Type de journal	Description	Taille (Taille de l'entrée)/ <Durée de stockage standard> Archivage	Méthode de référence
Journal de l'historique de la température (Historique de la température et de l'humidité)	Journal lié à l'environnement avec un historique de température du serveur	16 384 générations (x 16 o) (toutes les 10 minutes) <Quantité pour environ 1 an> Archivé	showlogs(8) XSCF Web

Remarque : si le journal est plein, le journal est écrasé en commençant par les données de journal les plus anciennes.

12.1.2 Comment afficher le journal

Cette section décrit comment afficher les informations dans chaque journal XSCF.

Vérification du journal sur le shell XSCF ou XSCF Web

La procédure commune pour référencer chaque journal est décrite ci-dessous.

1. **Vérifiez les privilèges utilisateur nécessaires pour référencer les journaux.**
Les privilèges d'utilisateur de chaque journal se trouvent dans [Tableau 12-5](#).

Tableau 12-5 Privilèges utilisateur nécessaires pour référencer les journaux

Type de journal	Privilège utilisateur nécessaire
Journal d'erreur	platadm, platop, fieldeng
Journal des messages de surveillance	platadm, platop, fieldeng
Journal d'alimentation	platadm, platop, pparadm, pparmgr, fieldeng
Journal des événements	platadm, platop, fieldeng
Journal de la console	platadm, platop, pparadm, pparmgr, pparop, fieldeng
Journal de panique	platadm, platop, pparadm, pparmgr, pparop, fieldeng
Journal IPL	platadm, platop, pparadm, pparmgr, pparop, fieldeng
Journal d'audit	auditadm, auditop
Journal COD	platadm, platop, fieldeng
Journal de l'historique de la température	platadm, platop, fieldeng
Journal Active Directory	useradm
Journal LDAP sur SSL	useradm

2. **Spécifiez le nom d'hôte ou l'adresse IP pour se connecter au terminal du Shell XSCF ou à XSCF Web.**
3. **Spécifiez un compte utilisateur XSCF disposant du privilège utilisateur nécessaire et un mot de passe pour vous connecter au XSCF.**
4. **Exécutez la commande pour consulter le journal correspondant ou sélectionnez cette opération depuis le menu.**
5. **Consultez le journal.**

Remarque : pour plus d'informations sur le menu de XSCF Web, consultez « [Annexe C](#)
[Liste des pages de XSCF Web](#) ».

12.1.3 Consultation du journal d'erreur

Le journal d'erreur est un journal lié aux informations sur les pannes. Utilisez la commande showlogs avec l'opérande d'erreur spécifiée afin de consulter le journal pour une notification ou une panne s'étant produite dans le système.

Utilisation des scénarios

Les scénarios pour utiliser le journal d'erreur sur le XSCF sont décrits ci-dessous.

- Un message a été émis à la console du domaine, au terminal du Shell XSCF ou à XSCF Web, ainsi le journal est utilisé pour vérifier si une panne s'est produite.
- Une notification a été envoyée à l'adresse e-mail déjà enregistrée, ainsi le journal est utilisé pour rechercher des informations sur la panne.

- Un trap a été généré par le gestionnaire SNMP, ainsi le journal est utilisé pour rechercher des informations sur la panne.

Procédure de fonctionnement

1. Exécutez la commande **showlogs error** avec l'opérande **error** spécifiée sur le shell **XSCF**.

```
XSCF> showlogs error
Date: Oct 20 17:45:31 JST 2012
Code: 00112233-444555666777-888999aaabbbcccddeeefff
Status: Warning Occurred: Oct 20 17:45:31.000 JST 2012
FRU: /PSU#1
Msg: ACFAIL occurred (ACS=3) (FEP type = A1)
Date: Oct 20 17:45:31 JST 2012
Code: 00112233-444555666777-888999aaabbbcccddeee000
Status: Alarm Occurred: Oct 20 17:45:31.000 JST 2012
FRU: /PSU#1
Msg: ACFAIL occurred (ACS=3) (FEP type = A1)
```

Le contenu suivant est affiché dans l'exemple ci-dessus.

- Heure enregistrée (Date) consignée dans le journal pour le problème
Elle est indiquée dans l'heure locale.
- DIAGCODE, que les techniciens sur site et les techniciens de maintenance utilisent pour le dépannage
(Code)

Remarque : les utilisateurs doivent indiquer ce code à un technicien sur site ou à un technicien de maintenance. Ce code permet de trouver une solution rapide au problème.

- Niveau de panne (État) de la pièce
L'un des éléments suivants est affiché :
Alarm : panne ou erreur de la partie concernée
Warning : détérioration partielle ou avertissement de la partie concernée
Information : notification
Notice : notification de l'état du système
- Heure à laquelle le problème s'est produit (Occurred)
Elle est indiquée dans l'heure locale.
- Pièce de rechange peut-être en panne (FRU)
Si la première, deuxième et troisième pièces les plus susceptibles d'être en panne sont affichées, elles sont délimitées par une virgule (,). S'il y a d'autres pièces susceptibles d'être en panne, un astérisque (*) est affiché après la dernière virgule (,). Chaque pièce est présentée de façon hiérarchique dans le format du chemin d'accès du montage de la pièce. La détermination d'afficher la deuxième pièce et les suivantes les plus susceptibles d'être en panne dépend de l'emplacement de la panne détectée.

Les cas suivants indiquent la signification du contenu « FRU: » affiché.

a. « /PSU#0,/PSU#1 » est affiché.

PSU#0 et PSU#1 ont été détectés respectivement comme la première et la deuxième pièces les plus susceptibles d'être en panne. Ceci signifie que chacune des pièces devra peut-être être remplacée en fonction de son état.

b. « /BB#1/XBU#0/CBL#0R,/XBBOX#80/XBU#0,/BB#1/XBU#0,* » est affiché.

CBL#0R entre BB#1 et XBBOX#80, XBU#0 dans XBBOX#80, et XBU#0 dans BB#1 ont été détectés respectivement comme la première, deuxième et troisième pièces les plus susceptibles d'être en panne, avec d'autres pièces également détectées comme telles. Ceci signifie que chacune des pièces devra peut-être être remplacée en fonction de son état.

c. « /BB#0/PCI#3 » s'affiche.

BB#0/PCI#3 a été détecté comme une pièce susceptible d'être en panne et l'emplacement PCI 3 du BB-ID 0 a un problème. Ceci signifie que le périphérique connecté à l'emplacement PCI 3 devra peut-être être remplacé en fonction de son état.

d. "/MBU/MEM#02A" s'affiche.

/MBU/MEM#02A a été détecté comme une pièce susceptible d'être en panne et l'emplacement mémoire 02A de l'unité de carte mère a un problème. Ceci signifie que l'emplacement mémoire 02A devra peut-être être remplacé en fonction de son état.

e. "/BB#0/CMUL/MEM#02A" s'affiche.

/BB#0/CMUL/MEM#02A a été détecté comme une pièce susceptible d'être en panne et l'emplacement de mémoire 02A de la mémoire CPU (inférieure) du BB-ID 0 a un problème. Ceci signifie que l'emplacement mémoire 02A devra peut-être être remplacé en fonction de son état.

f. "/BB#0/CMUL/MEM#02A-03A" s'affiche.

/BB#0/CMUL/MEM#02A-03A a été détecté comme une pièce susceptible d'être en panne et les emplacements de mémoire 02A et 02B de la mémoire CPU (inférieure) du BB-ID 0 ont des problèmes. Ceci signifie que les mémoires des emplacements mémoire 02A et 02B devront peut-être être remplacées en même temps, en fonction de leur état.

- Message d'une ligne résumant un problème (Msg)

Remarque : pour plus de détails sur la commande `showlogs(8)`, consultez les pages du manuel ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

12.1.4 Consultation du journal des messages de surveillance

Les événements qui se sont produits sur le système sont affichés en temps réel sous forme de messages de surveillance pour les utilisateurs qui se sont connectés au XSCF. Le microprogramme XSCF collecte ces messages dans le journal des messages

de surveillance. Utilisez la commande showlogs avec l'opérande monitor spécifiée pour consulter le journal des messages de surveillance.

Procédure de fonctionnement

1. **Exécutez la commande showlogs avec l'opérande monitor spécifiée sur le shell XSCF.**

```
XSCF> showlogs monitor
Oct 20 17:45:31 monitor message: xxxxxxxx
Oct 20 17:55:31 monitor message: xxxxxxxx
```

Le contenu suivant s'affiche.

- Heure de collecte du journal de messages de surveillance (Date)
Elle est indiquée dans l'heure locale.
- Message de surveillance (Message)

12.1.5 Consultation du journal d'alimentation

Le journal d'alimentation est collecté quand une opération d'alimentation ou de réinitialisation est effectuée sur ces systèmes. Utilisez la commande showlogs avec l'opérande power spécifiée pour consulter le journal d'alimentation.

Procédure de fonctionnement

1. **Exécutez la commande showlogs avec l'opérande power spécifiée sur le shell XSCF.**

L'exemple suivant affiche le journal d'alimentation.

```
XSCF> showlogs power
Date           Event           Cause           ID Switch
Oct 20 17:25:31 JST 2012 Cabinet Power On Operator        00 Service
Oct 20 17:35:31 JST 2012 PPAR Power On Operator        00 Locked
Oct 20 17:45:31 JST 2012 PPAR Power Off Software Request 00 Locked
Oct 20 17:50:31 JST 2012 Cabinet Power Off Self Reset    00 Service
```

L'exemple suivant spécifie les heures de début et de fin pour afficher le journal d'alimentation dans une liste, classée de la plus récente à la plus ancienne.

```
XSCF> showlogs power -t Oct2017:302012 -T Oct2017:492012 -r
Date           Event           Cause           ID Switch
Oct 20 17:45:31 JST 2012 PPAR Power Off Software Request 00 Locked
Oct 20 17:35:31 JST 2012 PPAR Power On Operator        00 Locked
```

Remarque : la mise en page de l'exemple de commande peut changer sans préavis, afin d'en améliorer le fonctionnement.

Le contenu suivant est affiché dans l'exemple ci-dessus.

- Heure de collecte du journal d'alimentation (Date)
Elle est indiquée dans l'heure locale.
- Type d'événement d'alimentation survenu (Event)
La table suivante répertorie les événements d'alimentation (Event) et leurs significations.

Événement	Signification
SCF Reset :	Le redémarrage ou la réinitialisation de XSCF a été effectué.
PPAR Power On :	La partition physique a été mise sous tension.
PPAR Power Off :	La partition physique a été mise hors tension.
PPAR Reset :	La partition physique a été réinitialisée.
Cabinet Power On :	Le serveur a été mis sous tension.
Cabinet Power Off :	Le serveur a été mis hors tension.
XIR :	Une réinitialisation XIR a été effectuée.

- Facteur causant une instruction d'événement d'alimentation (Cause)
Le tableau suivant répertorie les causes (Cause) et leurs significations.

Cause	Signification
Self Reset :	Le redémarrage de XSCF a été effectué.
Power On :	Un redémarrage de XSCF a été effectué en raison de la mise sous tension.
System Reset :	Une réinitialisation XSCF a été effectuée en raison d'une panne détectée.
Panel :	L'utilisation d'un commutateur du panneau de commande est à l'origine d'un événement d'alimentation.
Scheduled :	Un paramétrage du minuteur TOD est à l'origine d'un événement d'alimentation.
IPMI :	Un périphérique d'E/S connecté à la RCIL est à l'origine d'un événement d'alimentation.
Power Recover :	Mise sous tension en raison d'une reprise de l'alimentation.
Operator :	L'instruction d'un opérateur a causé un événement d'alimentation.
Power Failure :	Mise hors tension en raison d'une panne d'alimentation.
Software Request :	Une instruction d'Oracle Solaris est à l'origine d'un événement d'alimentation.
Alarme :	L'environnement du serveur ou une panne matérielle est à l'origine d'un événement d'alimentation.
Fatal :	Une erreur « Fatal » a causé un événement d'alimentation.

- PPAR-ID ou BB-ID d'un événement d'alimentation (ID)
Si l'événement est Mise sous tension système ou Mise hors tension système, un BB-ID est affiché.
Si l'événement est Mise sous tension PPAR, Mise hors tension PPAR ou Réinitialisation PPAR, un PPAR-ID est affiché.
Si l'événement est la cause sur tous les systèmes SPARC M12/M10 ou toutes les partitions physiques, « -- » est affiché.
- État du commutateur de mode sur le panneau de commande (Switch)
Voici une liste des états des commutateurs et de leurs significations.

État du commutateur	Signification
Locked :	Le commutateur de mode est défini sur Verrouillé.
Service :	Le commutateur de mode est défini sur Service.

12.1.6 Consultation du journal des événements

Dans ces systèmes, le journal des événements est collecté quand l'un des événements suivants se produit dans le système ou une partition physique : l'état du système change, la configuration est modifiée, le panneau de commande est utilisé ou un événement est notifié à Oracle Solaris. Utilisez la commande `showlogs` avec l'opérande `event` spécifiée pour consulter le journal des événements.

Procédure de fonctionnement

1. **Exécutez la commande `showlogs` avec l'opérande `event` spécifiée sur le shell XSCF.**

```
XSCF> showlogs event
Date                               Message
Oct 20 17:45:31 JST 2012          System power on
Oct 20 17:55:31 JST 2012          System power off
```

Le contenu suivant s'affiche.

- Heure de collecte du journal des événements (Date)
Elle est indiquée dans l'heure locale.
- Message d'événement (Message)

12.1.7 Consultation du journal de console

Le XSCF écrit les messages de la console du domaine de commande dans le journal de console. Le journal de console contient une entrée de message par ligne. Dans certains cas, le journal de console peut être appelé journal des messages de la console. Utilisez la commande `showlogs` avec l'opérande `console` spécifiée pour consulter le

journal de console.

Procédure de fonctionnement

1. **Exécutez la commande showlogs avec l'opérande console spécifiée sur le shell XSCF.**

```
XSCF> showlogs console -p 0
PPAR-ID: 00
Oct 20 17:45:31 JST 2012    console message: xxxxxxxx
Oct 20 17:55:31 JST 2012    console message: xxxxxxxx
```

Le contenu suivant s'affiche.

- ID de la partition physique (PPAR ID)
- Heure de collecte du journal de console (Date)
Elle est indiquée dans l'heure locale.
- Message de la console (Message)

12.1.8 Consultation du journal de panique

Un message de console est émis à la console du domaine quand un panique se produit. Ces messages de la console émis sont recueillis dans le journal de panique. Dans certains cas, le journal de panique peut être appelé un journal des messages de panique. Utilisez la commande showlogs avec l'opérande panic spécifiée pour consulter le journal de panique.

Procédure de fonctionnement

1. **Exécutez la commande showlogs avec l'opérande panic spécifiée sur le shell XSCF.**

```
XSCF> showlogs panic -p 0
<<panic>>
Date: Oct 20 18:45:31 JST 2012    PPAR-ID: 00
Oct 20 17:45:31 JST 2012    panic message: xxxxxxxx
Oct 20 17:55:31 JST 2012    panic message: xxxxxxxx
```

Le contenu suivant s'affiche.

- ID de la partition physique (PPAR-ID)
- Heure de collecte du journal de panique (Date)
Elle est indiquée dans l'heure locale.
- Message de panique (Message)

12.1.9 Consultation du journal IPL

Une fois une partition physique mise sous tension, les messages de la console sont émis vers la console du domaine de commande, jusqu'à ce que l'état devienne En cours d'exécution. Ces messages de la console sont recueillis dans le journal IPL. Dans certains cas, le journal IPL peut être appelé un journal des messages IPL. Utilisez la commande `showlogs` avec l'opérande `ipl` spécifiée pour consulter le journal IPL.

Procédure de fonctionnement

1. **Exécutez la commande `showlogs` avec l'opérande `ipl` spécifiée sur le shell XSCF.**

```
XSCF> showlogs ipl -p 0
<<ipl>>
Date: Oct 20 18:45:31 JST 2012      PPAR-ID: 00
Oct 20 17:45:31 JST 2012      ipl message: xxxxxxxx
Oct 20 17:55:31 JST 2012      ipl message: xxxxxxxx
```

Le contenu suivant s'affiche.

- ID de la partition physique (PPAR-ID)
- Heure de collecte du journal IPL (Date)
Elle est indiquée dans l'heure locale.
- Message IPL (Message)

12.1.10 Consultation du journal d'audit

Le journal d'audit est collecté quand la fonction audit est utilisée dans ces systèmes. Utilisez la commande `viewaudit` pour consulter le journal d'audit.

Procédure de fonctionnement

1. **Exécutez la commande `viewaudit` sur le Shell XSCF.**
L'exemple suivant affiche tous les enregistrements d'audit.

```
XSCF> viewaudit
file,1,2012-04-26 21:37:25.626
+00:00,20120426213725.0000000000.SCF-4-0
header,20,1,audit - start,0.0.0.0,2012-04-26 21:37:25.660 +00:00
header,43,1,authenticate,0.0.0.0,2012-04-26 22:01:28.902 +00:00
authentication,failure,,unknown user,telnet 27652 0.0.197.33
header,37,1,login - telnet,0.0.0.0,2012-04-26 22:02:26.459 +00:
00
subject,1,opl,normal,telnet 50466 10.18.108.4
header,78,1,command - setprivileges,0.0.0.0,2012-04-26
```

```

22:02:43.246
+00:00
subject,1,opl,normal,telnet 50466 10.18.108.4
command,setprivileges,opl,useradm
platform access,granted
return,0

```

Comme indiqué dans l'exemple ci-dessus, les enregistrements sont affichés en format texte par défaut. Un jeton est affiché par ligne avec une virgule comme caractère de délimitation des champs.

Les types de jetons et leurs champs sont indiqués dans [Tableau 12-6](#) (dans l'ordre d'affichage).

Tableau 12-6 Types de jetons et leurs champs (dans l'ordre d'affichage)

Type de jeton	Champ (ordre d'affichage)
Jeton de fichier	Étiquette, version, heure, nom du fichier
Jeton d'en-tête	Étiquette, nombre d'octets de l'enregistrement, version, type d'événement, adresse de la machine, heure (heure d'enregistrement de l'événement)
Jeton de sujet	Étiquette, ID de session d'audit, UID, mode de fonctionnement, type de terminal, adresse IP distante, port distant
Jeton Upriv	Étiquette, réussite/échec
Jeton Udpriv	Étiquette, réussite/échec, privilège d'utilisateur, ID 1 de domaine, ..., ID N de domaine
Jeton de commande	Étiquette, nom de commande, opérande 1, ..., opérande N
Jeton d'authentification	Étiquette, résultat d'authentification, nom d'utilisateur, message, type de terminal, adresse IP distante, port distant
Jeton de retour	Étiquette, valeur de retour
Jeton de texte	Étiquette, chaîne de texte

Remarque : certains champs peuvent ne pas être émis en fonction de l'environnement.

Les principaux événements et jetons d'audit sont les suivants :

- Connexion telnet
 - en-tête
 - sujet
 - texte
 - retour
- Connexion SSH
 - Identique à la connexion telnet
- Connexion BUI
 - Identique à la connexion telnet

- Déconnexion
En-tête
Objet
- Démarrage audit
En-tête
- Arrêt audit
En-tête
- Commande Shell
En-tête
Sujet
Commande
Texte
Upriv | Updpriv
Retour

Remarque : certains jetons peuvent ne pas être émis, en fonction de l'environnement. Ces informations peuvent être modifiées sans préavis, afin d'en améliorer le fonctionnement.

Remarque : pour plus de détails sur les options de journaux, les classes d'audit et les événements d'audit de la commande `viewaudit(8)`, consultez les pages du manuel ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

12.1.11 Consultation du journal de COD

Le journal de CoD est collecté en cas d'ajout ou de suppression d'une Activation de processeur. Un journal de COD est également appelé journal d'activation. Utilisez la commande `showcodactivationhistory` pour consulter le journal de CoD.

Procédure de fonctionnement

1. **Exécutez la commande `showcodactivationhistory` sur le Shell XSCF.**
L'exemple suivant affiche le journal de CoD.

```
XSCF> showcodactivationhistory
11/30/2012 01:42:41PM PST: Report Generated M10-1 SN: 843a996d
10/02/2012 02:08:49PM PST: Activation history initialized: PROC 0 cores
10/15/2012 01:36:13PM PST: Capacity added: PROC 2 cores
10/15/2012 01:46:13PM PST: Capacity added: PROC 2 cores
11/07/2012 01:36:23PM PST: Capacity deleted: PROC 2 cores
11/27/2012 01:46:23PM PST: Configuration backup created: PROC 2 cores
11/27/2012 21:26:22PM PST: Configuration restored: PROC 2 cores
11/28/2012 01:37:12PM PST: Capacity added: PROC 2 cores
11/28/2012 01:47:12PM PST: Capacity added: PROC 2 cores
11/30/2012 01:37:19PM PST: Capacity added: PROC 2 cores
11/30/2012 01:41:19PM PST: Capacity added: PROC 2 cores
11/30/2011 01:42:41PM PST: Summary: PROC 10 cores
Signature: yU27yb0oth41UL7hleA2vHL7SlaX4pmkBTIXesDlXEs
```

Remarque : pour plus de détails sur la commande `showcodactivationhistory(8)`, consultez les pages du manuel ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

12.1.12 Consultation des journaux Active Directory

Cette section explique la méthode de référence des journaux Active Directory utilisant la commande `showad`. Pour plus de détails sur les options de journaux de la commande `showad`, consultez le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual* ou les pages du manuel pour la commande `showad(8)`. Pour la taille et le numéro de génération de chaque journal, consultez [Tableau 12-3](#).

Référencement des journaux Active Directory à l'aide de la commande `showad`

Si l'authentification et l'autorisation utilisateur sont effectuées à l'aide de la fonction Active Directory, les journaux de messages des diagnostics sont collectés. Les journaux sont utilisés pour traiter une panne et sont effacés lors du redémarrage du XSCF. Les journaux Active Directory peuvent être référencés en exécutant la commande `showad` avec l'opérande `log` sur le shell XSCF. Les éléments suivants s'affichent.

- Heure à laquelle les journaux Active Directory ont été collectés
- Messages de diagnostic

12.1.13 Consultation des journaux LDAP sur SSL

Cette section explique la méthode de référence des journaux LDAP sur SSL utilisant la commande `showldapssl`. Pour plus de détails sur les options de journaux de la commande `showldapssl`, consultez le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual* ou les pages du manuel pour la commande `showldapssl(8)`. Pour la taille et le numéro de génération de chaque journal, consultez [Tableau 12-3](#).

Référencer les journaux LDAP sur SSL à l'aide de la commande `showldapssl`

Si l'authentification et l'autorisation utilisateur sont effectuées à l'aide de la fonction LDAP sur SSL, les journaux de messages des diagnostics sont collectés. Les journaux sont utilisés pour traiter une panne et sont effacés lors du redémarrage du XSCF. Les journaux LDAP sur SSL peuvent être référencés en spécifiant l'opérande `log` sur le shell XSCF et en exécutant la commande `showldapssl`. Les éléments suivants s'affichent.

- Heure de collecte du journal LDAP sur SSL
- Messages de diagnostic

12.1.14 Consultation du journal d'historique de la température

Le journal d'historique de la température est un journal des températures d'admission du serveur. La température d'admission est enregistrée toutes les 10 minutes. Utilisez la commande `showlogs` avec l'opérande `env` spécifiée pour consulter le journal d'historique de la température.

Procédure de fonctionnement

1. **Exécutez la commande `showlogs` avec l'opérande `env` spécifiée sur le shell XSCF.**

```
XSCF> showlogs env
BB#00
Date                Temperature    Power
Oct 20 17:45:31 JST 2012  32.56(C)      Cabinet Power On
Oct 20 17:55:31 JST 2012  32.56(C)      Cabinet Power Off
:
```

Le contenu suivant s'affiche.

- Heure de collecte du journal d'historique de la température (Date). Elle est indiquée dans l'heure locale.
- Température (Temperature)
- État d'alimentation du châssis (Sous ou Hors tension) (Power)

12.1.15 Sauvegarde d'un journal dans un fichier avec snapshot

Cette section décrit comment sauvegarder les informations du journal de XSCF dans un fichier.

Pour sauvegarder les informations du journal, exécutez la commande `snapshot` sur le Shell XSCF. Sinon, sélectionnez cette opération depuis le menu `snapshot` sur XSCF Web. Toutes les informations du journal de XSCF sont sauvegardées dans l'emplacement spécifié.

Un technicien sur site ou un technicien de maintenance enregistre les informations du journal. Il peut également être demandé à l'administrateur système de le faire.

Méthode de sauvegarde d'un journal

La méthode d'enregistrement d'un journal est décrite ci-dessous. Pour plus d'informations sur la méthode d'enregistrement, consultez la section suivante.

- Sauvegardez les informations du journal localement en connectant un périphérique

USB à un port USB de l'unité XSCF montée sur le panneau arrière du châssis maître XSCF.

- Sauvegardez les informations de journal par le réseau dans les terminaux utilisant XSCF Web.
Le transfert de données à ce moment-là utilise un protocole de chiffrement.
- Sauvegardez les informations de journal par le réseau, sur les serveurs spécifiés avec la commande snapshot.
Le transfert de données à ce moment-là utilise un protocole de chiffrement.

Remarque : le périphérique USB doit être formaté avec le système de fichier FAT32. Pour les points à noter concernant la capacité et le traitement du périphérique USB utilisé pour enregistrer le journal localement, contactez un technicien de maintenance.

Remarque : les données sauvegardées peuvent être cryptées en spécifiant l'option pour le cliché sur le XSCF. Pour plus d'informations sur le traitement ou l'envoi de fichiers journal cryptés, contactez un technicien de maintenance.

Remarque : dans les systèmes avec plusieurs XSCF, le journal d'un autre châssis, tel que le XSCF de veille, peut être collecté à partir du XSCF maître.

Format d'émission du fichier journal

Le format d'émission lors de l'enregistrement d'un fichier journal est le suivant.

- Nom de fichier : ce nom est généré automatiquement à partir du nom d'hôte XSCF, de l'adresse IP et de l'heure d'enregistrement du journal.
Le fichier journal ne peut pas être généré avec un nom de fichier spécifié par l'utilisateur.
- Format du fichier : zip

Dans les systèmes avec plusieurs XSCF, un fichier zip unique généré comprend les informations pour chaque châssis du SPARC M12-2S/SPARC M10-4S et pour le boîtier à barre transversale composant le bloc de construction. Si un seul numéro de châssis est indiqué, les journaux spécifiques au châssis indiqué sont sauvegardés en plus des journaux communs au système. Si tous les châssis sont indiqués, les journaux de tous les châssis sont sauvegardés en plus des journaux communs au système.

12.1.16 Sauvegarde d'un journal sur un périphérique USB local

Cette section décrit comment enregistrer les informations du journal sur un périphérique USB en utilisant XSCF Web ou le Shell XSCF.

Procédure de fonctionnement sur le shell XSCF

1. **Connectez un périphérique USB à un port USB de l'unité XSCF sur le panneau**

arrière du serveur.

2. **Exécutez la commande snapshot avec le périphérique USB spécifié pour le fichier de sortie, sur le Shell XSCF.**

```
XSCF> snapshot -d usb0 -a
```

Les données sont transférées.

3. **Confirmez que l'enregistrement du journal est terminé.**
Une fois la sauvegarde terminée, contactez un technicien de maintenance si nécessaire.

Remarque : la commande snapshot peut être utilisée pour crypter des données puis les sortir. Pour plus de détails sur l'option de cryptage de la commande snapshot, consultez sa page dans le manuel ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

Procédure de fonctionnement sur XSCF Web

1. **Connectez un périphérique USB à un port USB de l'unité XSCF sur le panneau arrière du serveur.**
2. **Affichez la page d'opération d'enregistrement en sélectionnant cette opération depuis le menu snapshot.**
3. **Sélectionnez le périphérique USB en tant qu'emplacement d'enregistrement, dans la fenêtre du navigateur Internet.**
4. **Si le fichier de destination du journal doit être crypté, cochez [Encrypt Output File] et saisissez le mot de passe du cryptage.**
Cliquez sur le bouton [Download] pour transférer les données.
5. **Confirmez que l'enregistrement du journal est terminé.**
Une fois la sauvegarde terminée, contactez un technicien de maintenance si nécessaire.

12.1.17 Sauvegarde du journal par le réseau sur les terminaux utilisant XSCF Web

La procédure pour sauvegarder le journal par le réseau dans un terminal utilisant XSCF Web, est décrite ci-dessous.

1. **Affichez la page d'opération d'enregistrement en sélectionnant le menu [Snapshot].**
2. **Indiquez le répertoire de destination comme emplacement d'enregistrement, dans la fenêtre du navigateur Web.**
3. **Si le fichier de destination du journal doit être crypté, cochez [Encrypt Output File] et saisissez le mot de passe du cryptage.**
Cliquez sur le bouton [Download] pour transférer les données.

4. **Confirmez que l'enregistrement du journal est terminé.**

Une fois la sauvegarde terminée, contactez un technicien de maintenance si nécessaire.

12.1.18 Sauvegarde du journal par le réseau, sur les serveurs spécifiés avec snapshot

La procédure pour sauvegarder le journal par le réseau sur le serveur spécifié avec la commande snapshot, est décrite ci-dessous.

1. **Indiquez le répertoire de destination complet, comme le serveur SSH et le répertoire sur le Shell XSCF, et exécutez la commande snapshot.**

```
XSCF> snapshot -t user@host:directory
```

Les données sont transférées.

2. **Confirmez que l'enregistrement du journal est terminé.**

Une fois la sauvegarde terminée, contactez un technicien de maintenance si nécessaire.

Remarque : la commande snapshot peut être utilisée pour crypter des données puis les sortir. Pour plus de détails sur l'option de cryptage de la commande snapshot, consultez la page du manuel correspondant à la commande snapshot(8), ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

12.2 Consultation des messages d'avertissement et de notification

Cette section décrit comment consulter les messages concernant les pannes et les notifications émis principalement sur la console du domaine de commande et reportés par e-mail et par la fonction d'agent SNMP.

12.2.1 Consultation des types de messages et des méthodes de référence

Type de message

Les messages suivants sont les plus communs que les utilisateurs peuvent voir lors de la notification d'une panne de serveur et de l'état du serveur :

- message syslog (*1)
 - Message FMA (*1)
 - Message IPL
 - Message de panique
 - Message de la console
 - Message de surveillance
 - Autres messages de notification
- *1 Ce message peut uniquement être référencé sur Oracle Solaris. Pour plus d'informations, consultez les manuels relatifs à Oracle Solaris.

Présentations et méthodes de référence des messages

Tableau 12-7 répertorie les types, les présentations et les méthodes de référence des messages individuels.

Tableau 12-7 Présentation de chaque message

Type de message	Description	Destination de l'affichage de sortie/ Méthode de référence
Message syslog	Ce message est une notification provenant d'Oracle Solaris.	Domaine/ Peut être consulté sur la console du domaine de commande.
Message FMA	Ce message comprend les résultats d'un diagnostic automatique sur une panne matérielle ou logicielle. L'Architecture de Gestion des Pannes (FMA) d'Oracle Solaris effectue le diagnostic. L'utilisateur peut ainsi savoir quelles parties du système correspondent à la notification de panne. Le message FMA est sauvegardé sous forme d'informations de journal (dans un journal de panne ou le journal d'erreur). La commande <code>fmdump</code> d'Oracle Solaris et la commande <code>showlogs</code> du Shell XSCF peuvent afficher son contenu pour obtenir des informations plus détaillées. L'utilisateur peut également vérifier le contenu à l'adresse URL spécifiée en fonction du MSG-ID affiché sur la console du domaine de commande.	Domaine/ Peut être consulté sur la console du domaine de commande.
Message IPL	Ce message est émis au démarrage du système d'exploitation du domaine de commande Oracle Solaris. Le message IPL est émis vers la console du domaine de commande et sauvegardé sous forme d'informations de journal (dans le journal IPL) dans le XSCF. Le journal IPL ne contient seulement que les informations de démarrage du système le plus récent, pour chaque domaine de commande. La commande <code>showlogs</code> du Shell XSCF peut afficher le journal IPL.	Domaine/ Peut être consulté sur la console du domaine de commande.

Tableau 12-7 Présentation de chaque message (*suite*)

Type de message	Description	Destination de l'affichage de sortie/ Méthode de référence
Message de panique	Ce message est émis quand une panique se produit. Le message de panique est émis vers la console du domaine et sauvegardé sous forme d'informations de journal (dans le journal de panique) dans le XSCF. Le journal de panique contient les informations pour un événement de panique unique, le plus récent, pour chaque domaine de commande. La commande showlogs du Shell XSCF peut afficher le journal de panique.	Domaine/ Peut être consulté sur la console du domaine de commande.
Message de la console	« Message de la console » est un terme générique pour les messages syslog, les messages FMA, les messages de panique, les messages IPL et d'autres messages émis par POST, OpenBoot PROM et Oracle Solaris. Ces messages de console qui sont émis vers la console de domaine de chaque domaine de commande sont sauvegardés sous forme d'informations de journal (dans le journal de console) dans le XSCF. La commande showlogs du Shell XSCF peut afficher le journal de la console. Veuillez noter que le gestionnaire de domaines logiques gère les messages de la console situés sur les domaines invités. Pour plus de détails, consultez « 8.10 Fonction de connexion de la console du domaine ». L'écrasement des messages de la console commence avec le message le plus ancien. Les messages de démarrage système sont conservés dans le journal IPL et les informations de journal respectives concernant les heures de panique sont conservées dans le journal de panique, même si leurs messages de console ont été écrasés. Dans les systèmes avec plusieurs XSCF, les messages de la console enregistrés sur le XSCF maître ne sont pas copiés sur le XSCF de veille. Ainsi, après le changement de XSCF, les messages de la console sur la précédente unité maître ne peuvent pas être référencés.	Domaine/ Peut être consulté sur la console du domaine de commande.

Tableau 12-7 Présentation de chaque message (*suite*)

Type de message	Description	Destination de l'affichage de sortie/ Méthode de référence
Message de surveillance	Le XSCF émet ce message en cas de panne ou de notification du système. Le message de surveillance est émis à l'aide de la commande showmonitorlog. Il est stocké en tant qu'information de journal (dans le journal de messages de surveillance ou le journal d'erreur) dans le XSCF. La commande showlogs du Shell XSCF peut afficher le journal de messages de surveillance et le journal d'erreur afin d'obtenir des informations plus détaillées. De plus, un technicien de maintenance utilise le DIAGCODE émis dans le message pour obtenir des informations détaillées. L'écrasement des messages de surveillance commence avec le message le plus ancien. Dans les systèmes avec plusieurs XSCF, les messages de surveillance émis par le XSCF maître sont également gérés sur le XSCF de veille. Même après le changement de XSCF, les messages de surveillance sur la précédente unité maître peuvent être référencés.	Domaine, XSCF/ Peut être consulté sur la console du domaine de commande. Peut être consulté à l'aide de la commande showmonitor-log.
Autres messages de notification	En plus des messages ci-dessus, les messages de notification sont affichés sur la console de domaine pour une mise hors tension normale, une opération de réinitialisation et certains autres événements.	Domaine/ Peut être consulté sur la console du domaine de commande.

12.2.2 Action à mener pour les messages de notification

Cette section décrit, avec les messages, les actions à mener après avoir identifié un message sur Oracle Solaris ou un message de notification provenant de chaque fonction XSCF.

Identification/Action à mener pour une notification ou une panne dans un message sur la console du domaine de commande

1. **L'utilisateur reconnaît la notification ou la panne dans un message de la console, tel qu'un message syslog ou FMA émis vers la console du domaine de commande.**

L'exemple suivant affiche un message FMA sur la console du domaine de commande.

```
SUNW-MSG-ID: SUNOS-8000-J0, TYPE: Fault, VER: 1, SEVERITY: Major
EVENT-TIME: Thu Apr 19 10:48:39 JST 2012
PLATFORM: ORCL,SPARC64-X, CSN: PP115300MX, HOSTNAME: 4S-LGA12-D0
SOURCE: eft, REV: 1.16
EVENT-ID: fcbb42a5-47c3-c9c5-f0b0-f782d69afb01
DESC: The diagnosis engine encountered telemetry from the listed devices for
which it was unable to perform a diagnosis - ereport.io.pciex.rc.epkt@
chassis0/cpuboard0/chip0/hostbridge0/pciexrc0 class and path are incompatible.
AUTO-RESPONSE: Error reports have been logged for examination.
IMPACT: Automated diagnosis and response for these events will not occur.
REC-ACTION: Use 'fmadm faulty' to provide a more detailed view of this event.
Use 'fmdump -eV' to view the unexpected telemetry. Please refer to the
associated reference document at http://support.oracle.com/msg/SUNOS-8000-J0
for the latest service procedures and policies regarding this diagnosis.
```

Remarque : l'exemple du message pourra être modifié sans préavis.

2. **Les informations concernant une panne du message FMA sont sauvegardées dans un journal. Ainsi, il convient de consulter le fichier journal sur la console du domaine de commande. À ce stade, exécutez une commande d'Oracle Solaris, telle que la commande syslog reference ou fmdump, sur la console du domaine de commande.**
Pour des détails sur comment identifier les informations concernant les pannes à l'aide de ces commandes, consultez le manuel de référence d'Oracle Solaris.
3. **Consultez les détails de la notification ou de la panne en accédant à l'URL spécifiée, en fonction de l'ID du message (SUNW-MSG-ID) affiché sur la console du domaine de commande.**
S'il n'y a aucun ID de message (MSG-ID), vous obtiendrez des informations détaillées dans les informations syslog.
4. **Pour obtenir plus d'informations détaillées, connectez-vous au XSCF et exécutez la commande showlogs afin d'identifier l'information de la panne.**
5. **Prenez une action basée sur les recommandations dans les informations à l'adresse URL spécifiée.**

Remarque : pour les dernières informations sur l'URL, consultez le site Internet concernant les messages indiqués dans les dernières *Notes de produit* pour votre serveur.

L'utilisateur peut être en mesure de reconnaître une panne, pas seulement à partir d'un message syslog ou FMA, mais également en consultant un message de la console, un message de panique, un message IPL ou un message de surveillance stockés en tant qu'informations de journal dans le XSCF. L'utilisateur peut consulter ces informations de journal en exécutant la commande showlogs du Shell XSCF avec chaque option de journal spécifiée.

Pour en savoir plus sur la commande showlogs, consultez « [12.1 Consultation d'un journal enregistré par le XSCF](#) ».

Identification/Action à mener pour une panne indiquée par e-mail

1. **L'utilisateur reconnaît une notification ou une panne depuis la ligne Sujet ou le corps du message dans un e-mail XSCF signalé.**
Pour un exemple d'e-mail dans le cas de l'apparition d'une panne, consultez « [10.2 Réception de notifications par e-mail lorsqu'une panne se produit](#) ».
2. **Pour obtenir plus d'informations détaillées, connectez-vous au XSCF et exécutez la commande showlogs afin d'identifier l'information de la panne.**
3. **Vérifiez l'information du journal. Si nécessaire, informez un technicien de maintenance du DIAGCODE indiqué dans l'e-mail ou dans le journal.**
Le technicien de maintenance peut utiliser le DIAGCODE pour acquérir des informations détaillées.

Identification/Action à mener pour une notification ou une panne dans un message SNMP trap

1. **L'utilisateur reconnaît une notification ou une panne dans l'information d'interruption émise depuis le XSCF par le gestionnaire SNMP.**
Pour un exemple de trap, consultez « [10.3 Surveillance/Gestion de l'état du système avec l'agent SNMP](#) ».
2. **Pour obtenir plus d'informations détaillées, connectez-vous au XSCF et exécutez la commande showlogs afin d'identifier l'information de la panne.**
3. **Vérifiez l'information du journal. Si nécessaire, informez un technicien de maintenance du DIAGCODE indiqué dans le journal.**

Identification/Action à mener pour une notification ou une panne dans un message de surveillance sur le shell XSCF

1. **L'utilisateur exécute la commande showmonitorlog et reconnaît une notification ou une panne dans le message de surveillance XSCF émis.**
L'exemple suivant affiche un message de surveillance.

```
XSCF> showmonitorlog
PAPL2-5-0:Alarm: /BB#0/CPU#0:XSCF:Uncorrectable
error ( 80006000-20010000-0108000112345678 ) :
```

Remarque : la commande d'exemple peut changer sans préavis, afin d'en améliorer le fonctionnement.

2. **Pour obtenir plus d'informations détaillées, connectez-vous au XSCF et exécutez la commande showlogs afin d'identifier l'information de la panne.**
3. **Vérifiez l'information du journal. Si nécessaire, informez un technicien de maintenance du DIAGCODE indiqué dans le journal.**

Passer en mode Verrouillé / Service

Ce chapitre décrit les différences entre le mode Service et le mode Verrouillé, utilisé pour les tâches de maintenance, et comment passer de l'un à l'autre.

- [Compréhension des différences entre le mode Verrouillé et le mode Service](#)
- [Changer le mode de fonctionnement](#)

13.1 Compréhension des différences entre le mode Verrouillé et le mode Service

Les systèmes SPARC M12/M10 ont deux modes de fonctionnement : le mode Verrouillé et le mode Service.

- **Mode Verrouillé**

Le mode Verrouillé est destiné aux opérations ordinaires. Dans ce mode, le commutateur de mode a été positionné sur « Verrouillé ».

Les comptes d'utilisateur configuré avec XSCF sont utilisés pour travailler. Les tâches à effectuer varient selon le compte d'utilisateur.

En mode Verrouillé, il n'est pas facile de couper l'alimentation car un mécanisme empêche une mise hors tension erronée par les utilisateurs. Le commutateur ALIMENTATION du panneau de commande peut être utilisé pour la mise sous tension mais pas pour la mise hors tension.

- **Mode Service**

Le mode Service est dédié aux tâches de maintenance. Dans ce mode, le commutateur de mode a été positionné sur « Service ». Une maintenance nécessitant l'arrêt de tout le système doit être effectuée en mode Service.

Le contrôle de la mise sous et hors tension dans les modes Verrouillé et Service affecte non seulement les opérations du commutateur ALIMENTATION, mais également le contrôle de l'alimentation effectué à distance, le contrôle automatique de l'alimentation, etc. [Tableau 13-1](#) indique les différences de contrôle d'alimentation entre les deux modes.

Tableau 13-1 Différences de contrôle d'alimentation entre le mode Verrouillé et le mode Service

Élément	Mode de fonctionnement	
	Mode Verrouillé	Mode Service
Mise sous tension par le commutateur ALIMENTATION	Mise sous tension autorisée	Mise sous tension non autorisée
Mise hors tension par le commutateur ALIMENTATION	Mise hors tension non autorisée	Mise hors tension autorisée Un appui long (4 secondes ou plus) met en route la mise hors tension.
Signal d'arrêt	Selon les paramètres (La valeur par défaut est activée)	Signal envoyé au domaine de commande
Mise sous tension lors d'une restauration	Alimentation activée	Alimentation désactivée
Vérification de l'activité	Selon les paramètres (La valeur par défaut est activée)	Désactivé
Réaction lorsque la surveillance Host Watchdog expire	Selon les paramètres (Réinitialisation de PPAR par défaut.)	Selon les paramètres (Réinitialisation de PPAR par défaut.)
Démarrage-arrêt automatique d'Oracle Solaris	Selon les paramètres (Le réglage par défaut est le démarrage automatique.)	Selon les paramètres (Le réglage par défaut est le démarrage automatique.) (*1)
Mise sous tension planifiée automatique	Mise sous tension autorisée	Mise sous tension non autorisée
Mise hors tension planifiée automatique	Mise hors tension autorisée	Mise hors tension non autorisée
Gestion de l'alimentation à distance	Contrôle autorisé	Contrôle avec d'autres hôtes non autorisé

*1 Pour plus de détails sur le démarrage-arrêt automatique d'Oracle Solaris, consultez « [6.4 Empêcher le démarrage d'Oracle Solaris lors de la mise sous tension](#) ».

Des articles contrôlés en mode Verrouillé et en mode Service, ceux représentés avec « Selon les paramètres » peuvent être configurés grâce à la commande setpparmode du microprogramme XSCF.

13.2 Changer le mode de fonctionnement

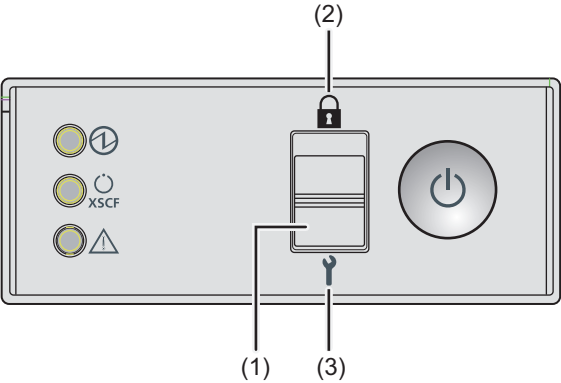
Pour changer le mode de fonctionnement des systèmes SPARC M12/M10, utilisez le commutateur de mode du panneau de commande.

Figure 13-1 Commutateur du mode de panneau de commande (SPARC M12-1/M10-1)



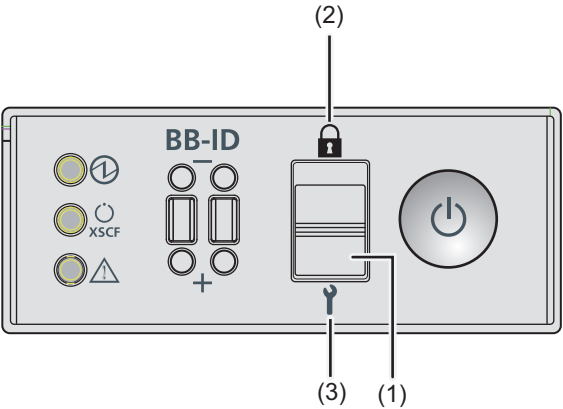
N°	Composant
1	Commutateur de mode
2	Mode Verrouillé
3	Mode Service

Figure 13-2 Commutateur du mode de panneau de commande (SPARC M12-2/M10-4)



N°	Composant
1	Commutateur de mode
2	Mode Verrouillé
3	Mode Service

Figure 13-3 Commutateur du mode de panneau de commande (SPARC M12-2S/M10-4S)



N°	Composant
1	Commutateur de mode
2	Mode Verrouillé
3	Mode Service

Pour chaque SPARC M12-2S ou SPARC M10-4S dans une configuration de bloc de construction, changez de mode en glissant le commutateur de mode sur le panneau de commande du SPARC M12-2S ou SPARC M10-4S disposant du XSCF maître ou du XSCF de veille. Si la configuration ne dispose pas de boîtier à barre transversale, le XSCF maître configuré est BB#00 ou BB#01. Si la configuration dispose de boîtiers à barre transversale, le XSCF maître configuré est XBBOX#80 ou XBBOX#81.

Remarque : pour le SPARC M12-2S ou SPARC M10-4S en configuration de bloc de construction, réglez les commutateurs de mode des XSCF maître et de veille sur le même mode. Si le XSCF maître et le XSCF en état de veille sont activés à l'aide de la commande switchscf lorsque les paramètres sont différents, l'état du commutateur de service qui reconnaît chaque châssis SPARC M12-2S ou SPARC M10-4S est modifié. Pour signaler cet état, un astérisque (*), indiquant un composant défectueux, est affiché dans le résultat des commandes showhardconf et showstatus.

Les procédures décrites ci-dessous expliquent comment passer du mode Verrouillé au mode Service et inversement.

Passage au mode Service

Pour effectuer des tâches de maintenance du système à froid ou pour configurer les paramètres initiaux de XSCF sur le système SPARC M12/M10, choisissez le mode Service.

La procédure pour passer du mode Verrouillé au mode Service est décrite ci-dessous.

1. **Placez le commutateur de mode du panneau de commande sur la position**

Service (ʔ).

Passage au mode Verrouillé

La procédure pour passer du mode Service au mode Verrouillé sur les systèmes SPARC M12/M10 est décrite ci-dessous.

1. **Placez le commutateur de mode du panneau de commande sur la position Verrouillé (ʔ).**

Configuration d'un système hautement fiable

Ce chapitre décrit les méthodes pour configurer des systèmes SPARC M12/M10 hautement fiables et sécurisés.

- Configuration de la mise en miroir de la mémoire
- Configuration du RAID matériel
- Utilisation du service LDAP
- Utilisation du démarrage SAN
- Utilisation d' iSCSI
- Gestion de l'alimentation à distance pour le SPARC M12/M10 et les périphériques d'E/S
- Utilisation de l'alimentation sans interruption
- Utilisation du démarrage vérifié

14.1 Configuration de la mise en miroir de la mémoire

Cette section décrit la méthode de configuration de la mise en miroir de la mémoire, prise en charge par le SPARC M12/M10.

14.1.1 Présentation de la mise en miroir de la mémoire

Le SPARC M12/M10 prend en charge la mise en miroir de la mémoire pour protéger les données en dupliquant la mémoire. La fiabilité des données augmente mais la quantité de mémoire disponible est réduite de moitié.

Le contrôleur d'accès à la mémoire contrôle l'écriture et la lecture des données de la mémoire. Le SPARC M12/M10 configure la mise en mémoire en groupant la mémoire dans des ensembles contrôlés par deux contrôleurs d'accès à la mémoire.

Remarque : toutes les mémoires appartenant au groupe mis en miroir doivent avoir la même capacité et le même rang.

Pour les règles de la configuration physique de la mémoire, consultez « Checking the Memory Configuration Rules » dans le *Service Manual* pour votre serveur.

14.1.2 Configuration de la mise en miroir de la mémoire

Utilisez la commande `setupfru` du microprogramme XSCF afin de configurer la mise en miroir de la mémoire installée dans le SPARC M12/M10.

Exécutez la commande avec un compte d'utilisateur disposant du privilège `platadm` ou `fieldeng`.

Remarque : pour configurer la mise en miroir de la mémoire, la partition physique à laquelle la PSB appartient doit être hors tension.

Configuration de la mise en miroir de la mémoire

■ SPARC M12

Pour configurer la mise en miroir de la mémoire dans le SPARC M12, spécifiez `-c mirror=yes`.

```
XSCF> setupfru [[-q] -{y|n}] -c function=mode device location
```

■ SPARC M10

Pour configurer la mise en miroir de la mémoire dans le SPARC M10, spécifiez `-m y`. L'option `-c mirror` ne peut pas être utilisée.

```
XSCF> setupfru [-m {y|n}] device location
```

Procédure de fonctionnement

1. Exécutez la commande `setupfru` pour configurer la mise en miroir de la mémoire.

L'exemple suivant indique tous les processeurs montés sur la carte système physique (PSB) 00-0 réglée sur le mode de mise en miroir de la mémoire dans le SPARC M12.

```
XSCF> setupfru -c mirror=yes sb 00-0
Notice:
- Logical domain config_name will be set to "factory-default".
Memory mirror mode setting will be changed, Continue? [y|n] :y
```

Remarque : pour le SPARC M10, spécifiez ce qui suit.
XSCF> setupfru -m y sb 00-0

L'exemple suivant indique que le processeur de la puce de processeur #1 dans la PSB 02-0 est réglé sur le mode de mise en miroir de la mémoire.

XSCF> **setupfru -m y cpu 02-0-1**

14.2 Configuration du RAID matériel

Cette section indique les configurations du RAID matériel prises en charge par le SPARC M12/M10, ainsi que comment configurer et gérer le RAID matériel.

Vous pouvez sélectionner à partir des deux utilitaires suivants afin de déterminer l'environnement de création et de gestion des volumes du RAID matériel sur le SPARC M12/M10.

- **Utilitaire FCode**
Cet utilitaire comprend un ensemble de commandes spéciales qui affichent les cibles et gèrent les volumes logiques d'un serveur. Utilisez ces commandes dans l'environnement OpenBoot PROM.
- **Utilitaire de configuration RAID intégré SAS-2 (SAS2IRCU)**
Vous pouvez configurer et gérer les volumes RAID sur le système à l'aide de l'utilitaire de configuration RAID intégré SAS-2 (SAS2IRCU) (ci-après désigné comme utilitaire SAS2IRCU) version 14.00.00.00 ou ultérieure de Broadcom Limited.
L'utilitaire de configuration RAID intégré SAS-2 (SAS2IRCU) est l'œuvre protégée de Broadcom Limited et de ses sociétés affiliées.
Pour obtenir l'utilitaire SAS2IRCU et la documentation y afférente de Broadcom Limited, consultez le lien suivant :

<https://www.broadcom.com/site-search?q=sas2ricu>

Le chapitre ci-dessus illustre un exemple d'utilitaire FCode.
Pour un exemple de sortie de l'utilitaire SAS2IRCU, consultez « [Annexe F Exemples d'affichage de la commande d'utilitaire SAS2IRCU](#) ».

Pour créer un volume du système (boot) dans une configuration de RAID matériel, utilisez l'utilitaire FCode. Les utilitaires FCode et SAS2IRCU peuvent prendre en charge les tâches suivantes.

Tableau 14-1 Tâches prises en charge par l'utilitaire du RAID matériel

Description de la tâche	Utilitaire Fcode	Utilitaire SAS2IRCU
Création du volume du système (boot)	Pris en charge	Non pris en charge
Création du volume des données	Pris en charge	Pris en charge

Tableau 14-1 Tâches prises en charge par l'utilitaire du RAID matériel (*suite*)

Description de la tâche	Utilitaire Fcode	Utilitaire SAS2IRCU
Création de l'échange à chaud	Non pris en charge	Pris en charge

14.2.1 Base du RAID matériel

Le RAID matériel est une technologie qui accélère la vitesse d'accès aux données et augmente la fiabilité de la protection des données en gérant collectivement au moins deux lecteurs de disques internes.

Le RAID matériel est fourni par le SPARC M12/M10 grâce à la fonction RAID intégrée sur le contrôleur SAS embarqué. RAID0, RAID1, RAID10 et RAID1E sont des types de RAID matériel pris en charge. Vous pouvez configurer jusqu'à deux volumes RAID par contrôleur SAS.

Tableau 14-2 Types de RAID pris en charge

Modèle	Nom de contrôleurs SAS par châssis	Type de RAID pris en charge
SPARC M12-1	1	RAID0/RAID1/RAID10/RAID1E
SPARC M12-2/M12-2S	2	RAID0/RAID1/RAID10/RAID1E
SPARC M10-1/M10-4/M10-4S	1	RAID0/RAID1/RAID1E

Dans le SPARC M12/M10, vous pouvez configurer jusqu'à deux volumes RAID par châssis pour le SPARC M10 ou jusqu'à quatre volumes RAID pour le SPARC M12 en combinant les types de RAID ci-dessus.

Remarque : vous ne pouvez pas configurer un volume RAID traversant plusieurs contrôleurs SAS dans le SPARC M12-2/M12-2S ou dans le M12-2S/M10-4S qui constitue plusieurs périphériques.

Lecteurs de disque pris en charge

Pour configurer le RAID matériel dans le SPARC M12/M10, utilisez des lecteurs de disque dotés de la même capacité et vitesse pour chaque volume RAID de la configuration.

Les disques SSD ne sont pas pris en charge. De même, les lecteurs de disque externes connectés au port SAS ne sont pas pris en charge.

Vient ensuite la description des mécanismes RAID0, RAID1, RAID10 et RAID1E.

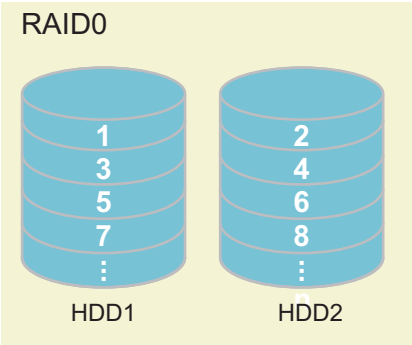
- RAID0 (agrégation par bande)
 Dans cette technique, l'écriture et la lecture des données sont décentralisées sur plusieurs lecteurs de disque internes pour pouvoir être exécutées en parallèle. RAID0 augmente la vitesse d'accès aux données, il est donc utilisé dans le cadre de travaux nécessitant une accélération de la vitesse du disque.

Dans le SPARC M12/M10, vous pouvez configurer un volume RAID0 à partir de deux à huit lecteurs de disque.

Tableau 14-3 Nombre de lecteurs de disque pouvant configurer un volume RAID0

Modèle	Nombre de lecteurs de disque à configurer
SPARC M12-1/M10-1/M10-4/M10-4S	2 à 8
SPARC M12-2/M12-2S	2 à 4

Figure 14-1 Mécanisme de RAID0



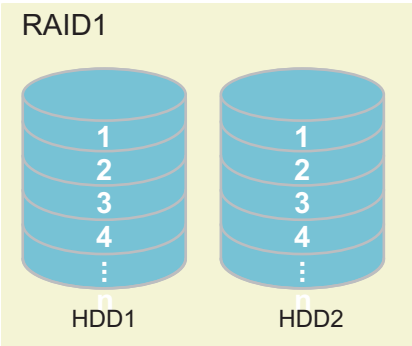
Remarque : RAID0 n'ayant pas de redondance, une panne d'un seul des lecteurs de disque constituant un RAID0 provoque un échec du volume RAID, et la perte de toutes les données. Si une panne d'un volume RAID se produit, il est nécessaire de le reconfigurer et de le restaurer à partir de données de sauvegarde.

- RAID1 (mise en miroir)
Cette technique duplique les lecteurs de disque internes et inscrit les mêmes données sur les lecteurs dupliqués afin d'augmenter la tolérance aux pannes. Ainsi, même si l'un des lecteurs de disque internes est défaillant, le système continue de fonctionner grâce à l'autre lecteur. De plus, le lecteur de disque interne en panne peut être remplacé sans interrompre les opérations. Toutefois, la capacité du disque destinée à la sauvegarde des données est réduite de moitié.
Dans le SPARC M12/M10, vous pouvez configurer un volume RAID1 à partir de deux lecteurs de disque.

Tableau 14-4 Nombre de lecteurs de disque pouvant configurer un volume RAID1

Modèle	Nombre de lecteurs de disque à configurer
SPARC M12-1/M12-2/M12-2S/M10-1/M10-4/M10-4S	2

Figure 14-2 Mécanisme de RAID1



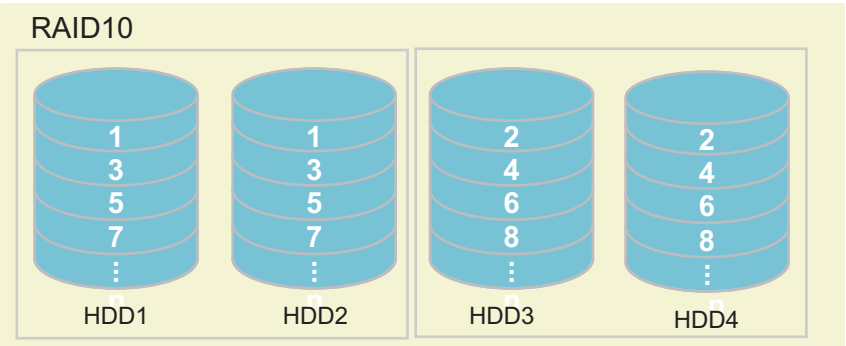
Remarque : avec RAID1, même lorsqu'un lecteur de disque subit une panne, le système continue de fonctionner en état détérioré. Cependant, une panne des deux lecteurs de disque provoque un échec du volume RAID, et la perte de toutes les données. Si le volume RAID entre en état détérioré, remplacez le disque en panne dès que possible pour restaurer la redondance.

- RAID10 (mise en miroir + agrégation par bande)
Cette technique duplique les lecteurs de disque internes et divise les données à écrire sur plusieurs groupes dupliqués. RAID10 permet d'utiliser quatre ou plusieurs lecteurs de disque internes.
Dans le SPARC M12, vous pouvez configurer un volume RAID10 à partir de quatre, six ou huit lecteurs de disque.
Le SPARC M10 ne prend pas en charge le RAID10.

Remarque : avec RAID10, même lorsqu'un des lecteurs de disque mis en miroir subit une panne, le système continue de fonctionner en état détérioré. Cependant, une panne des deux lecteurs de disque mis en miroir provoque un échec du volume RAID, et la perte de toutes les données. Si le volume RAID entre en état détérioré, remplacez le disque en panne dès que possible pour restaurer la redondance.

Tableau 14-5 Nombre de lecteurs de disque pouvant configurer un volume RAID10	
Modèle	Nombre de lecteurs de disque à configurer
SPARC M12-1	4, 6 ou 8
SPARC M12-2/M12-2S	4

Figure 14-3 Mécanisme de RAID10



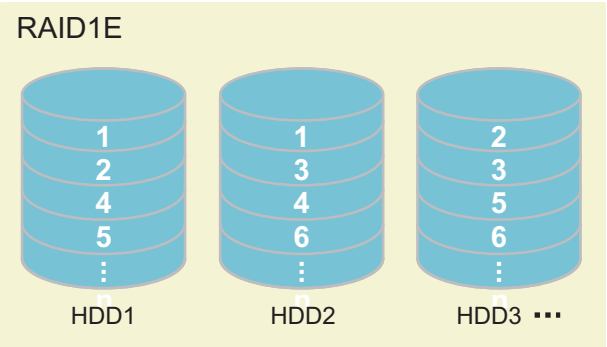
- RAID1E (mise en mémoire étendue)
Cette technique divise et copie les données, puis les écrit sur plusieurs unités de stockage internes. RAID1E est un type étendu de RAID1 et peut utiliser trois lecteurs de disque internes ou plus.

Dans le SPARC M12/M10, vous pouvez configurer un volume RAID1E à partir de trois, cinq ou sept lecteurs de disque.

Tableau 14-6 Nombre de lecteurs de disque pouvant configurer un volume RAID1E

Modèle	Nombre de lecteurs de disque à configurer
SPARC M12-2/M12-2S	3
SPARC M12-1/M10-1/M10-4/M10-4S	3, 5 ou 7

Figure 14-4 Mécanisme de RAID1E



Remarque : avec RAID1E, même lorsqu'un lecteur de disque subit une panne, le système continue de fonctionner en état détérioré. Cependant, une panne de deux lecteurs de disque ou plus provoque un échec du volume RAID, et la perte de toutes les données. Si le volume RAID entre en état détérioré, remplacez le disque en panne dès que possible pour restaurer la redondance.

14.2.2 Commandes de l'utilitaire FCode

L'utilitaire FCode permet de configurer le RAID matériel. Cet utilitaire offre les commandes suivantes.

Tableau 14-7 Liste des commandes de l'utilitaire FCode

Commande FCode	Description
show-children	Énumère tous les disques et volumes logiques connectés.
show-volumes	Énumère les informations relatives à tous les volumes logiques connectés.
create-raid0-volume	Crée un volume RAID0. Spécifiez au moins 2 cibles.
create-raid1-volume	Crée un volume RAID1. Spécifiez 2 cibles.
create-raid1e-volume	Crée un volume RAID1E. Spécifiez au moins 3 cibles. Remarque : si cette commande est utilisée avec un nombre de cibles spécifiées pair (au moins 4 cibles), la commande configure le RAID matériel comme un RAID10.
create-raid10-volume	Crée un volume RAID10. Spécifiez au moins 4 cibles. Remarque : si cette commande est utilisée avec un nombre de cibles spécifiées impair (au moins 5 cibles), la commande configure le RAID matériel comme un RAID1E.
delete-volume	Supprime un volume RAID.
activate-volume	Active à nouveau un volume RAID après le remplacement des unités de mémoire de processeur (inférieures) du SPARC M12-2/M12-2S/M10-4/M10-4S et des unités de la carte mère des systèmes SPARC M12-1/M10-1.

14.2.3 Précautions relatives au RAID matériel

Cette section indique les précautions à prendre lorsque vous utilisez le RAID matériel.

Éléments à prendre en compte lors de l'utilisation du RAID matériel

- Effectuez régulièrement une sauvegarde des données et programmes importants. Lorsque certaines erreurs surviennent, il peut s'avérer nécessaire de restaurer les données ou programmes à partir du support de sauvegarde, en reconfigurant le RAID matériel.
- Nous recommandons l'utilisation d'une alimentation sans coupure (UPS) pour garantir que les données contenues dans le système soient sécurisées en cas de panne de courant.
- Si une haute disponibilité telle que la duplication des contrôleurs ou les chemins de données s'avère nécessaire au fonctionnement du RAID matériel, installez un système RAID dédié.

- Une redondance des disques avec le RAID matériel est uniquement possible avec un contrôleur SAS.

Utilitaire SAS2IRCU

- Lorsque vous gérez l'environnement RAID matériel du SPARC M12/M10, nous recommandons l'utilitaire SAS2IRCU (sas2ircu: SAS-2 Integrated RAID Configuration Utility), fourni par Broadcom Limited, pour les raisons suivantes.
 - SAS2IRCU : vous pouvez configurer et gérer un RAID matériel pendant que les domaines logiques sont en cours d'exécution.
 - Environnement OpenBoot PROM : vous pouvez configurer un RAID matériel uniquement lorsque les domaines logiques sont arrêtés, mais vous ne pouvez pas le gérer.

Remarque : si vous utilisez ou prévoyez d'utiliser la fonction DR dans le SPARC M12-2S/ M10-4S, veuillez à installer l'utilitaire SAS2IRCU. Après intégration de la fonction DR, vous aurez besoin de l'utilitaire SAS2IRCU afin d'activer les volumes RAID.

- Pour plus de détails sur l'obtention de l'utilitaire SAS2IRCU, consultez le site web de Broadcom Limited dont l'adresse figure dans « [14.2 Configuration du RAID matériel](#) ». Pour plus d'informations sur son utilisation, consultez le *SAS-2 Integrated RAID Configuration Utility User Guide*, disponible sur le même site web.
- En cas de panne du volume RAID, vous pouvez spécifier le disque défaillant à l'aide de l'utilitaire SAS2IRCU.
- L'utilitaire SAS2IRCU est utilisé dans l'environnement Oracle Solaris et requiert un compte avec privilège de root. Par conséquent, l'utilitaire SAS2IRCU doit être utilisé par un administrateur système.
- L'utilitaire SAS2IRCU est utilisé dans le domaine logique auquel le contrôleur SAS est attribué. Par conséquent, installez l'utilitaire SAS2IRCU dans le domaine racine d'E/S auquel le contrôleur SAS se trouvant sur la carte mère est attribué.

Remarque : la fonction d'attribution pour les périphériques de point de destination PCIe n'est pas prise en charge sur le contrôleur SAS dans le SPARC M12/M10.

Éléments à prendre en compte lors de la configuration/retrait du RAID matériel

- Lors de la configuration ou du retrait du RAID matériel, la fiabilité des données contenues sur le disque n'est pas garantie. Veuillez à sauvegarder des données avant de configurer pour la première fois le RAID matériel pour le système ou de retirer un RAID matériel installé. Après configuration du RAID matériel, il est possible que vous deviez installer de nouvelles données ou les restaurer à partir du support de sauvegarde.
- L'exécution de la reconfiguration matérielle RAID modifie les informations de volume RAID (valeur WWID). Par conséquent, si vous effectuez une opération comme une activation, une spécification de périphérique, ou la gestion d'un montage Oracle Solaris, la configuration doit être modifiée.

- Le tableau suivant indique le délai standard de synchronisation d'un disque de 600 Go et d'un disque de 900 Go à l'état non chargé, suite à la configuration ou la maintenance du RAID matériel. Le délai de synchronisation varie largement en fonction de la génération et de l'état d'utilisation des lecteurs de disque ou de la condition de charge des systèmes.

Tableau 14-8 Délai de synchronisation standard du RAID matériel

RAID	Nombre de lecteurs de disque	Délai de synchronisation	
		lecteur de disque de 600 Go	lecteur de disque de 900 Go
1	2	6 heures	8 heures
10 (*1)	4	10 heures	15 heures
	6	16 heures	21 heures
	8	21 heures	31 heures
1E	3	20 heures	29 heures
	5	35 heures	45 heures
	7	54 heures	65 heures

*1 Seul le SPARC M12 prend en charge RAID10.

- N'effectuez pas de tâches nécessitant que vous accédiez aux lecteurs de disque telles que l'installation d' Oracle Solaris ou la restauration de données, lorsque les lecteurs de disque configurent ou synchronisent le RAID matériel. En ce qui concerne la sécurité du volume RAID, nous déconseillons la réécriture des contenus des lecteurs de disque avant l'achèvement de la configuration du volume RAID. Veuillez à effectuer ces tâches plutôt après avoir terminé la configuration du volume RAID.
- Vous ne pouvez configurer qu'un seul volume RAID à la fois par contrôleur SAS. Lorsqu'un autre groupe de commandes de configuration du volume RAID est émis pour un contrôleur SAS sur lequel la configuration du volume RAID est en cours, l'exécution de la première tâche de configuration est suivie par la configuration du volume RAID suivant.
- Lorsque vous configurez le RAID matériel, la taille du volume RAID devient plus petite que celle du disque de départ.
- En cas de redémarrage du système ou de panne de courant avec une restauration du courant pendant la configuration ou la synchronisation du RAID matériel, reprenez la procédure de configuration/synchronisation pour le SPARC M10. Pour le SPARC M12, la procédure de configuration/synchronisation redémarre au moment où la panne s'est produite.

Éléments à prendre en compte lors du fonctionnement du RAID matériel

La vitesse de votre système peut ralentir parce que le contrôleur du RAID matériel ne peut pas tout à fait déterminer si le disque est défaillant. Si votre système rencontre ce problème, suivez la procédure ci-après. Veuillez à sauvegarder vos données avant d'effectuer cette procédure car le RAID matériel sera retiré.

1. Empêchez les applications d'utiliser le stockage interne.
2. Retirez le RAID matériel.
3. Déterminez si le problème est lié au disque.
4. Si le problème persiste, remplacez tous les disques utilisés pour le RAID matériel.
5. Reconfigurez le RAID matériel.
6. Restaurez les données à partir du support de sauvegarde.

Vient ensuite la description des procédures d'utilisation des volumes du RAID matériel. Consultez l'élément approprié en fonction de votre type d'utilisation.

Tableau 14-9 Utilisations et références du RAID matériel

Utilisation du volume RAID	Références
Configuration du volume RAID	« 14.2.4 Préparation avant utilisation du RAID matériel » « 14.2.5 Création d'un volume RAID matériel » « 14.2.7 Gestion d'un composant de rechange à chaud d'un volume RAID matériel »
Suppression d'un volume RAID	« 14.2.4 Préparation avant utilisation du RAID matériel » « 14.2.6 Suppression d'un volume RAID matériel »
Remplacement des lecteurs de disque constituant le volume RAID	« 14.2.9 Vérification d'un lecteur de disque défaillant » « 14.2.10 Remplacement d'un lecteur de disque défaillant »
Nouvelle activation d'un RAID matériel après le remplacement des unités de mémoire de processeur (inférieures) du SPARC M12-2/M12-2S/M10-4/M10-4S et des unités de la carte mère des systèmes SPARCM12-1/M10-1	« 14.2.11 Réactivation d'un volume RAID matériel » « 14.2.12 Spécification d'un volume RAID de matériel en tant que périphérique de démarrage »

14.2.4 Préparation avant utilisation du RAID matériel

Utilisez l'utilitaire FCode en guise de préparation à l'utilisation du RAID matériel. Effectuez ces procédures sur xterm ou un terminal équivalent prenant en charge le défilement.

Procédure de fonctionnement

1. **Mettez le système sous tension.**
S'il est déjà sous tension,redémarrez le système et désactivez la fonction de redémarrage automatique dans OpenBoot PROM.
2. **Confirmez que l'invite ok s'affiche.**
3. **Exécutez la commande show-devs, et affichez une liste des chemins d'accès au périphérique du serveur.**
Vous trouverez ci-dessous un exemple du SPARC M10.

```
{0} ok show-devs
.
.
/pci@8000/pci@4/pci@0/pci@0/scsi@0
/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk
/pci@8000/pci@4/pci@0/pci@0/scsi@0/tape
.
.
{0} ok
```

4. Exécutez la commande select pour sélectionner le contrôleur et créer le volume RAID matériel.

Remarque : après exécution de la commande select, vous devez exécuter la commande unselect-dev. Une fois la procédure terminée, exécutez la commande unselect-dev en fonction des directions dans [14.2.5](#) ou [14.2.6](#).

```
{0} ok select /pci@8000/pci@4/pci@0/pci@0/scsi@0
{0} ok
```

5. Exécutez la commande .properties pour vérifier l'adresse SAS du contrôleur SAS interne.

```
{0} ok .properties
assigned-addresses 81030010 00000000 00000000 00000000 00000100
83030014 00000001 00000000 00000000 00010000
8303001c 00000001 00040000 00000000 00040000
82030030 00000000 00200000 00000000 00100000
firmware-version 17.00.00.00
mpt-version 2.00
local-wwid 50 00 00 e0 e0 45 00 00 <- Adresse SAS
:
Omis
:
{0} ok
```

Remarque : le résultat de sortie de la commande .properties affiche des informations nécessaires à l'entretien du volume RAID. Veuillez à noter ces informations.

6. Exécutez la commande show-children pour afficher les adresses SAS des lecteurs connectés.

```
{0} ok show-children

FCode    Version    1.00.56,    MPT    Version    2.00,    Firmware    Version    13.
00.66.00
```

```

Target  a
Unit    0          Disk      TOSHIBA      MBF2600RC          3706
1172123568  Blocks,    600  GB
SASDeviceName  50000393c813ae74      SASAddress  50000393c813ae76
PhyNum    0
Target  b
Unit    0          Disk      TOSHIBA      MBF2600RC          3706
1172123568  Blocks,    600  GB
SASDeviceName  50000393b81b24ec      SASAddress  50000393b81b24ee
PhyNum    1
:
Omis
:
Target  12
Unit    0          Encl     Serv     device      FUJITSU      NBBEXP
0d32
SASAddress  500000e0e04d003d      PhyNum    14

```

Remarque : le résultat de sortie de la commande `show-children` affiche des informations nécessaires à l'entretien du volume RAID. Veillez à noter ces informations.

Exécutez la commande `show-children` pour afficher les adresses SAS des lecteurs connectés.

14.2.5 Création d'un volume RAID matériel

Utilisez l'une des commandes suivantes afin de créer un volume RAID matériel, en fonction de la configuration du RAID matériel en cours de création.

- Pour configurer un volume RAID0

```
{0} ok target1 target2 create-raid0-volume
```

- Pour configurer un volume RAID1

```
{0} ok target1 target2 create-raid1-volume
```

- Pour configurer un volume RAID10

```
{0} ok target1 target2 target3 target4 create-raid10-volume
```

Remarque : RAID10 n'est pas pris en charge par le SPARC M10-4/M10-4S/M10-1.

- Pour configurer un volume RAID1E

```
{0} ok target1 target2 target3 create-raidle-volume
```

Les paramètres suivants sont les mêmes pour toutes ces commandes. Spécifiez un numéro cible pouvant être vérifié à partir de la commande show-children à cible 1, cible 2, cible 3 et cible 4. Une cible ne peut pas appartenir à plusieurs volumes. Ces commandes sont interactives, il est donc possible de spécifier une capacité de volume en MB et un nom comportant jusqu'à 15 caractères. Lorsque la capacité du volume n'est pas spécifiée, il est créé avec une capacité maximale.

Procédure de fonctionnement

1. **Préparez la création d'un volume RAID matériel.**
Pour plus de détails, consultez « [14.2.4 Préparation avant utilisation du RAID matériel](#) ».
2. **A partir des résultats d'exécution de la commande show-children, déterminez les cibles de création d'un volume RAID matériel.**
3. **Exécutez les commandes create-raid0-volume, create-raid1-volume, create-raid10-volume ou create-raid1e-volume pour créer un volume RAID matériel à l'aide des disques physiques.**

Dans l'exemple suivant, a et b sont spécifiés comme cibles et un volume RAID0 est créé avec un maximum de capacité et sans spécification de nom de volume.

```
{0} ok a b create-raid0-volume
Target a size is 1169920000 Blocks, 598 GB
Target b size is 1169920000 Blocks, 598 GB
The volume can be any size from 1 MB to 1142500 MB
What size do you want? [1142500] [Enter]
Volume size will be 2339840000 Blocks, 1197 GB
Enter a volume name: [0 to 15 characters] [Enter]
Volume has been created
```

Dans l'exemple suivant, a et b sont spécifiés comme cibles et un volume RAID1 est créé avec un maximum de capacité et sans spécification de nom de volume.

```
{0} ok a b create-raid1-volume
Target a size is 1169920000 Blocks, 598 GB
Target b size is 1169920000 Blocks, 598 GB
The volume can be any size from 1 MB to 571250 MB
What size do you want? [571250] [Enter]
Volume size will be 1169920000 Blocks, 598 GB
Enter a volume name: [0 to 15 characters] [Enter]
Volume has been created
```

Dans l'exemple suivant, a, b, c et d sont spécifiés comme cibles et un volume RAID10 est créé avec un maximum de capacité et sans spécification de nom de volume.


```
{0} ok a b c d create-raid10-volume
Target a size is 1169920000 Blocks, 598 GB
Target b size is 1169920000 Blocks, 598 GB
Target c size is 1169920000 Blocks, 598 GB
Target d size is 1169920000 Blocks, 598 GB
The volume can be any size from 1 MB to 1142500 MB
What size do you want? [1142500 ] [Enter]
Volume size will be 2339840000 Blocks, 1197 GB
Enter a volume name: [0 to 15 characters] [Enter]
Volume has been created
```

Dans l'exemple suivant, a, b et c sont spécifiés comme cibles et un volume RAID1E est créé avec un maximum de capacité et sans spécification de nom de volume.

```
{0} ok a b c create-raid1e-volume
Target a size is 1169920000 Blocks, 598 GB
Target b size is 1169920000 Blocks, 598 GB
Target c size is 1169920000 Blocks, 598 GB
The volume can be any size from 1 MB to 856875 MB
What size do you want? [856875] [Enter]
Volume size will be 1754880000 Blocks, 898 GB
Enter a volume name: [0 to 15 characters] [Enter]
Volume has been created
```

4. Exécutez la commande **show-volumes** pour vérifier le volume RAID créé.

Dans l'exemple suivant, les contenus du volume RAID 1 sont vérifiés.

```
{0} ok show-volumes
Volume 0 Target 11e Type RAID1 (Mirroring)
WWID 0d061173730f12d5
Optimal Enabled Data Scrub In Progress
2 Members 1169920000 Blocks, 598 GB
Disk 0
Primary Optimal
Target a TOSHIBA MBF2600RC 3706 PhyNum 0
Disk 1
Secondary Optimal
Target b TOSHIBA MBF2600RC 3706 PhyNum 1
{0} ok
```

Remarque : lorsque deux volumes RAID sont créés sous le même contrôleur SAS, le volume RAID créé en premier lieu est numéroté « 1 » et le volume RAID créé en second lieu est numéroté « 0 ».

5. Exécutez la commande **unselect-dev** afin de désélectionner le contrôleur sélectionné lors de la préparation.

```
{0} ok unselect-dev
{0} ok
```

Remarque : dans Oracle Solaris, elle est reconnue comme un lecteur de disque (Le distributeur est « LSI », le Produit est « Volume logique ») par volume RAID créé. En outre, l'incorporation du volume RAID modifie le chemin d'accès du périphérique comme ci-dessous. Chemin d'accès du lecteur de disque non incorporé dans le RAID matériel :

/chemin d'accès du contrôleur sas/iport@f/disk@w[adresse SAS du lecteur de disque] (ou, /scsi_vhci/disk@g[nom de périphérique SAS du lecteur de disque])

est modifié en :

Chemin d'accès de périphérique du volume RAID :

/chemin d'accès de périphérique du contrôleur sas/iport@v0/disk@w[nom de périphérique du volume RAID]

Les exemples ci-dessous montrent la sortie lorsque la commande `format` est exécutée dans un environnement où des [Lecteurs de disque non incorporés dans le RAID matériel] et un [Volume RAID matériel] coexistent.

- Exemple de message de sortie 1
Lors de et juste après l'installation d'Oracle Solaris

```
root# format
Searching for disks... done

AVAILABLE DISK SELECTIONS:
[Lecteur de disque non incorporé dans le RAID matériel]
  0. c2t50000394882899F6d0 <TOSHIBA-AL13SEB600-3702 cyl 64986 alt 2 hd 27
sec 668>
    /pci@8000/pci@4/pci@0/pci@0/scsi@0/iport@f/disk@w50000394882899f6,0
    /dev/chassis/FUJITSU-BBEXP.500000e0e06d257f/013P_HDD00/disk
[Volume RAID]
  1. c3t3DF694DFC21FFDA9d0 <LSI-Logical Volume-3000 cyl 65533 alt 2 hd 32
sec 557>
    /pci@8000/pci@4/pci@0/pci@0/scsi@0/iport@v0/disk@w3df694dfc21ffda9,0
```

- Exemple de message de sortie 2
Environnement ou une configuration pour rendre le lecteur de disque intégré MPxIO a été effectuée (ou Enhanced Support Facility 5.0 ou supérieur est appliqué)

```
root# format
Searching for disks... done

AVAILABLE DISK SELECTIONS:
[Lecteur de disque non incorporé dans le RAID matériel]
  0. c0t50000394882899F4d0 <TOSHIBA-AL13SEB600-3702 cyl 64986 alt 2 hd 27
sec 668>
    /scsi_vhci/disk@g50000394882899f4
    /dev/chassis/FUJITSU-BBEXP.500000e0e06d257f/013P_HDD00/disk
[Volume RAID]
  1. c3t3DF694DFC21FFDA9d0 <LSI-Logical Volume-3000 cyl 65533 alt 2 hd 32
```

```
sec 557>
```

```
/pci@8000/pci@4/pci@0/pci@0/scsi@0/iport@v0/disk@w3df694dfc21ffda9,0
```

Remarque : les messages suivants peuvent s'afficher au démarrage d' Oracle Solaris. Ceci signifie que l'étiquette ne comporte pas d'informations relatives au volume RAID. Un tel volume RAID ne peut pas être utilisé sur Oracle Solaris. Il est possible de l'utiliser sur Oracle Solaris après exécution de la commande de formatage, sélection du volume RAID approprié, et étiquetage.

- Exemple de message de sortie

```
Jan 16 02:46:48 solaris cmlb: WARNING: /pci@8000/pci@4/pci@0/pci@0/scsi@0/
iport@v0/disk@w3aa6d102f1bf517a,0 (sd2):
Jan 16 02:46:48 solaris          Corrupt label; wrong magic number
```

- Exemple d'exécution de la commande format

```
root@solaris:/root# format
Searching for disks...
Jan 16 02:46:35 solaris cmlb: WARNING: /pci@8000/pci@4/pci@0/pci@0/scsi@0/
iport@v0/disk@w3aa6d102f1bf517a,0 (sd2):
Jan 16 02:46:35 solaris          Corrupt label; wrong magic number
Jan 16 02:46:35 solaris cmlb: WARNING: /pci@8000/pci@4/pci@0/pci@0/scsi@0/
iport@v0/disk@w3aa6d102f1bf517a,0 (sd2):
Jan 16 02:46:35 solaris          Corrupt label; wrong magic number
done
c2t3AA6D102F1BF517Ad0: configured with capacity of 556.97GB
AVAILABLE DISK SELECTIONS:
    0. c2t3AA6D102F1BF517Ad0 <LSI-Logical Volume-3000 cyl 65533 alt 2 hd 32
    sec 557>
        /pci@8000/pci@4/pci@0/pci@0/scsi@0/iport@v0/disk@w3aa6d102f1bf517a,0
Specify disk (enter its number): 0
selecting c2t3AA6D102F1BF517Ad0
[disk formatted]
Jan 16 02:46:48 solaris cmlb: WARNING: /pci@8000/pci@4/pci@0/pci@0/scsi@0/
iport@v0/disk@w3aa6d102f1bf517a,0 (sd2):
Jan 16 02:46:48 solaris          Corrupt label; wrong magic number
Jan 16 02:46:54 solaris cmlb: WARNING: /pci@8000/pci@4/pci@0/pci@0/scsi@0/
iport@v0/disk@w3aa6d102f1bf517a,0 (sd2):
Jan 16 02:46:54 solaris          Corrupt label; wrong magic number
Disk not labeled. Label it now? yes
```

14.2.6 Suppression d'un volume RAID matériel

Utilisez la commande `delete-volume` de l'utilitaire FCode afin de supprimer un volume RAID matériel créé.

```
{0} ok volume_number delete-volume
```

Pour ce qui est de `volume_number`, indiquez un numéro de volume émis par la commande `show-volumes`.

L'exécution de cette commande permet d'afficher un message de demandant la confirmation de suppression du volume RAID. Sélectionnez « yes » ou « no » selon la situation.

Procédure de fonctionnement

1. Préparez la suppression d'un volume RAID matériel.

Pour plus de détails, consultez « [14.2.4 Préparation avant utilisation du RAID matériel](#) ».

2. Exécutez la commande `show-volumes` pour vérifier le volume RAID à supprimer.

Dans l'exemple suivant, un volume RAID1 a été créé avec le numéro de volume 0.

```
{0} ok show-volumes
Volume 0 Target 11e Type RAID1 (Mirroring)
  Name raid1-volume WWID 0c233a838262c6c5
  Optimal Enabled Data Scrub In Progress
  2 Members 1169920000 Blocks, 598 GB
  Disk 0
    Primary Optimal
    Target a TOSHIBA MBF2600RC 3706 PhyNum 0
  Disk 1
    Secondary Optimal
    Target b TOSHIBA MBF2600RC 3706 PhyNum 1
{0} ok
```

3. Exécutez la commande `delete-volume` pour supprimer le volume RAID.

Dans l'exemple suivant, le volume RAID dont le numéro de volume est 0 est supprimé.

```
{0} ok 0 delete-volume
The volume and its data will be deleted
Are you sure (yes/no)? [no] yes
Volume 0 has been deleted
{0} ok
```

4. Exécutez la commande `show-volumes` pour vérifier que le volume RAID a été supprimé.

```
{0} ok show-volumes
No volumes to show
{0} ok
```

5. Exécutez la commande `unselect-dev` afin de désélectionner le contrôleur

sélectionné lors de la préparation.

```
{0} ok unselect-dev  
{0} ok
```

14.2.7 Gestion d'un composant de rechange à chaud d'un volume RAID matériel

Sur un disque d'échange à chaud déjà créé, si l'un des lecteurs de disque d'un volume RAID mis en miroir (RAID1, RAID10 ou RAID1E) est défaillant, le contrôleur RAID embarqué remplace le lecteur de disque défaillant par le lecteur d'échange à chaud et resynchronise les données.

Utilisez l'utilitaire SAS2IRCU pour créer ou supprimer l'échange à chaud d'un volume RAID. Pour plus d'informations sur l'utilitaire SAS2IRCU, consultez le début de « [14.2 Configuration du RAID matériel](#) ». Ou, pour obtenir des exemples de sortie, consultez « [Annexe F Exemples d'affichage de la commande d'utilitaire SAS2IRCU](#) ».

Remarque : si vous configurez deux volumes RAID volumes avec des lecteurs de disque de capacités différentes, nous ne recommandons pas de créer un composant de rechange à chaud, pour les raisons suivantes.

- Lorsque la capacité du lecteur de disque d'un composant de rechange à chaud est inférieure au lecteur de disque configurant le volume RAID
La resynchronisation n'est pas exécutée, car le lecteur de rechange à chaud ne peut pas remplacer le lecteur de disque en panne.
 - Lorsque la capacité du lecteur de disque d'un composant de rechange à chaud est supérieure au lecteur de disque configurant le volume RAID
Le lecteur de rechange à chaud remplace le lecteur de disque en panne et la resynchronisation est exécutée. Cependant, le volume de disque RAID est configuré avec une capacité de lecteur de disque différente. (Cette configuration n'est pas prise en charge).
-

14.2.8 Vérification du statut d'un volume RAID matériel et d'un lecteur de disque

Cette section décrit comment vérifier l'état d'un volume RAID matériel et du lecteur de disque interne dans le volume RAID matériel.

Pour vérifier l'état d'un volume RAID matériel et du lecteur de disque interne dans le volume RAID matériel, utilisez l'utilitaire Fcode ou l'utilitaire SAS2IRCU, avec les commandes suivantes.

Tableau 14-10 Commandes d'affichage du statut du RAID matériel

Nom de l'utilitaire	Nom de la commande
Utilitaire FCode	Commande show-volumes
Utilitaire SAS2IRCU	Commande STATUS Commande DISPLAY

Les éléments suivants décrivent l'état principal et la description lors de l'exécution de chaque commande de l'utilitaire.

Tableau 14-11 États affichés par les commandes d'utilitaire du RAID matériel

Élément	Valeur de sortie		Description
	Utilitaire Fcode Commande show-volume	Utilitaire SAS2IRCU Commande STATUS Commande DISPLAY	
Niveau de RAID	RAID0 (Striping)	RAID0	Volume RAID0 (agrégation par bande)
	RAID1 (Mirroring)	RAID1	Volume RAID1 (mise en miroir)
	RAID10 (Striped Mirroring)	RAID10	Volume RAID10 (mise en miroir + agrégation par bande)
	RAID1E (Mirroring Extended)	RAID1E	Volume RAID1E (Mise en miroir étendue)
État du volume RAID matériel (exemple type)	Optimal	Optimal	Volume RAID matériel fonctionnant normalement
	Degraded	Degraded	Volume RAID matériel dégradé
	Missing	Missing	Volume RAID matériel manquant
	Failed	Failed	Volume RAID matériel défaillant
	Enabled	Enabled	Volume RAID matériel activé
	Inactive	Inactive	Volume RAID matériel désactivé
	Data Scrub In Progress	None	État du nettoyage des données d'un volume RAID matériel Cette indication ne représente pas un problème car le microprogramme du RAID matériel effectue automatiquement l'opération.
	Background Init In Progress	Background Init	Configuration du volume RAID matériel en cours La configuration du volume RAID matériel n'est pas complète.
	Resync In Progress	Synchronize	La resynchronisation du volume RAID est en cours. La configuration du volume RAID matériel n'est pas complète.
	Consistency Check In Progress	Consistency Check	Vérification de cohérence du volume RAID matériel en cours

Tableau 14-11 États affichés par les commandes d'utilitaire du RAID matériel (suite)

Élément	Valeur de sortie		Description
	Utilitaire Fcode Commande show- volume	Utilitaire SAS2IRCU Commande STATUS Commande DISPLAY	
Statut du lecteur de disque (exemple type)	Optimal	Optimal (OPT)	Lecteur de disque cible incorporé dans un volume RAID matériel
	Offline	Failed (FLD)	Lecteur de disque cible non incorporé dans un volume RAID matériel
	Degraded	Degraded (DGD)	Lecteur de disque cible dégradé
	Rebuilding	Rebuilding (RBLD)	Lecteur de disque cible en cours d'incorporation dans un volume RAID matériel
	Out Of Sync	Out of Sync (OSY)	Lecteur de disque cible hors synchronisation avec le volume RAID matériel

Affichage de l'état à l'aide de l'utilitaire Fcode

Pour vérifier l'état d'un volume RAID matériel et du lecteur de disque interne dans le volume RAID matériel, arrêtez le système et utilisez la commande show-volumes à partir de l'utilitaire FCode.

1. **Confirmez que l'invite ok s'affiche.**
2. **Exécutez la commande select avec le nom du contrôleur pour afficher les volumes RAID matériel.**

Remarque : après exécution de la commande select, vous devez exécuter la commande unselect-dev. Une fois cette procédure terminée, exécutez la commande unselect-dev en fonction des instructions données à l'Étape 4.

```
{0} ok select /pci@8000/pci@4/pci@0/pci@0/scsi@0
{0} ok
```

3. **Exécutez la commande show-volumes pour vérifier les volumes RAID.**
L'exemple suivant montre les points suivants :
 - (1) Le type de RAID du volume RAID matériel est « RAID1 (Mirroring) ».
 - (2) Le volume RAID matériel est « Degraded » (détérioré) et « Enabled » (Activé).
 - (3) Parmi les lecteurs de disque composant le volume RAID matériel, Disk 0 est « incorporé en tant que primaire (optimal) ».
 - (4) Parmi les lecteurs de disque composant le volume RAID matériel, Disk 1 est « not incorporated as the Secondary (Offline) » (non incorporé en tant que secondaire (déconnecté)), et « out of synchronization » (désynchronisé).

```
{0} ok show-volumes
Volume 0 Target 11e   Type RAID1 (Mirroring) <-- (1)
  Name raid1-volume   WWID 0c233a838262c6c5
  Degraded   Enabled <-- (2)
  2 Members                                     1169920000 Blocks, 598 GB
  Disk 0
    Primary   Optimal <-- (3)
    Target a   TOSHIBA MBF2600RC          3706   PhyNum 0
  Disk 1
    Secondary Offline   Out Of Sync <-- (4)
    Target b   TOSHIBA MBF2600RC          3706   PhyNum 1
{0} ok
```

Remarque : le statut d'erreur du lecteur de disque lui-même peut être affiché après qu'il soit libéré du RAID matériel.

4. **Utilisez la commande `unselect-dev` afin de désélectionner le contrôleur sélectionné lors de la préparation.**

```
{0} ok unselect-dev
{0} ok
```

Affichage de l'état à l'aide de l'utilitaire SAS2IRCU

Vous pouvez également utiliser l'utilitaire SAS2IRCU pour vérifier l'état d'un volume RAID matériel et du lecteur de disque interne dans le volume RAID matériel. Pour plus d'informations sur l'utilitaire SAS2IRCU, consultez le début de « [14.2 Configuration du RAID matériel](#) ».

14.2.9 Vérification d'un lecteur de disque défaillant

Cette section décrit comment rechercher des pannes de lecteurs de disque internes qui composent un volume RAID.

Vous pouvez confirmer des pannes de lecteurs de disque à partir d'une ou de la combinaison des méthodes énumérées ci-après.

Vérification des DEL des lecteurs de disque

En cas de panne de l'un des lecteurs de disque du système, la DEL DE CONTRÔLE (orange) située à l'avant du lecteur s'allume. Grâce à cette DEL DE CONTRÔLE, il est possible d'identifier le lecteur de disque du système présentant une panne. Pour les emplacements et les descriptions détaillées de ces DEL, consultez « Understanding the System Components » dans le *Service Manual* pour votre serveur.

Vérification d'un message d'erreur

Lorsqu'un lecteur de disque rencontre une panne, l'écran de la console affiche un message d'erreur. Il est également possible de vérifier le message en ouvrant le fichier

/var/adm/messages.

Dans l'exemple suivant, portant sur les résultats de sortie de la commande `show-children`, affichés dans « [14.2.4 Préparation avant utilisation du RAID matériel](#) », le message d'erreur s'affichant sur l'écran vous indique que le disque cible 11 (DevHandle 0x11) du volume RAID1 créé avec l' ID de cible 10 et 11 est en panne, et que le volume RAID est dégradé. Étant donné que la valeur `PhyNum` de Cible 11, comme sortie de la commande `show-children`, indique l'emplacement du disque dur, cette valeur peut être utilisée pour déterminer l'emplacement du disque dur défaillant. Dans cet exemple, il peut être déterminé à partir des résultats de sortie de la commande `show-children`, tel qu'illustré dans « [14.2.4 Préparation avant utilisation du RAID matériel](#) », que la valeur `PhyNum` de la Cible 11 est 7. Par conséquent, le lecteur de disque défaillant se trouve à l'emplacement 7.

Remarque : si vous changez le statut de montage du lecteur de disque, la valeur `DevHandle` changera également.

```
Jun 10 16:33:33 A4U4S429-D0 scsi: /pci@8000/pci@4/pci@0/pci@0/scsi@0 (mpt_sas0):
Jun 10 16:33:33 A4U4S429-D0 PhysDiskNum 1 with DevHandle 0x11 in slot 0 for
enclosure with handle 0x0 is now offline
Jun 10 16:33:33 A4U4S429-D0 scsi: /pci@8000/pci@4/pci@0/pci@0/scsi@0 (mpt_sas0):
Jun 10 16:33:33 A4U4S429-D0 PhysDiskNum 1 with DevHandle 0x11 in slot 0 for
enclosure with handle 0x0 is now , active, out of sync, write cache enabled
Jun 10 16:33:33 A4U4S429-D0 scsi: /pci@8000/pci@4/pci@0/pci@0/scsi@0 (mpt_sas0):
Jun 10 16:33:33 A4U4S429-D0 PhysDiskNum 1 with DevHandle 0x11 in slot 0 for
enclosure with handle 0x0 is now , active, out of sync
Jun 10 16:33:33 A4U4S429-D0 scsi: WARNING: /pci@8000/pci@4/pci@0/pci@0/scsi@0
(mpt_sas0):
Jun 10 16:33:33 A4U4S429-D0 Volume 286 is degraded
Jun 10 16:33:33 A4U4S429-D0 scsi: /pci@8000/pci@4/pci@0/pci@0/scsi@0 (mpt_sas0):
Jun 10 16:33:33 A4U4S429-D0 Volume 0 is now degraded
Jun 10 16:33:33 A4U4S429-D0 scsi: WARNING: /pci@8000/pci@4/pci@0/pci@0/scsi@0
(mpt_sas0):
Jun 10 16:33:33 A4U4S429-D0 Volume 286 is degraded
Jun 10 16:33:33 A4U4S429-D0 scsi: /pci@8000/pci@4/pci@0/pci@0/scsi@0 (mpt_sas0):
Jun 10 16:33:33 A4U4S429-D0 Volume 0 is now , enabled, active, data scrub in
progress
Jun 10 16:33:33 A4U4S429-D0 scsi: WARNING: /pci@8000/pci@4/pci@0/pci@0/scsi@0
(mpt_sas0):
Jun 10 16:33:33 A4U4S429-D0 Volume 286 is degraded
Jun 10 16:33:33 A4U4S429-D0 scsi: /pci@8000/pci@4/pci@0/pci@0/scsi@0 (mpt_sas0):
Jun 10 16:33:33 A4U4S429-D0 Volume 0 is now , enabled, active, data scrub in
progress
```

Dans l'exemple suivant, portant sur les résultats de sortie de la commande `show-children`, affichés dans « [14.2.4 Préparation avant utilisation du RAID matériel](#) », le message d'erreur s'affichant sur l'écran vous indique que l'échange à chaud créé à partir de l'ID cible c (DevHandle 0xc) n'a pas réussi.

```
Jun 4 18:05:53 1S-341-D0 scsi: /pci@8000/pci@4/pci@0/pci@0/scsi@0 (mpt_sas0):  
Jun 4 18:05:53 1S-341-D0 PhysDiskNum 5 with DevHandle 0xc in slot 0 for  
enclosure with handle 0x0 is now offline
```

Affichage de l'état à l'aide de l'utilitaire Fcode

Pour rechercher une panne de lecteur de disque, arrêtez le système et utilisez la commande `show-volumes` de l'utilitaire FCode.

Pour plus de détails, consultez « [14.2.8 Vérification du statut d'un volume RAID matériel et d'un lecteur de disque](#) ».

Affichage de l'état à l'aide de l'utilitaire SAS2IRCU

Vous pouvez également utiliser l'utilitaire SAS2IRCU pour vérifier une panne du lecteur de disque.

Pour plus de détails sur l'utilitaire SAS2IRCU, consultez le début de « [14.2 Configuration du RAID matériel](#) ». De même, pour afficher l'état à l'aide de l'utilitaire SAS2IRCU, consultez « [14.2.8 Vérification du statut d'un volume RAID matériel et d'un lecteur de disque](#) » et pour afficher des exemples, consultez « [Annexe F Exemples d'affichage de la commande d'utilitaire SAS2IRCU](#) ».

14.2.10 Remplacement d'un lecteur de disque défaillant

Cette section décrit comment remplacer un lecteur de disque défaillant au sein des lecteurs de disque qui composent un volume RAID.

RAID0

Si un lecteur de disque se trouvant dans un volume RAID0 s'avère défaillant, toutes les données contenues dans ce volume seront perdues. Remplacez le lecteur de disque défaillant par un nouveau lecteur de disque de même capacité, recréez le volume RAID0, et restaurez les données à partir de la sauvegarde.

RAID1/RAID10/RAID1E

Remplacez le lecteur de disque défaillant par un nouveau lecteur de disque de même capacité. La synchronisation débute lorsque le nouveau lecteur de disque est incorporé au volume RAID.

Remarque : si deux lecteurs de disque subissent une panne au même moment, le volume RAID entre en état (Failed).

Remplacez le lecteur de disque en panne, recréez le volume RAID, puis restaurez les données depuis une sauvegarde.

Dans une configuration d'échange à chaud, le lecteur de disque d'échange à chaud est automatiquement resynchronisé de manière à restaurer les données. Remplacez le lecteur de disque défectueux immédiatement sans démarrer ou redémarrer Oracle Solaris ni démarrer OpenBoot PROM.

Autrement, si vous remplacez le lecteur de disque après avoir démarré ou redémarré Oracle Solaris ou avoir démarré OpenBoot PROM, le basculement vers le lecteur de disque de rechange à chaud ne se produira pas lorsque le lecteur de disque sera à nouveau en panne.

Dans ce cas, après avoir remplacé le lecteur de disque défectueux, effacez la configuration de rechange à chaud du lecteur de disque, et recréez-en une pour permettre la récupération.

Utilisez l'utilitaire SAS2IRCU pour effacer/créer un composant de rechange à chaud. Consultez les Annexes « [F.6 Suppression d'un composant de rechange à chaud d'un volume RAID matériel](#) » et « [F.5 Création d'un composant de rechange à chaud d'un volume RAID matériel](#) ».

14.2.11 Réactivation d'un volume RAID matériel

Cette section indique comment réactiver un volume RAID matériel après avoir remplacé l'unité de mémoire de processeur (inférieure) du SPARC M12-2/M12-2S/ M10-4/M10-4S ou de l'unité de la carte mère SPARC M12-1/M10-1.

Après le remplacement de l'unité susmentionnée, le volume RAID matériel est désactivé parce qu'aucune information relative au RAID matériel ne figure sur le contrôleur SAS (contrôleur RAID matériel). Par conséquent, vous devez réactiver le volume RAID matériel en suivant les procédures suivantes.

1. **Sélectionnez un périphérique pour afficher les informations du volume et vérifier qu'il n'est pas activé.**

Remarque : après exécution de la commande `select`, vous devez exécuter la commande `unselect-dev`. Une fois cette procédure terminée, exécutez la commande `unselect-dev` en fonction des instructions données à l'Étape 4.

Dans l'exemple suivant, il est indiqué que le statut est désactivé, ce qui signifie que le volume RAID est désactivé.

```
{0} ok select /pci@8000/pci@4/pci@0/pci@0/scsi@0
{0} ok show-volumes
Volume 0 Target 11e Type RAID1 (Mirroring)
  Name raid1-volume WWID 0c233a838262c6c5
  Optimal Enabled Inactive Consistent
  2 Members 1169920000 Blocks, 598 GB
  Disk 0
    Primary Optimal
    Target a TOSHIBA MBF2600RC 3706 PhyNum 0
  Disk 1
    Secondary Optimal
    Target b TOSHIBA MBF2600RC 3706 PhyNum 1
{0} ok
```

2. **Exécutez la commande `activate-volume` pour activer le volume RAID.**
L'exemple suivant indique que le volume RAID dont le numéro est 0 est réactivé.

```
{0} ok 0 activate-volume
Volume 0 is now activated
{0} ok
```

3. **Exécutez la commande show-volumes pour vérifier que le volume RAID est activé.**

Dans l'exemple suivant, il est indiqué que le nettoyage des données est en cours, ce qui signifie que le volume RAID est activé.

```
{0} ok show-volumes
Volume 0 Target 11e Type RAID1 (Mirroring)
Name raid1-volume WWID 0c233a838262c6c5
Optimal Enabled Data Scrub In Progress
2 Members 1169920000 Blocks, 598 GB
Disk 0
Primary Optimal
Target a TOSHIBA MBF2600RC 3706 PhyNum 0
Disk 1
Secondary Optimal
Target b TOSHIBA MBF2600RC 3706 PhyNum 1
{0} ok
```

4. **Exécutez la commande unselect-dev afin de désélectionner le contrôleur sélectionné lors de la préparation.**

```
{0} ok unselect-dev
{0} ok
```

Remarque : effectuez un arrêt correctement avant de remplacer l'unité de mémoire de processeur (inférieure) du SPARC M12-2/M12-2S/M10-4/M10-4S ou de l'unité de carte mère SPARC M12-1/M10-1. Puis, confirmez que le système est arrêté, et remplacez le composant. Si le système s'arrête sans que l'arrêt soit correctement géré, à cause d'une panne d'électricité ou autre, une vérification de périphériques (media check) non prévue peut s'exécuter après l'activation du volume RAID.

Lors d'une vérification de périphérique, vous ne pouvez obtenir l'état de vérification de périphérique à partir des utilitaires Fcode et SAS2IRCU. Pendant cette période, l'état du volume RAID devient Optimal. Vérifiez si la DEL du lecteur de disque clignote pour confirmer le statut d'exécution de la vérification de périphérique. Lorsque la DEL passe de l'état clignotant à l'état allumé, cela signifie que la vérification de périphérique est terminée. Lors de la vérification de périphérique, vous pouvez accéder au volume RAID matériel comme d'habitude, mais les performances d'E/S peuvent être insuffisantes par rapport au volume RAID matériel lorsque la vérification de périphérique n'est pas en cours d'exécution. La durée nécessaire pour la vérification de périphérique est la même que celle de la synchronisation pour la configuration ou la maintenance du RAID matériel. Pour le temps nécessaire standard, consultez « [Tableau 14-8 Délai de synchronisation standard du RAID matériel](#) ».

14.2.12 Spécification d'un volume RAID de matériel en tant que périphérique de démarrage

Cette section indique comment spécifier un volume RAID matériel comme périphérique de démarrage.

Pour plus de détails sur la spécification d'un périphérique de démarrage, consultez « [Annexe I Comment spécifier le périphérique de démarrage](#) ».

1. **Sélectionnez le périphérique et afficher les informations relatives à son volume.**
Vérifiez le WWID du volume RAID.

Ci-dessous se trouve un exemple du SPARC M10. Vérifiez le WWID du volume RAID.

```
{0} ok select /pci@8000/pci@4/pci@0/pci@0/scsi@0
{0} ok show-volumes
Volume 0 Target 11e Type RAID1 (Mirroring)
  Name raid1-volume WWID 0c233a838262c6c5
  Optimal Enabled Data Scrub In Progress
  2 Members 1169920000 Blocks, 598 GB
  Disk 1
    Primary Optimal
    Target a TOSHIBA MBF2600RC 3706 PhyNum 0
  Disk 0
    Secondary Optimal
    Target b TOSHIBA MBF2600RC 3706 PhyNum 1
{0} ok unselect-dev
{0} ok
```

2. **Spécifiez le volume RAID qui a été confirmé à l'étape 1 comme périphérique de démarrage.**

Respectez les règles lorsque vous spécifiez le volume RAID.

- a. Remplacez le numéro « 0 » au début du WWID du volume RAID par « 3 ».
Puisque le WWID du volume RAID qui a été confirmé à l'étape 1 est « 0c233a838262c6c5 », il devient « 3c233a838262c6c5 ».
- b. Sur le WWID du volume RAID de l'étape 2a (celui sur lequel vous avez remplacé un chiffre), ajoutez « disk@w » au début, et « ,0:a » à la fin.
- c. Spécifiez le chemin d'accès complet du périphérique de démarrage RAID comme argument de la commande `setenv boot-device` ci-dessous. Le chemin d'accès complet est le chemin d'accès de périphérique sélectionné à l'étape 1 « /pci@8000/pci@4/pci@0/pci@0/scsi@0/ », suivi du nom du périphérique de démarrage RAID de l'étape 2b « disk@w3c233a838262c6c5,0:a ».

```
{0} ok setenv boot-device /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@
w3c233a838262c6c5,0:a
```

14.3 Utilisation du service LDAP

Lightweight Directory Access Protocol (LDAP) est un protocole utilisé pour accéder à un service de répertoire sur réseau. En principe, l'authentification et le privilège d'utilisateur d'un compte d'utilisateur XSCF sur le SPARC M12/M10 sont gérés par le XSCF maître local. Cependant, en utilisant LDAP, ils peuvent être gérés par un service de répertoire (serveur LDAP) sur un réseau. En outre, si plusieurs systèmes SPARC M12/M10 sont installés, le compte d'utilisateur XSCF commun à tous ces systèmes peut être utilisé avec LDAP.

Pour gérer les paramètres de compte d'utilisateur XSCF, tels que l'authentification et les privilèges d'utilisateur, à partir du protocole LDAP, configurez le XSCF comme un client LDAP.

Pour plus de détails sur la gestion des paramètres du compte d'utilisateur XSCF via un service de répertoire sur un réseau utilisant le protocole LDAP, consultez « [3.5.12 Gestion de comptes d'utilisateur XSCF à l'aide de LDAP](#) ».

14.4 Utilisation du démarrage SAN

Le SPARC M12/M10 prend en charge le démarrage SAN.

Le démarrage SAN est un système doté de stockage externe, plutôt qu'un lecteur de disque interne intégré au serveur, configuré comme disque de démarrage.

Le SPARC M12/M10 utilise une carte Fibre Channel pour la connexion entre les périphériques de stockage externes et le système peut être configuré de manière à utiliser le démarrage SAN avec la fonction Fcode d'OpenBoot PROM.

Pour plus d'informations sur la construction d'un système avec le démarrage SAN, consultez les documents Oracle suivants :

- Oracle Solaris Administration: SAN Configuration and Multipathing

14.5 Utilisation d' iSCSI

iSCSI est un protocole utilisé pour échanger les commandes SCSI via un réseau IP. Ces commandes sont utilisées pour la communication entre le serveur et le stockage externe.

Dans le SPARC M12/M10, vous pouvez configurer le système de manière à utiliser iSCSI. Une fois que le système est configuré de manière à utiliser iSCSI, plusieurs serveurs peuvent partager une grande capacité de stockage via un réseau TCP/IP.

14.6 Gestion de l'alimentation à distance pour le SPARC M12/M10 et les périphériques d'E/S

Cette section offre un aperçu de la fonction de gestion de l'alimentation à distance et une description de ses paramètres pour le SPARC M12/M10.

14.6.1 Fonction de gestion de l'alimentation à distance pour SPARC M12/M10

La fonction de gestion d'alimentation à distance pour le système SPARC M12/M10 (RCIL, Remote Cabinet Interface over LAN : interface d'armoire distante par LAN) est une interface contrôlant la fonction de gestion d'alimentation à distance pour l'alimentation entre des systèmes SPARC M12/M10 ou des périphériques d'E/S. La fonction RCIL utilise une interface propriétaire basée sur IPMI over LAN. Si les fonctions IPMI générales suivantes sont prises en charge, la fonction RCIL peut être définie comme cible de la gestion de l'alimentation à distance sans tenir compte des différences au niveau du matériel contrôlé ou des systèmes d'exploitation. La fonction RCIL utilise le XSCF-LAN du SPARC M12/M10.

- Mise sous tension et hors tension : Chassis Control
- Obtention de l'état de l'alimentation : Get Chassis Status

Tableau 14-12 affiche les termes et définitions utilisés avec la fonction de gestion de l'alimentation à distance pour le SPARC M12/M10.

Tableau 14-12 Termes et définitions utilisés pour la gestion de l'alimentation à distance	
Terme	Définition
Nœud d'hôte	Un châssis SPARC M12/M10 prenant en charge la fonction de gestion d'alimentation à distance. Les SPARC M12-2, M12-2S, M10-1, M10-4 et M10-4S prennent en charge la fonction de gestion de l'alimentation à distance pour le système. Le nœud d'hôte défini comme nœud principal lors de la création d'un groupe de gestion de l'alimentation à distance est appelé nœud d'hôte principal. Le nœud d'hôte principal est un nœud d'hôte qui contrôle les connexions avec les autres nœuds d'hôte et nœuds E/S.
Sous-nœud	C'est une partition physique se trouvant dans le SPARC M12/M10
Nœud d' E/S	Périphérique d'E/S ou boîtier de commande d'alimentation prenant en charge la fonction de gestion de l'alimentation à distance du SPARC M12/M10
Groupe de gestion de l'alimentation à distance	Groupe obtenu par le regroupement des cibles de gestion de l'alimentation à distance, comme un nœud d'hôte, un sous-nœud et un nœud E/S. Un ID de groupe unique est attribué à un groupe de gestion de l'alimentation à distance.

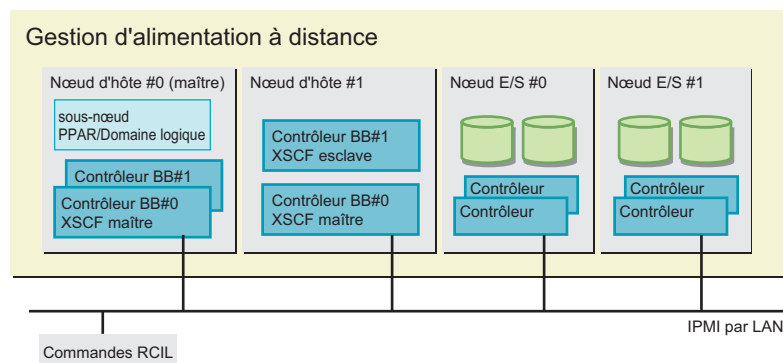
Tableau 14-12 Termes et définitions utilisés pour la gestion de l'alimentation à distance
(suite)

Terme	Définition
Contrôleur	Un mécanisme permettant de contrôler la fonction de gestion d'alimentation à distance. Un contrôleur doit être installé dans chaque nœud. Dans le SPARC M12/M10, le XSCF est un contrôleur.

Si la fonction de gestion de l'alimentation à distance est utilisée, créez un groupe de gestion de l'alimentation à distance en combinaison avec des nœuds verrouillés en alimentation. Vous pouvez contrôler la gestion de l'alimentation à distance par groupe de gestion de l'alimentation à distance créé.

Remarque : chaque nœud d'hôte, sous-nœud et nœud d' E/S ne peut être défini que pour un seul groupe de gestion de l'alimentation à distance.

Figure 14-5 Exemple de groupe de gestion de l'alimentation à distance du SPARC M12/M10



14.6.2 Compréhension des formes de connexion pour la gestion de l'alimentation à distance

Connectez via un LAN les nœuds hôtes, sous-nœuds, et nœuds E/S qui prennent en charge la fonction de gestion d'alimentation à distance pour le SPARC M12/M10.

Ci-après, les spécifications de connexion.

Tableau 14-13 Spécifications de connexion du contrôle de l'alimentation

Élément	Description
Types de connexion	Connexion LAN La connexion prend l'une des formes suivantes : - Utilisation de XSCF-LAN#0 - Utilisation de XSCF-LAN#0 et XSCF-LAN#1

Tableau 14-13 Spécifications de connexion du contrôle de l'alimentation (*suite*)

Élément	Description
Vitesse de transmission	100 Mbit/s ou plus
Protocole Internet	IPv4
DHCP	Non pris en charge Si la fonction de gestion de l'alimentation à distance du SPARC M12/M10 est utilisée, vous devez définir une adresse IP fixe pour une cible de connexion.
Protocole de connexion	IPMI(*1) par LAN (Intelligent Platform Management Interface)

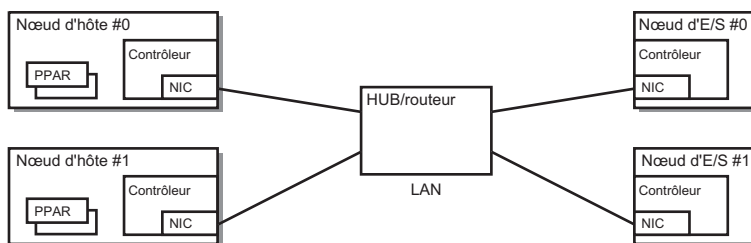
*1 La version IPMI prise en charge est IPMI 2.0.

Dans un SPARC M12/M10, IPMI peut uniquement être utilisé en interne par la fonction de gestion de l'alimentation à distance. IPMI ne peut pas être utilisé par ipmitool ou n'importe quelle fonction autre que celle de gestion d'alimentation à distance du SPARC M12/M10.

Connexion standard pour gestion de l'alimentation à distance

Connectez via un LAN identique les nœuds hôtes, sous-nœuds, et nœuds E/S équipés d'un contrôleur qui prend en charge la fonction de gestion d'alimentation à distance pour le SPARC M12/M10.

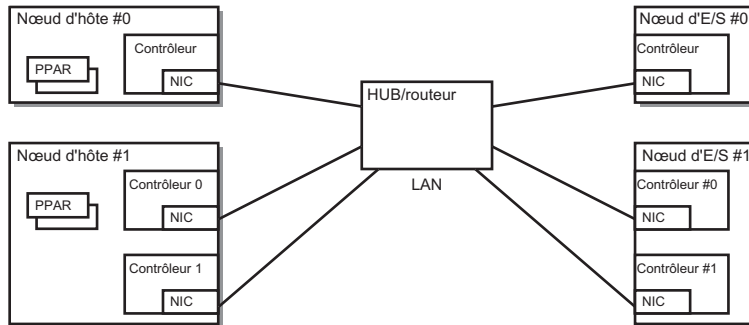
Figure 14-6 Formes de connexion pour la gestion de l'alimentation à distance



Connexion en cas de contrôleurs en mode duplex

Si les contrôleurs d'un nœud hôte sont en mode duplex, alors chaque contrôleur peut être connecté à un même LAN. La gestion de l'alimentation à distance fonctionne à partir du XSCF maître.

Figure 14-7 Formes de connexion pour la gestion de l'alimentation à distance lorsque les contrôleurs sont dupliqués



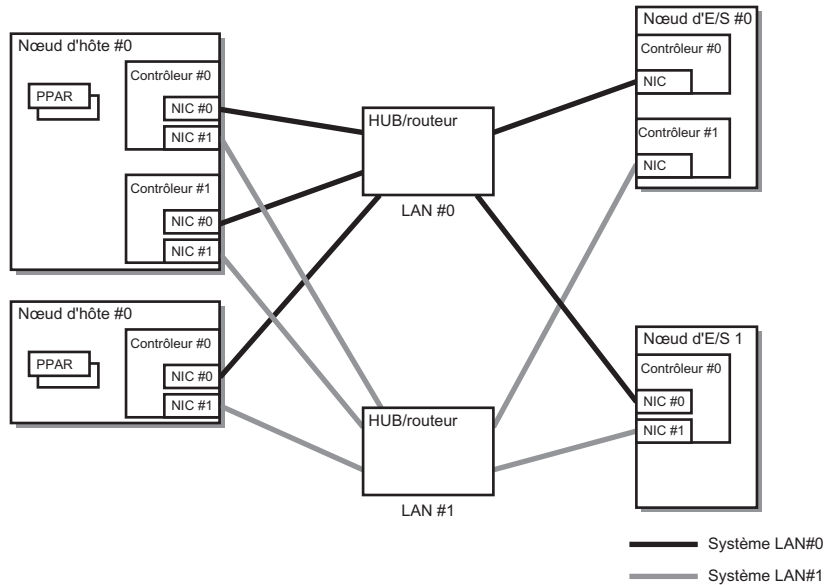
Remarque : lorsque les contrôleurs sont en mode duplex, si les contrôleurs partagent l'adresse IP d'une carte LAN comme adresse virtuelle, configurez l'un des contrôleurs.

Connexion en cas de chemins en mode duplex

Si les conditions suivantes sont réunies, les chemins de connexion pour la gestion de l'alimentation à distance peuvent être en mode duplex.

- Deux cartes LAN peuvent être installées sur chaque contrôleur de tous les nœuds
- Deux cartes LAN peuvent être montées sur le contrôleur du nœud d'hôte et le nœud d' E/S dispose de l'une des configurations suivantes
 - Les contrôleurs d'un nœud E/S sont en mode duplex
 - Deux cartes LAN peuvent être montées sur le contrôleur du nœud d' E/S

Figure 14-8 Formes de connexion pour la gestion de l'alimentation à distance en cas de chemins en mode duplex



14.6.3 Structure de la gestion de l'alimentation à distance

La gestion de l'alimentation à distance pour le SPARC M12/M10 est contrôlée par le groupe de gestion de l'alimentation à distance.

Parmi les nœuds d'hôte dans un groupe, ceux dont la fonction de gestion de l'alimentation à distance est activée sont sujets à la gestion de l'alimentation à distance. L'état d'alimentation d'un groupe de gestion de l'alimentation à distance est déterminé par l'état du nœud d'hôte du groupe.

- **État actif**
L'état d'alimentation d'un des nœuds d'hôte du groupe de gestion de l'alimentation à distance est activé
- **État inactif**
L'état d'alimentation d'un des nœuds d'hôte du groupe de gestion de l'alimentation à distance est désactivé

Cette section décrit les structures de gestion de la mise sous tension et hors tension à distance selon les paramètres suivants.

Tableau 14-14 Structure de la gestion de l'alimentation à distance (Exemple)

Élément de réglage	Nœud d'hôte#0	Nœud d'hôte#1	Nœud d'hôte#2	Nœud E/S#0	Nœud E/S#1
Paramétrage de la gestion à distance	Désactivé	Activé	Activé	Paramètre désactivé	Paramètre désactivé
Nœud maître	Oui	Non	Oui	Paramètre désactivé	Paramètre désactivé

Mécanisme de verrouillage lors de la mise sous tension

Si l'un des nœuds d'hôte se trouvant dans un groupe de gestion de l'alimentation à distance est mis sous tension, alors tous les nœuds d'hôte, sous-nœuds et nœuds E/S de ce groupe sont mis sous tension. Les nœuds d'hôte sont mis sous tension, suivis des nœuds E/S.

Remarque :vous pouvez définir le délai d'attente des nœuds d'hôte jusqu'à ce que les périphériques du nœud E/S soient accessibles. Utilisez la commande `setpowerupdelay` du microprogramme XCSF pour effectuer la configuration. Pour plus de détails, consultez « 4.2.2 Réglage/Vérification du temps d'attente au démarrage ».

Si vous ne réglez pas le délai d'attente, le démarrage du système peut échouer car un périphérique de nœud E/S est inaccessible lorsque les nœuds d'hôte tentent d'y accéder. De plus, si des nœuds E/S sont commutés ou le réglage est modifié, la durée pour accéder aux appareils change. Les périphériques ne seront donc peut-être pas accessibles lorsque un nœud d'hôte tentera d'y accéder.

Si vous avez commuté des nœuds E/S ou modifié le réglage, utilisez la commande `setpowerupdelay` pour définir un nouveau délai d'attente.

Structure de la gestion de la mise hors tension à distance

Tous les nœuds d'hôte d'un groupe de gestion de l'alimentation à distance sont mis hors tension, suivis par les nœuds E/S du groupe.

Gestion d'alimentation à distance via Wake on LAN

En général, les nœuds cibles de la fonction de gestion de l'alimentation à distance des SPARC M12/M10 sont les hôtes et les périphériques d'E/S sur lesquels un contrôleur est monté. Le contrôleur permet la communication IPMI même lorsque les hôtes et les périphériques d'E/S sont mis hors tension.

Lorsque toutes les conditions suivantes sont satisfaites, ces périphériques sur lesquels ce contrôleur n'est pas monté peuvent également assurer la gestion de l'alimentation à distance à l'aide de la fonction de gestion de l'alimentation à distance du SPARC M12/M10.

- Conditions des périphériques
 - Wake on LAN est pris en charge.
La mise sous tension est effectuée avec Wake on LAN.
 - La communication IPMI peut être effectuée.
Après avoir mis sous tension avec Wake on LAN, la communication IPMI via le LAN sert à effectuer la mise hors tension et à obtenir l'état d'alimentation.

Remarque : un nœud d'hôte pour lequel Wake on LAN est réglé ne peut pas devenir un nœud maître.

Remarque : Wake on LAN ne peut pas être défini pour le châssis SPARC M12/M10. Par conséquent, Wake on LAN ne peut pas être utilisé pour mettre sous tension le châssis SPARC M12/M10.

Remarque : le réglage Wake on LAN varie selon le nœud. Consultez les manuels de chaque nœud.

Verrouillage en cas de temps de récupération de panne

Si un nœud au sein d'un groupe de gestion de l'alimentation à distance ne peut pas communiquer après une récupération suite à une panne ou autre problème, l'opération est comme suit.

- S'il s'agit d'une panne de nœud E/S
Si le statut d'alimentation d'un groupe de gestion de l'alimentation à distance est activé, le nœud d'hôte maître émet une instruction de mise sous tension.
- S'il s'agit d'une panne de nœud d'hôte
Même si le statut d'alimentation d'un groupe de gestion de l'alimentation à distance est activé, le nœud d'hôte maître n'émet pas une instruction de mise sous tension.

14.6.4 Avant de régler la gestion de l'alimentation à distance

Si vous paramétrez la gestion d'alimentation à distance, raccordez les câbles LAN et configurez au préalable les paramètres réseau sur le XSCF-LAN et les périphériques d'E/S qui effectuent une gestion d'alimentation à distance.

14.6.5 Flux pour régler la gestion de l'alimentation à distance

Cette section décrit le flux pour définir la gestion de l'alimentation à distance, selon les cas suivants :

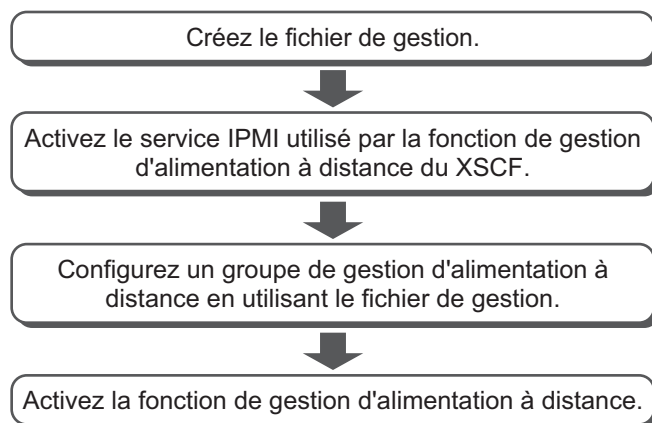
- Réglage de la fonction de gestion de l'alimentation à distance pour la première fois
- Ajouter, supprimer ou remplacer des nœuds dans un groupe de gestion de l'alimentation à distance existant

Réglage de la gestion de l'alimentation à distance pour la première fois

La figure suivante présente un exemple des tâches permettant de régler la gestion de l'alimentation à distance pour la première fois.

Remarque : si un paramètre de gestion de l'alimentation à distance existant est activé, initialisez le réglage de la gestion de l'alimentation à distance.

Figure 14-9 Flux pour régler la gestion de l'alimentation à distance pour la première fois

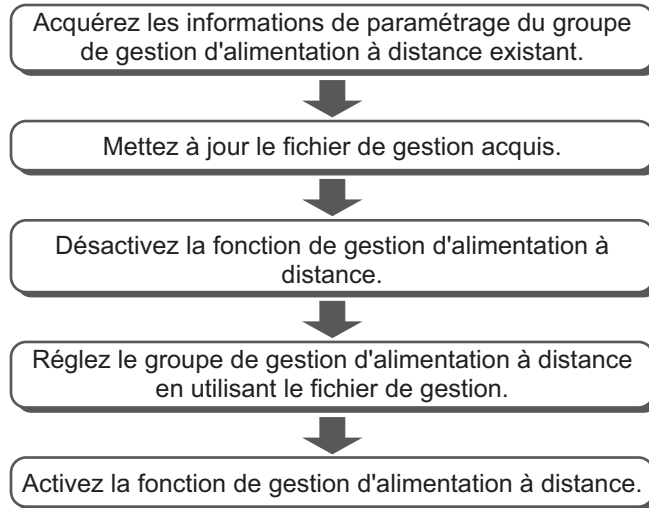


Remarque : XCP 2290 et les versions ultérieures prennent en charge le paramètre activer/désactiver pour le service IPMI.

Ajouter, supprimer ou remplacer des nœuds dans un groupe de gestion de l'alimentation à distance existant

La figure suivante décrit le flux pour l'ajout, la suppression ou le remplacement de nœuds dans un groupe de gestion de l'alimentation à distance existant.

Figure 14-10 Flux pour ajouter, supprimer ou remplacer des nœuds dans un groupe de gestion de l'alimentation à distance existant



14.6.6 Vérification du réglage de la gestion de l'alimentation à distance

Utilisez la commande `showremotepwrmgmt` du microprogramme XSCF afin de vérifier le paramètre de la gestion de l'alimentation à distance.

```
XSCF> showremotepwrmgmt [-a|-G groupid [-N gnodeid]]
```

Pour vérifier tous les paramètres de la gestion de l'alimentation à distance, spécifiez `-a`. Pour spécifier un groupe de gestion de l'alimentation à distance, spécifiez `-G groupid`. Pour spécifier un nœud dans un groupe de gestion de l'alimentation à distance, spécifiez « `-N gnodeid` ».

14.6.7 Initialisation du réglage de la gestion de l'alimentation à distance

Utilisez la commande `clearremotepwrmgmt` du microprogramme XSCF afin d'initialiser le paramètre de la gestion de l'alimentation à distance.

```
XSCF> clearremotepwrmgmt [-a|-G groupid]
```

Pour initialiser les paramètres de tous les groupes de gestion de l'alimentation à distance, spécifiez `-a`. Pour spécifier un groupe de gestion de l'alimentation à distance, spécifiez une ID de groupe avec l'option `-G`. Si `-a` et `-G` sont omis, le système

suppose que -a est spécifié.

14.6.8 Activation/Désactivation de la fonction de gestion de l'alimentation à distance

Utilisez la commande `setremotepwrmgmt` du microprogramme XSCF afin d'activer/désactiver la fonction de gestion de l'alimentation à distance.

```
XSCF> setremotepwrmgmt -c enable|disable
```

Pour activer la fonction de gestion de l'alimentation à distance, spécifiez `-c enable`.
Pour la désactiver, spécifiez `-c disable`.

14.6.9 Création d'un fichier de gestion

Créez un fichier de gestion sous format csv afin de paramétrer les groupes de gestion de l'alimentation à distance. Vous pouvez créer le fichier de gestion et le conserver en utilisant une adresse URL accessible à partir du `http`, `https`, `ftp`, ou du modèle de fichier.

Le format de description du fichier de gestion est le suivant.

```
1,1,0x01,8a041209b35947899e7bfa5d578dbd3f,0x03,0x00,default,,10.
24.0.0,0x10,xx:xx:xx:xx:xx:xx,,,,,,,,,"4,5,6,7,8,9,10,11,12"
1,2,0x00,8a041209b35947899e7bfa5d578dbd40,0x03,0x00,default,,
10.
24.0.0,0x10,xx:xx:xx:xx:xx:xx,,,,,,,,
1,3,0x10,8a041209b35947899e7bfa5d578dbd41,0x03,0x00,default,,10.
24.0.0,0x10,xx:xx:xx:xx:xx:xx,,,,,,,,(Omis)
1,128,0x20,8a041209b35947899e7bfa5d578dbd42,0x03,0x00,default,,1
0.24.0.0,0x10,xx:xx:xx:xx:xx:xx,,,,,,,,
```

Pour chaque rangée, spécifiez dans l'ordre correspondant au GroupID, NodeID, NodeType, NodeIdentName, Linkage, Operation, User, Password, IP0-0, Slave0-0, MAC0-0, IP0-1, Slave0-1, MAC0-1, IP1-0, Slave1-0, MAC1-0, IP1-1, Slave1-1, MAC1-1 et SubNode.

Ci-après, les informations relatives au réglage.

Tableau 14-15	Éléments de réglage du fichier de gestion de la gestion de l'alimentation à distance
Élément	Description
GroupID	ID du groupe de gestion de l'alimentation à distance Vous pouvez spécifier un entier (décimale) compris entre 1 et 32. Tous les ID de groupe contenus dans un fichier de gestion doivent être identiques.

Tableau 14-15 Éléments de réglage du fichier de gestion de la gestion de l'alimentation à distance (*suite*)

Élément	Description
NodeID	ID de nœud du périphérique de gestion de l'alimentation à distance Vous pouvez spécifier un entier (décimale) compris entre 1 et 128. Tous les ID de nœud contenus dans un fichier de gestion doivent être identiques.
NodeType	Type de nœud du périphérique de gestion de l'alimentation à distance Spécifiez l'une des valeurs suivantes. 0x00 : nœud hôte, 0x01 : nœud hôte maître, 0x10 : nœud d'E/S, 0x20 : boîtier de gestion de l'alimentation à distance
NodeIdentName	Nom unique du périphérique de gestion de l'alimentation à distance Vous pouvez spécifier GUID système ou une chaîne de caractère unique. Comme illustré dans l'exemple, le GUID système est spécifié comme 32 chiffres consécutifs. La valeur est hexadécimale et ne tient pas compte de la casse. S'il s'agit d'une chaîne de caractère, vous pouvez spécifier une valeur décimale en utilisant jusqu'à 32 chiffres.
Linkage	Valeur indiquant la gestion de la mise sous tension à distance (hexadécimale) Spécifiez l'une des valeurs suivantes. 0x00 : désactivation, 0x01 : activation (On), 0x02 : activation (Off), 0x03 : activation (On+Off)
Operation	Valeur représentant la méthode de mise sous tension Spécifiez-la en faisant recours à l'une des méthodes suivantes. 0x00:IPMI, 0x01:WakeOnLAN
User	Nom d'utilisateur IPMI Laissez ce champ vide. Si le champ n'est pas vide, l'opération ne peut être garantie.
Password	Mot de passe IPMI Laissez ce champ vide.
IPAddress	Adresse IP du port IPMI du contrôleur Vous pouvez spécifier une adresse IPv4 avec une chaîne de caractère.
SlaveAddress	Valeur représentant l'adresse de l'esclave IPMI du contrôleur (hexadécimale) Spécifiez « 0x20 ».
SubNodeID	Chaîne de caractère représentant une ID de sous-nœud qui est cible de contrôle 0 à 31, ou vide. Vous pouvez spécifier les ID du sous-nœud cible (décimal) en les séparant par une virgule (,), et en encadrant le tout par des guillemets doubles (« »). Le vide indique que tout le nœud représente la cible de contrôle.

14.6.10 Activation/Désactivation du service IPMI utilisé par la fonction de gestion de l'alimentation à distance du XSCF

Pour utiliser la fonction de gestion de l'alimentation à distance, vous devez activer le service IPMI.

Le service IPMI peut uniquement être utilisé par la fonction de gestion de l'alimentation à distance.

Activez/désactivez le service IPMI à l'aide de la commande `setpacketfilters` sur le XSCF.

```
XSCF> setpacketfilters -c ipmi_port [enable|disable]
```

Pour activer le service IPMI, spécifiez `-c ipmi_port enable`. Pour la désactiver, spécifiez `-c ipmi_port disable`.

La valeur par défaut est `disable`.

Remarque : XCP 2290 et les versions ultérieures prennent en charge le paramètre activer/désactiver pour le service IPMI.

Sur XCP 2280 et les versions précédentes, le service IPMI est activé et vous ne pouvez pas le désactiver.

Si le microprogramme est mis à jour à partir d'une version XCP 2280 ou antérieure vers une version XCP 2290 ou plus ultérieure, le service IPMI sera toujours activé comme suit :

- Lorsque la fonction de gestion de l'alimentation à distance est utilisée : activer
 - Lorsque la fonction de gestion de l'alimentation à distance n'est pas utilisée : désactiver
-

14.6.11 Acquisition d'informations de réglage du groupe de gestion de l'alimentation à distance

Utilisez la commande `getremotepwrmgmt` du microprogramme XSCF afin d'obtenir les informations de réglage d'un groupe de gestion de l'alimentation à distance.

```
XSCF> getremotepwrmgmt -G groupid configuration_file
```

Pour `groupid`, vous pouvez spécifier l'ID d'un groupe de gestion de l'alimentation à distance dont les informations de réglage sont obtenues. En ce qui concerne le fichier de gestion, vous pouvez spécifier le nom du fichier de gestion qui conserve les informations de réglage obtenues.

14.6.12 Réglage d'un groupe de gestion de l'alimentation à distance

Utilisez la commande `setremotepwrmgmt` pour configurer un groupe de gestion de l'alimentation à distance à l'aide d'un fichier de gestion.

```
XSCF> setremotepwrmgmt -c config configuration_file
```

Vous pouvez spécifier `-c config` si vous configurez un groupe de gestion de l'alimentation à distance. Pour `configuration_file`, vous pouvez spécifier le nom du fichier de gestion utilisé pour la configuration.

14.7 Utilisation de l'alimentation sans interruption

Le SPARC M12/M10 prend en charge la connexion de l'alimentation sans interruption (UPS) en option.

L'utilisation d'une alimentation sans interruption (UPS) permet une fourniture d'alimentation électrique stable au système, en cas de panne de courant, panne d'électricité, etc. Une alimentation sans interruption (UPS) APC est prise en charge, et un LAN sert d'interface entre les domaines et l'UPS.

Pour plus de détails sur la façon de connecter une alimentation non interruptible, consultez « Connexion d'une alimentation sans interruption (UPS) (en option) » dans le *Guide d'installation* de votre serveur.

14.8 Utilisation du démarrage vérifié

Cette section décrit la fonction de démarrage vérifié qui fournit une protection sécurisée au démarrage d'Oracle Solaris.

14.8.1 Bases du démarrage vérifié

Le démarrage vérifié est une fonction qui protège le SPARC M12/M10 des menaces qui peuvent être présentes dans les pilotes, les modules ou les autres programmes chargés au démarrage d'Oracle Solaris.

Le processus de démarrage d'un système est vérifié et sécurisé pour les menaces

suivantes :

- L'altération d'un module de noyau
- L'insertion de programmes malveillants (cheval de Troie, logiciel espion, outil de dissimulation d'activité, etc.) qui usurpent l'identité des modules de noyau légitimes, ou le remplacement d'un programme avec un tel programme
- L'installation de modules de noyau tiers non-autorisés

Le système Oracle Solaris 11.2 fournit deux types de méthodes de configuration pour la fonction de démarrage vérifié : l'utilisation d'un XSCF et l'utilisation d'Oracle Solaris. Dans Oracle Solaris 11.3 ou ultérieur, seule la méthode de configuration utilisant un XSCF est disponible.

Cette section décrit la méthode pour la configuration de la fonction avec un XSCF.

Pour la méthode de configuration de la fonction avec Oracle Solaris, consultez

« How to Enable Verified Boot on Legacy SPARC Systems and x86 Systems » dans *Securing Systems and Attached Devices in Oracle Solaris 11.2* d'Oracle Solaris.

14.8.2 Mécanisme de vérification du démarrage par le démarrage vérifié

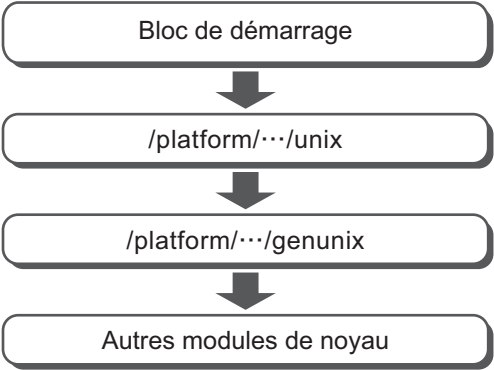
La vérification du démarrage par le démarrage vérifié nécessite les certificats de clé publique X.509 enregistrés avec le XSCF. Le processus de démarrage du système effectue une vérification du démarrage en utilisant les clés publiques contenues dans les certificats de clé publique X.509.

Le mécanisme pour effectuer la vérification du démarrage est le suivant :

- Un utilisateur configure le démarrage vérifié avec le XSCF qui prend en charge la fonction de démarrage vérifié. Dans ce travail de configuration, l'utilisateur enregistre ou sélectionne un certificat de clé publique X.509 et règle les stratégies qui contrôlent le comportement de la vérification du démarrage. Les données de configuration sont enregistrées dans le XSCF maître.
- Supposons que les données de configuration du démarrage vérifié dans le XSCF ont été modifiées. Les données de configuration modifiées seront activées pour la vérification du démarrage de tous les modules la prochaine fois qu'OpenBoot PROM est lancé.
- Au démarrage d'une partition physique, les données de configuration sont rapportées dans le microprogramme OpenBoot PROM et Oracle Solaris via le XSCF, et ils effectuent une vérification du démarrage. La vérification du démarrage est également effectuée quand une partition physique, le microprogramme OpenBoot PROM ou Oracle Solaris est redémarré.

La vérification du démarrage par le microprogramme OpenBoot PROM et Oracle Solaris est effectuée dans l'ordre montré dans [Figure 14-11](#).

Figure 14-11 Ordre de vérification du démarrage



14.8.3 Certificats de clé publique X.509 pour le démarrage vérifié

Tableau 14-16 affiche les deux types de certificats de clé publique X.509 utilisés pour le démarrage vérifié.

Tableau 14-16 Certificats de clé publique X.509 utilisés pour le démarrage vérifié

Type de certificat	Description
Certificat par défaut du système (système par défaut)	Certificat par défaut du système du XSCF Le XSCF a le même certificat que le certificat de clé publique (/etc/certs/*SE) contenu dans Oracle Solaris. Le XSCF a 1 ou 2 certificats par défaut du système, qui sont remplacés par les derniers certificats de clé publique au moment de la mise à jour du microprogramme. Les certificats par défaut du système n'ont donc pas besoin d'être enregistrés/restaurés à partir du système. De plus, ce ne sont pas des certificats que les utilisateurs peuvent traiter.
Certificat d'utilisateur	Certificat enregistré par un utilisateur Un certificat émis par un tiers est enregistré comme certificat d'utilisateur avec XSCF. Jusqu'à 5 certificats d'utilisateur peuvent être enregistrés avec le XSCF pour chaque partition physique. Quand il est activé, un certificat enregistré peut être utilisé pour une vérification du démarrage. Les certificats d'utilisateur peuvent être enregistrés/restaurés sur le système. Cependant, les certificats enregistrés ne peuvent pas être restaurés dans un autre SPARC M12/M10.

La vérification du démarrage est effectuée en utilisant le(s) certificat(s) par défaut du système et les certificats d'utilisateur activés.

14.8.4 Stratégies de démarrage vérifié

Tableau 14-17 répertorie les deux stratégies qui contrôlent le démarrage vérifié.

Tableau 14-17 Stratégies de démarrage vérifié

Version système d'exploitation	Stratégie	Description
Oracle Solaris 11.2	Stratégie de démarrage (boot_policy)	Règle la vérification du démarrage pour le bloc de démarrage, unix et genunix. Ces modules sont d'abord chargés pendant le processus de démarrage.
	Stratégie de module (module_policy)	Règle la vérification du démarrage pour les modules de noyau qui ont besoin d'être chargés après genunix.
Oracle Solaris 11.3	Stratégie de démarrage (boot_policy)	Règle la vérification du démarrage pour le bloc de démarrage et unix. Ces modules sont d'abord chargés pendant le processus de démarrage.
	Stratégie de module (module_policy)	Définit la vérification du démarrage pour les modules genunix et de noyau.

Utilisez la commande setvbootconfig du microprogramme XSCF pour régler chaque stratégie.
Les utilisateurs peuvent régler le comportement du processus de démarrage au moment d'une panne de la vérification du démarrage en réglant les stratégies.
Tableau 14-18 répertorie les valeurs qui peuvent être réglées pour chaque stratégie de démarrage et de module. La valeur réglée détermine le fonctionnement de la vérification.

Tableau 14-18 Valeurs de réglages de stratégie

Valeur de réglages de stratégie	Opération
none	La vérification du démarrage n'est pas effectuée. (Par défaut)
warning	La vérification du démarrage est effectuée. La vérification est effectuée avant que la cible de la vérification ne soit chargée. Même si la vérification échoue, la cible de la vérification est chargée et le processus de démarrage continue. Si la vérification du bloc de démarrage et d'unix échoue, l'échec de la vérification est enregistré sur la console du système. Il n'est pas enregistré dans le journal système ni dans le journal d'erreurs XSCF. Si la vérification de genunix et d'autres modules de noyau échoue, l'échec de la vérification est enregistré sur la console du système et dans le journal système. Il n'est pas enregistré dans le journal d'erreurs XSCF.

Tableau 14-18 Valeurs de réglages de stratégie (suite)

Valeur de réglages de stratégie	Opération
enforce	La vérification du démarrage est effectuée. La vérification est effectuée avant que la cible de la vérification ne soit chargée. Si la vérification du bloc de démarrage et d'unix échoue, le processus de démarrage s'arrête. À ce moment-là, l'échec de la vérification est enregistré sur la console du système et le journal d'erreurs XSCF. Il n'est pas enregistré dans le journal système. Si la vérification de genunix échoue, le processus de démarrage s'arrête. À ce moment-là, l'échec de la vérification est enregistré sur la console du système. Il n'est pas enregistré dans le journal d'erreurs XSCF ni dans le journal système. Si la vérification des autres modules de noyau échoue, le démarrage continue sans charger le module. À ce moment-là, l'échec de la vérification est enregistré sur la console du système et dans le journal système. Il n'est pas enregistré dans le journal d'erreurs XSCF.

Remarque : dans Oracle Solaris 11.2 SRU11.2.8.4.0 ou une version ultérieure, si la valeur de réglage de stratégie est appliquée, l'opération suivant l'échec de la vérification de genunix est différente. Si la variable d'environnement auto-boot? d'OpenBoot PROM est true, une panique se produit de façon répétitive. Si ce phénomène persiste, exécutez la commande sendbreak pour le domaine de commande, la commande d'arrêt ldm pour un domaine invité, ou la commande d'arrêt zoneadm pour une zone noyau pour l'arrêter.

Tableau 14-19 montre un exemple des messages émis quand la vérification du démarrage échoue.

Tableau 14-19 Exemple de messages émis quand la vérification du démarrage échoue

Valeur de réglages de stratégie	Message
none	La vérification du démarrage n'est pas effectuée.
warning	Le message d'avertissement suivant apparaît, mais le démarrage d'Oracle Solaris est maintenu. - Message de la console du système dans le cas de genunix WARNING: module /platform/sun4v/kernel/sparcv9/genunix failed elfsign verification. - Message de la console du système ou du journal système dans le cas d'autres modules de noyau WARNING: module /kernel/drv/sparcv9/module failed elfsign verification.
enforce	- Dans le cas du bloc de démarrage Le message d'erreur suivant apparaît, et le démarrage s'arrête à l'invite ok. - Message de la console du système FATAL: Bootblk signature verification failed, verified boot policy = enforce, halting boot - XSCF Journal d'erreurs procédure de démarrage échouée - Message de la console du système ou du journal système dans le cas d'autres modules de noyau Le message d'erreur suivant apparaît, mais le démarrage d'Oracle Solaris est maintenu. Module /kernel/drv/sparcv9/module failed elfsign verification; "module-policy enforce" requested.

14.8.5 Versions d'Oracle Solaris et XCP qui prennent en charge le démarrage vérifié

Tableau 14-20 répertorie les versions d'Oracle Solaris et XCP qui prennent en charge le démarrage vérifié. Le démarrage vérifié peut être utilisé quand les deux conditions dans Tableau 14-20 sont remplies.

Tableau 14-20 Versions d'Oracle Solaris et XCP avec lesquelles le démarrage vérifié peut être utilisé

Oracle Solaris et XCP	Version
Oracle Solaris	11.2 ou version ultérieure
XCP	2250 ou version ultérieure

Le démarrage vérifié depuis un réglage Oracle Solaris est disponible uniquement avec la combinaison de XCP 2240 ou version précédente et d'Oracle Solaris 11.2. Dans XCP 2250 ou ultérieur, son fonctionnement se base sur les données de configuration qui se trouvent dans le XSCF. Une mise à jour du microprogramme depuis la version XCP 2240 ou plus récente ou XCP 2250 ou ultérieure réglera le paramètre par défaut sur « none » pour la stratégie de démarrage vérifié de XSCF. Ce réglage a la priorité, même sur les réglages de configuration d'Oracle Solaris. Pour utiliser le démarrage vérifié, réglez la stratégie avec XSCF.

14.8.6 Liste de prise en charge du démarrage vérifié

Démarrage vérifié sur les domaines invités et les zones noyau

Le démarrage vérifié est seulement pris en charge pour les zones globales dans Oracle Solaris 11.2. De plus, le démarrage vérifié est pris en charge pour les zones de noyau dans Oracle Solaris 11.3 ou versions ultérieures. Pour plus de détails sur la configuration du démarrage vérifié dans les zones de noyau, consultez *Creating and Using Oracle Solaris Kernel Zones*. Pour plus d'informations sur la configuration du démarrage vérifié dans les domaines invités, consultez « Utilisation du démarrage vérifié » dans *Oracle VM Server for SPARC 3.4 Administration Guide*.

Périphérique de démarrage et réglages de stratégie de démarrage vérifié

Le démarrage vérifié prend en charge le démarrage depuis un disque dur (HDD) et le démarrage depuis le réseau. Pour les autres méthodes de démarrage, réglez la stratégie de démarrage vérifié sur « none ».

De plus, lorsque vous effectuez un démarrage vérifié, assurez-vous d'effectuer le démarrage à partir d'un périphérique signé. Sinon, la vérification du démarrage par le démarrage vérifié échoue.

Tableau 14-21 affiche la liste du support de démarrage vérifié.

Tableau 14-21 Liste de prise en charge du démarrage vérifié

	Domaine de commande		Domaine invité	
	Zone globale	Zone noyau	Zone globale	Zone noyau
Démarrage depuis HDD	Oracle Solaris 11.2 ou version ultérieure (*1) XCP 2250 ou version ultérieure	Oracle Solaris 11.3 ou version ultérieure XCP 2250 ou version ultérieure	Domaine de commande : Oracle Solaris 11.3 SRU11.3.8.7.0 ou version ultérieure Domaine invité : Oracle Solaris 11.2 ou version ultérieure XCP 2280 ou version ultérieure	Oracle Solaris 11.3 ou version ultérieure XCP 2250 ou version ultérieure
Démarrage depuis le réseau	Oracle Solaris 11.2 ou version ultérieure (*1) XCP 2320 ou version ultérieure	-	Domaine de commande : Oracle Solaris 11.3 SRU11.3.8.7.0 ou version ultérieure Domaine invité : Oracle Solaris 11.2 ou version ultérieure XCP 2320 ou version ultérieure	-

*1 Les réglages dans XSCF sont utilisés et les réglages dans Oracle Solaris sont ignorés.

14.8.7 Remarques et restrictions

Notez ce qui suit lorsque vous utilisez le démarrage vérifié.

Valeur de réglage de la variable d'environnement OpenBoot PROM use-nvramrc?

Pour utiliser le démarrage vérifié, réglez la valeur de la variable d'environnement use-nvramrc? d'OpenBoot PROM sur « false ». Si vous utilisez le démarrage vérifié avec la variable réglée sur « vrai », la vérification du démarrage échoue. Les opérations répertoriées dans [Tableau 14-22](#) peuvent être effectuées quand la vérification du démarrage échoue, selon la valeur de réglage de la stratégie de démarrage.

Tableau 14-22 Opération de vérification du démarrage quand use-nvramrc? est « true »

Valeur de réglage de la stratégie de démarrage	Opération
none	La vérification du démarrage n'est pas effectuée.

Tableau 14-22 Opération de vérification du démarrage quand use-nvramrc? est « true »
(suite)

Valeur de réglage de la stratégie de démarrage	Opération
warning	Le message suivant apparaît, et Oracle Solaris démarre. La variable use-nvramrc? est réglée, et poursuit avec la vérification des signatures
enforce	Le message suivant apparaît, et le démarrage s'arrête à l'invite ok. De plus, le journal d'erreurs « le processus de démarrage a échoué » est enregistré avec le XSCF. use-nvramrc? variable is set, verified boot policy = enforce, halting boot

Réglage de la configuration du démarrage vérifié à l'invite ok d'OpenBoot PROM

Supposons que vous modifiez les données de configuration du démarrage vérifié dans le XSCF à partir de l'invite ok d'OpenBoot PROM, puis que vous démarrez Oracle Solaris. Les données de configuration modifiées seront activées seulement pour genunix et les autres modules de noyau.
Les données de configuration modifiées seront activées pour tous les modules au prochain démarrage d'OpenBoot PROM.

14.8.8 Vérification des réglages et des commandes liés au démarrage vérifié

Tableau 14-23 répertorie les réglages liés au démarrage vérifié et aux commandes de shell XSCF correspondantes. Configurer le démarrage vérifié pour chaque partition physique.

Tableau 14-23 Commandes liées à la configuration du démarrage vérifié

Élément de réglage	Commande liée
Enregistrer/Effacer/Afficher un certificat	addvbootcerts(8), deletevbootcerts(8), showvbootcerts(8)
Régler/Afficher les données de configuration - Sélectionner un certificat - Régler les stratégies de démarrage et de module	setvbootconfig(8), showvbootconfig(8)

Remarque - N'exécutez pas la commande setvbootconfig quand le processus de démarrage ou d'arrêt pour la partition physique est en cours. Sinon, la commande aboutit à une erreur.

14.8.9 Procédures de réglage du démarrage vérifié

Figure 14-12 affiche les procédures pour effectuer les réglages afin d'utiliser le démarrage vérifié.

Figure 14-12 Procédures de réglage lors de l'utilisation de la vérification du démarrage

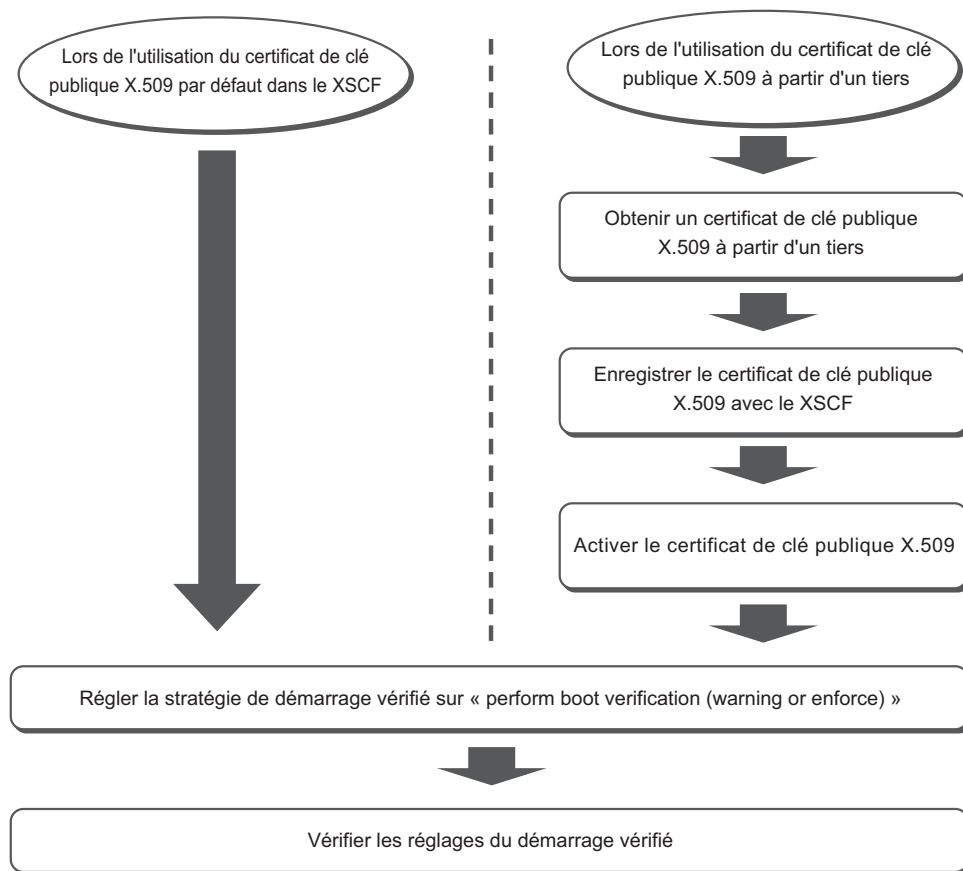
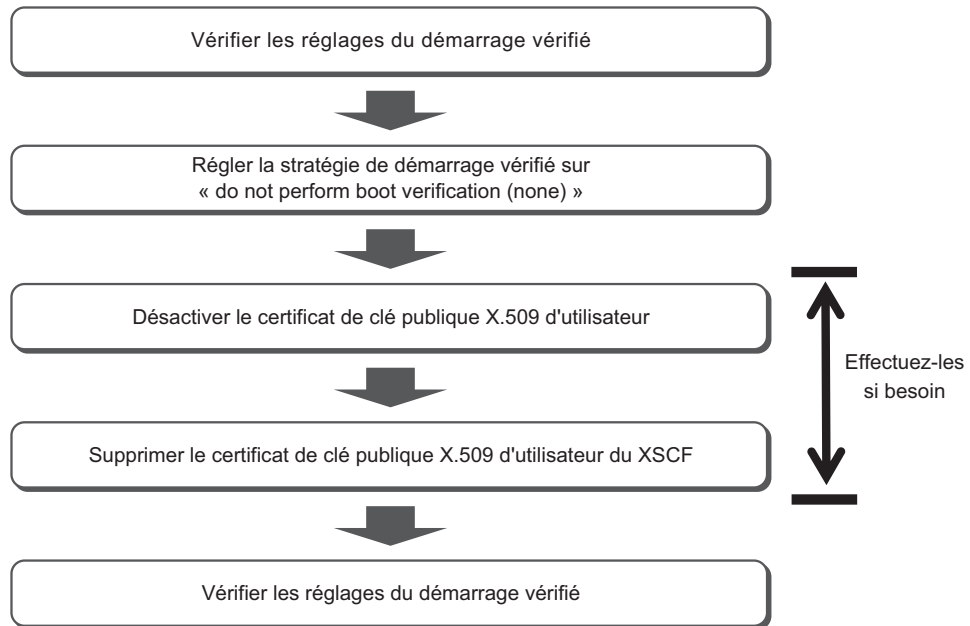


Figure 14-13 affiche les procédures de réglage quand vous n'utilisez pas la vérification du démarrage par le démarrage vérifié.

Figure 14-13 Procédures de réglage quand vous n'effectuez pas la vérification du démarrage



14.8.10 Enregistrement d'un certificat de clé publique X.509

Utilisez la commande `advbootcerts` pour enregistrer un certificat de clé publique X.509 avec le XSCF. Exécutez la commande `advbootcerts` avec le compte d'un utilisateur disposant du privilège `platadm` ou `pparadm`.

```
XSCF> advbootcerts -p ppar_id certname {-F URL | signature}
```

Pour `ppar_id`, indiquez la partition physique de destination. Pour `certname`, spécifiez le nom du certificat de clé publique X.509 à enregistrer. Pour spécifier un certificat de clé publique, copiez-collez le contenu du certificat de clé publique, ou lisez-le à partir d'un périphérique USB ou d'un serveur `http/https` en spécifiant l'option `-F`.

Le certificat de clé publique est enregistré avec le XSCF en tant que certificat d'utilisateur. Jusqu'à cinq certificats de clé publique peuvent être enregistrés.

Dans l'exemple suivant, un certificat de clé publique stocké sur un périphérique USB est spécifié.

```
XSCF> addvbootcerts -p ppar_id certname -F file:///media/usb_msd/file
```

Remarque - Vous pouvez également enregistrer un certificat de clé publique X.509 en utilisant le site Web XSCF.

Remarque - Enregistrer des certificats de clé publique X.509 en les spécifiant un par un. Vous ne pouvez pas spécifier plusieurs certificats de clé publique en même temps.

Remarque - Dans le cas où le format de données du certificat de clé publique à enregistrer n'est pas X.509 et si les données sont corrompues, le certificat de clé publique ne peut pas être enregistré avec le XSCF. La commande addvbootcerts aboutit à une erreur.

Remarque - Un certificat par défaut du système est un certificat de clé publique que XSCF a par défaut. Les certificats de clé publique X.509 ne peuvent pas être enregistrés comme certificats par défaut du système.

Procédure de fonctionnement

1. **Connectez-vous au XSCF.**

Pour plus de détails, consultez « [2.2 Connexion au Shell XSCF](#) ».

2. **Exécutez la commande addvbootcerts pour enregistrer un certificat d'utilisateur avec le XSCF.**

Dans l'exemple suivant, un certificat de clé publique X.509 stocké sur un support USB est ajouté à PPAR-ID 4 sous le nom « CUSTOM_CERT_2 ». La réponse au message de confirmation est « y (yes) ».

```
XSCF> addvbootcerts -p 4 CUSTOM_CERT_2 -F file:///media/usb_msd/vboot/3rd_perty_
cert_xyz
The above elfsign X.509 key certificate will be added to PPAR-ID 4,
Continue?[y|n]:y
.... done.
successfully added this certificate to PPAR-ID 4 as index 2.
```

3. **Exécutez la commande showvbootcerts pour confirmer que le certificat de clé publique X.509 a été correctement enregistré avec le XSCF.**

Dans l'exemple suivant, les informations détaillées du certificat de clé publique X.509 enregistré comme numéro d'index 2 dans PPAR-ID 4 sont affichées.

```
XSCF> showvbootcerts -v -p 4 -u -i 2
-----
PPAR-ID 4 User Index : 2 name : CUSTOM_CERT_2 [Enable]
-----
Data:
  Version: 3 (0x2)
  Serial Number:
```

```

07:ad:b3:06:99:82:39:db:dd:60:41:44:71:be:aa:70
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=US, O=Thirdparty Corporation, OU=Thirdparty CA, CN=www.example.com
Subject: O=Thirdparty Corporation, OU=Thirdparty Signed Execution,
CN=www.example.com
Subject Public Key Info:
  Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
      Modulus:
        00:de:f0:2c:45:61:7f:10:c7:16:56:a9:14:b4:a4:
        39:44:b9:2f:65:4f:7e:a7:c0:15:89:b0:e2:1d:c0:
        25:4c:a6:31:75:14:a3:c4:cd:11:d2:87:b7:1a:7c:
        b2:0d:41:99:4f:a6:e9:d4:8e:77:55:19:ce:f1:a4:
        3c:cf:00:8d:e6:d1:c6:bc:06:f7:71:85:28:a4:c5:
        e0:8d:b3:e1:62:25:d5:df:93:d2:d9:1c:5b:48:35:
        70:e1:8a:9b:bf:9d:8b:41:b3:be:b6:c0:50:66:3b:
        d8:9d:2f:82:49:11:f7:6d:43:95:6e:ea:bc:57:dc:
        1c:90:6b:7e:8b:e3:0f:89:bd:32:3a:88:50:f0:48:
        d3:98:8c:bc:eb:7f:44:31:2b:86:01:d0:80:4c:a2:
        36:6e:24:47:48:d5:86:8e:86:06:c3:8e:df:5f:fb:
        6b:fe:6a:aa:0c:a8:ca:b6:ed:60:47:ea:8e:5d:63:
        b1:4f:ff:94:00:34:52:82:cf:a6:6a:84:69:4c:26:
        ac:a3:dc:d7:45:eb:7c:4e:fc:fc:92:4a:73:12:9f:
        31:7a:75:b9:de:33:54:34:af:0b:cf:46:c0:ac:2f:
        ec:28:af:0d:f7:c6:50:c0:e7:4c:88:16:13:95:54:
        0e:01:6e:1a:b6:33:bf:20:52:34:f4:69:a6:9e:bf:
        02:95
      Exponent: 65537 (0x10001)
Signature Algorithm: sha256WithRSAEncryption
44:65:95:e1:33:a4:ce:d1:c1:02:1a:ce:b3:2c:fa:c0:b2:34:
4e:12:d0:86:c7:09:23:9d:5b:46:f4:b2:bf:88:8b:5b:5d:d7:
57:c3:f9:9a:ba:95:bc:ed:4b:29:4b:19:97:ca:6c:bc:e1:44:
e0:e1:89:a3:ed:bd:29:ad:a7:91:c8:76:ea:62:d2:2c:e3:ff:
50:01:0a:3b:5a:28:53:38:53:82:ea:de:bc:24:84:bc:31:63:
ab:b2:10:81:81:73:f4:02:46:5f:2d:6d:22:b0:af:d7:70:c0:
db:de:ea:b9:23:87:3c:19:ef:c0:24:de:05:77:eb:89:d2:36:
d0:85:8a:ed:d1:7f:12:b0:58:5f:f5:53:f1:db:0b:44:53:a0:
72:8c:1a:e6:4a:fd:e8:8e:f8:ee:9e:7e:4e:85:59:42:44:fa:
1f:d3:70:4f:81:95:8e:a9:0f:83:49:a2:b0:fd:5b:f4:2d:5e:
86:ef:f3:56:b3:31:f3:58:3a:37:42:bb:39:c4:c1:b5:8c:e9:
b4:01:d2:2e:e8:7d:86:1a:66:88:34:1e:e5:36:ee:6d:6c:90:
78:45:a0:5b:a9:50:84:62:a8:88:ee:a6:70:fa:7c:ad:81:b7:
89:f1:d6:64:94:c4:17:69:c8:35:81:b2:f3:79:ad:a2:5a:a0:
02:28:a9:7f
-----

```

4. Exécutez la commande exit pour vous déconnecter du shell XSCF.

Si vous n'avez plus besoin d'utiliser le shell XSCF, vous pouvez vous déconnecter du XSCF. Pour passer à la configuration d'un autre réglage, allez à l'étape correspondante.

Remarque - Si les informations d'un certificat de clé publique X.509 sont corrompues à cause d'une opération inattendue, le certificat de clé publique peut être requis par le XSCF. Assurez-vous que les certificats de clé publique sont stockés en sécurité pour une restauration

14.8.11 Activation/Désactivation d'un certificat de clé publique X.509

Pour utiliser un certificat de clé publique X.509 d'un utilisateur qui a été enregistré, exécutez la commande `setvbootconfig` du shell XSCF pour activer le certificat de clé publique. Exécutez la commande `setvbootconfig` avec le compte d'un utilisateur disposant du privilège `platadm` ou `pparadm`.

Dans l'exemple suivant, un certificat de clé publique désactivé est activé.

```
XSCF> setvbootconfig -p ppar_id -i index -c enable
```

Pour `ppar_id`, indiquez la partition physique de destination. Pour l'index, spécifiez le numéro d'index du certificat d'utilisateur à activer.

Vous pouvez utiliser une liste de certificats d'utilisateur pour vérifier les numéros d'index et si un certificat de clé publique est activé/désactivé. Pour afficher une liste de certificats d'utilisateur, exécutez la commande `showvbootcerts` avec l'option `-a` spécifiée.

```
XSCF> showvbootcerts -p ppar_id -a
```

Dans l'exemple suivant, un certificat de clé publique activé est désactivé.

```
XSCF> setvbootconfig -p ppar_id -i index -c disable
```

Pour `ppar_id`, indiquez la partition physique de destination. Pour l'index, spécifiez le numéro d'index du certificat d'utilisateur à désactiver.

Remarque - Vous pouvez également utiliser le site Web XSCF pour activer/désactiver un certificat de clé publique X.509.

Remarque : vous pouvez activer/désactiver un certificat de clé publique X.509 pendant que la partition physique est hors tension ou que Oracle Solaris est en exécution sur un domaine logique. Si la partition physique ou le domaine logique est en cours de démarrage ou d'arrêt, une erreur survient. Effectuez à nouveau l'opération après que le démarrage ou l'arrêt est complet.

Remarque - Un certificat par défaut du système est un certificat de clé publique que XSCF a par défaut. Les certificats par défaut du système ne peuvent pas être activés/désactivés.

Procédure de fonctionnement

1. Connectez-vous au XSCF.

Pour plus de détails, consultez « [2.2 Connexion au Shell XSCF](#) ».

2. Exécutez la commande `showvbootcerts` pour vérifier le numéro d'index du certificat d'utilisateur à utiliser et si le certificat est activé.

Si le certificat de clé publique enregistré est déjà activé, les étapes suivantes ne sont pas nécessaires.

Dans l'exemple suivant, tous les certificats de clé publique X.509 enregistrés dans PPAR-ID 2 sont affichés.

```
XSCF> showvbootcerts -p 2 -a
-----
PPAR-ID 2 System Index : 1 name : SYSTEM_CERT_1 [Enable(Unchangeable)]
-----
Data:
  Version: 3 (0x2)
  Serial Number:
    0d:fb:b1:5a:2d:2a:e5:81:80:86:eb:34:5e:a4:7e:ed
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=US, O=Oracle Corporation, OU=VeriSign Trust Network, OU=Class 2
Managed PKI Individual Subscriber CA, CN=Object Signing CA
  Subject: O=Oracle Corporation, OU=Corporate Object Signing, OU=Solaris
Signed Execution, CN=Solaris 11
-----
PPAR-ID 2 User Index : 2 name : CUSTOM_CERT_2 [Enable]
-----
Data:
  Version: 3 (0x2)
  Serial Number:
    07:ad:b3:06:99:82:39:db:dd:60:41:44:71:be:aa:70
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=US, O=Thirdparty Corporation, OU=Thirdparty CA, CN=www.example.com
  Subject: O=Thirdparty Corporation, OU=Thirdparty Signed Execution, CN=www.
example.com
-----
PPAR-ID 2 User Index : 5 name : CUSTOM_CERT_5 [Disable]
-----
Data:
  Version: 3 (0x2)
  Serial Number:
    07:ad:b3:06:99:82:39:db:dd:60:41:44:71:be:bb:71
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=US, O=Thirdparty Corporation, OU=Thirdparty CA, CN=www.example.com
  Subject: O=Thirdparty Corporation, OU=Thirdparty Signed Execution, CN=www.
example.com
-----
```

3. Exécutez la commande `setvbootconfig` pour activer le certificat de clé publique.

Dans l'exemple suivant, le certificat de clé publique X.509 enregistré comme numéro d'index 5 dans PPAR-ID 2 est activé. La réponse au message de

confirmation est « y (yes) ».

```
XSCF> setvbootconfig -p 2 -i 5 -c enable
Index 5, CUSTOM_CERT_5 on PPAR-ID 2 will be enabled,
Continue?[y|n]: y
```

4. **Exécutez la commande `showvbootcerts` pour confirmer que le certificat de clé publique a été activé.**

Dans l'exemple suivant, il est confirmé que le certificat de clé publique X.509 enregistré comme numéro d'index 5 dans PPAR-ID 2 est activé.

```
XSCF> showvbootcerts -p 2 -a
-----
PPAR-ID 2 System Index : 1 name : SYSTEM_CERT_1 [Enable(Unchangeable)]
-----
Data:
  Version: 3 (0x2)
  Serial Number:
    0d:fb:b1:5a:2d:2a:e5:81:80:86:eb:34:5e:a4:7e:ed
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=US, O=Oracle Corporation, OU=VeriSign Trust Network, OU=Class 2
Managed PKI Individual Subscriber CA, CN=Object Signing CA
  Subject: O=Oracle Corporation, OU=Corporate Object Signing, OU=Solaris
Signed Execution, CN=Solaris 11
-----
PPAR-ID 2 User Index : 2 name : CUSTOM_CERT_2 [Enable]
-----
Data:
  Version: 3 (0x2)
  Serial Number:
    07:ad:b3:06:99:82:39:db:dd:60:41:44:71:be:aa:70
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=US, O=Thirdparty Corporation, OU=Thirdparty CA, CN=www.example.com
  Subject: O=Thirdparty Corporation, OU=Thirdparty Signed Execution, CN=www.
example.com
-----
PPAR-ID 2 User Index : 5 name : CUSTOM_CERT_5 [Enable]
-----
Data:
  Version: 3 (0x2)
  Serial Number:
    07:ad:b3:06:99:82:39:db:dd:60:41:44:71:be:bb:71
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=US, O=Thirdparty Corporation, OU=Thirdparty CA, CN=www.example.com
  Subject: O=Thirdparty Corporation, OU=Thirdparty Signed Execution, CN=www.
example.com
-----
```

5. **Exécutez la commande `exit` pour vous déconnecter du shell XSCF.**

Si vous n'avez plus besoin d'utiliser le shell XSCF, vous pouvez vous déconnecter du XSCF. Pour passer à la configuration d'un autre réglage, allez à l'étape correspondante.

14.8.12 Suppression d'un certificat de clé publique X.509 enregistré

Pour supprimer un certificat de clé publique X.509 du système, utilisez la commande `deletevbootcerts` dans le shell XSCF. Exécutez la commande `deletevbootcerts` avec le compte d'un utilisateur disposant du privilège `platadm` ou `ppradm`. Vous pouvez supprimer un certificat de clé publique quand le certificat de clé publique est désactivé.

```
XSCF> deletevbootcerts -p ppar_id -i index
```

Pour `ppar_id`, indiquez la partition physique de destination. Pour l'index, spécifiez le numéro d'index du certificat d'utilisateur à supprimer. Vous pouvez vérifier le numéro d'index d'une liste des certificats d'utilisateur émise en exécutant la commande `showvbootcerts` avec l'option `-a` spécifiée.

```
XSCF> showvbootcerts -p ppar_id -a
```

Remarque - Vous ne pouvez pas supprimer un certificat de clé publique quand il est activé. Supprimez-le après l'avoir désactivé en utilisant la commande `setvbootconfig`. Consultez « [14.8.11 Activation/Désactivation d'un certificat de clé publique X.509](#) ».

Remarque - Vous pouvez également utiliser le site Web XSCF pour activer/désactiver un certificat de clé publique X.509.

Remarque - Un certificat par défaut du système est un certificat de clé publique que XSCF a par défaut. Les certificats par défaut du système ne peuvent pas être supprimés.

Procédure de fonctionnement

1. **Connectez-vous au XSCF.**
Pour plus de détails, consultez « [2.2 Connexion au Shell XSCF](#) ».
2. **Exécutez la commande `showvbootcerts` pour vérifier le numéro d'index du certificat d'utilisateur à supprimer et si le certificat est désactivé.**
Vous ne pouvez pas supprimer un certificat de clé publique quand il est activé. Exécutez la commande `setvbootconfig` pour le désactiver.

Dans l'exemple suivant, tous les certificats de clé publique X.509 enregistrés dans PPAR-ID 2 sont affichés.

```

XSCF> showvbootcerts -p 2 -a
-----
PPAR-ID 2 System Index : 1 name : SYSTEM_CERT_1 [Enable(Unchangeable)]
-----
Data:
  Version: 3 (0x2)
  Serial Number:
    0d:fb:b1:5a:2d:2a:e5:81:80:86:eb:34:5e:a4:7e:ed
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=US, O=Oracle Corporation, OU=VeriSign Trust Network, OU=Class 2
Managed PKI Individual Subscriber CA, CN=Object Signing CA
  Subject: O=Oracle Corporation, OU=Corporate Object Signing, OU=Solaris
Signed Execution, CN=Solaris 11
-----
PPAR-ID 2 User Index : 2 name : CUSTOM_CERT_2 [Enable]
-----
Data:
  Version: 3 (0x2)
  Serial Number:
    07:ad:b3:06:99:82:39:db:dd:60:41:44:71:be:aa:70
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=US, O=Thirdparty Corporation, OU=Thirdparty CA, CN=www.example.com
  Subject: O=Thirdparty Corporation, OU=Thirdparty Signed Execution, CN=www.
example.com
-----
PPAR-ID 2 User Index : 5 name : CUSTOM_CERT_5 [Enable]
-----
Data:
  Version: 3 (0x2)
  Serial Number:
    07:ad:b3:06:99:82:39:db:dd:60:41:44:71:be:bb:71
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=US, O=Thirdparty Corporation, OU=Thirdparty CA, CN=www.example.com
  Subject: O=Thirdparty Corporation, OU=Thirdparty Signed Execution, CN=www.
example.com
-----

```

3. **Exécutez la commande `deletevbootcerts` pour supprimer le certificat de clé publique.**

Dans l'exemple suivant, le certificat de clé publique X.509 enregistré comme numéro d'index 5 dans PPAR-ID 2 est supprimé. La réponse au message de confirmation est « y (yes) ».

```

XSCF> deletevbootcerts -p 2 -i 5
Index 5, CUSTOM_CERT_5 will be deleted from PPAR-ID 2,
Continue?[y|n]: y

```

4. **Exécutez la commande `showvbootcerts` pour confirmer que le certificat de clé publique a été supprimé.**

Dans l'exemple suivant, tous les certificats de clé publique X.509 enregistrés dans PPAR-ID 2 sont affichés. Vous pouvez voir que le certificat de clé publique avec

le numéro d'index 5 a été supprimé.

```
XSCF> showvbootcerts -p 2 -a
-----
PPAR-ID 2 System Index : 1 name : SYSTEM_CERT_1 [Enable(Unchangeable)]
-----
Data:
Version: 3 (0x2)
Serial Number:
0d:fb:b1:5a:2d:2a:e5:81:80:86:eb:34:5e:a4:7e:ed
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=US, O=Oracle Corporation, OU=VeriSign Trust Network, OU=Class 2
Managed PKI Individual Subscriber CA, CN=Object Signing CA
Subject: O=Oracle Corporation, OU=Corporate Object Signing, OU=Solaris Signed
Execution, CN=Solaris 11
-----
PPAR-ID 2 User Index : 2 name : CUSTOM_CERT_2 [Enable]
-----
Data:
Version: 3 (0x2)
Serial Number:
07:ad:b3:06:99:82:39:db:dd:60:41:44:71:be:aa:70
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=US, O=Thirdparty Corporation, OU=Thirdparty CA, CN=www.example.com
Subject: O=Thirdparty Corporation, OU=Thirdparty Signed Execution, CN=www.
example.com
-----
```

5. **Exécutez la commande exit pour vous déconnecter du shell XSCF.**

Si vous n'avez plus besoin d'utiliser le shell XSCF, vous pouvez vous déconnecter du XSCF. Pour passer à la configuration d'un autre réglage, allez à l'étape correspondante.

14.8.13 Affichage d'un certificat de clé publique X.509 enregistré

Utilisez la commande `showvbootcerts` pour afficher les informations d'un certificat de clé publique X.509 enregistré avec le XSCF.

Si vous voulez afficher une liste de tous les certificats de clé publique X.509 enregistrés, spécifiez la partition physique de destination et l'option `-a`. Ceci affiche une liste des certificats par défaut du système et des certificats d'utilisateur. Vous pouvez également afficher les informations détaillées en spécifiant l'option `-v`.

```
XSCF> showvbootcerts -p ppar_id -a
```

Pour afficher les informations pour un certificat par défaut du système, spécifiez la partition physique cible, l'option `-s` et le numéro d'index du certificat par défaut du

système. Vous pouvez également afficher les informations détaillées en spécifiant l'option -v.

```
XSCF> showvbootcerts -p ppar_id -s -i index
```

Pour afficher les informations d'un certificat d'utilisateur enregistré avec la commande addvbootcerts, spécifiez la partition physique de destination, l'option -u et le numéro d'index du certificat d'utilisateur. Vous pouvez également afficher les informations détaillées en spécifiant l'option -v.

```
XSCF> showvbootcerts -p ppar_id -u -i index
```

Remarque : vous pouvez également utiliser XSCF Web pour afficher le certificat de clé publique X.509.

14.8.14 Réglage des stratégies de démarrage vérifié

Utilisez la commande setvbootconfig du shell XSCF pour régler les stratégies de démarrage vérifié. Exécutez la commande avec un compte d'utilisateur disposant du privilège platadm ou pparadm.

```
XSCF> setvbootconfig -p ppar_id -s policy=value
```

Pour ppar_id, indiquez la partition physique de destination. Pour la stratégie, spécifiez la stratégie de démarrage « boot_policy » ou la stratégie de module « module_policy ». Pour la valeur, spécifiez « none », « warning », ou « enforce ». Pour plus de détails, consultez « [14.8.4 Stratégies de démarrage vérifié](#) ».

Procédure de fonctionnement

1. **Connectez-vous au XSCF.**
Pour plus de détails, consultez « [2.2 Connexion au Shell XSCF](#) ».
2. **Exécutez la commande showvbootconfig pour vérifier les valeurs de réglages des stratégies de démarrage vérifié.**
Si la stratégie est réglée sur la valeur désirée, le réglage d'une stratégie n'est pas requis.

```
XSCF> showvbootconfig -p ppar_id
```

3. **Exécutez la commande showvbootconfig pour régler les stratégies de démarrage vérifié. Répondez « y » au message de confirmation.**
Dans l'exemple suivant, la stratégie de démarrage (boot_policy) est réglée sur « warning » et la stratégie de module (module_policy) est réglée sur « enforce » dans PPAR-ID 2.

```
XSCF> setvbootconfig -p 2 -s boot_policy=warning
XSCF> setvbootconfig -p 2 -s module_policy=enforce
```

4. **Exécutez la commande showvbootcerts pour vérifier que les valeurs de réglages des stratégies de démarrage vérifiées ont été modifiées.**

```
XSCF> showvbootconfig -p ppar_id
```

5. **Exécutez la commande exit pour vous déconnecter du shell XSCF.**
Si vous n'avez plus besoin d'utiliser le shell XSCF, vous pouvez vous déconnecter du XSCF. Pour passer à la configuration d'un autre réglage, allez à l'étape correspondante.

14.8.15 Affichage des stratégies de démarrage vérifiées

Utilisez la commande showvbootconfig pour afficher les stratégies de démarrage réglées pour la partition physique.

```
XSCF> showvbootconfig -p ppar_id
```

Pour ppar_id, spécifiez la partition physique cible où les stratégies doivent être affichées.

Remarque - Vous pouvez également utiliser le site Web XSCF pour afficher les stratégies de démarrage vérifiées.

Extension de la configuration du système

Ce chapitre décrit comment modifier la configuration des périphériques d'E/S et des ressources matérielles, tels que les processeurs virtuels et la mémoire dans le système.

- [Modification de la configuration des processeurs virtuels](#)
- [Modification de la configuration de la mémoire](#)
- [Fonction de reconfiguration dynamique pour les périphériques de destination PCIe](#)
- [Utilisation de l'unité d'extension PCI](#)
- [Extension de SPARC M12-2S/M10-4S](#)

15.1 Modification de la configuration des processeurs virtuels

Cette section décrit comment modifier la configuration des processeurs virtuels à l'aide de la fonction de reconfiguration dynamique (DR) d'Oracle VM Server pour SPARC.

Remarque : pour modifier les ressources du domaine logique de façon dynamique, le démon de reconfiguration dynamique du domaine logique (drd) doit être exécuté sur le domaine cible.

Pour les systèmes SPARC M12/M10, différents processus spécifiques à l'activité s'exécutent sur chaque domaine logique. La configuration des processeurs virtuels peut être modifiée de façon flexible en fonction de l'état de fonctionnement du système. Dans certains processus actifs, la charge est concentrée dans un domaine logique donné, les performances en utilisant uniquement les processeurs virtuels configurés peuvent donc être considérées comme inférieures. Dans une telle situation, les domaines logiques de la même partition physique peuvent laisser le système fonctionner. Ce résultat est obtenu en attribuant de façon dynamique les processeurs virtuels des domaines ayant une charge relativement faible.

La configuration des processeurs virtuels peut être modifiée pour chaque thread.

Pour modifier la configuration des processeurs virtuels, utilisez d'abord la commande `ldm remove-vcpu` d'Oracle VM Server pour SPARC afin de supprimer les processeurs virtuels des domaines logiques ayant une charge relativement faible. Puis utilisez la commande `ldm add-vcpu` d'Oracle VM Server pour SPARC pour ajouter des processeurs virtuels aux domaines logiques qui présentent des problèmes de performances inférieures en raison d'une charge accrue. Exécutez ces commandes avec le privilège racine.

Suppression d'un processeur virtuel

```
primary# ldm remove-vcpu number ldom
```

Pour le nombre, spécifiez le nombre de processeurs virtuels à supprimer. Vous pouvez le spécifier en unités de threads. Pour `ldom`, spécifiez le domaine logique duquel supprimer les processeurs virtuels.

Ajout d'un processeur virtuel

```
primary# ldm add-vcpu number ldom
```

Pour le nombre, spécifiez le nombre de processeurs virtuels à ajouter. Vous pouvez le spécifier en unités de threads. Pour `ldom`, spécifiez le domaine logique auquel ajouter les processeurs virtuels.

Procédure de fonctionnement

1. **Passez de la console XSCF à la console du domaine de commande à laquelle appartient le domaine logique cible.**

Pour plus de détails sur le passage à la console du domaine de commande, consultez « [8.3 Passage à la console du domaine de commande depuis le shell XSCF](#) ».

2. **Vérifiez le nombre de processeurs virtuels dans chaque domaine avec la commande `ldm list-domain`.**

L'exemple suivant effectue une vérification de l'état des domaines logiques `primary`, `ldom1`, `ldom2` et `ldom3`.

```
primary# ldm list-domain
NAME STATE FLAGS CONS VCPU MEMORY UTIL UPTIME
primary active -n-cv- SP 8 4G 3.1% 1d 36m
ldom1 active -n---- 5001 16 2G 34% 1m
ldom2 active -n---- 5002 16 1G 34% 17h 48m
ldom3 active -n---- 5003 24 4G 17% 17h 48m
```

3. **Supprimez un processeur virtuel d'un domaine à l'aide de la commande `ldm remove-vcpu`.**

L'exemple suivant supprime huit processeurs virtuels de `ldom3`.


```
primary# ldm remove-vcpu 8 ldom3
```

4. **Ajoutez un processeur virtuel à un domaine à l'aide de la commande ldm add-vcpu.**

Dans l'exemple suivant, huit processeurs virtuels sont ajoutés à ldom1.

```
primary# ldm add-vcpu 8 ldom1
```

5. **Vérifiez une modification de la configuration dans le nombre de processeurs virtuels de chaque domaine à l'aide de la commande ldm list-domain.**

Dans l'exemple suivant, vérifiez les modifications des configurations des domaines logiques primary, ldom1, ldom2 et ldom3.

```
primary# ldm list-domain
NAME STATE FLAGS CONS VCPU MEMORY UTIL UPTIME
primary active -n-cv- SP 8 4G 3.1% 1d 36m
ldom1 active -n---- 5001 24 2G 34% 1m
ldom2 active -n---- 5002 16 1G 34% 17h 48m
ldom3 active -n---- 5003 16 4G 17% 17h 48m
```

Vous pouvez constater que les processeurs virtuels ont été supprimés de ldom3 et ajoutés à ldom1.

6. **Déconnectez-vous de la console du domaine de commande pour revenir à la console XSCF.**

Pour plus de détails sur comment revenir à la console XSCF depuis la console du domaine de commande, consultez « [8.4 Retour au shell XSCF depuis la console du domaine de commande](#) ».

15.2 Modification de la configuration de la mémoire

Cette section décrit comment modifier la configuration de la mémoire à l'aide de la fonction de reconfiguration dynamique (DR) d'Oracle VM Server pour SPARC.

Remarque : pour modifier les ressources du domaine logique de façon dynamique, le démon de reconfiguration dynamique du domaine logique (drd) doit être exécuté sur le domaine cible.

Pour les systèmes SPARC M12/M10, différents processus spécifiques à l'activité s'exécutent sur chaque domaine logique. La configuration de la mémoire peut être modifiée de façon flexible en fonction de l'état de fonctionnement du système. Dans certains processus actifs, la charge est concentrée dans un domaine logique donné, les performances en utilisant uniquement la mémoire configurée peuvent donc être

considérées comme inférieures. Dans une telle situation, les domaines logiques de la même partition physique peuvent être réattribués. Ce résultat est obtenu en attribuant de façon dynamique la mémoire des domaines ayant une charge relativement faible.

La configuration de la mémoire peut être modifiée en unités de 256 Mo.

Pour modifier la configuration de la mémoire, utilisez d'abord la commande `ldm remove-memory` d'Oracle VM Server pour SPARC afin de supprimer la mémoire des domaines logiques ayant une charge relativement faible. Puis utilisez la commande `ldm add-memory` d'Oracle VM Server pour SPARC pour ajouter la mémoire aux domaines logiques qui présentent des problèmes de performances inférieures en raison d'une charge accrue.

Suppression de mémoire

```
primary# ldm remove-memory size[unit] ldom
```

Pour la taille, spécifiez la taille de la mémoire à supprimer. Pour l'unité, spécifiez l'unité de mémoire. Pour `ldom`, spécifiez le domaine logique duquel supprimer la mémoire.

Ajout de mémoire

```
primary# ldm add-memory size[unit] ldom
```

Pour la taille, spécifiez la taille de la mémoire à ajouter. Pour l'unité, spécifiez l'unité de mémoire. Pour `ldom`, spécifiez le domaine logique auquel ajouter la mémoire.

Procédure de fonctionnement

1. **Passez de la console XSCF à la console du domaine de commande à laquelle appartient le domaine logique cible.**

Pour plus de détails sur le passage à la console du domaine de commande, consultez « [8.3 Passage à la console du domaine de commande depuis le shell XSCF](#) ».

2. **Vérifiez la capacité de la mémoire de chaque domaine avec la commande `ldm list-domain`.**

L'exemple suivant effectue une vérification de l'état des domaines logiques `primary`, `ldom1`, `ldom2` et `ldom3`.

```
primary# ldm list-domain
NAME STATE FLAGS CONS VCPU MEMORY UTIL UPTIME
primary active -n-cv- SP 8 4G 3.1% 1d 36m
ldom1 active -n---- 5001 16 2G 34% 1m
ldom2 active -n---- 5002 16 1G 34% 17h 48m
```

```
ldom3 active -n---- 5003 24 4G 17% 17h 48m
```

3. **Supprimez la mémoire d'un domaine à l'aide de la commande `ldm remove-memory`.**

L'exemple suivant supprime 1 Go de mémoire de ldom3.

```
primary# ldm remove-memory 1G ldom3
```

4. **Ajoutez la mémoire à un domaine à l'aide de la commande `ldm add-memory`.**

Dans l'exemple suivant, 1 Go de mémoire est ajouté à ldom1.

```
primary# ldm add-memory 1G ldom1
```

5. **Vérifiez la modification de la configuration dans la capacité de la mémoire de chaque domaine avec la commande `ldm list-domain`.**

Dans l'exemple suivant, vérifiez les modifications des configurations des domaines logiques primary, ldom1, ldom2 et ldom3.

```
primary# ldm list-domain
NAME STATE FLAGS CONS VCPU MEMORY UTIL UPTIME
primary active -n-cv- SP 8 4G 3.1% 1d 36m
ldom1 active -n---- 5001 16 3G 34% 1m
ldom2 active -n---- 5002 16 1G 34% 17h 48m
ldom3 active -n---- 5003 16 3G 17% 17h 48m
```

Vous pouvez constater que la mémoire a été supprimée du domaine ldom3 et ajoutée à ldom1.

6. **Déconnectez-vous de la console du domaine de commande pour revenir à la console XSCF.**

Pour plus de détails sur comment revenir à la console XSCF depuis la console du domaine de commande, consultez « [8.4 Retour au shell XSCF depuis la console du domaine de commande](#) ».

15.3 Fonction de reconfiguration dynamique pour les périphériques de destination PCIe

La fonction de reconfiguration dynamique pour les périphériques de destination (endpoint) PCIe est prise en charge à partir d'Oracle VM Server pour SPARC 3.1.1.1. Elle permet d'attribuer ou de supprimer des périphériques de destination PCIe sans reconfigurer le domaine racine ni arrêter le domaine d'E/S.

Pour utiliser cette fonction, vérifiez la carte correspondante dans « Cards That

Support the Dynamic Reassignment Function for the PCIe End Point Device (PCIe Card) » dans le *PCI Card Installation Guide* pour votre serveur.

Le tableau ci-dessous montre la version de XCP/Oracle Solaris requise et les SRU/correctifs principaux pour l'exécution de la reconfiguration dynamique des périphériques de point de destination PCIe.

Tableau 15-1 Versions de XCP et Oracle Solaris requises pour exécuter la reconfiguration dynamique des périphériques de point de destination PCIe (SPARC M10)

Serveur	XCP	Oracle Solaris	Package requis Produit requis	SRU requis Correctif requis
SPARC M10-1 SPARC M10-4 SPARC M10-4S	2230 ou version supérieure	Oracle Solaris 11.3	system/ldoms (*1) system/ldoms/ldomsmanager (*2)	None
		Oracle Solaris 11.2	system/ldoms (*1) system/ldoms/ldomsmanager (*2)	SRU 11.2.2.5.0 ou version ultérieure
		Oracle Solaris 11.1 (*4)	system/ldoms (*1)	SRU 11.1.17.5.0 ou version ultérieure (*3)
		Oracle Solaris 10 1/13	Oracle VM pour SPARC 3.1 (*5)(*6)	150817-03 ou version supérieure (*5)

*1 Requis pour le domaine de commande ou d'autres domaines. Included in group/system/solaris-large-server and group/system/solaris-small-server.

*2 Requis pour le domaine de contrôle uniquement. Included in group/system/solaris-large-server and group/system/solaris-small-server.

*3 Requis pour le domaine de commande ou d'autres domaines.

*4 Ne peut être utilisé qu'avec d'autres domaines que le domaine de commande.

*5 Requis pour le domaine de contrôle uniquement.

*6 Des correctifs autres que le correctif Oracle VM Server pour SPARC sont requis. Pour plus de détails, consultez « Required Oracle Solaris OS Versions for Oracle VM Server for SPARC 3.1.1.1 » dans les *Oracle VM Server for SPARC 3.1.1.1, 3.1.1, and 3.1 Release Notes*.

Tableau 15-2 Version d'Oracle Solaris requise pour exécuter la reconfiguration dynamique des périphériques de destination PCIe (SPARC M12)

Version système d'exploitation	Type de domaine		
	Domaine de commande Environnement sans virtualisation	Domaine racine (Avec location E/S)	Domaine d'E/S
Oracle Solaris 11	Oracle Solaris 11.3 (*1) SRU 11.3.17.5.0 ou version ultérieure	Oracle Solaris 11.3 ou version ultérieure (*2)	Oracle Solaris 11.3 ou version ultérieure (*2)
	Oracle Solaris 11.2 (*1) SRU11.2.15.5.1	Oracle Solaris 11.2 ou version ultérieure (*2)	Oracle Solaris 11.2 ou version ultérieure (*2)
			Oracle Solaris 11.1 SRU 11.1.17.5.0 ou version ultérieure

Tableau 15-2 Version d'Oracle Solaris requise pour exécuter la reconfiguration dynamique des périphériques de destination PCIe (SPARC M12) (suite)

Version système d'exploitation	Type de domaine		
	Domaine de commande Environnement sans virtualisation	Domaine racine (Avec location E/S)	Domaine d'E/S
Oracle Solaris 10	Oracle Solaris 10 1/13 (*3) Oracle VM Server pour SPARC 3.2 (*4) 151934-03 ou plus récent	—	—

*1 Les packages system/ldoms et system/ldoms/ldomsmanager sont nécessaires. Ces packages sont compris dans group/system/solaris-large-server et group/system/solaris-small-server.
*2 Le package system/ldoms est nécessaire. Ce package est compris dans group/system/solaris-large-server et group/system/solaris-small-server.
*3 Lorsqu'Oracle Solaris 10 1/13 est utilisé dans le domaine de commande, les processeurs possédant un numéro LSB de 0 à 7 installés sur la carte système logique peuvent être attribués au domaine de commande.
*4 N'est pas inclus dans Oracle Solaris 10 1/13. Installez-le séparément.

Pour utiliser cette fonction, le service de connexion à chaud (hotplug) du domaine logique cible doit être activé au préalable.

```
# svcadm enable svc:/system/hotplug:default
```

15.3.1 Ajout d'un périphérique physique d'E/S à un domaine d'E/S

Cette section décrit la procédure d'ajout d'un périphérique physique d'E/S à un domaine d'E/S en utilisant la fonction de reconfiguration dynamique pour les périphériques de destination PCIe.

1. Retirez le périphérique physique d'E/S du domaine racine.

```
# ldm remove-io device root_domain
```

2. Attribuez le périphérique physique d'E/S retiré à l'étape 1 au domaine d'E/S.

```
# ldm add-io device io_domain
```

3. Définissez le périphérique physique d'E/S dans le domaine d'E/S.
La procédure pour effectuer cette configuration varie en fonction de la version d'Oracle Solaris du domaine d'E/S cible, et du périphérique physique d'E/S. Pour plus d'informations, consultez les manuels d'Oracle Solaris suivants.
 - Pour une carte Ethernet
 - Pour Oracle Solaris 11.2
Configuring and Administering Network Components in Oracle Solaris 11.2

- Managing Network Datalinks in Oracle Solaris 11.2*
- Administering TCP/IP Networks, IPMP, and IP Tunnels in Oracle Solaris 11.2*
- Pour Oracle Solaris 11.1
 - Connecting Systems Using Fixed Network Configuration in Oracle Solaris 11.1*
 - Managing Oracle Solaris 11.1 Network Performance*
- Pour Oracle Solaris 10
 - Oracle Solaris Administration: IP Services*
- Pour une carte SAS ou une carte Fibre Channel
 - Pour Oracle Solaris 11.2
 - Managing SAN Devices and Multipathing in Oracle Solaris 11.2*
 - Pour Oracle Solaris 11.1
 - Oracle Solaris SAN Configuration and Multipathing Guide*
 - Pour Oracle Solaris 10
 - Oracle Solaris SAN Configuration and Multipathing Guide*

15.3.2 Retrait d'un périphérique physique d'E/S d'un domaine d'E/S

Cette section décrit la procédure de retrait d'un périphérique physique d'E/S d'un domaine d'E/S en utilisant la fonction de reconfiguration dynamique pour les périphériques de destination PCIe.

1. **Annulez la configuration du périphérique physique d'E/S dans le domaine d'E/S.**

Avant de pouvoir retirer le périphérique physique d'E/S, sa configuration dans le domaine d'E/S doit être annulée.

La procédure pour effectuer cette configuration varie en fonction de la version d'Oracle Solaris du domaine d'E/S cible, et du périphérique physique d'E/S. Pour plus d'informations, consultez les manuels d'Oracle Solaris suivants.

- Pour une carte Ethernet
 - Pour Oracle Solaris 11.2
 - Configuring and Administering Network Components in Oracle Solaris 11.2*
 - Managing Network Datalinks in Oracle Solaris 11.2*
 - Administering TCP/IP Networks, IPMP, and IP Tunnels in Oracle Solaris 11.2*
 - Pour Oracle Solaris 11.1
 - Connecting Systems Using Fixed Network Configuration in Oracle Solaris 11.1*
 - Managing Oracle Solaris 11.1 Network Performance*
 - Pour Oracle Solaris 10
 - Oracle Solaris Administration: IP Services*
- Pour une carte SAS ou une carte Fibre Channel
 - Pour Oracle Solaris 11.2
 - Managing SAN Devices and Multipathing in Oracle Solaris 11.2*
 - Pour Oracle Solaris 11.1
 - Oracle Solaris SAN Configuration and Multipathing Guide*

2. **Retirez le périphérique physique d'E/S du domaine d'E/S.**

```
# ldm remove-io device io_domain
```

3. **Pour effectuer une maintenance active de la carte PCIe en utilisant la connexion PCI à chaud (PHP), etc. , réattribuez le périphérique physique d'E/S retiré à l'étape 2 au domaine racine.**

```
# ldm add-io device root_domain
```

15.4 Utilisation de l'unité d'extension PCI

Cette section fournit une vue d'ensemble de l'unité d'extension PCI, qui est une option pour le SPARC M12/M10.

L'unité d'extension PCI est un périphérique monté sur un rack qui permet une extension jusqu'à 11 emplacements PCI-Express. L'unité peut être montée dans le même rack que le SPARC M12/M10. Supposons qu'il y ait un manque d'emplacements PCI-Express intégrés pour le SPARC M12/M10. Dans un tel cas, installer l'unité d'extension PCI permet d'étendre de façon flexible le système.

Vous pouvez vérifier l'état de l'unité d'extension PCI et la mettre sous/hors tension à l'aide de la commande `ioxadm` du microprogramme XSCF. Pour plus de détails sur la commande `ioxadm`, consultez la page du manuel correspondant à la commande ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

Si vous envisagez l'installation de l'unité d'extension PCI, contactez un représentant commercial.

Pour plus de détails sur le montage de l'unité d'extension PCI, consultez « Monter l'unité d'extension PCI dans un rack » dans le *Guide d'installation* pour votre serveur.

15.4.1 Vérification de l'unité d'extension PCI

Vous pouvez notamment vérifier une liste de l'unité d'extension PCI gérée par le système ainsi que la température, la tension, le courant, les valeurs mesurées des capteurs de vitesse des ventilateurs, l'état des DEL de localisation et l'état du microprogramme de l'appareil.

15.4.2 Contrôle de l'alimentation de l'unité d'extension PCI

Cette section décrit comment mettre sous/hors tension pour supprimer l'unité d'extension PCI, une carte d'E/S, une unité d'alimentation etc.

La mise sous ou hors tension doit être effectuée avec un compte utilisateur ayant le privilège platadm ou fieldeng.

Procédure de fonctionnement

1. **Mettez hors tension l'unité d'alimentation de l'unité d'extension PCI à l'aide de la commande ioxadm.**

L'exemple suivant met hors tension les éléments spécifiés, dont une unité d'alimentation, afin qu'ils puissent être retirés.

```
XSCF> ioxadm -f poweroff PCIBOX#12B4/PSU#1
```

Remarque : pour forcer une coupure de l'alimentation, spécifiez l'option -f. Notez que l'utilisation de l'option -f peut endommager le domaine.

2. **Restaurez l'alimentation dans l'unité d'alimentation de l'unité d'extension PCI à l'aide de la commande ioxadm.**

L'exemple suivant remet sous tension les éléments hors tension.

```
XSCF> ioxadm poweron PCIBOX#12B4/PSU#1
```

Remarque : pour retirer une unité d'alimentation ou une carte d'E/S, mettez hors tension l'élément spécifié. Pour remettre sous tension avec le commutateur ALIMENTATION sur « on », exécutez la commande ioxadm.

15.4.3 Remarques sur la configuration dans laquelle le système est connecté à une unité d'extension PCI

SPARC M12-2/M12-2S/M10-4/M10-4S

Supposons que l'une des opérations suivantes soit effectuée avec la commande setpciboxdio dans le SPARC M12-2/M12-2S ou à l'aide du microprogramme suivant

sur d'autres systèmes : XCP 2044 ou version ultérieure sur le SPARC M10-4 ou XCP 2050 ou version ultérieure sur le SPARC M10-4S. Ensuite, la configuration du domaine logique de la partition physique reviendra à l'état d'usine par défaut à la prochaine heure de démarrage du domaine de commande. Les variables d'environnement OpenBoot PROM du domaine de commande peuvent également être initialisées.

- La modification du paramètre d'activation/désactivation de la fonction d'E/S directe pour l'unité d'extension PCI
- Si une unité d'extension PCI est ajoutée à/retirée de/remplacée sur un emplacement PCI d'un SPARC M12/M10 avec une unité d'extension PCI dont la fonction d'E/S directe est activée

Vous pouvez exécuter la commande `setpciboxdio` qu'une unité d'extension PCI soit présente ou non. Avant de le faire, enregistrez les informations de configuration du domaine logique d'Oracle Solaris dans un fichier XML. Notez également les informations de paramétrage des variables d'environnement OpenBoot PROM du domaine de commande pour les définir à nouveau.

Tableau 15-3 indique quelles informations il pourra être nécessaire d'enregistrer/de restaurer lors de la modification du paramètre activer/désactiver de la fonction d'E/S directe pour l'unité d'extension PCI en exécutant la commande `setpciboxdio`.

Tableau 15-3 Opérations nécessaires pour basculer le paramètre activer/désactiver des fonctions directes d'E/S

Configuration de l'unité d'extension PCI	Configuration actuelle du domaine	Reconstruction de la configuration Oracle VM Server pour SPARC	Nouveau paramétrage de variable d'environnement OpenBoot PROM
Non	factory-default (Domaine de commande uniquement)	Non requis	Non requis
Non	Avec des domaines logiques autres que le domaine de commande	Requis (Fichier XML)	Requis (*1)
Oui	factory-default (Domaine de commande uniquement)	Non requis	Non requis
Oui	Avec des domaines logiques autres que le domaine de commande	Requis (Fichier XML)	Requis (*1)

*1 Ceci n'est pas requis pour XCP 2230 ou ultérieur ou SPARC M12-2/M12-2S.

Tableau 15-4 indique quelles informations il pourra être nécessaire d'enregistrer/de restaurer lors de l'ajout/retrait/remplacement d'une unité d'extension PCI dans un emplacement PCI d'un SPARC M12/M10 où la fonction d'E/S directe pour l'unité d'extension PCI est activée. Ici, la commande `setpciboxdio` a été exécutée pour activer la fonction.

Remarque : Lors de la maintenance de l'unité d'extension PCI à l'aide de la fonction PCI de connexion à chaud (hot plug - PHP), la fonction d'E/S directe est désactivée, de sorte que les informations ci-dessus ne doivent pas être enregistrées/restaurées.

Tableau 15-4 Opérations nécessaires pour l'ajout/le retrait/le remplacement d'une unité d'extension PCI dans un emplacement PCI du serveur SPARC M12/M10 où la fonction d'E/S directe est activée

Environnement de maintenance	Configuration actuelle du domaine	Reconstruction de la configuration Oracle VM Server pour SPARC	Nouveau paramétrage de variable d'environnement OpenBoot PROM
Ajout/retrait avec PPAR arrêtée	factory-default (Domaine de commande uniquement)	Non requis	Non requis
	Avec des domaines logiques autres que le domaine de commande	Requis (Fichier XML)	Requis (*2)
Remplacement d'une unité d'extension PCI défectueuse (*1) avec PPAR arrêtée	factory-default (Domaine de commande uniquement)	Non requis	Non requis
	Avec des domaines logiques autres que le domaine de commande	Requis (Fichier XML)	Requis (*2)
Remplacement d'une unité d'extension PCI normale (*1) avec PPAR arrêtée	factory-default (Domaine de commande uniquement)	Non requis	Non requis
	Avec des domaines logiques autres que le domaine de commande	Non requis	Non requis

*1 Cela comprend même le remplacement d'une carte de liaison, d'un câble de liaison, d'un câble de gestion et d'une carte de liaison.

*2 Ceci n'est pas requis pour XCP 2230 ou ultérieur ou SPARC M12-2/M12-2S.

Remarque : exécutez la commande `ldm list-constraints -x` pour sauvegarder sur un fichier XML, et exécutez la commande `ldm init-system -i` pour restaurer à partir d'un fichier XML. Pour afficher les variables d'environnement OpenBoot PROM, exécutez la commande `printenv` à partir de l'invite de validation. Pour obtenir une procédure détaillée, consultez le « 1.7.3 How to Save/Restore the Logical Domain Configuration Information and the OpenBoot PROM Environment Variable » du *PCI Expansion Unit for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Service Manual*.

SPARC M12-1/M10-1

Si une unité d'extension PCI est ajoutée ou retirée du SPARC M12-1, ou si une des opérations suivantes est effectuée sur le SPARC M10-1, la configuration du domaine logique de la partition physique reviendra à l'état par défaut à la prochaine heure de démarrage du domaine de commande. Les variables d'environnement OpenBoot PROM du domaine de commande peuvent également être initialisées.

- Mise à jour du microprogramme depuis XCP 2043 ou une version antérieure vers XCP 2044 ou une version ultérieure, dans un système connecté à une unité d'extension PCI
- Ajout/retrait d'une unité d'extension PCI dans un système où le microprogramme XCP 2044 ou version ultérieure est appliqué

Avant l'opération, enregistrez les informations de configuration du domaine logique d'Oracle Solaris dans un fichier XML. Notez également à l'avance les informations de paramétrage des variables d'environnement OpenBoot PROM du domaine de commande pour les définir à nouveau.

Tableau 15-5 indique quelles informations il pourra être nécessaire d'enregistrer/de restaurer lors de la mise à jour du microprogramme de XCP 2043 ou antérieur à XCP 2044 ou ultérieur dans un système raccordé à une unité d'extension PCI.

Tableau 15-5 Opérations requises lors de la mise à jour du microprogramme de XCP 2043 ou antérieur à XCP 2044 ou ultérieur			
Connexion de l'unité d'extension PCI	Configuration actuelle du domaine	Reconstruction de la configuration Oracle VM Server pour SPARC	Nouveau paramétrage de variable d'environnement OpenBoot PROM
Non	factory-default (Domaine de commande uniquement)	Non requis	Non requis
Non	Avec des domaines logiques autres que le domaine de commande	Non requis	Non requis
Oui	factory-default (Domaine de commande uniquement)	Non requis	Non requis
Oui	Avec des domaines logiques autres que le domaine de commande	Requis (Fichier XML)	Requis

Tableau 15-6 indique quelles informations il pourra être nécessaire d'enregistrer/de restaurer lors de l'ajout/du retrait d'une unité d'extension PCI dans un système auquel le microprogramme XCP 2044 ou ultérieur est appliqué.

Tableau 15-6 Opérations requises lors de l'ajout/du retrait d'une unité d'extension PCI dans un système auquel le microprogramme XCP 2044 ou ultérieur est appliqué

Connexion de l'unité d'extension PCI	Configuration actuelle du domaine	Reconstruction de la configuration Oracle VM Server pour SPARC	Nouveau paramétrage de variable d'environnement OpenBoot PROM
Non (ajout)	factory-default (Domaine de commande uniquement)	Non requis	Non requis
Non (ajout)	Avec des domaines logiques autres que le domaine de commande	Requis (Fichier XML)	Requis (*1)
Oui (ajout/retrait)	factory-default (Domaine de commande uniquement)	Non requis	Non requis
Oui (ajout/retrait)	Avec des domaines logiques autres que le domaine de commande	Requis (Fichier XML)	Requis (*1)

*1 Ceci n'est pas requis pour XCP 2230 ou ultérieur ou le SPARC M12-1.

Remarque : exécutez la commande `ldm list-constraints -x` pour sauvegarder sur un fichier XML, et exécutez la commande `ldm init-system -i` pour restaurer à partir d'un fichier XML. Pour afficher les variables d'environnement OpenBoot PROM, exécutez la commande `printenv` à partir de l'invite de validation. Pour obtenir une procédure détaillée, consultez le « 1.7.3 How to Save/Restore the Logical Domain Configuration Information and the OpenBoot PROM Environment Variable » du *PCI Expansion Unit for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Service Manual*.

15.5 Extension de SPARC M12-2S/M10-4S

Pour les tâches d'ajout du SPARC M12-2S/M10-4S afin d'étendre le système ainsi que les procédures de préparation et d'addition en détail, consultez « Chapitre 8 Extension d'un système avec configuration de bloc de construction » dans le *Guide d'installation Fujitsu SPARC M12-2S* ou « Chapitre 8 Avant d'installer/retraiter un système de bloc de construction » dans le *Guide d'installation Fujitsu M10-4S/SPARC M10-4S*.

Pour plus de détails sur comment ajouter un châssis SPARC M12-2S/M10-4S ajouté à une partition physique et comment l'attribuer à un domaine logique, consultez le *Guide de configuration du domaine Fujitsu SPARC M12 et Fujitsu M10/SPARCM10*.

Mise à jour du microprogramme XCP

Ce chapitre décrit comment mettre à jour le microprogramme actuel vers le dernier microprogramme en téléchargeant le programme (XCP) qui gère le microprogramme des systèmes SPARC M12/M10.

- Bases de la mise à jour du microprogramme
- Avant de mettre à jour le microprogramme
- Procédure de mise à jour
- Préparation d'un fichier image XCP
- Mise à jour du microprogramme
- Mettre à jour le microprogramme depuis XSCF Web
- Correspondance de la version du microprogramme avec le remplacement d'éléments
- Problème lors de la mise à jour du microprogramme
- FAQ concernant la mise à jour du microprogramme

L'administrateur système et les techniciens sur site sont chargés de la mise à jour du microprogramme.

16.1 Bases de la mise à jour du microprogramme

16.1.1 Types de microprogrammes à mettre à jour

Ces systèmes disposent de plusieurs microprogrammes pour contrôler le matériel et les logiciels. Le module de programme qui regroupe ces microprogrammes s'appelle XCP (XSCF Control Package).

Télécharger le microprogramme XCP depuis notre site, par exemple, et effectuer une mise à jour rend les fonctions du nouveau microprogramme disponible aux utilisateurs.

Le microprogramme XCP comprend les types suivants.

- Microprogramme POST, microprogramme OpenBoot PROM et microprogramme superviseur (appelés ci-après microprogramme CMU)
Ces trois éléments de microprogramme sont regroupés en un paquet du microprogramme pour le mettre à jour sur l'unité de mémoire CPU et pour gérer leurs versions. Dans ce manuel, ces trois éléments de microprogramme sont appelés ensemble « microprogramme CMU ».
- Microprogramme XSCF
Ce microprogramme est mis à jour sur l'unité XSCF.

Les utilisateurs peuvent choisir de mettre à jour le microprogramme dans son ensemble (nommé ci-dessous microprogramme XCP) ou de mettre à jour uniquement le microprogramme XSCF.

16.1.2 Fonctionnalités de la mise à jour du microprogramme

La mise à jour du microprogramme XCP comprend les fonctions suivantes.

- Une nouvelle mise à jour du microprogramme peut être effectuée sans mettre hors tension une partition physique. La partition physique doit être mise hors tension puis sous tension lors de la mise à jour du microprogramme CMU.
- Si une pièce a été remplacée à l'aide du menu de maintenance dans une configuration de bloc de construction, le microprogramme de la pièce de remplacement est mis automatiquement en correspondance avec la version du microprogramme en fonctionnement.

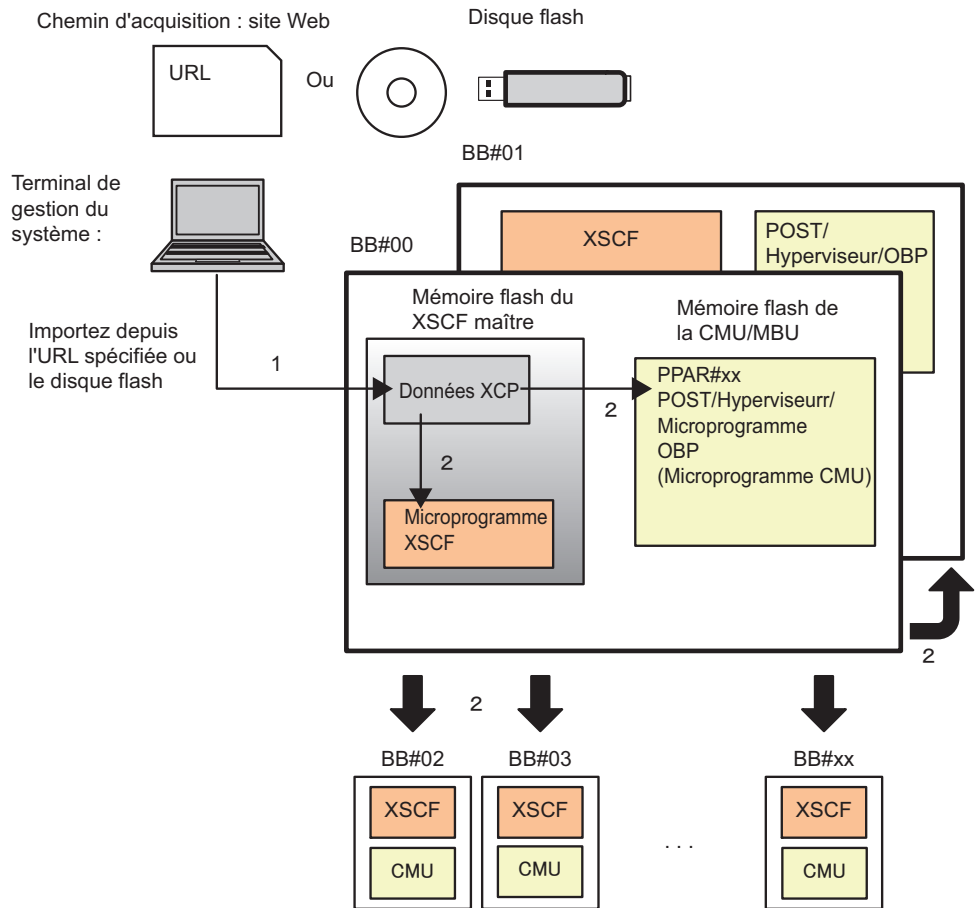
Remarque : pour des informations complémentaires sur la mise en correspondance automatique lorsque l'alimentation est hors tension, et que des pièces sont remplacées ou ajoutées sans passer par le menu de maintenance, consultez les dernières *Notes de produit* pour votre serveur.

- Le microprogramme peut être mis à jour vers la dernière version sans effet sur les autres partitions physiques, même si le système est composé de plusieurs partitions physiques.

16.1.3 Mécanisme de la mise à jour du microprogramme

Figure 16-1 est un schéma conceptuel présentant le mécanisme de mise à jour du microprogramme.

Figure 16-1 Concept de mise à jour du microprogramme



1 Importation de XCP

2 Mise à jour

Les deux opérations suivantes (importation et mise à jour XCP) procurent des mises à jour des microprogrammes pour ces systèmes.

1. **Importation de XCP (téléchargement)**

Enregistrer un fichier image XCP décompressé obtenu depuis un site Internet, par exemple, sur l'un de ces systèmes est appelé « Importation XCP ». Si XCP vient d'être importé, le microprogramme utilisé n'est pas encore mis à jour.

2. **Mise à jour**

L'écriture du fichier image du microprogramme XCP importé dans la mémoire flash de l'un de ces systèmes est appelée « mise à jour ». Les mises à jour du microprogramme XSCF et du microprogramme CMU hors tension sont terminées dans cette mise à jour.

Remarque : pour terminer la mise à jour du microprogramme CMU sur les partitions physiques cibles sous tension, mettez hors et sous tension les partitions physiques.

Dans le SPARC M10-1/M10-4/M10-4S, la mémoire flash avec le microprogramme écrit comprend deux zones : la banque courante et la banque de réserve. La mise à jour du microprogramme est contrôlée avec ces deux banques. Avec le microprogramme CMU, la mise à jour du microprogramme est contrôlée en utilisant uniquement la banque courante.

Remarque : Avec le microprogramme CMU sur le système SPARC M10, la banque de réserve est également affichée. Avec le microprogramme CMU, où la commande est traitée uniquement par la banque courante, il n'existe aucun problème avec une version dépassée de la banque de réserve.

16.1.4 Correspondance des versions

Dans tous les cas suivants, ces systèmes mettent automatiquement en correspondance la version du microprogramme.

- Supposons que plusieurs blocs de construction (cartes système) dans une partition physique disposent de différentes versions du microprogramme CMU. Dans ce cas, les versions du microprogramme sont mises automatiquement en correspondance quand la partition physique est mise sous tension.
- Si les pièces de maintenance (unité XSCF ou unité de mémoire de processeur (inférieure)) ont été remplacées ou ajoutées à l'aide du menu de maintenance, leurs versions de microprogramme sont mises automatiquement en correspondance avec la version du microprogramme en fonctionnement.
- Si la commande flashupdate -c sync a été exécutée, toutes les versions du microprogramme XSCF sont mises en correspondance avec le XSCF maître.

16.1.5 Mise à jour en utilisant plusieurs XSCF

Dans les systèmes avec plusieurs XSCF, le XSCF maître met à jour le microprogramme. Le microprogramme est automatiquement mis à jour dans l'ordre, en commençant par le XSCF de veille puis en suivant par le XSCF maître. Dans ce cas, le XSCF se redémarre ou échange les réseaux des XSCF maître et de veille. Ainsi, le réseau est déconnecté immédiatement. L'utilisateur doit donc se connecter à nouveau.

Pour plus de détails sur la mise à jour, consultez « [16.5 Mise à jour du microprogramme](#) ».

16.2 Avant de mettre à jour le microprogramme

16.2.1 Remarques sur la mise à jour

- Avec une version XCP, les notes de produit pour cette version sont également mises à la disposition du public. Les notes de produit décrivent les éléments suivants : fonctions ajoutées, informations sur les correctifs du logiciel, correspondance entre le nouveau matériel et le microprogramme, informations sur les bogues, corrections apportées aux documents, etc. Les dernières notes de produit contiennent également les corrections des notes de produit précédentes. Il est recommandé de lire les notes de produit de la version du microprogramme appliquée et celles de la dernière version.
- N'appliquez pas de version plus ancienne que le microprogramme XCP sur le système en cours de fonctionnement. Si une version plus ancienne est appliquée, le fonctionnement du système n'est pas garanti.
- Aucune mise à jour de microprogramme n'est possible en cas de panne matérielle. Avant la mise à jour, assurez-vous de vérifier qu'il n'y a aucune panne matérielle. S'il y a une panne matérielle, résolvez la panne puis mettez à jour le microprogramme. Vérifiez l'état du matériel à l'aide de la commande `showhardconf`. Vérifiez qu'aucun matériel n'est identifié avec un astérisque (*).
- La communication du XSCF est déconnectée une fois lors d'une mise à jour de l'ensemble du microprogramme du XCP et du microprogramme XSCF car le XSCF est redémarré. Dans ce cas, raccordez et connectez-vous au XSCF à nouveau.
- Pour mettre à jour le microprogramme en toute sécurité, n'effectuez pas d'opérations d'alimentation pour les partitions physiques jusqu'à ce que vous ayez confirmé le message de mise à jour terminée « XCP update has been completed » du microprogramme XCP.
- Une ou plusieurs partitions physiques peuvent être mises à jour. Pour effectuer une mise à jour de microprogramme CMU quand la partition physique cible est sous tension, mettez hors et sous tension la partition physique.
- Lorsque vous mettez à jour le microprogramme XCP, consultez les « dernières informations » et les « Versions existantes du microprogramme XCP et informations de support » dans les dernières *Notes de produit* pour votre serveur, afin de vérifier si le microprogramme CMU a été mis à jour. Pour la méthode de vérification de la version du microprogramme CMU, consultez « [16.2.3 Méthode de vérification de la version du microprogramme](#) ».

16.2.2 Méthode et format de la distribution du fichier de mise à jour

Les fichiers image du microprogramme XCP sont distribués dans les formats et aux emplacements suivants.

- Méthode d'obtention : site web
Pour plus de détails sur le site Web, consultez les descriptions liées au téléchargement du microprogramme dans les dernières *Notes de produit* pour votre serveur. Les techniciens sur site peuvent effectuer cette tâche avec un CD-ROM, un DVD-ROM ou un disque flash.
- Format : fichier tar compressé (tar.gz) ou fichier exécutable Windows (exe)
Exemple : XCP2020.tar.gz

16.2.3 Méthode de vérification de la version du microprogramme

La version du microprogramme de ces systèmes est appelée « version XCP ». Plus le numéro de version est élevé, plus le microprogramme est récent. Avant de mettre à jour le microprogramme, assurez-vous de vérifier la version XCP du système actuel.

Dans l'exemple suivant, utilisez la commande version avec l'option -c xcp spécifiée pour afficher la version XCP.

```
XSCF> version -c xcp
BB#00-XSCF#0 (Master)
XCP0 (Current): 2044
XCP1 (Reserve): 2044
BB#01-XSCF#0 (Standby)
XCP0 (Current): 2044
XCP1 (Reserve): 2044
BB#02-XSCF#0
XCP0 (Current): 2044
XCP1 (Reserve): 2044
```

Vous pouvez également vérifier la version de chaque microprogramme dans XCP à l'aide de la commande version.

Les quatre chiffres « xyz » représentent la version XCP. Chaque nombre a la signification suivante :

- x : numéro de version majeure
- yy : numéro de version mineure
- z : numéro de version micro

Il peut y avoir plus de révisions de micro-versions que de révisions de documents. Pour cette raison, le document peut indiquer le numéro de micro-version comme une variable.

Exemple : XCP201x

Vous pouvez confirmer les versions individuelles du microprogramme XSCF et du microprogramme CMU dans le XCP à l'aide de l'option -c xcp -v de la commande version.

L'exemple suivant affiche la version du microprogramme XCP du SPARC M10-1.

```
XSCF> version -c xcp -v
BB#00-XSCF#0 (Master)
XCP0 (Current): 2041
CMU          : 02.04.0001
POST         : 1.42.0
OpenBoot PROM : 4.34.0+1.16.0
Hypervisor   : 0.26.9
XSCF         : 02.04.0001
XCP1 (Reserve): 2041
CMU          : 02.04.0001
POST         : 1.42.0
OpenBoot PROM : 4.34.0+1.16.0
Hypervisor   : 0.26.9
XSCF         : 02.04.0001
CMU BACKUP
#0: 02.04.0001
#1: ..
```

L'exemple suivant affiche la version du microprogramme XCP du SPARC M12-2. Dans le SPARC M12-1/M12-2/M12-2S, il n'y a aucune zone de réserve de CMU.

```
XSCF> version -c xcp -v
BB#00-XSCF#0 (Master)
XCP0 (Reserve): 3010
XSCF         : 03.01.0000
XCP1 (Current): 3010
XSCF         : 03.01.0000
CMU          : 03.01.0000
  POST       : X.X.X
  OpenBoot PROM : X.XX.X+X.XX.X
  Hypervisor   : X.X.X
CMU BACKUP
#0: 03.01.0000
#1: ..
```

Le microprogramme CMU peut être différent de la version XCP.

Exemple : si la version de XCP est 2042, la version de microprogramme XSCF est 02.04.0002 tandis que la version de microprogramme CMU est 02.04.0001.

Pour connaître la version du microprogramme CMU correspondant à la version de XCP, consultez « Versions existantes du microprogramme XCP et informations de support » dans les dernières *Notes de produit* pour votre serveur.

16.2.4 Méthodes de mise à jour et durées des tâches

Tableau 16-1 répertorie les méthodes de mise à jour et des estimations de la durée des tâches.

Tableau 16-1 Méthodes de mise à jour et durées des tâches

Méthode de mise à jour	État du système	Durée
Dans un système avec un XSCF, mettez à jour XCP.	La partition physique est hors ou sous tension.	Environ 45 minutes
Dans un système de configuration de bloc de construction avec plusieurs XSCF, mettez à jour XCP. Le microprogramme suivant est mis à jour : le microprogramme CMU de toutes les partitions physiques et le microprogramme XSCF sur toutes les unités XSCF. Seul le microprogramme du XSCF maître peut également être mis à jour. Cependant, pour terminer la mise à jour du microprogramme CMU sur les partitions physiques cibles sous tension, mettez hors et sous tension les partitions physiques.	La partition physique est hors ou sous tension.	Environ 120 minutes
Le microprogramme est automatiquement mis à jour lors du remplacement de pièces afin de mettre en correspondance les versions de microprogramme. La version de microprogramme de chaque pièce de remplacement est mise automatiquement en correspondance avec la version de microprogramme de pré-remplacement. Les tâches suivantes sont effectuées pour les pièces remplacées. - L'unité XSCF du SPARC M12-2S ou l'unité de mémoire de processeur (inférieure) du SPARC M10-4 est ajoutée/remplacée et les versions sont mises en correspondance. - L'unité XSCF d'un boîtier à barre transversale est remplacée/ajoutée et les versions sont mises en correspondance.	La partition physique est hors ou sous tension.	Environ 5 minutes

Remarque : après le remplacement des unités de carte mère des systèmes M12-1/M10-1, des unités de mémoire de processeur (inférieures) du système SPARC M10-4 et de tous les systèmes SPARC M10-4S, des unités XSCF de tous les systèmes SPARC M12-2S et des unités XSCF de tous les boîtiers à barre transversale, la mise en correspondance automatique de version vers la version de microprogramme de pré-remplacement n'est pas possible. Demandez à l'opérateur de mettre à jour le microprogramme.

Remarque : pour des informations complémentaires sur la mise en correspondance automatique des versions lors du remplacement de l'unité de mémoire (inférieure) (CMUL),

du remplacement de l'unité XSCF, de l'ajout du SPARC M10-4S ou de l'ajout du boîtier à barre transversale sans utiliser le menu de maintenance et avec l'alimentation mise hors tension, consultez les *Notes de produit des systèmes Fujitsu M10/SPARC M10* pour la dernière version XCP.

16.3 Procédure de mise à jour

L'ordre de mise à jour du microprogramme avec le Shell XSCF ou XSCF Web est 1) Importation XCP et 2) Mise à jour XCP.

La procédure de base de mise à jour du microprogramme est décrite ci-dessous.

1. **Récupérez le fichier du microprogramme XCP (format tar.gz) depuis le site puis placez-le sur votre périphérique USB ou dans un répertoire en réseau.**
2. **Décompressez le fichier du microprogramme XCP.**
3. **Connectez-vous au XSCF avec un compte d'utilisateur bénéficiant du privilège platadm ou fieldeng. Si les systèmes ont plusieurs XSCF, connectez-vous au XSCF maître.**
4. **Importez le fichier image du microprogramme XCP (BBXCPxxxx.tar.gz) depuis votre périphérique USB ou le répertoire en réseau vers le système (voir getflashimage(8)).**
XCP peut être importé dans le système lorsque Oracle Solaris est actif ou arrêté.
5. **Procédez à la mise à jour du microprogramme XCP ou XSCF (voir flashupdate(8)).**
6. **Pour le microprogramme CMU sur les partitions physiques cibles sous tension, mettez hors et sous tension les partitions physiques (voir poweroff(8) et poweron(8)).**

Remarque : dans le cas d'une configuration du domaine logique, exécutez la commande `ldm add-spconfig` d'Oracle VM Server pour SPARC dans le domaine de commande pour sauvegarder les informations de configuration les plus récentes dans le XSCF avant d'arrêter la partition physique.

Pour plus de détails, consultez « [6.2.2 Sauvegarde des informations de configuration du domaine logique avant l'arrêt du système](#) » et « [10.11.1 Sauvegarde/Affichage des informations de réglage du domaine logique](#) ».

7. **Vérifiez la version du microprogramme (voir la version (8)).**

Pour plus de détails sur ces cinq commandes, consultez la page du manuel correspondant à chaque commande ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*. Pour plus de détails sur le menu XSCF Web associé, consultez « [Annexe C Liste des pages de XSCF Web](#) ».

16.4 Préparation d'un fichier image XCP

Cette section explique comment préparer un fichier image XCP.

1. **Téléchargez le fichier du microprogramme XCP (XCPxxxx.tar.gz ou XCPxxxx.exe) depuis le site Internet vers n'importe quel dossier d'un PC connecté à ce système.**
2. **Vérifiez la version de XCP.**
La version de XCP est indiquée par les 4 chiffres du nom du fichier du microprogramme (format tar.gz).
Exemple : la version de XCP de XCP2044.tar.gz est 2044.
3. **Décompressez le microprogramme XCP téléchargé.**
Le fichier image XCP à importer dans le système est étendu.
Exemple : si XCP2044.tar.gz est décompressé, BBXCP2044.tar.gz est étendu.

16.5 Mise à jour du microprogramme

Cette section décrit comment mettre à jour le microprogramme avec le Shell XSCF. Avec XSCF Web, la procédure est identique. Pour plus de détails sur la procédure XSCF Web, consultez « [16.6 Mettre à jour le microprogramme depuis XSCF Web](#) ».

16.5.1 Mise à jour de XCP sur un système avec un XSCF

1. **Connectez-vous au XSCF.**
2. **Exécutez la commande showhardconf et vérifiez que l'état de XSCF (État MBU) est Normal.**
Vous trouverez ci-dessous des exemples du SPARC M10-1.

```
XSCF> showhardconf
SPARC M10-1;
+ Serial:2101151019A; Operator_Panel_Switch:Service;
+ System_Power:Off; System_Phase:Cabinet Power Off;
Partition#0 PPAR_Status:Powered Off;
MBU Status:Normal; Ver:2046h; Serial:USDA-P00008 ;
+ FRU-Part-Number:CA20366-B10X 002AB/LGA-MBU -01 ;
+ Power_Supply_System: ;
+ Memory_Size:32 GB;
```

3. **Exécutez la commande version pour vérifier la version du microprogramme utilisé.**

```

XSCF> version -c xcp -v
BB#00-XSCF#0 (Master)
XCP0 (Current): 2041
CMU          : 02.04.0001
  POST       : 1.42.0
  OpenBoot PROM : 4.34.0+1.16.0
  Hypervisor  : 0.26.9
XSCF         : 02.04.0001
XCP1 (Reserve): 2041
CMU          : 02.04.0001
  POST       : 1.42.0
  OpenBoot PROM : 4.34.0+1.16.0
  Hypervisor  : 0.26.9
XSCF         : 02.04.0001
CMU BACKUP
#0: 02.04.0001
#1: ..

```

Pour le SPARC M12-1/M12-2, il n'y a aucune banque de réserve du microprogramme CMU. Voici un exemple d'affichage.

```

XSCF> version -c xcp -v
BB#00-XSCF#0 (Master)
XCP0 (Reserve): 3010
XSCF         : 03.01.0000
XCP1 (Current): 3010
XSCF         : 03.01.0000
CMU          : 03.01.0000
  POST       : X.X.X
  OpenBoot PROM : X.XX.X+X.XX.X
  Hypervisor  : X.X.X
CMU BACKUP
#0: 03.01.0000
#1: ..

```

4. **Exécutez la commande `getflashimage` pour importer le fichier image XCP.**
L'exemple suivant importe le fichier image XSCF depuis un périphérique USB connecté à un port USB (où « MAINTENANCE UNIQUEMENT » est indiqué) sur le panneau de l'unité XSCF (panneau arrière).

```

XSCF> getflashimage file:///media/usb_msd/xxxx/BXCP2044.tar.gz
Existing versions:
      Version          Size  Date
      BXCP2041.tar.gz  90004045  Tue Apr 09 04:40:12 JST 2013
Mounted USB device
0MB received
1MB received
...
44MB received
45MB received
Download successful: 46827 Kbytes in 109 secs (430.094 Kbytes/sec)
Checking file...

```

```
MD5: e619e6dd367c888507427e58cdb8e0a4
XSCF>
```

L'importation du fichier image XCP est terminée lorsque les messages de fin normale « Download successful: ... » et « MD5: ... » s'affichent.

Remarque : si le message « Error: File is invalid or corrupt » apparaît après l'importation de XCP, cela signifie que le fichier image XCP importé n'est pas le fichier correct. Cela peut être causé par l'obtention d'un fichier image XCP non autorisé ou car le fichier image XCP téléchargé par le client a ensuite été modifié par un accès non autorisé. Dans de tels cas, obtenez le fichier image XCP correct et importez XCP à nouveau.

5. **Utilisez la commande `getflashimage -l` pour vérifier la version du fichier image XCP importé.**

```
XSCF> getflashimage -l
Existing versions:
      Version                Size  Date
      BBXCP2044.tar.gz      90005045  Wed May 29 13:56:50 JST 2013
```

6. **Exécutez la commande `flashupdate -c check` pour vérifier si le fichier image XCP importé peut être utilisé pour la mise à jour.**

Immédiatement après avoir exécuté la commande `flashupdate`, exécutez la commande `showresult`. Si la valeur finale retournée est 0, vous pouvez utiliser le fichier pour la mise à jour.

```
XSCF> flashupdate -c check -m xcp -s 2044
XSCF> showresult
0
XSCF>
```

7. **Exécutez la commande `flashupdate` pour mettre à jour le microprogramme.**

Remarque :

- La mise à jour prend environ 30 minutes.
 - Pour mettre à jour en toute sécurité le microprogramme, n'effectuez pas d'opérations d'alimentation pour les partitions physiques lors de la tâche (étapes 7 à 11).
-

```
XSCF> flashupdate -c update -m xcp -s 2044
The XSCF will be reset. Continue? [y|n] :y
XCP update is started. [3600sec]
  0..... 30..... 60..... 90.....120.....150.....180.....210.....240.....-
270.....300.....330.....360.....390.....420.....450.....480.....510.....
:
```

Ici, le XSCF est réinitialisé, et la session XSCF est déconnectée.

À ce niveau, la mise à jour du microprogramme XCP n'est pas encore terminée.

8. **Connectez-vous de nouveau au XSCF.**
9. **Exécutez la commande `showlogs monitor` pour vérifier la finalisation de la mise à jour du microprogramme XCP.**

```
XSCF> showlogs monitor
May 29 14:30:09 M10-1-0 Event: SCF:XCP update is started (XCP version=2044:
last version=2041)
May 29 14:31:59 M10-1-0 Event: SCF:XSCF update is started (BBID=0, bank=1)
May 29 14:32:18 M10-1-0 Event: SCF:XSCF writing is performed (BBID=0, XSCF
version=02040004)
May 29 14:39:27 M10-1-0 Event: SCF:XSCF update has been completed (BBID=0,
bank=1)
May 29 14:39:28 M10-1-0 Event: SCF:XSCF bank apply has been completed (BBID=0,
bank=1, XCP version=2044:last version=2041)
May 29 14:47:12 M10-1-0 Event: SCF:XSCF ready
May 29 14:48:32 M10-1-0 Event: SCF:XSCF update is started (BBID=0, bank=0)
May 29 14:48:52 M10-1-0 Event: SCF:XSCF writing is performed (BBID=0, XSCF
version=02040004)
May 29 14:55:51 M10-1-0 Event: SCF:XSCF update has been completed (BBID=0,
bank=0)
May 29 14:57:04 M10-1-0 Event: SCF:CMU update is started (BBID=0)
May 29 14:57:07 M10-1-0 Event: SCF:CMU writing is performed (BBID=0, CMU
version=02040004)
May 29 14:59:07 M10-1-0 Event: SCF:CMU update has been completed (BBID=0)
May 29 15:00:19 M10-1-0 Event: SCF:CMU update is started (BBID=0)
May 29 15:00:20 M10-1-0 Event: SCF:CMU writing is performed (BBID=0, CMU
version=02040004)
May 29 15:02:18 M10-1-0 Event: SCF:CMU update has been completed (BBID=0)
May 29 15:02:20 M10-1-0 Event: SCF:XCP update has been completed (XCP
version=2044:last version=2041)
```

L'exemple suivant affiche les messages sur le SPARC M12-2.

```
XSCF> showlogs monitor
Mar 15 15:29:34 M12-2-0 Event: SCF:XCP update is started (XCP version=3010:
last version=3009)
Mar 15 15:39:20 M12-2-0 Event: SCF:Updating XCP:Preparing to update XSCF
(BBID=0, bank=0)
Mar 15 15:42:59 M12-2-0 Event: SCF:Updating XCP:Updating XSCF (BBID=0, XSCF
version=03010000)
Mar 15 15:43:13 M12-2-0 Event: SCF:Updating XCP:XSCF updated (BBID=0, bank=0)
Mar 15 15:43:20 M12-2-0 Event: SCF:Updating XCP:XSCF bank has changed (BBID=0,
bank=0, XCP version=3010:last version=3009)
Mar 15 16:02:49 M12-2-0 Event: SCF:Updating XCP:Preparing to update XSCF
(BBID=0, bank=1)
Mar 15 16:04:18 M12-2-0 Event: SCF:Updating XCP:Updating XSCF (BBID=0, XSCF
version=03010000)
Mar 15 16:04:22 M12-2-0 Event: SCF:Updating XCP:XSCF updated (BBID=0, bank=1)
Mar 15 16:04:47 M12-2-0 Event: SCF:XSCF ready
Mar 15 16:07:47 M12-2-0 Event: SCF:Updating XCP:Preparing to update CMU (BBID=0)
Mar 15 16:08:17 M12-2-0 Event: SCF:Updating XCP:Updating CMU (BBID=0, CMU
version=03010000)
Mar 15 16:08:28 M12-2-0 Event: SCF:Updating XCP:CMU updated (BBID=0)
```

Si le message « XCP update has been completed » apparaît, la mise à jour du microprogramme XCP est terminée.

Remarque : un message similaire à « XSCF update has been completed » ou « CMU update has been completed » apparaîtra sur le SPARC M10. Cependant, la mise à jour de tout le microprogramme XCP ne pourra être terminée une fois le message apparu. Pour mettre à jour le microprogramme en toute sécurité, n'effectuez pas d'opérations d'alimentation pour les partitions physiques jusqu'à ce que vous ayez confirmé le message de mise à jour terminée « XCP update has been completed » pour le microprogramme XCP.

Si le message « XCP update has been completed » n'apparaît pas, la mise à jour n'est pas encore terminée. Exécutez à nouveau la commande `showlogs monitor` pour vérifier la finalisation de la mise à jour. Généralement, la mise à jour est terminée environ 20 minutes après l'apparition du message « XSCF ready ».

Si la partition physique est hors tension et si vous avez confirmé le message « XCP update has been completed », la mise à jour du microprogramme XCP est terminée. Passez à l'étape 11.

Si la partition physique est sous tension, le microprogramme CMU cible n'a pas encore été mis à jour à ce stade. Par conséquent, le message n'apparaît pas pour le microprogramme CMU. Une fois que vous avez confirmé le message « XCP update has been completed », passez à l'étape 10.

10. Pour effectuer la mise à jour du microprogramme CMU quand la partition physique est sous tension, mettez hors et sous tension la partition physique.

Remarque : dans le cas d'une configuration du domaine logique, exécutez la commande `ldm add-spconfig` d'Oracle VM Server pour SPARC dans le domaine de commande pour sauvegarder les informations de configuration les plus récentes dans le XSCF avant d'arrêter la partition physique.

Pour plus de détails, consultez « [6.2.2 Sauvegarde des informations de configuration du domaine logique avant l'arrêt du système](#) » et « [10.11.1 Sauvegarde/Affichage des informations de réglage du domaine logique](#) ».

Exécutez la commande `poweroff` pour mettre la partition physique hors tension.

```
XSCF> poweroff -p 0
```

Exécutez la commande `showpparstatus power` et vérifiez que la partition physique est hors tension.

```
XSCF> showpparstatus -p 0
PPAR-ID          PPAR Status
00                Powered Off
```

Exécutez la commande `poweron` pour mettre la partition physique sous tension.

```
XSCF> poweron -p 0
```

Exécutez la commande `showpparstatus` et confirmez que l'état de PPAR est « Running ».

```
XSCF> showpparstatus -p 0
PPAR-ID          PPAR Status
00               Running
```

11. **Exécutez la commande `version` et vérifiez que la version du microprogramme est à jour.**

```
XSCF> version -c xcp -v
BB#00-XSCF#0 (Master)
XCP0 (Reserve): 2044
CMU          : 02.04.0004
  POST       : 1.43.0
  OpenBoot PROM : 4.34.0+1.19.0
  Hypervisor  : 0.27.3
XSCF         : 02.04.0004
XCP1 (Current): 2044
CMU          : 02.04.0004
  POST       : 1.43.0
  OpenBoot PROM : 4.34.0+1.19.0
  Hypervisor  : 0.27.3
XSCF         : 02.04.0004
CMU BACKUP
#0: 02.04.0004
#1: ..
```

Remarque : sur le SPARC M10-1/M10-4/M10-4S, si le microprogramme est mis à jour en mettant la partition physique sous tension, la banque courante du microprogramme CMU est mise à jour.

Si le microprogramme est mis à jour en coupant l'alimentation d'une partition physique, la banque de réserve et la banque courante du microprogramme CMU sont alors mis à jour. Pour connaître la version du microprogramme CMU correspondant à la version de XCP, consultez « Versions existantes du microprogramme XCP et informations de support » dans les dernières *Notes de produit* pour votre serveur.

16.5.2

Mise à jour de XCP dans un système de configuration de bloc de construction avec plusieurs XSCF

1. **Connectez-vous au XSCF maître.**
2. **Exécutez la commande `showhardconf` et vérifiez que l'État est Normal pour le XSCF maître et le XSCF de veille.**

Vous trouverez ci-dessous des exemples du SPARC M10-4S.

```
XSCF> showhardconf
SPARC M10-4S;
+ Serial:2081230011; Operator_Panel_Switch:Locked;
+ System_Power:Off; System_Phase:Cabinet Power Off;
Partition#0 PPAR_Status:Powered Off;
Partition#1 PPAR_Status:Powered Off;
BB#00 Status:Normal; Role:Master; Ver:2003h; Serial:2081231002;
+ FRU-Part-Number:CA07361-D202 A1
:
BB#01 Status:Normal; Role:Standby Ver:0101h; Serial:7867000297;
+ FRU-Part-Number:CA20393-B50X A2 ;
```

3. **Exécutez la commande `version` pour vérifier la version du microprogramme utilisé.**

```
XSCF> version -c xcp -v
BB#00-XSCF#0 (Master)
XCP0 (Current): 2041
CMU          : 02.04.0001
  POST       : 1.42.0
  OpenBoot PROM : 4.34.0+1.16.0
  Hypervisor   : 0.26.9
XSCF         : 02.04.0001
XCP1 (Reserve): 2041
CMU          : 02.04.0001
  POST       : 1.42.0
  OpenBoot PROM : 4.34.0+1.16.0
  Hypervisor   : 0.26.9
XSCF         : 02.04.0001
BB#01-XSCF#0 (Standby)
XCP0 (Reserve): 2041
CMU          : 02.04.0001
  POST       : 1.42.0
  OpenBoot PROM : 4.34.0+1.16.0
  Hypervisor   : 0.26.9
XSCF         : 02.04.0001
XCP1 (Current): 2041
CMU          : 02.04.0001
  POST       : 1.42.0
```

```

OpenBoot PROM : 4.34.0+1.16.0
Hypervisor    : 0.26.9
XSCF          : 02.04.0001
CMU BACKUP
#0: 02.04.0001
#1: ..

```

Pour le SPARC M12-2S, il n'y a aucune banque de réserve du microprogramme CMU. Voici un exemple d'affichage.

```

XSCF# version -c xcp -v
BB#00-XSCF#0 (Standby)
XCP0 (Reserve): 3010
XSCF          : 03.01.0000
XCP1 (Current): 3010
XSCF          : 03.01.0000
CMU           : 03.01.0000
    POST      :
    OpenBoot PROM :
    Hypervisor  :
BB#01-XSCF#0 (Master)
XCP0 (Reserve): 3010
XSCF          : 03.01.0000
XCP1 (Current): 3010
XSCF          : 03.01.0000
CMU           : 03.01.0000
    POST      :
    OpenBoot PROM :
    Hypervisor  :
CMU BACKUP
#0: 03.01.0000
#1: ..
XSCF#

```

4. **Exécutez la commande getflashimage pour importer le fichier image XCP.**
L'exemple suivant importe le fichier image XSCF depuis un périphérique USB connecté à un port USB (où « MAINTENANCE UNIQUEMENT » est indiqué) sur le panneau de l'unité XSCF (panneau arrière) du XSCF maître.

```

XSCF> getflashimage file:///media/usb_msd/xxxx/BBXCP2044.tar.gz
Existing versions:
      Version              Size  Date
      BBXCP2041.tar.gz    90004045  Tue Apr 09 04:40:12 JST 2013
Mounted USB device
0MB received
1MB received
...
44MB received
45MB received
Download successful: 46827 Kbytes in 109 secs (430.094 Kbytes/sec)
Checking file...
MD5: e619e6dd367c888507427e58cdb8e0a4

```

L'importation du fichier image XCP est terminée lorsque les messages de fin normale « Download successful: ... » et « MD5: ... » s'affichent.

Remarque : si le message « Error: File is invalid or corrupt » apparaît après l'importation de XCP, cela signifie que le fichier image XCP importé n'est pas le fichier correct. Cela peut être causé par l'obtention d'un fichier image XCP non autorisé ou car le fichier image XCP téléchargé par le client a ensuite été modifié par un accès non autorisé. Dans de tels cas, obtenez le fichier image XCP correct et importez XCP à nouveau.

5. Utilisez la commande `getflashimage -l` pour vérifier la version du fichier image XCP importé.

```
XSCF> getflashimage -l
Existing versions:
      Version              Size   Date
BBXCP2044.tar.gz      90005045  Wed May 29 09:11:40 JST 2013
```

6 Exécutez la commande `flashupdate -c check` pour vérifier si le fichier image XCP importé peut être utilisé pour la mise à jour.

Immédiatement après avoir exécuté la commande `flashupdate`, exécutez la commande `showresult`. Si la valeur finale retournée est 0, vous pouvez utiliser le fichier pour la mise à jour.

```
XSCF> flashupdate -c check -m xcp -s 2044
XSCF> showresult
0
XSCF>
```

7. Exécutez la commande `flashupdate` pour mettre à jour le microprogramme.

Remarque :

- La mise à jour prend environ 60 minutes.
- Pour mettre à jour en toute sécurité le microprogramme, n'effectuez pas d'opérations d'alimentation pour les partitions physiques lors de la tâche (étapes 7 à 11).

```
XSCF> flashupdate -c update -m xcp -s 2044
The XSCF will be reset. Continue? [y|n] :y
XCP update is started. [3600sec]
  0..... 30..... 60..... 90.....120.....150.....180.....210.....240.....-
270.....300.....330.....360.....390.....420.....450.....480.....510.....|
540.....570.....600.....630.....660.....690.....720.....750.....780.....-
810.....840.....870.....900.....930
:
```

Ici, le XSCF est redémarré, la session XSCF est déconnectée.

À ce niveau, la mise à jour du microprogramme XCP n'est pas encore terminée.

8. **Connectez-vous de nouveau au XSCF maître.**

Immédiatement après le redémarrage du XSCF, les états des XSCF maître et de veille reviennent à leur état d'origine. Par exemple, lorsque la mise à jour du microprogramme est exécutée avec le numéro BB-ID 0 sur le XSCF maître, rebrancher à XSCF changera l'état du numéro BB-ID 1 sur le maître et mettra le numéro BB-ID 0 en état de veille. Dans cet exemple, le XSCF maître (BB-ID 1) est connecté.

Remarque : pour les clients ayant défini l'adresse IP de prise de contrôle, les machines sont automatiquement connectées au XSCF maître quand elles sont connectées en utilisant l'adresse IP de prise de contrôle.

9. **Exécutez la commande showbbstatus et vérifiez que vous êtes connecté au XSCF maître. Si vous êtes connecté au XSCF de veille, reconnectez-vous au XSCF maître.**

Remarque : si le microprogramme est mis à jour à la version XCP 2050 ou supérieure, lorsque la mise à jour du microprogramme XCP est terminée, le XSCF maître/de veille commuté reviendra à son état d'origine. Dans ce cas, connectez-vous à nouveau au XSCF maître, car le XSCF est redémarré et la session XSCF est déconnectée.

```
XSCF> showbbstatus
BB#01 (Master)
```

10. **Exécutez la commande showlogs monitor pour vérifier la finalisation de la mise à jour du microprogramme XCP.**

```
XSCF> showlogs monitor
May 29 09:38:05 M10-4S-0 Event: SCF:XCP update is started (XCP version=2044:
last version=2041)
May 29 09:40:31 M10-4S-0 Event: SCF:XSCF update is started (BBID=0, bank=0)
May 29 09:40:46 M10-4S-0 Event: SCF:XSCF update is started (BBID=1, bank=0)
May 29 09:41:03 M10-4S-0 Event: SCF:XSCF writing is performed (BBID=0, XSCF
version=02040004)
May 29 09:41:12 M10-4S-0 Event: SCF:XSCF writing is performed (BBID=1, XSCF
version=02040004)
May 29 09:48:18 M10-4S-0 Event: SCF:XSCF update has been completed (BBID=0,
bank=0)
May 29 09:50:39 M10-4S-0 Event: SCF:XSCF update has been completed (BBID=1,
bank=0)
May 29 09:50:41 M10-4S-0 Event: SCF:XSCF bank apply has been completed
(BBID=1, bank=0, XCP version=2044:last version=2041)
May 29 10:01:50 M10-4S-0 Event: SCF:XSCF bank apply has been completed
(BBID=0, bank=0, XCP version=2044:last version=2041)
May 29 10:01:51 M10-4S-0 Event: SCF:Change Master Start (BB#01)
May 29 10:03:26 M10-4S-1 Event: SCF:Change Master Complete (BB#01)
May 29 10:05:00 M10-4S-1 Event: SCF:Standby XSCF Ready (BBID#00)
```

```

May 29 10:12:56 M10-4S-1 Event: SCF:XSCF update is started (BBID=1, bank=1)
May 29 10:13:23 M10-4S-1 Event: SCF:XSCF update is started (BBID=0, bank=1)
May 29 10:13:24 M10-4S-1 Event: SCF:XSCF writing is performed (BBID=0, XSCF
version=02040004)
May 29 10:13:42 M10-4S-1 Event: SCF:XSCF writing is performed (BBID=1, XSCF
version=02040004)
May 29 10:20:22 M10-4S-1 Event: SCF:XSCF update has been completed (BBID=0,
bank=1)
May 29 10:23:34 M10-4S-1 Event: SCF:XSCF update has been completed (BBID=1,
bank=1)
May 29 10:24:42 M10-4S-1 Event: SCF:CMU update is started (BBID=0)
May 29 10:24:58 M10-4S-1 Event: SCF:CMU writing is performed (BBID=0, CMU
version=02040004)
May 29 10:25:44 M10-4S-1 Event: SCF:CMU update is started (BBID=1)
May 29 10:25:46 M10-4S-1 Event: SCF:CMU writing is performed (BBID=1, CMU
version=02040004)
May 29 10:26:44 M10-4S-1 Event: SCF:CMU update has been completed (BBID=0)
May 29 10:27:51 M10-4S-1 Event: SCF:CMU update has been completed (BBID=1)
May 29 10:29:30 M10-4S-1 Event: SCF:CMU update is started (BBID=0)
May 29 10:29:36 M10-4S-1 Event: SCF:CMU writing is performed (BBID=0, CMU
version=02040004)
May 29 10:29:45 M10-4S-1 Event: SCF:CMU update is started (BBID=1)
May 29 10:30:04 M10-4S-1 Event: SCF:CMU writing is performed (BBID=1, CMU
version=02040004)
May 29 10:31:18 M10-4S-1 Event: SCF:CMU update has been completed (BBID=0)
May 29 10:31:51 M10-4S-1 Event: SCF:CMU update has been completed (BBID=1)
May 29 10:32:38 M10-4S-1 Event: SCF:XCP update has been completed (XCP
version=2044:last version=2041)
May 29 10:32:39 M10-4S-1 Event: SCF:This XSCF will be switched back to standby
mode after completion of firmware update
May 29 10:32:39 M10-4S-1 Event: SCF:Change Master Start(BB#00)
May 29 10:33:29 M10-4S-1 Event: SCF:Change Master Complete(BB#00)
May 29 10:42:29 M10-4S-1 Event: SCF:Standby XSCF Ready (BBID#01)

```

L'exemple suivant affiche les messages sur le SPARC M12-2S.

```

XSCF> showlogs monitor
Apr  5 06:51:06 M12-2S-1 Event: SCF:XCP update is started (XCP version=3010:
last version=3009)
Apr  5 07:01:41 M12-2S-1 Event: SCF:Updating XCP:Preparing to update XSCF
(BBID=1, bank=1)
Apr  5 07:03:46 M12-2S-1 Event: SCF:Updating XCP:Updating XSCF (BBID=1, XSCF
version=03010000)
Apr  5 07:03:54 M12-2S-1 Event: SCF:Updating XCP:XSCF updated (BBID=1, bank=1)
Apr  5 07:06:58 M12-2S-1 Event: SCF:Updating XCP:Preparing to update XSCF
(BBID=0, bank=0)
Apr  5 07:09:22 M12-2S-1 Event: SCF:Updating XCP:Updating XSCF (BBID=0, XSCF
version=03010000)
Apr  5 07:10:39 M12-2S-1 Event: SCF:Updating XCP:XSCF updated (BBID=0, bank=0)
Apr  5 07:12:50 M12-2S-1 Event: SCF:Updating XCP:XSCF bank has changed
(BBID=1, bank=1, XCP version=3010:last version=3009)
Apr  5 07:20:06 M12-2S-1 Event: SCF:Updating XCP:XSCF bank has changed
(BBID=0, bank=0, XCP version=3010:last version=3009)
Apr  5 07:21:27 M12-2S-1 Event: SCF:Change Master Start(BB#01)

```



```

Apr  5 07:22:28 M12-2S-2 Event: SCF:Standby XSCF Ready(BB#01)
Apr  5 07:24:05 M12-2S-2 Event: SCF:Change Master Complete(BB#01)
Apr  5 07:30:08 M12-2S-2 Event: SCF:Updating XCP:Preparing to update XSCF
(BBID=1, bank=0)
Apr  5 07:30:35 M12-2S-2 Event: SCF:Updating XCP:Preparing to update XSCF
(BBID=0, bank=0)
Apr  5 07:34:41 M12-2S-2 Event: SCF:Standby XSCF Ready(BB#00)
Apr  5 07:35:21 M12-2S-2 Event: SCF:Updating XCP:Updating XSCF (BBID=0, XSCF
version=03010000)
Apr  5 07:40:32 M12-2S-2 Event: SCF:Updating XCP:XSCF updated (BBID=0, bank=1)
Apr  5 07:40:39 M12-2S-2 Event: SCF:Updating XCP:Updating XSCF (BBID=1, XSCF
version=03010000)
Apr  5 07:45:49 M12-2S-2 Event: SCF:Updating XCP:XSCF updated (BBID=1, bank=0)
Apr  5 07:46:18 M12-2S-2 Event: SCF:Updating XCP:Preparing to update CMU
(BBID=0)
Apr  5 07:46:41 M12-2S-2 Event: SCF:Updating XCP:Updating CMU (BBID=0, CMU
version=03010000)
Apr  5 07:48:21 M12-2S-2 Event: SCF:Updating XCP:CMU updated (BBID=0)
Apr  5 07:49:00 M12-2S-2 Event: SCF:Updating XCP:Preparing to update CMU
(BBID=1)
Apr  5 07:49:30 M12-2S-2 Event: SCF:Updating XCP:Updating CMU (BBID=1, CMU
version=03010000)
Apr  5 07:51:24 M12-2S-2 Event: SCF:Updating XCP:CMU updated (BBID=1)
Apr  5 07:51:25 M12-2S-2 Event: SCF:XCP update has been completed (XCP
version=3010:last version=3009)
Apr  5 07:51:26 M12-2S-2 Event: SCF:This XSCF will be switched back to standby
mode after completion of firmware update
Apr  5 07:51:57 M12-2S-1 Event: SCF:Change Master Complete(BB#00)

```

Si le message « XCP update has been completed » apparaît, la mise à jour du microprogramme XCP est terminée.

Remarque : un message similaire à « XSCF update has been completed » ou « CMU update has been completed » apparaîtra sur le SPARC M10. Cependant, la mise à jour de tout le microprogramme XCP ne pourra être terminée une fois le message apparu. Pour mettre à jour le microprogramme en toute sécurité, n'effectuez pas d'opérations d'alimentation pour les partitions physiques jusqu'à ce que vous ayez confirmé le message de mise à jour terminée « XCP update has been completed » pour le microprogramme XCP.

Si le message « XCP update has been completed » n'apparaît pas, la mise à jour n'est pas encore terminée. Exécutez à nouveau la commande showlogs monitor pour vérifier la finalisation de la mise à jour. Généralement, la mise à jour est terminée environ 40 minutes après un redémarrage du XSCF.

- Si la partition physique est sous tension

La mise à jour du microprogramme CMU cible n'a pas encore commencé au stade où la commande flashupdate est exécutée et la finalisation de la mise à jour est vérifiée. Par conséquent, le message n'apparaît pas pour le microprogramme CMU. La mise à jour du microprogramme CMU cible commence quand la partition physique est mise hors et sous tension dans l'étape 12.

- Si le microprogramme est mis à jour à la version XCP 2050 ou ultérieure

Une fois la mise à jour du microprogramme terminée, le XSCF maître et le XSCF de veille sont automatiquement permutés. La permutation automatique prend environ 10 minutes.

Si les messages « This XSCF will be switched back to standby mode after completion of firmware update, », « Change Master Complete » et « Standby XSCF Ready » apparaissent, la permutation a été effectuée.

Pour vérifier la finalisation de la permutation, exécutez la commande `showhardconf` et vérifiez que l'État est Normal pour le XSCF maître et le XSCF de veille.

```
XSCF> showhardconf
SPARC M10-4S;
+ Serial:2081230011; Operator_Panel_Switch:Locked;
+ System_Power:Off; System_Phase:Cabinet Power Off;
Partition#0 PPAR_Status:Powered Off;
Partition#1 PPAR_Status:Powered Off;
BB#00 Status:Normal; Role:Master; Ver:2003h; Serial:2081231002;
+ FRU-Part-Number:CA07361-D202 A1
:
BB#01 Status:Normal; Role:Standby Ver:0101h; Serial:7867000297;
+ FRU-Part-Number:CA20393-B50X A2 ;
```

Après avoir vérifié que la permutation a été effectuée, passez à l'étape 12.

Remarque : si l'exécution de la commande `showhardconf` affiche « Cannot communicate with the other XSCF. Check the other XSCF's state. », la permutation des XSCF maître et de veille n'a pas été effectuée. Exécutez à nouveau la commande `showhardconf` pour vérifier la finalisation de la permutation.

Remarque : le traitement de mise à jour du microprogramme permute les XSCF maître et de veille deux fois. Ainsi, le XSCF où vous avez exécuté la commande `flashupdate` redevient le XSCF maître. Permuter les XSCF maître et de veille peut déconnecter la session du XSCF. Si la session du XSCF est déconnectée, reconnectez-vous.

- Si le microprogramme est mis à jour à la version XCP 2044 ou antérieure

Le traitement de mise à jour du microprogramme permute les XSCF maître et de veille. Ainsi, l'autre XSCF couplé avec le XSCF où vous avez exécuté la commande `flashupdate` devient le XSCF maître.

11. Exécutez la commande `switchscf` pour revenir à l'état des XSCF maître et de veille avant la mise à jour.

Remarque : lors de la mise à jour du microprogramme vers la version XCP 2050 ou ultérieure, vous n'avez pas à effectuer cette tâche, car les XSCF ont déjà été permutés.

```
XSCF> switchscf -t Standby
The XSCF unit switch between the Active and Standby states.
Continue? [y|n] :y
```

Vu que le redémarrage d'un XSCF déconnecte la session du XSCF, le XSCF maître est à nouveau connecté.

Pour vérifier la finalisation de la permutation, exécutez la commande `showhardconf` et vérifiez que l'État est Normal pour le XSCF maître et le XSCF de veille.

```
XSCF> showhardconf
SPARC M10-4S;
+ Serial:2081230011; Operator_Panel_Switch:Locked;
+ System_Power:Off; System_Phase:Cabinet Power Off;
Partition#0 PPAR_Status:Powered Off;
Partition#1 PPAR_Status:Powered Off;
BB#00 Status:Normal; Role:Master; Ver:2003h; Serial:2081231002;
+ FRU-Part-Number:CA07361-D202 A1
:
BB#01 Status:Normal; Role:Standby Ver:0101h; Serial:7867000297;
+ FRU-Part-Number:CA20393-B50X A2 ;
```

Remarque : si l'exécution de la commande `showhardconf` affiche « Cannot communicate with the other XSCF. Check the other XSCF's state. », la permutation des XSCF maître et de veille n'a pas été effectuée. Exécutez à nouveau la commande `showhardconf` pour vérifier la finalisation de la permutation.

12. Pour effectuer la mise à jour du microprogramme CMU quand la partition physique est sous tension, mettez hors et sous tension la partition physique.

Remarque : dans le cas d'une configuration du domaine logique, exécutez la commande `ldm add-sponconfig` d'Oracle VM Server pour SPARC dans le domaine de commande pour sauvegarder les informations de configuration les plus récentes dans le XSCF avant d'arrêter la partition physique.

Pour plus de détails, consultez « [6.2.2 Sauvegarde des informations de configuration du domaine logique avant l'arrêt du système](#) » et « [10.11.1 Sauvegarde/Affichage des informations de réglage du domaine logique](#) ».

Remarque : si la partition physique est hors tension, vous n'avez pas à effectuer cette tâche car la mise à jour du microprogramme CMU a été effectuée. Passez à l'étape 13.

Si la partition physique est sous tension, exécutez la commande `poweroff` pour mettre hors tension la partition physique.

```
XSCF> poweroff -p xx
```

Exécutez la commande `showpparstatus power` et vérifiez que la partition

physique est hors tension.

```
XSCF> showpparstatus -p xx
PPAR-ID          PPAR Status
xx               Powered Off
```

Exécutez la commande `poweron` pour mettre la partition physique sous tension.

```
XSCF> poweron -p xx
```

Exécutez la commande `showpparstatus` et confirmez que l'état de PPAR est « Running ».

```
XSCF> showpparstatus -p xx
PPAR-ID          PPAR Status
xx               Running
```

13. Exécutez la commande `version` et vérifiez que la version du microprogramme est à jour.

```
XSCF> version -c xcp -v
BB#00-XSCF#0 (Master)
XCP0 (Reserve): 2044
CMU          : 02.04.0004
  POST       : 1.43.0
  OpenBoot PROM : 4.34.0+1.19.0
  Hypervisor  : 0.27.3
XSCF         : 02.04.0004
XCP1 (Current): 2044
CMU          : 02.04.0004
  POST       : 1.43.0
  OpenBoot PROM : 4.34.0+1.19.0
  Hypervisor  : 0.27.3
XSCF         : 02.04.0004
BB#01-XSCF#0 (Standby)
XCP0 (Current): 2044
CMU          : 02.04.0004
  POST       : 1.43.0
  OpenBoot PROM : 4.34.0+1.19.0
  Hypervisor  : 0.27.3
XSCF         : 02.04.0004
XCP1 (Reserve): 2044
CMU          : 02.04.0004
  POST       : 1.43.0
  OpenBoot PROM : 4.34.0+1.19.0
  Hypervisor  : 0.27.3
XSCF         : 02.04.0004
CMU BACKUP
#0: 02.04.0004
#1: ..
```

Remarque : sur le SPARC M10-1/M10-4/M10-4S, si le microprogramme est mis à jour en mettant la partition physique sous tension, la banque courante du microprogramme CMU est mise à jour.

Si le microprogramme est mis à jour en coupant l'alimentation d'une partition physique, la banque de réserve et la banque courante du microprogramme CMU sont alors mis à jour.

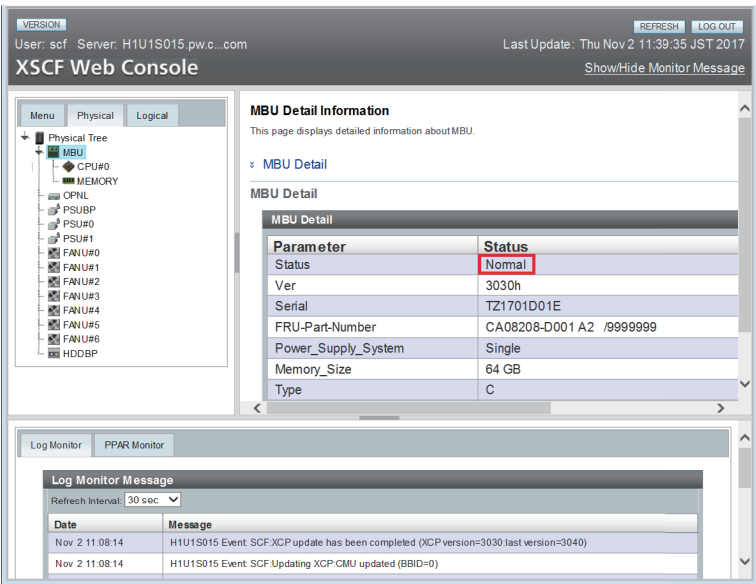
Pour connaître la version du microprogramme CMU correspondant à la version de XCP, consultez « Versions existantes du microprogramme XCP et informations de support » dans les dernières *Notes de produit des systèmes Fujitsu M10/SPARC M10*.

16.6 Mettre à jour le microprogramme depuis XSCF Web

Cette section décrit comment mettre à jour le microprogramme depuis XSCF Web avec un exemple pour le SPARC M12-1.

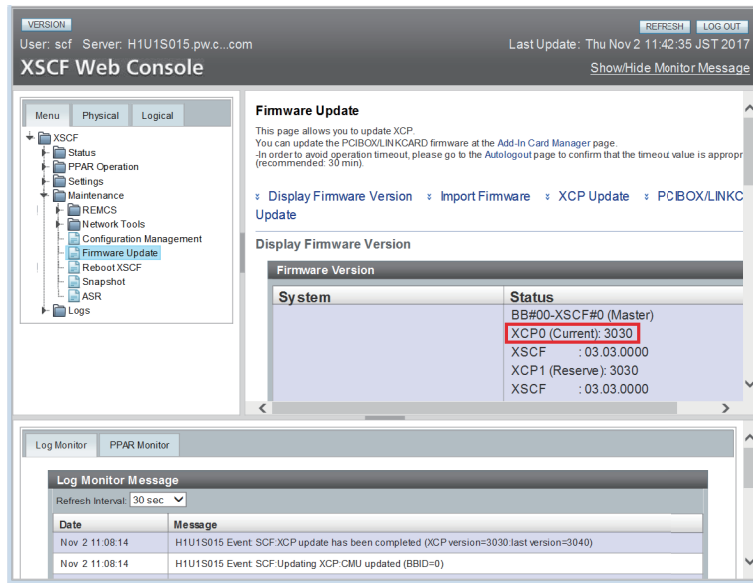
- 1. **Connectez-vous à XSCF Web.**
- 2. **Sélectionnez [Physical] - [MBU].**
- 3. **Vérifiez que l'état est Normal pour la MBU sur l'écran [MBU Detail] comme indiqué dans Figure 16-2.**

Figure 16-2 Écran [MBU Detail]



- 4. **Sélectionnez [Menu] - [Maintenance] - [Firmware Update].**
- 5. **Vérifiez la version du microprogramme XCP utilisé, sur l'écran [Display Frimware Version] indiqué dans Figure 16-3.**

Figure 16-3 Écran [Display Firmware Version]

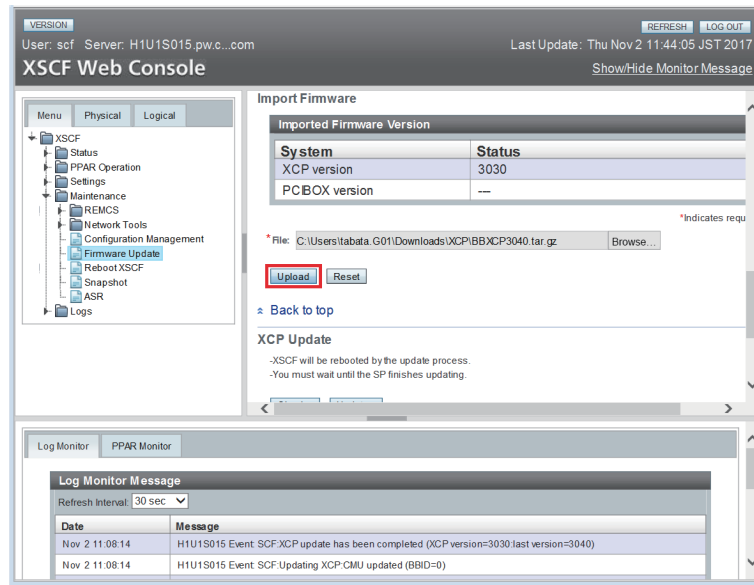


6. **Importez le fichier image XCP depuis l'écran [Import Firmware] indiqué dans Figure 16-4.**

Spécifiez le chemin du fichier image XCP et cliquez sur le bouton [Upload].
L'importation prend environ cinq minutes.

Remarque : si le message d'avertissement d'écrasement « An existing file will be overwritten, continue to process? » apparaît, cliquez sur le bouton [OK].

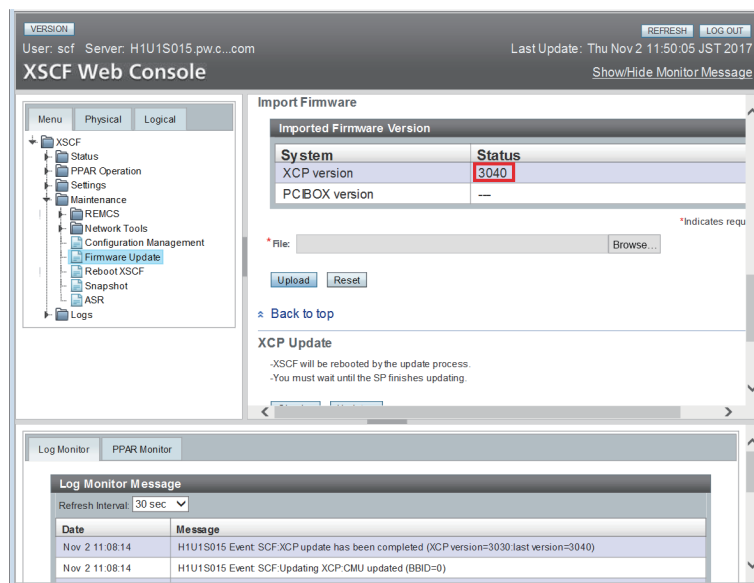
Figure 16-4 Écran [Import Firmware]



L'importation est complète lorsque « The file has been uploaded successfully. » apparaît.

La ligne de la version XCP de l'écran [Import Firmware] indiqué dans Figure 16-5 est mise à jour. Vérifiez que la version du microprogramme du fichier image XCP importé s'affiche.

Figure 16-5 Écran [Import Firmware] une fois l'importation terminée

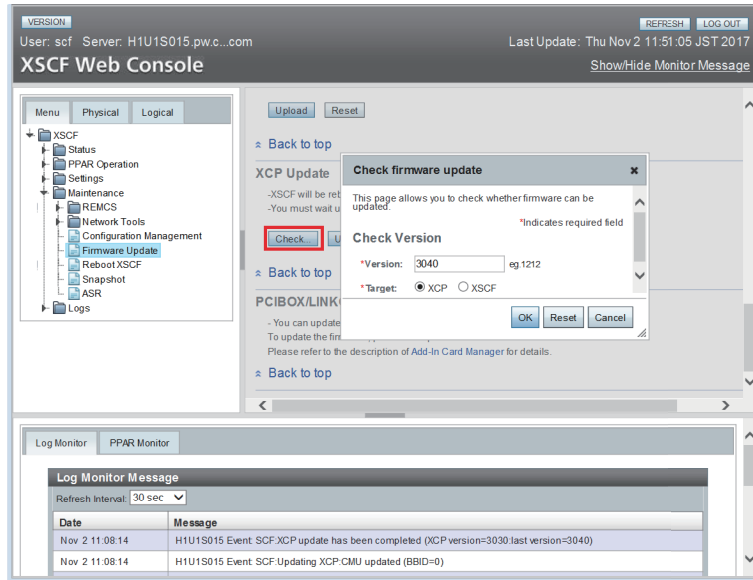


7. Vérifier l'écran [XCP Update] indiqué dans Figure 16-6 pour voir si le fichier

image XCP importé peut être utilisé pour mettre à jour le microprogramme.

Cliquez sur le bouton [Check] et indiquez la version du microprogramme dans la fenêtre de dialogue pour lancer la vérification du fichier. Si « The XCP file has been checked successfully » apparaît, le fichier peut être utilisé pour la mise à jour du microprogramme.

Figure 16-6 Vérification du fichier image XCP depuis l'écran [XCP Update]

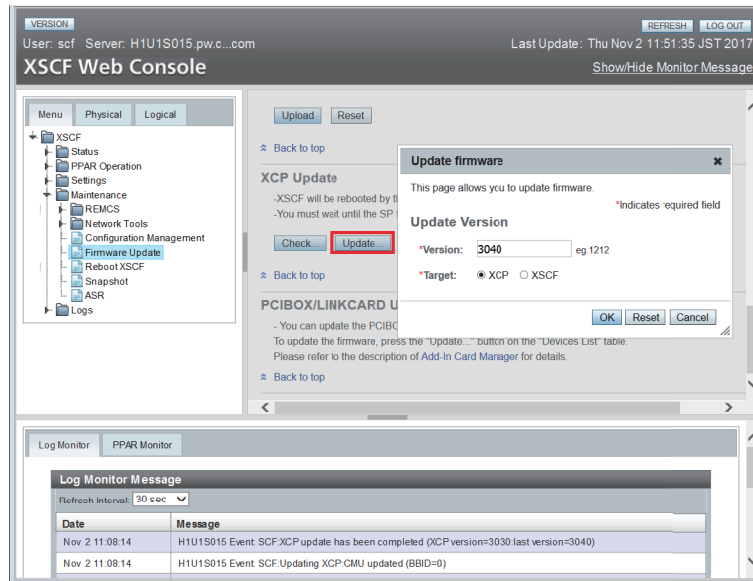


8. **Mettez à jour le microprogramme depuis l'écran [XCP Update] indiqué dans Figure 16-7.**

Cliquez sur le bouton [Update] et indiquez la version du microprogramme dans la fenêtre de dialogue pour lancer la mise à jour du microprogramme. La mise à jour prend environ 30 minutes.

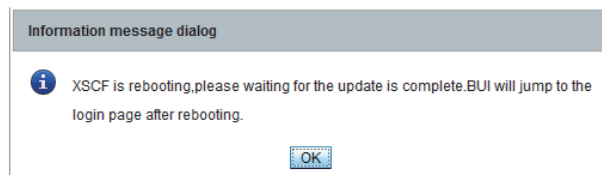
Remarque : dans une configuration de bloc de construction, la mise à jour prend environ 60 minutes.

Figure 16-7 Mise à jour du microprogramme depuis l'écran [XCP Update]



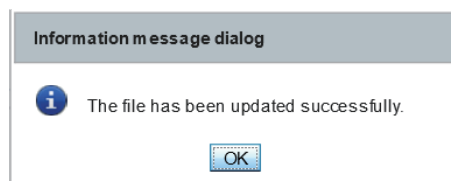
Pendant la mise à jour, le XSCF est réinitialisé, et la session XSCF est déconnectée. Le message indiqué dans Figure 16-8 est généré.

Figure 16-8 Message de redémarrage de XSCF



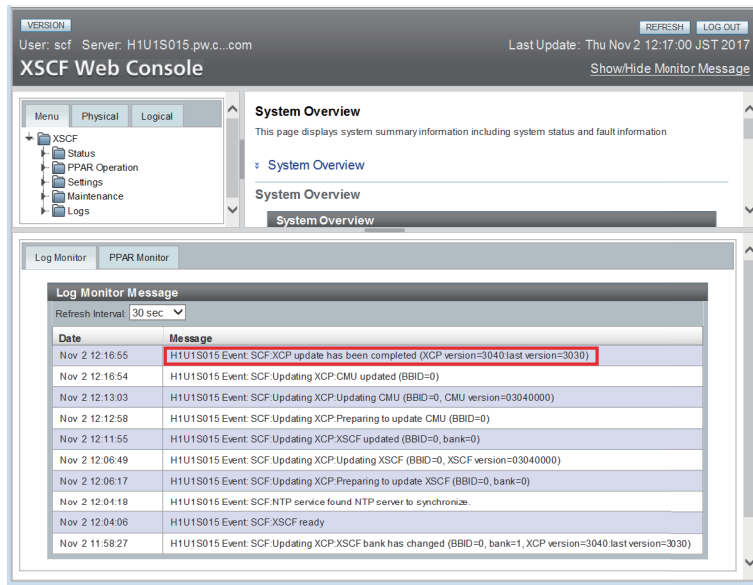
Le message « The file has been updated successfully » indiqué dans Figure 16-9 apparaît également pendant la mise à jour. À ce niveau, la mise à jour du microprogramme n'est pas encore terminée.

Figure 16-9 Message pendant la mise à jour



9. **Connectez-vous à nouveau à XSCF Web.**
10. **Vérifiez le message de mise à jour du microprogramme sur l'écran [Log Monitor Message] dans le cadre inférieur de la fenêtre montrée dans Figure 16-10.**

Figure 16-10 Écran [Log Monitor Message]



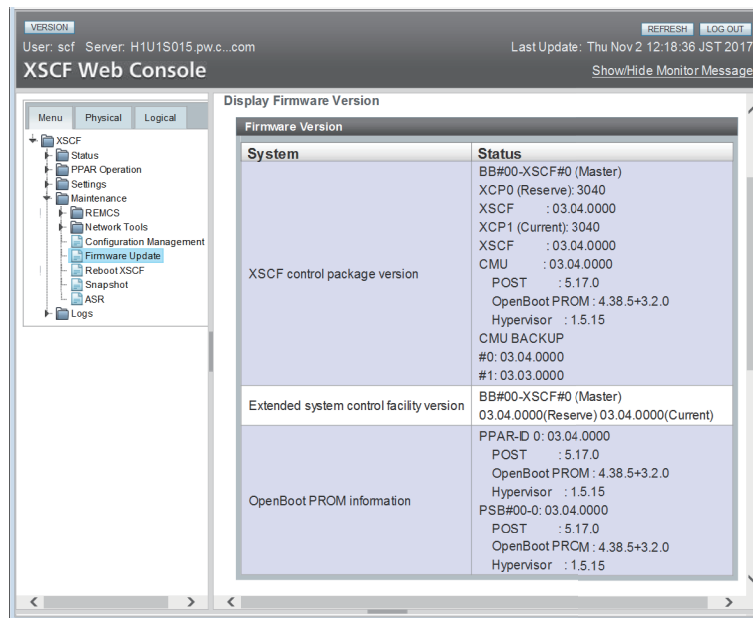
Si le message « XCP update has been completed » apparaît, la mise à jour du microprogramme XCP est terminée.

Remarque : un message similaire à « XSCF update has been completed » ou « CMU update has been completed » apparaîtra sur le SPARC M10. Cependant, la mise à jour de tout le microprogramme XCP ne pourra être terminée une fois le message apparu. Pour mettre à jour le microprogramme en toute sécurité, n'effectuez pas d'opérations d'alimentation pour les partitions physiques jusqu'à ce que vous ayez confirmé le message de mise à jour terminée « XCP update has been completed » pour le microprogramme XCP.

- La partition physique est sous tension : le microprogramme CMU cible n'a pas encore été mis à jour à ce stade. Par conséquent, le message n'apparaît pas pour le microprogramme CMU. Pour effectuer la mise à jour du microprogramme CMU une fois la mise à jour du microprogramme XCP terminée, mettez hors et sous tension la partition physique.
- Dans une configuration de bloc de construction : immédiatement après la mise à jour du microprogramme XCP, les états du XSCF maître et du XSCF de veille dans une configuration de bloc de construction sont inversés par rapport à leurs états précédant la mise à jour. Le XSCF maître et le XSCF de veille sont permutés afin de revenir à leur état d'origine. La permutation automatique prend environ 10 minutes.

11. Vérifiez que la version du microprogramme est à jour dans l'écran [Display Firmware Version] indiqué dans Figure 16-11.

Figure 16-11 Écran [Display Firmware Version]



16.7 Correspondance de la version du microprogramme avec le remplacement d'éléments

Des éléments sont remplacés et les versions du microprogramme sont adaptées comme décrit dans les cas suivants.

- La version du microprogramme est mise en correspondance quand l'unité XSCF du SPARC M12-2S ou l'unité de mémoire de processeur (inférieure) du SPARC M10-4S a été ajoutée/remplacée en utilisant le menu de maintenance.
- La version du microprogramme du XSCF est mise en correspondance quand l'unité XSCF d'un boîtier à barre transversale a été ajoutée/remplacée en utilisant le menu de maintenance.

Remarque : après le remplacement des unités de carte mère des systèmes SPARC M12-1/M10-1, des unités de mémoire de processeur (inférieures) du système SPARC M10-4 et de tous les systèmes SPARC M10-4S, des unités XSCF du SPARC M12-2 et de tous les systèmes SPARC M12-2S et des unités XSCF de tous les boîtiers à barre transversale, la mise en correspondance automatique de version vers la version de microprogramme de pré-remplacement n'est pas possible. Demandez à l'opérateur de mettre à jour le microprogramme.

Remarque : pour des informations complémentaires sur la mise en correspondance automatique des versions lors du remplacement de l'unité de mémoire (inférieure) (CMUL), du remplacement de l'unité XSCF, de l'ajout du SPARC M10-4S ou de l'ajout du boîtier à barre transversale sans utiliser le menu de maintenance et avec l'alimentation mise hors tension, consultez les *Notes de produit des systèmes Fujitsu M10/SPARC M10* pour la dernière version XCP.

16.7.1 Correspondance de la version du microprogramme pour l'ajout/remplacement avec l'alimentation sous tension

Cette section explique comment mettre en correspondance la version lors du remplacement des unités de mémoire de processeur (inférieures) (CMUL), du remplacement des unités XSCF, de l'ajout du SPARC M12-2S/M10-4S ou de l'ajout d'un boîtier à barre transversale avec l'alimentation sous tension.

1. **Après avoir exécuté la commande `addfru` ou `replacefru`, si la tâche d'ajout/de remplacement est effectuée en utilisant le menu de maintenance, la version du microprogramme du XSCF est mise automatiquement en correspondance.**
Si les commandes `addfru`, `replacefru` ou `testsb` effectuent un test de diagnostic, la version du microprogramme CMU est mise automatiquement en correspondance.
2. **Après la finalisation de la commande `addfru`, `replacefru` ou `testsb`, exécutez la commande `version` pour vérifier la version du microprogramme XCP.**

```
XSCF> version -c xcp -v
BB#00-XSCF#0 (Master)
XCP0 (Reserve): 2044
CMU          : 02.04.0004
  POST       : 1.43.0
  OpenBoot PROM : 4.34.0+1.19.0
  Hypervisor   : 0.27.3
XSCF         : 02.04.0004
XCP1 (Current): 2044
CMU          : 02.04.0004
  POST       : 1.43.0
  OpenBoot PROM : 4.34.0+1.19.0
  Hypervisor   : 0.27.3
XSCF         : 02.04.0004
BB#01-XSCF#0 (Standby)
XCP0 (Reserve): 2044
CMU          : 02.04.0004
  POST       : 1.43.0
  OpenBoot PROM : 4.34.0+1.19.0
  Hypervisor   : 0.27.3
XSCF         : 02.04.0004
XCP1 (Current): 2044
CMU          : 02.04.0004
  POST       : 1.43.0
  OpenBoot PROM : 4.34.0+1.19.0
```

```
Hypervisor      : 0.27.3
XSCF            : 02.04.0004
CMU BACKUP
#0: 02.04.0001
#1: ..
```

16.7.2 Correspondance de la version du microprogramme pour l'ajout/remplacement avec l'alimentation hors tension

Cette section explique comment mettre en correspondance la version lors du remplacement des unités de mémoire de processeur (inférieures) (CMUL), du remplacement des unités XSCF, de l'ajout du SPARC M12-2S/M10-4S ou de l'ajout d'un boîtier à barre transversale avec l'alimentation hors tension.

1. **Après avoir remplacé les unités de mémoire de processeur (inférieures) (CMUL), remplacé les unités XSCF, ajouté le SPARC M10-4S ou ajouté le boîtier à barre transversale, connectez-vous au XSCF et exécutez la commande version pour vérifier la version du microprogramme XCP.**

Remarque : après la connexion, si le message « XSCF firmware update now in progress. BB#xx, please wait for XSCF firmware update complete. » est affiché, la mise en correspondance de la version du microprogramme XCP est exécutée automatiquement. Avant de démarrer la tâche suivante, exécutez la commande showlogs monitor et confirmez que le message « XCP firmware version synchronization completed » s'affiche.

L'exemple suivant montre qu'après une tâche d'ajout/remplacement effectuée sans utiliser le menu de maintenance, la version du microprogramme de BB#01 ne correspond pas.

```
XSCF> version -c xcp -v
BB#00-XSCF#0 (Master)
XCP0 (Reserve): 2044
CMU          : 02.04.0004
  POST       : 1.43.0
  OpenBoot PROM : 4.34.0+1.19.0
  Hypervisor   : 0.27.3
XSCF        : 02.04.0004
XCP1 (Current): 2044
CMU          : 02.04.0004
  POST       : 1.43.0
  OpenBoot PROM : 4.34.0+1.19.0
  Hypervisor   : 0.27.3
XSCF        : 02.04.0004
BB#01-XSCF#0 (Standby)
XCP0 (Reserve): 2041
CMU          : 02.04.0001
  POST       : 1.42.0
```

```

OpenBoot PROM : 4.34.0+1.16.0
Hypervisor    : 0.26.9
XSCF          : 02.04.0001
XCP1 (Current): 2041
CMU           : 02.04.0001
POST          : 1.42.0
OpenBoot PROM : 4.34.0+1.16.0
Hypervisor    : 0.26.9
XSCF          : 02.04.0001
CMU BACKUP
#0: 02.04.0001
#1: ..

```

Remarque : après une tâche d'ajout/remplacement en utilisant le menu de maintenance, les versions des microprogrammes correspondent sur les unités XSCF de tous les systèmes SPARC M12-2S/M10-4S et de tous les boîtiers à barre transversale.

2. **Si une version de microprogramme ne correspond pas, exécutez la commande `flashupdate -c sync` pour la mettre en correspondance avec la version du microprogramme du XSCF maître.**

```

XSCF> flashupdate -c sync
XCP update is started. [3600sec]
  0..... 30..... 60..... 90.....120.....150.....180.....210.....240.....-
270.....300.....330.....360.....390.....420.....450.....480.....510.....|
540.....570.....600.....630.....660.....690.....720.....750.....780.....-
810.....840.....870.....900.....930.....960.....990.....1020.....1050.....\
1080.....1110.....1140.....1170.....1200.....1230.....1260.....1290.....
1320...../
1350.....1380.....1410.....1440.....1470.....1500.....1530.....1560.....15
90.....\
1620.....1650.....1680.....1710.....1740.....1770.....1800.....1830.....
1860...../
1890.....1920.....1950.....1980.....2010.....2040.....2070.....2100.....
2130.....\
2160.....2190..XSCF>
XSCF>

```

3. **Exécutez la commande `version` et vérifiez que la version du microprogramme XCP correspond à la version du microprogramme XSCF.**

```

XSCF> version -c xcp -v
BB#00-XSCF#0 (Master)
XCP0 (Reserve): 2044
CMU           : 02.04.0004
POST          : 1.43.0
OpenBoot PROM : 4.34.0+1.19.0
Hypervisor    : 0.27.3
XSCF          : 02.04.0004
XCP1 (Current): 2044

```

```

CMU          : 02.04.0004
  POST       : 1.43.0
  OpenBoot PROM : 4.34.0+1.19.0
  Hypervisor  : 0.27.3
XSCF        : 02.04.0004
BB#01-XSCF#0 (Standby)
XCP0 (Reserve): 2044
CMU          : 02.04.0001
  POST       : 1.42.0
  OpenBoot PROM : 4.34.0+1.16.0
  Hypervisor  : 0.26.9
XSCF        : 02.04.0004
XCP1 (Current): 2044
CMU          : 02.04.0001
  POST       : 1.42.0
  OpenBoot PROM : 4.34.0+1.16.0
  Hypervisor  : 0.26.9
XSCF        : 02.04.0004
CMU BACKUP
#0: 02.04.0001
#1: ..

```

Le microprogramme CMU cible n'est pas mis à jour à ce stade.

4. **Mettez sous tension la partition physique cible afin que la version du microprogramme CMU corresponde.**

Exécutez la commande `poweron` pour mettre la partition physique sous tension.

```
XSCF> poweron -p xx
```

Exécutez la commande `showpparstatus` et confirmez que l'état de PPAR est « Running ».

```

XSCF> showpparstatus -p xx
PPAR-ID      PPAR Status
XX           Running

```

5. **Exécutez la commande `version` pour vérifier la version du microprogramme CMU de la partition physique cible.**

```

XSCF> version -c xcp -v
BB#00-XSCF#0 (Master)
XCP0 (Reserve): 2044
CMU          : 02.04.0004
  POST       : 1.43.0
  OpenBoot PROM : 4.34.0+1.19.0
  Hypervisor  : 0.27.3
XSCF        : 02.04.0004
XCP1 (Current): 2044
CMU          : 02.04.0004
  POST       : 1.43.0

```

```

OpenBoot PROM : 4.34.0+1.19.0
Hypervisor    : 0.27.3
XSCF          : 02.04.0004
BB#01-XSCF#0 (Standby)
XCP0 (Reserve): 2044
CMU           : 02.04.0004
  POST        : 1.43.0
  OpenBoot PROM : 4.34.0+1.19.0
  Hypervisor   : 0.27.3
XSCF          : 02.04.0004
XCP1 (Current): 2044
CMU           : 02.04.0004
  POST        : 1.43.0
  OpenBoot PROM : 4.34.0+1.19.0
  Hypervisor   : 0.27.3
XSCF          : 02.04.0004
CMU BACKUP
#0: 02.04.0001
#1: ..

```

16.8 Problème lors de la mise à jour du microprogramme

Si un arrêt anormal se produit ou si un message d'erreur tel que le suivant est émis pendant la mise à jour du microprogramme, l'unité XSCF anormale ne peut pas être utilisée et est traitée comme un élément en panne :

- Dans les systèmes avec un XSCF
Erreur liée à un échec d'écriture ou de redémarrage
- Dans les systèmes avec plusieurs XSCF
Erreur liée à un échec d'écriture ou de redémarrage sur le XSCF de veille ou le XSCF maître

Toutefois, si une panne se produit pendant la mise à jour du microprogramme, essayez de mettre à jour le microprogramme à nouveau. La mise à jour du microprogramme peut se terminer normalement lors de la seconde tentative.

16.9 FAQ concernant la mise à jour du microprogramme

Q : Peut-on redémarrer deux fois lors de la mise à jour du microprogramme CMU ?

R : Cela ne poserait pas de problème.

Q : Dans les systèmes avec plusieurs XSCF, pourquoi les XSCF maître et de veille sont-ils permutés pendant une mise à jour ?

R : Le XSCF maître exerce le contrôle pour appliquer la mise à jour du microprogramme au XSCF de veille. À la finalisation de la mise à jour du microprogramme sur l'élément de veille, l'élément de veille a un nouveau microprogramme. L'élément de veille est permuté avec l'élément maître pour appliquer à nouveau la mise à jour du microprogramme au XSCF côté veille (ancien côté maître).

Q : Le microprogramme CMU peut-il être mis à jour sur toutes les partitions physiques en une fois ?

R : Oui. Si toutes les partitions physiques sont hors tension, le microprogramme peut être mis à jour en une fois. Si une partition physique est sous tension, vous pouvez la mettre à jour avec le nouveau microprogramme en exécutant la commande poweroff -a puis la commande poweron -a avec toutes les partitions physiques spécifiées.

Mise à jour d'Oracle Solaris et d'Oracle VM Server pour SPARC

Ce chapitre décrit comment mettre à jour Oracle Solaris installé sur un domaine logique.

Oracle Solaris est déjà installé sur tous les domaines logiques configurés pour une partition physique. Vous pouvez mettre à jour Oracle Solaris individuellement sur chaque domaine logique.

Avant la mise à jour

Avant de mettre Oracle Solaris à jour sur le domaine de commande, sauvegardez les données répertoriées ci-dessous à l'avance. Restaurez les données après la mise à jour.

- Répertoires de configuration de la sauvegarde automatique
`/var/opt/SUNWldm/autosave-*`
- Fichiers de base de données des contraintes des domaines logiques
`/var/opt/SUNWldm/ldom-db.xml` fournit une référence aux fichiers de base de données des contraintes des domaines logiques.

Pour plus d'informations, consultez « Installing and Enabling Software » dans le *Oracle VM Server for SPARC Administration Guide* de la version utilisée.

Mise à jour

Utilisez la dernière SRU (mise à jour du référentiel support) lors de la mise à jour d'Oracle Solaris.

Pour connaître les versions prises en charge d'Oracle Solaris et les dernières informations sur les SRU, consultez les dernières *Notes de produit* pour votre serveur.

Pour plus de détails sur la mise à jour d'Oracle Solaris et d'Oracle VM Server pour SPARC, consultez les manuels d'Oracle Solaris et « Installing and Enabling Software » dans le *Oracle VM Server for SPARC Administration Guide* de la version utilisée.

Dépannage

Ce chapitre traite des problèmes pouvant survenir lors de l'utilisation du XSCF ou pendant le fonctionnement du système et des solutions à y apporter.

- [Dépannage du XSCF](#)
- [Précautions relatives à l'utilisation du commutateur RESET](#)
- [Foire aux questions/FAQ](#)
- [Dépannage du système avec le XSCF](#)

18.1 Dépannage du XSCF

Cette section traite des problèmes pouvant survenir lors de l'utilisation du XSCF et des solutions à y apporter.

Impossibilité de se connecter au XSCF

- Vérifiez si le nom d'utilisateur saisi pour se connecter est correct.
- Vérifiez si le mot de passe utilisé est correct.
- Vérifiez le nombre d'utilisateurs connectés au XSCF au même moment. Pour plus de détails sur le nombre d'utilisateurs, consultez « [2.6 Nombre d'utilisateurs pouvant se connecter](#) ».

Mot de passe d'identification au XSCF oublié

- Demandez à l'administrateur système la réinitialisation du mot de passe. Un administrateur système disposant du privilège d'utilisateur platadm ou useradm peut réinitialiser le mot de passe à l'aide de la commande password.
- Si l'administrateur système oublie le mot de passe d'identification, connectez-vous à l'aide du compte « default », puis réinitialisez le mot de passe à l'aide de la commande password. Pour plus de détails sur l'authentification avec le compte par « défaut », consultez « Réalisation d'un diagnostic initial du système » dans le *Guide d'installation* de votre serveur.

Impossibilité de se connecter au XSCF via le port série

- Vérifiez si le logiciel du terminal est connecté au port série.
- Vérifiez les paramètres du logiciel du terminal. (débit en bauds de 9 600 b/s, retard d'une valeur autre que 0, etc.). Pour plus de détails sur ces paramètres, consultez « [2.2.1 Comment se connecter au shell XSCF avec une connexion série](#) ».

Remarque : si la connexion au XSCF échoue même après que vous avez effectué les opérations mentionnées ci-dessus, le problème peut être résolu en appuyant sur le commutateur RESET placé sur le panneau arrière. Pour plus de détails, consultez « [18.2 Précautions relatives à l'utilisation du commutateur RESET](#) ».

Impossibilité de se connecter au XSCF via le XSCF-LAN en utilisant Telnet

- Vérifiez que le câble LAN est correctement connecté entre le terminal du shell XSCF et le serveur.
- Vérifiez si le logiciel du terminal est connecté au port Telnet.
- Utilisez la commande `shownetwork` pour vérifier si XSCF-LAN est activé.
- Utilisez la commande `showtelnet` pour vérifier si le service Telnet est activé.
- Vérifiez que l'adresse IP et le numéro de port saisis correspondent aux paramètres.
- Vérifiez que le nombre de connexions utilisant Telnet/SSH n'excède pas le nombre maximal. Pour plus de détails sur ce nombre maximal, consultez « [2.6 Nombre d'utilisateurs pouvant se connecter](#) ».
- Si nécessaire, utilisez la console de l'ordinateur qui est directement connecté au XSCF via le port série pour vous connecter au shell XSCF et vérifiez les paramètres de XSCF-LAN à l'aide de la commande `shownetwork`.

Remarque : si la connexion au XSCF échoue même après que vous avez effectué les opérations mentionnées ci-dessus, le problème peut être résolu en appuyant sur le commutateur RESET placé sur le panneau arrière. Pour plus de détails, consultez « [18.2 Précautions relatives à l'utilisation du commutateur RESET](#) ».

Impossibilité de se connecter au XSCF via le XSCF-LAN en utilisant SSH

- Vérifiez que le câble LAN est correctement connecté entre le terminal du shell XSCF et le serveur.
- Exécutez la commande `shownetwork` pour vérifier si XSCF-LAN est activé.
- Exécutez la commande `showssh` pour vérifier si le service SSH est activé.
- Vérifiez que l'adresse IP et le numéro de port saisis correspondent aux paramètres.
- Vérifiez que le nombre de connexions utilisant Telnet/SSH n'excède pas le nombre maximal. Pour plus de détails sur ce nombre maximal, consultez « [2.6 Nombre d'utilisateurs pouvant se connecter](#) ».

- Si nécessaire, utilisez la console de l'ordinateur qui est directement connecté au XSCF via le port série pour vous connecter au shell XSCF et vérifiez les paramètres de XSCF-LAN à l'aide de la commande `shownetwork`.
- Vérifiez si la clé d'hôte est correctement paramétrée. Prenez note du fait que le remplacement d'une unité XSCF fait revenir la clé d'hôte à sa valeur prédéfinie sur le XSCF.
- Vérifiez si le logiciel client est correctement paramétré.

Remarque : si la connexion au XSCF échoue même après que vous avez effectué les opérations mentionnées ci-dessus, le problème peut être résolu en appuyant sur le commutateur RESET placé sur le panneau arrière. Pour plus de détails, consultez « [18.2 Précautions relatives à l'utilisation du commutateur RESET](#) ».

Adresse IP du XSCF inconnue

- Utilisez la commande `shownetwork` pour vérifier la configuration actuelle du réseau. Si l'adresse n'a pas été définie, contactez l'administrateur réseau pour vérifier les paramètres.
- Si nécessaire, utilisez la console de l'ordinateur qui est directement connecté au XSCF via le port série pour vous connecter au shell XSCF et vérifiez les paramètres de XSCF-LAN à l'aide de la commande `shownetwork`.

Le terminal du shell XSCF ou la console du domaine a été déconnecté brusquement

- Après que les commandes `setnetwork`, `setroute`, `sethostname`, `setnameserver` et `setsscp` relatives au réseau XSCF ont été utilisées par un autre utilisateur, il se peut que les commandes `applynetwork` et `rebootxscf` aient été exécutées. La commande `flashupdate` peut également avoir été utilisée. Pour utiliser le XSCF, établissez une autre connexion et connectez-vous de nouveau.
- Il se peut qu'un autre utilisateur ait exécuté la commande `setdate` ou `switchscf`. Pour utiliser le XSCF, établissez une autre connexion et connectez-vous de nouveau.
- Si le shell XSCF n'est pas utilisé pendant une durée définie après l'identification, il est automatiquement arrêté par le XSCF. Cet arrêt forcé se produit à l'issue de la durée définie uniquement si la fonction de surveillance du temps est activée et qu'une durée est définie pour cette fonction dans les paramètres du XSCF.
- Le shell sécurisé d'Oracle Solaris ou le client SSH d'OpenSSH sont déconnectés lorsque sont saisis le caractère d'échappement (exemple : « # ») défini par le client et la touche « . » (point). Si les paramètres du caractère d'échappement du shell sécurisé d'Oracle Solaris ou du client SSH d'OpenSSH et le caractère d'échappement défini à l'aide de la commande console sont les mêmes, le terminal est déconnecté. Il est donc nécessaire de modifier la valeur de l'un de ces paramètres. Pour plus de détails, consultez le manuel du client SSH.

Impossibilité de mettre le serveur sous/hors tension

- Lors du fonctionnement avec un privilège d'utilisateur autre que `platadm` ou

fieldeng, les opérations de mise sous/hors tension du système complet ne sont pas disponibles. Pour des informations plus détaillées sur les privilèges d'utilisateur, consultez « [3.5.3 Types de privilège d'utilisateur](#) ».

Impossibilité d'ajouter un utilisateur XSCF

- Vérifiez le nombre d'utilisateurs XSCF enregistrés. Pour des informations plus détaillées sur le nombre d'utilisateurs enregistrés, consultez « [2.6 Nombre d'utilisateurs pouvant se connecter](#) ». Sinon, contactez l'administrateur système.

Aucune notification par e-mail en provenance du XSCF

- Le XSCF ne communique pas nécessairement tous les événements. Il envoie un e-mail pour chaque panne de composant ou événement d'erreur d'authentification. Consultez « [12.1 Consultation d'un journal enregistré par le XSCF](#) » pour vérifier la notification souhaitée le journal d'erreur ou savoir s'il s'agit d'un événement d'un journal des événements faisant l'objet d'un rapport.
- Utilisez la commande `shownemailreport` pour vérifier si ce paramètre est activé. Si aucun e-mail n'a été reçu, vérifiez si un e-mail contenant un message d'erreur a été envoyé au destinataire prévu ou vérifiez le journal des erreurs enregistrées.
- Si un téléphone portable est utilisé pour recevoir les e-mails, vérifiez les paramètres du téléphone en cas de restriction sur la réception des messages.

Impossibilité d'accéder à la page supérieure de XSCF Web

- Utilisez la commande `showhttps` pour vérifier si XSCF-LAN est activé.
- Vérifiez si l'URL entrée est correcte. (Exemple : si le « s » de « https » est manquant)
- Vérifiez avec l'administrateur système les paramètres d'autorisation pour l'adresse IP.
- Vérifiez si le paramètre de connexion avec TLS 1.0 du navigateur web est activé.

Impossibilité d'afficher les fenêtres de XSCF Web

- Si les fenêtres de XSCF Web ne s'affichent pas même après une identification sur la page supérieure de XSCF Web, JavaScript peut être désactivé dans les paramètres du navigateur web. Activez JavaScript dans les paramètres du navigateur et connectez-vous de nouveau.
- Si l'affichage des fenêtres contextuelles est désactivé dans les paramètres du navigateur web, les fenêtres de XSCF Web ne peuvent pas s'afficher. Vérifiez les paramètres du navigateur.

Mot de passe de XSCF Web oublié

- L'authentification à XSCF Web est la même que pour le Shell XSCF. Consultez « [Mot de passe d'identification au XSCF oublié](#) » ci-dessus.

Échec de la première tentative d'accès à XSCF Web après l'identification

- Vérifiez si les cookies sont autorisés dans les paramètres du navigateur web.

XSCF Web ne s'affiche pas correctement dans la fenêtre du navigateur

- Certaines versions de navigateur n'affichent pas les fenêtre XSCF correctement. Consultez « [2.4 Connexion à XSCF Web](#) » pour connaître les navigateurs pris en charge et mettre votre navigateur à jour avec la dernière version.

Message d'avertissement affiché sur XSCF Web

- Vérifiez le contenu du message d'avertissement sur la sécurité puis arrêtez d'utiliser XSCF Web. Prenez les mesures appropriées en fonction du contenu du message d'avertissement vérifié. Si le délai d'expiration est écoulé, reconfigurez le service HTTPS du XSCF. Pour des informations plus détaillées sur les paramètres du service HTTPS, consultez « [3.8 Configuration du service HTTPS pour la connexion à XSCF](#) ».

Autres problèmes

- Prenez contact avec l'administrateur système. S'il est nécessaire de recueillir/sauvegarder un journal XSCF, utilisez les commandes du shell XSCF pour le sauvegarder. Pour plus de détails concernant la façon de sauvegarder un journal, consultez « [12.1.15 Sauvegarde d'un journal dans un fichier avec snapshot](#) ».

18.2 Précautions relatives à l'utilisation du commutateur RESET

Le commutateur RESET est un commutateur d'urgence, situé sur le panneau arrière du SPARC M12/M10 et du boîtier à barre transversale, permettant de redémarrer le XSCF.

Utilisez le commutateur RESET comme une mesure d'urgence lorsque le XSCF ne démarre pas et qu'aucun accès au XSCF n'est possible après avoir appliqué les mesures décrites dans cette section.

Lorsque vous utilisez le commutateur RESET, prenez note des points suivants.

- N'utilisez le commutateur RESET qu'en dernier ressort pour démarrer le XSCF.
- Si le XSCF ne démarre pas même après avoir actionné le commutateur RESET, contactez un technicien de maintenance.
- N'appuyez pas sur le commutateur RESET à plusieurs reprises lorsque le XSCF est en cours de fonctionnement. Si vous appuyez de manière répétée sur le commutateur RESET, la DEL DE CONTRÔLE continue d'être allumée et la DEL PRÊT du XSCF s'éteint. Ensuite, le XSCF s'arrête. Si cela se produit, vous devez désactiver puis activer l'alimentation en entrée pour vous connecter au XSCF.

Pour connaître l'emplacement du commutateur RESET, consultez le *Service Manual* pour votre serveur ou « Annexe C External Interface Specifications » dans le *Crossbar Box for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Service Manual*.

18.3 Foire aux questions/FAQ

Cette section contient des questions fréquemment posées sur l'utilisation de XSCF.

Q : Les adresses IP utilisées avec le XSCF-LAN sont-elles attribuées par défaut aux ports LAN ?

R : Aucune adresse IP n'est attribuée par défaut à XSCF-LAN. Pour plus de détails sur les adresses IP de XSCF-LAN, consultez « [3.9.2 Compréhension des interfaces du réseau XSCF](#) ».

Q : Une adresse IP par défaut est-elle attribuée à SSCP ?

R : Une adresse IP lui est attribuée par défaut. Pour plus d'informations sur l'adresse IP par défaut de SSCP, consultez « [3.9.5 Compréhension des adresses IP définies avec SSCP](#) ». Si l'adresse IP par défaut risque d'affecter l'environnement du LAN de l'utilisateur, modifiez-la.

Q : Si une interruption d'Oracle Solaris survient lors d'un démarrage d'Oracle Solaris après la mise sous tension du serveur, est-il possible de mettre le serveur hors tension depuis le XSCF ?

R : Si un domaine invité s'interrompt, utilisez la commande `ldm panic-domain` pour recueillir le fichier dump d'Oracle Solaris. Pour plus de détails sur la commande `ldm`, consultez le *Oracle VM Server for SPARC Reference Manual* de la version utilisée.

En cas d'interruption d'un domaine de commande, effectuez les étapes suivantes.

1. **Exécutez la commande `reset` en indiquant l'option `panic` sur le shell XSCF pour ordonner le vidage d'Oracle Solaris.**
2. **Si, même après l'étape 1., le vidage d'Oracle Solaris échoue, exécutez la commande `poweroff` sur le shell XSCF pour le mettre hors tension.**

Q : Quel traitement est effectué par XSCF après la mise sous tension du serveur jusqu'au démarrage d'Oracle Solaris ?

R : Les processus intervenant avant le démarrage du système sont les suivants. Pour plus de détails, consultez « [Chapitre 6 Démarrage/Arrêt du système](#) ».

1. **L'opérateur active l'alimentation.**
2. **Le XSCF démarre.**
3. **L'opérateur active l'alimentation du serveur.**
4. **Le XSCF initialise le matériel.**
5. **POST démarre et effectue un diagnostic initial du matériel.**
6. **OpenBoot PROM démarre.**
7. **OpenBoot PROM lance le processus de démarrage.**
8. **Oracle Solaris démarre.**

Q : Pendant une connexion ou une déconnexion de XSCF normale, quels types de messages s'affichent sur le terminal ?

R : Une réussite/échec de la connexion au XSCF est décrite ci-dessous.
L'exemple suivant indique une réussite de la connexion.

```
login: jsmith
Password: xxxxxxxx
XSCF>
```

L'exemple suivant indique un échec de la connexion.

```
login: jsmith
Password: xxxxxxxx
Login incorrect
```

R : Une réussite/échec de la déconnexion au XSCF est décrite ci-dessous.
L'exemple suivant indique une réussite de la déconnexion.

```
XSCF> exit
Logout
```

L'exemple suivant indique un échec de la déconnexion.

```
XSCF> exit
Not supported in this system.
```

Remarque : les exemples ci-dessus varient en fonction du logiciel client sur le terminal.

Q : Quel est le lien entre le journal d'erreur de XSCF et les informations sur les erreurs du fichier de définition de la MIB ?

R : Les informations sur les erreurs appliquées dans le fichier de définition de la MIB correspondent au journal d'erreur de XSCF le plus récent.

18.4 Dépannage du système avec le XSCF

Cette section décrit comment utiliser XSCF efficacement dans le cas où le serveur ne répond pas, ce qui signifie qu'un problème ou une panique est survenu dans le système.

Avant de contacter un technicien de maintenance

Avant de contacter le technicien sur site, suivez d'abord la procédure indiquée ci-dessous. Cette procédure peut non seulement être utile pour résoudre le problème,

mais peut également vous éviter de formuler une requête.

1. **Si le serveur ne répond pas, placez le commutateur de mode du panneau de commande en mode Service.**
2. **Vérifiez l'état du système en utilisant l'une des méthodes suivantes.**
 - Méthode lorsque le shell XSCF ne peut pas être utilisé via SSH/Telnet
 - a. Connectez un terminal au port série du XSCF.
 - b. Entrez votre compte d'utilisateur et votre mot de passe pour vous connecter au shell XSCF.
 - c. Utilisez le shell XSCF pour vérifier le journal d'erreur et d'autres informations.
 - Méthode lorsque le shell XSCF peut être utilisé via SSH/Telnet et le port en série
 - a. Connectez-vous au XSCF à l'aide de votre compte d'utilisateur XSCF.
 - b. Connectez le port XSCF-LAN et utilisez le shell XSCF pour vérifier le journal d'erreur ainsi que d'autres informations.

Pour plus de détails sur le journal d'erreur, consultez « [12.1 Consultation d'un journal enregistré par le XSCF](#) ». Vérifiez et effectuez l'action corrective correspondante.
 - c. Sinon, vérifiez le journal d'événement XSCF et l'état du serveur à l'aide du shell XSCF via le port série.

Utilisez les commandes suivantes pour vérifier les événements survenus lorsque le problème s'est produit :

```
showlogs error
showlogs event
showlogs power
showlogs monitor
showlogs console
```

Si vous constatez une erreur, consultez « [12.1 Consultation d'un journal enregistré par le XSCF](#) ». Vérifiez et effectuez l'action corrective correspondante.
 - d. Vérifiez le journal de la console XSCF ou le journal de panique pour les derniers messages.

Oracle Solaris peut avoir détecté un problème et affiché un message. En outre, dans les cas impliquant une panique, utilisez la commande showlogs avec l'option panic pour vérifier les événements survenus au moment de la panique.
3. **Si vous n'identifiez aucun problème après avoir vérifié les points ci-dessus, redémarrez le système.**
4. **En cas de panne, consultez « [12.1 Consultation d'un journal enregistré par le XSCF](#) ». Prenez des mesures conformément aux instructions de maintenance des commandes du shell XSCF pour remplacer un composant.**

Listes des chemins d'accès de périphériques des systèmes SPARC M12/M10

L'annexe décrit les chemins d'accès de périphériques des systèmes SPARC M12/M10.

- Chemins d'accès de périphériques SPARC M12-1
- Chemins d'accès de périphériques SPARC M12-2
- Chemins d'accès de périphériques SPARC M12-2S
- Chemins d'accès de périphériques SPARC M10-1
- Chemins d'accès de périphériques SPARC M10-4
- Chemins d'accès de périphériques SPARC M10-4S

A.1 Chemins d'accès de périphériques SPARC M12-1

Les chemins d'accès de périphériques reconnus par le SPARC M12-1 et le schéma fonctionnel du matériel correspondant aux chemins d'accès de périphériques sont comme suit.

Tableau A-1 Chemins d'accès au périphérique d'E/S du châssis du SPARC M12-1 et sur côté unité d'extension PCI

Priorité d'instance	Périphérique	Chemin d'accès de périphériques	Nombre dans schéma
1	LAN#0 interne	/pci@8000/pci@4/pci@0/pci@1/network@0	1
2	LAN#1 interne	/pci@8000/pci@4/pci@0/pci@1/network@0,1	2
3	SAS interne	/pci@8100/pci@4/pci@0/pci@0/scsi@0	3
-	HDD#0 interne	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p0	4
-	HDD#1 interne	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p1	5
-	HDD#2 interne	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p2	6
-	HDD#3 interne	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p3	7

Tableau A-1 Chemins d'accès au périphérique d'E/S du châssis du SPARC M12-1 et sur côté unité d'extension PCI (*suite*)

Priorité d'instance	Périphérique	Chemin d'accès de périphériques	Nombre dans schéma
-	HDD#4 interne	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p4	8
-	HDD#5 interne	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p5	9
-	HDD#6 interne	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p6	10
-	HDD#7 interne	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p7	11
-	SAS externe	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p5xx	12
4	Port USB interne (arrière : USB 3.0)	/pci@8100/pci@4/pci@0/pci@8/usb@0/hub@1/****@1	13
	Port USB interne (arrière : USB 2.0/1.1)	/pci@8100/pci@4/pci@0/pci@8/usb@0/hub@5/****@1	14
5	Port USB interne (avant : USB 2.0/1.1)	/pci@8100/pci@4/pci@0/pci@8/usb@0/****@6	15
6	Stockage à distance	/pci@8100/pci@4/pci@0/pci@8/usb@0/storage@7	16
7	PCI#0	/pci@8100/pci@4/pci@0/pci@9/****@0	17
	Unité d'extension PCI sous PCI#0		
8	PCI#1	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0	
9	PCI#2	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0	
10	PCI#3	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0	
11	PCI#4	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@0/****@0	
12	PCI#5	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@1/****@0	
13	PCI#6	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@10/****@0	
14	PCI#7	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@11/****@0	
15	PCI#8	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@0/****@0	
16	PCI#9	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@1/****@0	
17	PCI#10	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@10/****@0	
18	PCI#11	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@11/****@0	
19	LAN#2 interne	/pci@8200/pci@4/pci@0/pci@0/network@0	18

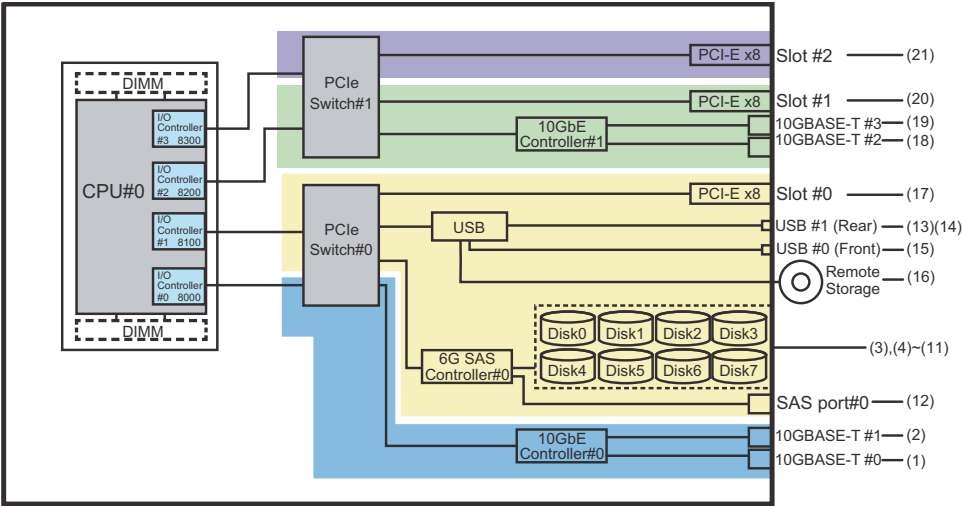
Tableau A-1 Chemins d'accès au périphérique d'E/S du châssis du SPARC M12-1 et sur côté unité d'extension PCI (*suite*)

Priorité d'instance	Périphérique	Chemin d'accès de périphériques	Nombre dans schéma
20	LAN#3 interne	/pci@8200/pci@4/pci@0/pci@0/network@0,1	19
21	PCI#1 Unité d'extension PCI sous PCI#1	/pci@8200/pci@4/pci@0/pci@8/****@0	20
22	PCI#1	/pci@8200/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@0/****@0	
23	PCI#2	/pci@8200/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@1/****@0	
24	PCI#3	/pci@8200/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@8/****@0	
25	PCI#4	/pci@8200/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@10/pci@0/pci@0/****@0	
26	PCI#5	/pci@8200/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@10/pci@0/pci@1/****@0	
27	PCI#6	/pci@8200/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@10/pci@0/pci@10/****@0	
28	PCI#7	/pci@8200/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@10/pci@0/pci@11/****@0	
29	PCI#8	/pci@8200/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@11/pci@0/pci@0/****@0	
30	PCI#9	/pci@8200/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@11/pci@0/pci@1/****@0	
31	PCI#10	/pci@8200/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@11/pci@0/pci@10/****@0	
32	PCI#11	/pci@8200/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@11/pci@0/pci@11/****@0	
33	PCI#2 Unité d'extension PCI sous PCI#2	/pci@8300/pci@4/pci@0/pci@1/****@0	21
34	PCI#1	/pci@8300/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@0/****@0	
35	PCI#2	/pci@8300/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@1/****@0	
36	PCI#3	/pci@8300/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@8/****@0	
37	PCI#4	/pci@8300/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@10/pci@0/pci@0/****@0	
38	PCI#5	/pci@8300/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@10/pci@0/pci@1/****@0	

Tableau A-1 Chemins d'accès au périphérique d'E/S du châssis du SPARC M12-1 et sur côté unité d'extension PCI (suite)

Priorité d'instance	Périphérique	Chemin d'accès de périphériques	Nombre dans schéma
39	PCI#6	/pci@8300/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@10/pci@0/pci@10/****@0	
40	PCI#7	/pci@8300/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@10/pci@0/pci@11/****@0	
41	PCI#8	/pci@8300/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@11/pci@0/pci@0/****@0	
42	PCI#9	/pci@8300/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@11/pci@0/pci@1/****@0	
43	PCI#10	/pci@8300/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@11/pci@0/pci@10/****@0	
44	PCI#11	/pci@8300/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/ pci@1/pci@0/pci@11/pci@0/pci@11/****@0	

Figure A-1 Schéma fonctionnel du SPARC M12-1



A.2 Chemins d'accès de périphériques SPARC M12-2

Les chemins d'accès de périphériques reconnus par le SPARC M12-2 et le schéma fonctionnel du matériel correspondant aux chemins d'accès de périphériques sont

comme suit.

A.2.1 Pour une configuration à 1 processeur au moment de l'installation initiale

Les chemins d'accès de périphériques pour une configuration à 1 processeur à l'installation initiale, ainsi que le schéma fonctionnel du matériel correspondant aux chemins d'accès de périphériques sont comme suit.

Remarque : si vous désactivez la reconfiguration de bus E/S (ioreconfigure) avec la commande setpparmode, les chemins d'accès de périphériques suivants s'appliquent également aux installations passant d'une configuration à 1 processeur à une configuration à 2 processeurs. Dans ce cas, vous n'avez pas besoin de reconfigurer les domaines logiques, réinstallez Oracle Solaris, puis configurez-le à nouveau.

Si vous activez la reconfiguration de bus E/S (ioreconfigure) et étendez une configuration à 1 processeur en configuration à 2 processeurs, les chemins d'accès de périphériques passent à ceux pour la configuration à 2 processeurs ([Tableau A-4](#)) lors de la réinitialisation de PPAR. À ce moment, le système passe en configuration d'usine par défaut. Dans ce cas, les domaines logiques doivent être reconfigurés.

De plus, il est possible que vous deviez réinstaller Oracle Solaris et le configurer à nouveau. Si vous souhaitez conserver la configuration de domaine logique, désactivez la reconfiguration de bus E/S et étendez la configuration.

Chemins d'accès de périphériques d'E/S du châssis du SPARC M12-2

Tableau A-2 Chemins d'accès de périphériques d'E/S du châssis du SPARC M12-2 (au moment de l'installation initiale : 1 processeur)

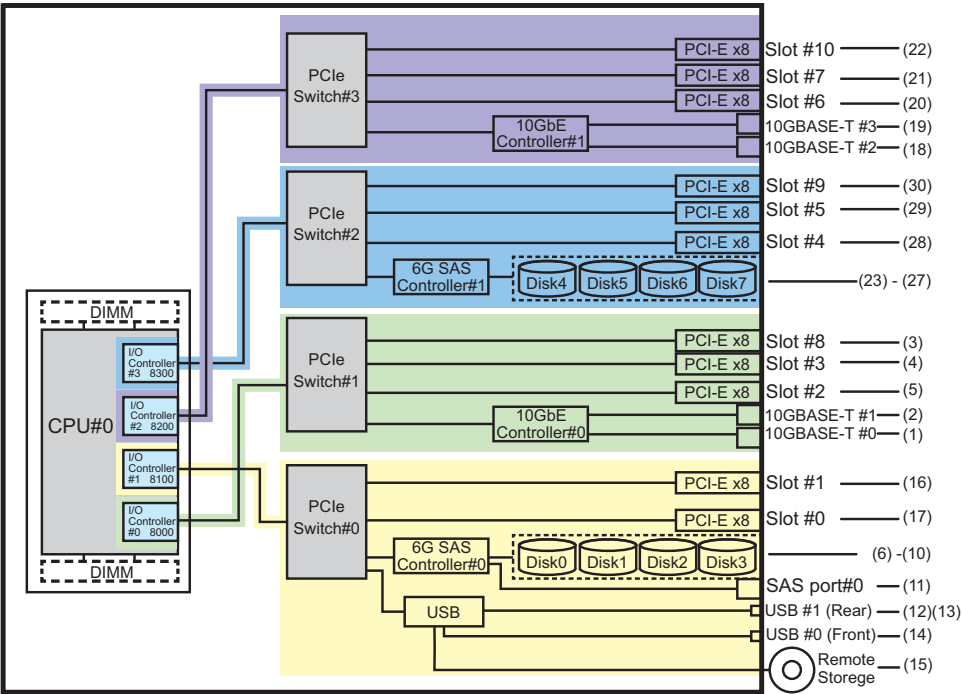
Instance Priorité	Périphérique	Chemin d'accès de périphériques	Nombre dans schéma
1	LAN#0 interne	/pci@8000/pci@4/pci@0/pci@0/network@0	1
2	LAN#1 interne	/pci@8000/pci@4/pci@0/pci@0/network@0,1	2
3	PCI#8	/pci@8000/pci@4/pci@0/pci@1/****@0	3
4	PCI#3	/pci@8000/pci@4/pci@0/pci@10/****@0	4
5	PCI#2	/pci@8000/pci@4/pci@0/pci@11/****@0	5
6	SAS#0 interne	/pci@8100/pci@4/pci@0/pci@0/scsi@0	6
-	HDD#0 interne	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p0	7
-	HDD#1 interne	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p1	8
-	HDD#2 interne	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p2	9
-	HDD#3 interne	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p3	10
-	SAS externe	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p5xx	11
7	Port USB interne (arrière : USB3.0)	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@1/****@1	12

Tableau A-2 Chemins d'accès de périphériques d'E/S du châssis du SPARC M12-2 (au moment de l'installation initiale : 1 processeur) *(suite)*

Instance Priorité	Périphérique	Chemin d'accès de périphériques	Nombre dans schéma
8	Port USB interne (arrière : USB2.0/1.1)	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@5/****@1	13
9	Port USB interne (avant : USB3.0/2.0/1.1) (*1)	/pci@8100/pci@4/pci@0/pci@1/usb@0/****@6	14
10	Stockage à distance	/pci@8100/pci@4/pci@0/pci@1/usb@0/storage@7	15
11	PCI#1	/pci@8100/pci@4/pci@0/pci@10/****@0	16
12	PCI#0	/pci@8100/pci@4/pci@0/pci@11/****@0	17
13	LAN#2 interne	/pci@8200/pci@4/pci@0/pci@0/network@0	18
14	LAN#3 interne	/pci@8200/pci@4/pci@0/pci@0/network@0,1	19
15	PCI#6	/pci@8200/pci@4/pci@0/pci@1/****@0	20
16	PCI#7	/pci@8200/pci@4/pci@0/pci@8/****@0	21
17	PCI#10	/pci@8200/pci@4/pci@0/pci@9/****@0	22
18	SAS#1 interne	/pci@8300/pci@4/pci@0/pci@0/scsi@0	23
-	HDD#4 interne	/pci@8300/pci@4/pci@0/pci@0/scsi@0/disk@p4	24
-	HDD#5 interne	/pci@8300/pci@4/pci@0/pci@0/scsi@0/disk@p5	25
-	HDD#6 interne	/pci@8300/pci@4/pci@0/pci@0/scsi@0/disk@p6	26
-	HDD#7 interne	/pci@8300/pci@4/pci@0/pci@0/scsi@0/disk@p7	27
19	PCI#4	/pci@8300/pci@4/pci@0/pci@1/****@0	28
20	PCI#5	/pci@8300/pci@4/pci@0/pci@8/****@0	29
21	PCI#9	/pci@8300/pci@4/pci@0/pci@9/****@0	30

*1 Si un périphérique USB3.0 est utilisé, il fonctionne comme un USB2.0.

Figure A-2 Schéma fonctionnel du SPARC M12-2 (1 processeur)



Chemins d'accès de périphériques d'E/S sur le côté de l'unité d'extension PCI

Si l'emplacement du serveur PCI possédant une carte de liaison connectée à l'unité d'extension PCI est PCI#X, les chemins d'accès de périphériques suivants sont créés avec le vvvv et le u correspondants indiqués dans le chemin d'accès de périphériques de PCI#X /pci/vvvvv/pci@4/pci@0/pci@u/****@0 dans [Tableau A-2](#).

Tableau A-3 Chemins d'accès de périphériques d'E/S sur le côté de l'unité d'extension PCI (1 processeur)

Priorité d'instance	Périphérique	Chemin d'accès de périphériques
Unité d'extension PCI sous PCI#X		
1	PCI#1	/pci/vvvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0
2	PCI#2	/pci/vvvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0
3	PCI#3	/pci/vvvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0
4	PCI#4	/pci/vvvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@0/****@0
5	PCI#5	/pci/vvvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@1/****@0
6	PCI#6	/pci/vvvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@10/****@0

Tableau A-3 Chemins d'accès de périphériques d'E/S sur le côté de l'unité d'extension PCI (1 processeur)
(suite)

Priorité d'instance	Périphérique	Chemin d'accès de périphériques
7	PCI#7	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@11/****@0
8	PCI#8	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@0/****@0
9	PCI#9	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@1/****@0
10	PCI#10	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@10/****@0
11	PCI#11	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@11/****@0

A.2.2 Pour une configuration à 2 processeurs au moment de l'installation initiale

Les chemins d'accès de périphériques pour une configuration à 2 processeurs à l'installation initiale, ainsi que le schéma fonctionnel du matériel correspondant aux chemins d'accès de périphériques sont comme suit.

Remarque : si vous désactivez la reconfiguration de bus E/S (ioreconfigure) avec la commande setpparmode, les chemins d'accès de périphériques suivants s'appliquent également aux retraits passant d'une configuration à 2 processeurs à une configuration à 1 processeur. Dans ce cas, vous n'avez pas besoin de reconfigurer les domaines logiques, réinstallez Oracle Solaris, puis configurez-le à nouveau.

Si vous activez la reconfiguration de bus E/S (ioreconfigure) et réduisez une configuration à 2 processeurs en configuration à 1 processeur, les chemins d'accès de périphériques passent à ceux pour la configuration à 1 processeur (Tableau A-2) lors de la réinitialisation de PPAR. À ce moment, le système passe en configuration d'usine par défaut. Dans ce cas, les domaines logiques doivent être reconfigurés.

De plus, il est possible que vous deviez réinstaller Oracle Solaris et le configurer à nouveau. Si vous souhaitez conserver la configuration de domaine logique, désactivez la reconfiguration de bus E/S et réduisez la configuration.

Chemins d'accès de périphériques d'E/S du châssis du SPARC M12-2

Tableau A-4 Chemins d'accès de périphériques d'E/S du châssis du SPARC M12-2 (au moment de l'installation initiale : 2 processeurs)

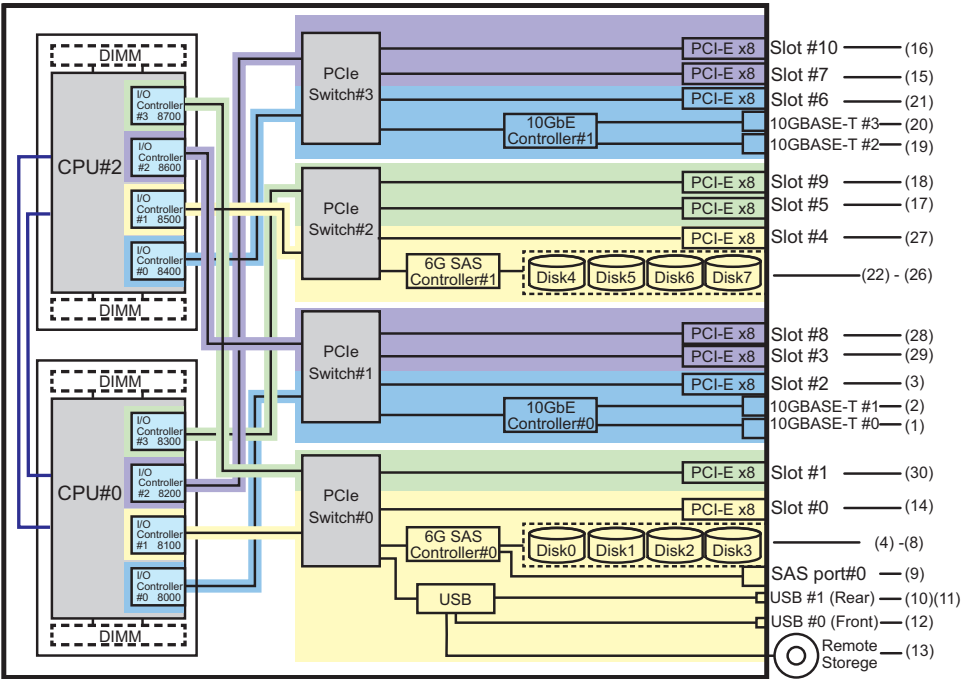
Instance Priorité	Périphérique	Chemin d'accès de périphériques	Nombre dans schéma
1	LAN#0 interne	/pci@8000/pci@4/pci@0/pci@0/network@0	1
2	LAN#1 interne	/pci@8000/pci@4/pci@0/pci@0/network@0,1	2
3	PCI#2	/pci@8000/pci@4/pci@0/pci@11/****@0	3
4	SAS#0 interne	/pci@8100/pci@4/pci@0/pci@0/scsi@0	4
-	HDD#0 interne	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p0	5
-	HDD#1 interne	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p1	6
-	HDD#2 interne	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p2	7
-	HDD#3 interne	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p3	8
-	SAS externe	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p5xx	9
5	Port USB interne (arrière : USB3.0)	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@1/****@1	10
6	Port USB interne (arrière : USB2.0/1.1)	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@5/****@1	11
7	Port USB interne (avant : 3.0/2.0/1.1) (*1)	/pci@8100/pci@4/pci@0/pci@1/usb@0/****@6	12
8	Stockage à distance	/pci@8100/pci@4/pci@0/pci@1/usb@0/storage@7	13
9	PCI#0	/pci@8100/pci@4/pci@0/pci@11/****@0	14
10	PCI#7	/pci@8200/pci@4/pci@0/pci@8/****@0	15
11	PCI#10	/pci@8200/pci@4/pci@0/pci@9/****@0	16
12	PCI#5	/pci@8300/pci@4/pci@0/pci@8/****@0	17
13	PCI#9	/pci@8300/pci@4/pci@0/pci@9/****@0	18
14	LAN#2 interne	/pci@8400/pci@4/pci@0/pci@0/network@0	19
15	LAN#3 interne	/pci@8400/pci@4/pci@0/pci@0/network@0,1	20
16	PCI#6	/pci@8400/pci@4/pci@0/pci@1/****@0	21
17	SAS#1 interne	/pci@8500/pci@4/pci@0/pci@0/scsi@0	22
-	HDD#4 interne	/pci@8500/pci@4/pci@0/pci@0/scsi@0/disk@p4	23
-	HDD#5 interne	/pci@8500/pci@4/pci@0/pci@0/scsi@0/disk@p5	24
-	HDD#6 interne	/pci@8500/pci@4/pci@0/pci@0/scsi@0/disk@p6	25
-	HDD#7 interne	/pci@8500/pci@4/pci@0/pci@0/scsi@0/disk@p7	26
18	PCI#4	/pci@8500/pci@4/pci@0/pci@1/****@0	27

Tableau A-4 Chemins d'accès de périphériques d'E/S du châssis du SPARC M12-2 (au moment de l'installation initiale : 2 processeurs) (suite)

Instance Priorité	Périphérique	Chemin d'accès de périphériques	Nombre dans schéma
19	PCI#8	/pci@8600/pci@4/pci@0/pci@1/****@0	28
20	PCI#3	/pci@8600/pci@4/pci@0/pci@10/****@0	29
21	PCI#1	/pci@8700/pci@4/pci@0/pci@10/****@0	30

*1 Si un périphérique USB3.0 est utilisé, il fonctionne comme un USB2.0.

Figure A-3 Schéma fonctionnel du SPARC M12-2 (2 processeurs)



Chemins d'accès de périphériques d'E/S sur le côté de l'unité d'extension PCI

Si l'emplacement du serveur PCI possédant une carte de liaison connectée à l'unité d'extension PCI est PCI#X, les chemins d'accès de périphériques suivants sont créés avec le vvvv et le u correspondants indiqués dans le chemin d'accès de périphériques de PCI#X /pci@vvvv/pci@4/pci@0/pci@u/****@0 dans [Tableau A-4](#).

Tableau A-5 Chemins d'accès de périphériques d'E/S sur le côté de l'unité d'extension PCI (2 processeurs)

Priorité d'instance	Périphérique	Chemin d'accès de périphériques
Unité d'extension PCI sous PCI#X		
1	PCI#1	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0
2	PCI#2	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0
3	PCI#3	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0
4	PCI#4	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@0/****@0
5	PCI#5	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@1/****@0
6	PCI#6	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@10/****@0
7	PCI#7	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@11/****@0
8	PCI#8	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@0/****@0
9	PCI#9	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@1/****@0
10	PCI#10	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@10/****@0
11	PCI#11	/pci@vwww/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@11/****@0

A.3 Chemins d'accès de périphériques SPARC M12-2S

Les chemins d'accès reconnus par le SPARC M12-2S et le schéma fonctionnel du matériel correspondant aux chemins d'accès de périphériques sont comme suit.

A.3.1 Pour une configuration à 1 processeur au moment de l'installation initiale

Les chemins d'accès de périphériques pour une configuration à 1 processeurs à l'installation initiale, ainsi que le schéma fonctionnel du matériel correspondant aux chemins d'accès de périphériques sont comme suit.

Remarque : si vous désactivez la reconfiguration de bus E/S (ioreconfigure) avec la commande setpparmode, les chemins d'accès de périphériques suivants s'appliquent également aux installations passant d'une configuration à 1 processeur à une configuration à 2 processeurs. Dans ce cas, vous n'avez pas besoin de reconfigurer les domaines logiques, réinstallez Oracle Solaris, puis configurez-le à nouveau.

Si vous activez la reconfiguration de bus E/S (ioreconfigure) et étendez une configuration à 1 processeur en configuration à 2 processeurs, les chemins d'accès de périphériques passent à ceux pour la configuration à 2 processeurs ([Tableau A-9](#)) lors de la réinitialisation de PPAR.

À ce moment, le système passe en configuration d'usine par défaut. Dans ce cas, les domaines logiques doivent être reconfigurés.

De plus, il est possible que vous deviez réinstaller Oracle Solaris et le configurer à nouveau.

Si vous souhaitez conserver la configuration de domaine logique, désactivez la reconfiguration de bus E/S et étendez la configuration.

Chemins d'accès de périphériques d'E/S du châssis du SPARC M12-2S

Tableau A-6 Chemins d'accès de périphériques d'E/S du châssis du SPARC M12-2S (au moment de l'installation initiale : 1 processeur)

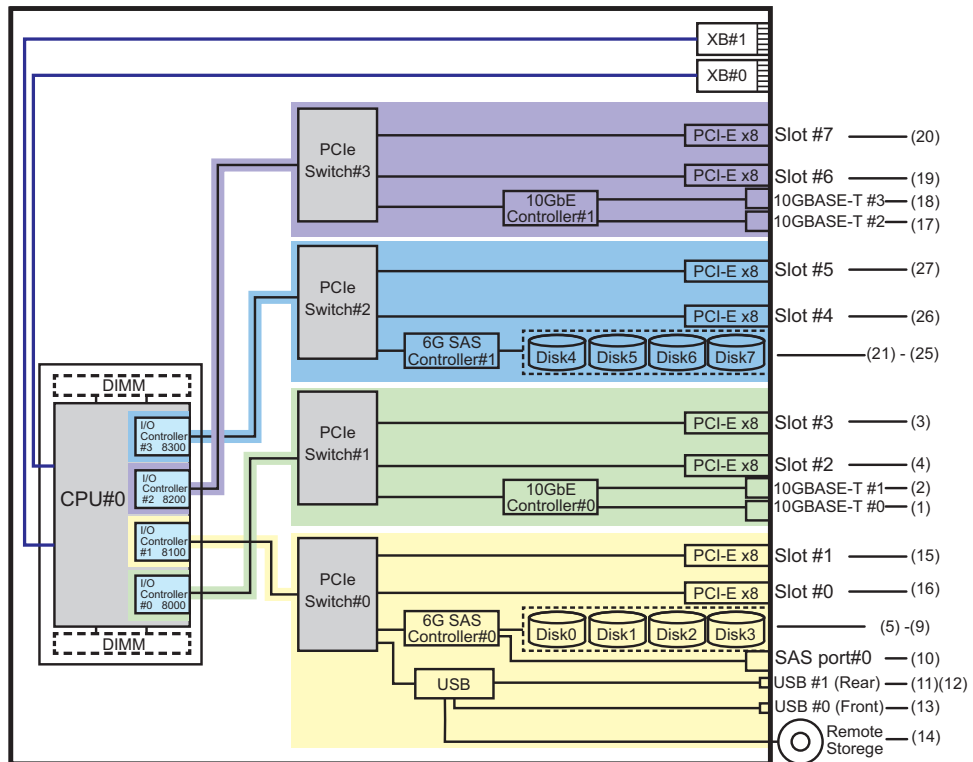
Priorité d'instance	Périphérique	Chemin d'accès de périphériques	Nombre dans schéma
1	LSB#0	LAN#0 interne /pci@8000/pci@4/pci@0/pci@0/network@0	1
2		LAN#1 interne /pci@8000/pci@4/pci@0/pci@0/network@0,1	2
3		PCI#3 /pci@8000/pci@4/pci@0/pci@10/****@0	3
4		PCI#2 /pci@8000/pci@4/pci@0/pci@11/****@0	4
5		SAS#0 interne /pci@8100/pci@4/pci@0/pci@0/scsi@0	5
-		HDD#0 interne /pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p0	6
-		HDD#1 interne /pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p1	7
-		HDD#2 interne /pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p2	8
-		HDD#3 interne /pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p3	9
-		SAS externe /pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p5xx	10
6	Port USB interne (arrière : USB3.0)	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@1/****@1	11
7	Port USB interne (arrière : USB2.0/1.1)	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@5/****@1	12
8	Port USB interne (avant : USB3.0/2.0/1.1) (*1)	/pci@8100/pci@4/pci@0/pci@1/usb@0/****@6	13
9	Stockage à distance	/pci@8100/pci@4/pci@0/pci@1/usb@0/storage@7	14

Tableau A-6 Chemins d'accès de périphériques d'E/S du châssis du SPARC M12-2S (au moment de l'installation initiale : 1 processeur) *(suite)*

Priorité d'instance	Périphérique	Chemin d'accès de périphériques	Nombre dans schéma
10	PCI#1	/pci@8100/pci@4/pci@0/pci@10/****@0	15
11	PCI#0	/pci@8100/pci@4/pci@0/pci@11/****@0	16
12	LAN#2 interne	/pci@8200/pci@4/pci@0/pci@0/network@0	17
13	LAN#3 interne	/pci@8200/pci@4/pci@0/pci@0/network@0,1	18
14	PCI#6	/pci@8200/pci@4/pci@0/pci@1/****@0	19
15	PCI#7	/pci@8200/pci@4/pci@0/pci@8/****@0	20
16	SAS#1 interne	/pci@8300/pci@4/pci@0/pci@0/scsi@0	21
-	HDD#4 interne	/pci@8300/pci@4/pci@0/pci@0/scsi@0/disk@p4	22
-	HDD#5 interne	/pci@8300/pci@4/pci@0/pci@0/scsi@0/disk@p5	23
-	HDD#6 interne	/pci@8300/pci@4/pci@0/pci@0/scsi@0/disk@p6	24
-	HDD#7 interne	/pci@8300/pci@4/pci@0/pci@0/scsi@0/disk@p7	25
17	PCI#4	/pci@8300/pci@4/pci@0/pci@1/****@0	26
18	PCI#5	/pci@8300/pci@4/pci@0/pci@8/****@0	27

*1 Si un périphérique USB3.0 est utilisé, il fonctionne comme un USB2.0.

Figure A-4 Schéma fonctionnel du SPARC M12-2S



Chemins d'accès de périphériques d'E/S sur le côté de l'unité d'extension PCI

Si l'emplacement PCI du côté du serveur possédant une carte de liaison connectée à l'unité d'extension PCI est PCI#X, les chemins d'accès de périphériques suivants sont créés avec le vvvv et le u correspondants indiqués dans le chemin d'accès de périphériques de PCI#X /pci@vvvv/pci@4/pci@0/pci@u/****@0 dans [Tableau A-6](#).

Tableau A-7 Chemins d'accès de périphériques d'E/S sur le côté de l'unité d'extension PCI

Priorité d'instance	Périphérique	Chemin d'accès de périphériques
Unité d'extension PCI sous PCI#X		
1	PCI#1	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0
2	PCI#2	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0
3	PCI#3	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0
4	PCI#4	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@0/****@0
5	PCI#5	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@1/****@0

Tableau A-7 Chemins d'accès de périphériques d'E/S sur le côté de l'unité d'extension PCI (suite)

Priorité d'instance	Périphérique	Chemin d'accès de périphériques
6	PCI#6	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@10/****@0
7	PCI#7	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@11/****@0
8	PCI#8	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@0/****@0
9	PCI#9	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@1/****@0
10	PCI#10	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@10/****@0
11	PCI#11	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@11/****@0

Chemins d'accès de périphériques d'E/S des cartes de système logique

Pour les chemins d'accès de périphériques d'E/S de LSB#1 à LSB#15, les nœuds de périphériques (/pci@vvvv) au début du chemin d'accès de périphériques d'E/S dans [Tableau A-7](#) deviennent ceux indiqués dans [Tableau A-8](#). Les autres nœuds de périphérique sont les mêmes que ceux dans [Tableau A-7](#). À titre d'exemple, pour LSB#1, interprétez les valeurs de nœud dans [Tableau A-7](#) comme indiqué ci-dessous. De la même manière, interprétez également la valeur en un nœud pour LSB#2 à LSB#15.

/pci@8000->/pci@8800, /pci@8100->/pci@8900, /pci@8200->/pci@8a00, /pci@8300->/pci@8b00

Tableau A-8 Chemins d'accès de périphériques d'E/S de LSB#1 à LSB#15 (au moment de l'installation initiale : 1 processeur)

Numéro de LSB	Chemin d'accès de périphériques
LSB#1	/pci@8800/ ... /pci@8900/ ... /pci@8a00/ ... /pci@8b00/ ...
LSB#2	/pci@9000/ ... /pci@9100/ ... /pci@9200/ ... /pci@9300/ ...
LSB#3	/pci@9800/ ... /pci@9900/ ... /pci@9a00/ ... /pci@9b00/ ...

Tableau A-8 Chemins d'accès de périphériques d'E/S de LSB#1 à LSB#15 (au moment de l'installation initiale : 1 processeur) *(suite)*

Numéro de LSB	Chemin d'accès de périphériques
LSB#4	/pci@a000/ ... /pci@a100/ ... /pci@a200/ ... /pci@a300/ ...
LSB#5	/pci@a800/ ... /pci@a900/ ... /pci@aa00/ ... /pci@ab00/ ...
LSB#6	/pci@b000/ ... /pci@b100/ ... /pci@b200/ ... /pci@b300/ ...
LSB#7	/pci@b800/ ... /pci@b900/ ... /pci@ba00/ ... /pci@bb00/ ...
LSB#8	/pci@c000/ ... /pci@c100/ ... /pci@c200/ ... /pci@c300/ ...
LSB#9	/pci@c800/ ... /pci@c900/ ... /pci@ca00/ ... /pci@cb00/ ...
LSB#10	/pci@d000/ ... /pci@d100/ ... /pci@d200/ ... /pci@d300/ ...
LSB#11	/pci@d800/ ... /pci@d900/ ... /pci@da00/ ... /pci@db00/ ...
LSB#12	/pci@e000/ ... /pci@e100/ ... /pci@e200/ ... /pci@e300/ ...
LSB#13	/pci@e800/ ... /pci@e900/ ... /pci@ea00/ ... /pci@eb00/ ...
LSB#14	/pci@f000/ ... /pci@f100/ ... /pci@f200/ ... /pci@f300/ ...

Tableau A-8 Chemins d'accès de périphériques d'E/S de LSB#1 à LSB#15 (au moment de l'installation initiale : 1 processeur) (suite)

Numéro de LSB	Chemin d'accès de périphériques
LSB#15	/pci@f800/...
	/pci@f900/...
	/pci@fa00/...
	/pci@fb00/...

A.3.2

Pour une configuration à 2 processeurs au moment de l'installation initiale

Les chemins d'accès de périphériques pour une configuration à 2 processeurs à l'installation initiale, ainsi que le schéma fonctionnel du matériel correspondant aux chemins d'accès de périphériques sont comme suit.

Remarque : si vous désactivez la reconfiguration de bus E/S (ioreconfigure) avec la commande setpparmode, les chemins d'accès de périphériques suivants s'appliquent également aux retraits passant d'une configuration à 2 processeurs à une configuration à 1 processeurs. Dans ce cas, vous n'avez pas besoin de reconfigurer les domaines logiques, réinstallez Oracle Solaris, puis configurez-le à nouveau.

Si vous activez la reconfiguration de bus E/S (ioreconfigure) et réduisez une configuration à 2 processeurs en configuration à 1 processeur, les chemins d'accès de périphériques passent à ceux pour la configuration à 1 processeur (Tableau A-6) lors de la réinitialisation de PPAR. À ce moment, le système passe en configuration d'usine par défaut. Dans ce cas, les domaines logiques doivent être reconfigurés.

De plus, il est possible que vous deviez réinstaller Oracle Solaris et le configurer à nouveau. Si vous souhaitez conserver la configuration de domaine logique, désactivez la reconfiguration de bus E/S et réduisez la configuration.

Chemins d'accès de périphériques d'E/S du châssis du SPARC M12-2S

Tableau A-9 Chemins d'accès de périphériques d'E/S du châssis du SPARC M12-2S (au moment de l'installation initiale : 2 processeurs)

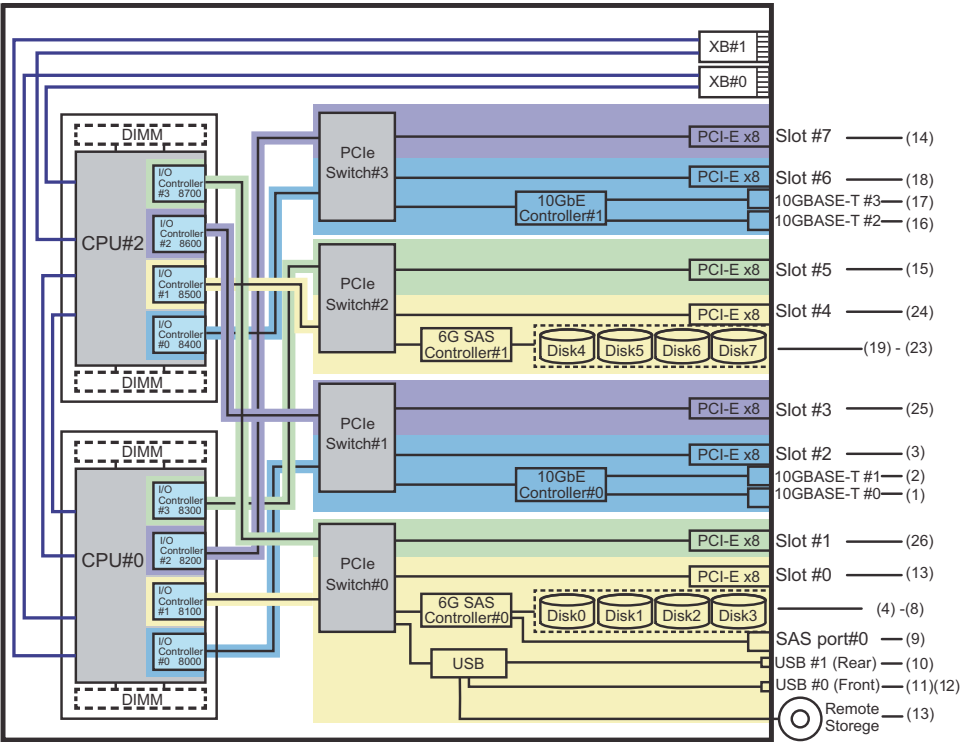
Priorité d'instance	Périphérique	Chemin d'accès de périphériques	Nombre dans schéma
1	LSB#0 LAN#0 interne	/pci@8000/pci@4/pci@0/pci@0/network@0	1
2	LAN#1 interne	/pci@8000/pci@4/pci@0/pci@0/network@0,1	2
3	PCI#2	/pci@8000/pci@4/pci@0/pci@11/****@0	3
4	SAS#0 interne	/pci@8100/pci@4/pci@0/pci@0/scsi@0	4
-	HDD#0 interne	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p0	5
-	HDD#1 interne	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p1	6
-	HDD#2 interne	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p2	7

Tableau A-9 Chemins d'accès de périphériques d'E/S du châssis du SPARC M12-2S (au moment de l'installation initiale : 2 processeurs) (suite)

Priorité d'instance	Périphérique	Chemin d'accès de périphériques	Nombre dans schéma
-	HDD#3 interne	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p3	8
-	SAS externe	/pci@8100/pci@4/pci@0/pci@0/scsi@0/disk@p5xx	9
5	Port USB interne (arrière : USB3.0)	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@1/****@1	10
6	Port USB interne (arrière : USB2.0/1.1)	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@5/****@1	11
7	Port USB interne (avant : USB3.0/2.0/1.1) (*1)	/pci@8100/pci@4/pci@0/pci@1/usb@0/****@6	12
8	Stockage à distance	/pci@8100/pci@4/pci@0/pci@1/usb@0/storage@7	13
9	PCI#0	/pci@8100/pci@4/pci@0/pci@11/****@0	14
10	PCI#7	/pci@8200/pci@4/pci@0/pci@8/****@0	15
11	PCI#5	/pci@8300/pci@4/pci@0/pci@8/****@0	16
12	LAN#2 interne	/pci@8400/pci@4/pci@0/pci@0/network@0	17
13	LAN#3 interne	/pci@8400/pci@4/pci@0/pci@0/network@0,1	18
14	PCI#6	/pci@8400/pci@4/pci@0/pci@1/****@0	19
15	SAS#1 interne	/pci@8500/pci@4/pci@0/pci@0/scsi@0	20
-	HDD#4 interne	/pci@8500/pci@4/pci@0/pci@0/scsi@0/disk@p4	21
-	HDD#5 interne	/pci@8500/pci@4/pci@0/pci@0/scsi@0/disk@p5	22
-	HDD#6 interne	/pci@8500/pci@4/pci@0/pci@0/scsi@0/disk@p6	23
-	HDD#7 interne	/pci@8500/pci@4/pci@0/pci@0/scsi@0/disk@p7	24
16	PCI#4	/pci@8500/pci@4/pci@0/pci@1/****@0	25
17	PCI#3	/pci@8600/pci@4/pci@0/pci@10/****@0	26
18	PCI#1	/pci@8700/pci@4/pci@0/pci@10/****@0	27

*1 Si un périphérique USB3.0 est utilisé, il fonctionne comme un USB2.0.

Figure A-5 Schéma fonctionnel du SPARC M12-2S



Chemins d'accès de périphériques d'E/S sur le côté de l'unité d'extension PCI

Si l'emplacement du serveur PCI possédant une carte de liaison connectée à l'unité d'extension PCI est PCI#X, les chemins d'accès de périphériques suivants sont créés avec le vvvv et le u correspondants indiqués dans le chemin d'accès de périphériques de PCI#X /pci@vvvv/pci@4/pci@0/pci@u/****@0 dans [Tableau A-9](#).

Tableau A-10 Chemins d'accès de périphériques d'E/S sur le côté de l'unité d'extension PCI

Priorité d'instance	Périphérique	Chemin d'accès de périphériques
Unité d'extension PCI sous PCI#X		
1	PCI#1	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0
2	PCI#2	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0
3	PCI#3	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0
4	PCI#4	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@0/****@0
5	PCI#5	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@1/****@0

Tableau A-10 Chemins d'accès de périphériques d'E/S sur le côté de l'unité d'extension PCI (suite)

Priorité d'instance	Périphérique	Chemin d'accès de périphériques
6	PCI#6	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@10/****@0
7	PCI#7	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@11/****@0
8	PCI#8	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@0/****@0
9	PCI#9	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@1/****@0
10	PCI#10	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@10/****@0
11	PCI#11	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@11/****@0

Chemins d'accès de périphériques d'E/S des cartes de système logique

Les chemins d'accès de périphériques pour LSB#1 à LSB#15 ont la priorité d'instance en ordre croissant de LSB#, comme LSB#0. Les nœuds de périphériques (/pci@vvvv dans [Tableau A-10](#)) au début deviennent ceux indiqués dans [Tableau A-11](#). Les autres nœuds de périphérique sont les mêmes que ceux dans [Tableau A-10](#). À titre d'exemple, pour LSB#1, interprétez les valeurs de nœud dans [Tableau A-11](#) comme indiqué ci-dessous. De la même manière, interprétez également la valeur en un nœud pour LSB#2 à LSB#15.

/pci@8000->/pci@8800, /pci@8100->/pci@8900, /pci@8200->/pci@8a00, /pci@8300->/pci@8b00

/pci@8400->/pci@8c00, /pci@8500->/pci@8d00, /pci@8600->/pci@8e00, /pci@8700->/pci@8f00

Tableau A-11 Chemins d'accès de périphériques d'E/S de LSB#1 à LSB#15 (au moment de l'installation initiale : 2 processeurs)

Número de LSB	Chemin d'accès de périphériques
LSB#1	/pci@8800/ ... /pci@8900/ ... /pci@8a00/ ... /pci@8b00/ ... /pci@8c00/... /pci@8d00/... /pci@8e00/... /pci@8f00/...

Tableau A-11 Chemins d'accès de périphériques d'E/S de LSB#1 à LSB#15 (au moment de l'installation initiale : 2 processeurs) *(suite)*

Numéro de LSB	Chemin d'accès de périphériques
LSB#2	/pci@9000/ ...
	/pci@9100/ ...
	/pci@9200/ ...
	/pci@9300/ ...
	/pci@9400/...
	/pci@9500/...
	/pci@9600/...
LSB#3	/pci@9700/...
	/pci@9800/ ...
	/pci@9900/ ...
	/pci@9a00/ ...
	/pci@9b00/ ...
	/pci@9c00/...
	/pci@9d00/...
LSB#4	/pci@9e00/...
	/pci@9f00/...
	/pci@a000/ ...
	/pci@a100/ ...
	/pci@a200/ ...
	/pci@a300/ ...
	/pci@a400/...
LSB#5	/pci@a500/...
	/pci@a600/...
	/pci@a700/...
	/pci@a800/ ...
	/pci@a900/ ...
	/pci@aa00/ ...
	/pci@ab00/ ...
LSB#6	/pci@ac00/...
	/pci@ad00/...
	/pci@ae00/...
	/pci@af00/...
	/pci@b000/ ...
	/pci@b100/ ...
	/pci@b200/ ...
LSB#7	/pci@b300/ ...
	/pci@b400/...
	/pci@b500/...
	/pci@b600/...
	/pci@b700/...
	/pci@b800/ ...
	/pci@b900/ ...
	/pci@ba00/ ...
	/pci@bb00/ ...
	/pci@bc00/...
	/pci@bd00/...
	/pci@be00/...
	/pci@bf00/...

Tableau A-11 Chemins d'accès de périphériques d'E/S de LSB#1 à LSB#15 (au moment de l'installation initiale : 2 processeurs) (*suite*)

Numéro de LSB	Chemin d'accès de périphériques
LSB#8	/pci@c000/ ... /pci@c100/ ... /pci@c200/ ... /pci@c300/ ... /pci@c400/... /pci@c500/... /pci@c600/... /pci@c700/...
LSB#9	/pci@c800/ ... /pci@c900/ ... /pci@ca00/ ... /pci@cb00/ ... /pci@cc00/... /pci@cd00/... /pci@ce00/... /pci@cf00/...
LSB#10	/pci@d000/ ... /pci@d100/ ... /pci@d200/ ... /pci@d300/ ... /pci@d400/... /pci@d500/... /pci@d600/... /pci@d700/...
LSB#11	/pci@d800/ ... /pci@d900/ ... /pci@da00/ ... /pci@db00/ ... /pci@dc00/... /pci@dd00/... /pci@de00/... /pci@df00/...
LSB#12	/pci@e000/ ... /pci@e100/ ... /pci@e200/ ... /pci@e300/ ... /pci@e400/... /pci@e500/... /pci@e600/... /pci@e700/...
LSB#13	/pci@e800/ ... /pci@e900/ ... /pci@ea00/... /pci@eb00/... /pci@ec00/... /pci@ed00/... /pci@ee00/... /pci@ef00/...

Tableau A-11 Chemins d'accès de périphériques d'E/S de LSB#1 à LSB#15 (au moment de l'installation initiale : 2 processeurs) <i>(suite)</i>	
Numéro de LSB	Chemin d'accès de périphériques
LSB#14	/pci@f000/...
	/pci@f100/...
	/pci@f200/...
	/pci@f300/...
	/pci@f400/...
	/pci@f500/...
	/pci@f600/...
LSB#15	/pci@f700/...
	/pci@f800/...
	/pci@f900/...
	/pci@fa00/...
	/pci@fb00/...
	/pci@fc00/...
	/pci@fd00/...
	/pci@fe00/...
	/pci@ff00/...



A.4 Chemins d'accès de périphériques SPARC M10-1

Les chemins d'accès reconnus par le SPARC M10-1 et le schéma fonctionnel du matériel correspondant aux chemins d'accès de périphériques sont comme suit.

Tableau A-12 Chemins d'accès au périphérique d'E/S du châssis du SPARC M10-1 et sur côté unité d'extension PCI

Instance Priorité	Périphérique	Chemin d'accès de périphériques	Nombre dans schéma
1	SAS interne	/pci@8000/pci@4/pci@0/pci@0/scsi@0	1
-	HDD#0 interne	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p0	2
-	HDD#1 interne	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p1	3
-	HDD#2 interne	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p2	4
-	HDD#3 interne	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p3	5
-	HDD#4 interne	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p4	6
-	HDD#5 interne	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p5	7
-	HDD#6 interne	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p6	8
-	HDD#7 interne	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p7	9

Tableau A-12 Chemins d'accès au périphérique d'E/S du châssis du SPARC M10-1 et sur côté unité d'extension PCI (*suite*)

Instance Priorité	Périphérique	Chemin d'accès de périphériques	Nombre dans schéma
-	SAS externe	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p5xx	10
2	LAN#0 interne	/pci@8000/pci@4/pci@0/pci@1/network@0	11
3	LAN#1 interne	/pci@8000/pci@4/pci@0/pci@1/network@0,1	12
4	Port USB interne (arrière : USB 1.1)	/pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4/****@1	13
5	Port USB interne (avant : USB 1.1)	/pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4/****@2	14
6	Port USB interne (arrière : USB 2.0)	/pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/****@1	13
7	Port USB interne (avant : USB 2.0)	/pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/****@2	14
8	Stockage à distance	/pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/storage@3	15
9	PCI#0	/pci@8000/pci@4/pci@0/pci@8/****@0	16
Unité d'extension PCI sous PCI#0			
10	PCI#1	/pci@8000/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0	
11	PCI#2	/pci@8000/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0	
12	PCI#3	/pci@8000/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0	
13	PCI#4	/pci@8000/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/ pci@0/pci@0/****@0	
14	PCI#5	/pci@8000/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/ pci@0/pci@1/****@0	
15	PCI#6	/pci@8000/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/ pci@0/pci@10/****@0	
16	PCI#7	/pci@8000/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/ pci@0/pci@11/****@0	
17	PCI#8	/pci@8000/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/ pci@0/pci@0/****@0	
18	PCI#9	/pci@8000/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/ pci@0/pci@1/****@0	
19	PCI#10	/pci@8000/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/ pci@0/pci@10/****@0	
20	PCI#11	/pci@8000/pci@4/pci@0/pci@8/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/ pci@0/pci@11/****@0	
21	LAN#2 interne	/pci@8100/pci@4/pci@0/pci@0/network@0	17
22	LAN#3 interne	/pci@8100/pci@4/pci@0/pci@0/network@0,1	18
23	PCI#1	/pci@8100/pci@4/pci@0/pci@1/****@0	19

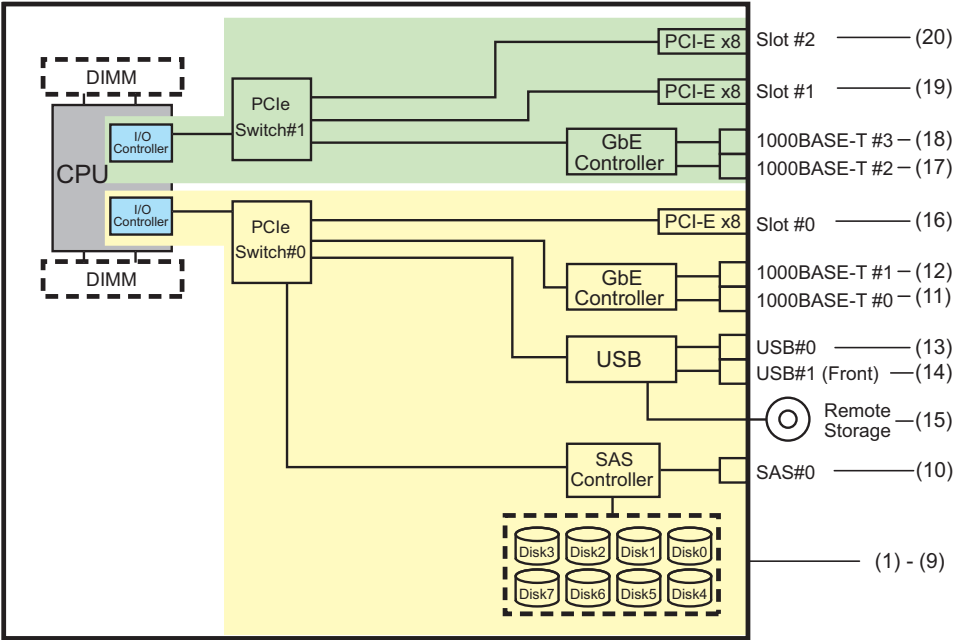
Tableau A-12 Chemins d'accès au périphérique d'E/S du châssis du SPARC M10-1 et sur côté unité d'extension PCI (*suite*)

Instance Priorité	Périphérique	Chemin d'accès de périphériques	Nombre dans schéma
Unité d'extension PCI sous PCI#1			
24	PCI#1	/pci@8100/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0	
25	PCI#2	/pci@8100/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0	
26	PCI#3	/pci@8100/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0	
27	PCI#4	/pci@8100/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/ pci@0/pci@0/****@0	
28	PCI#5	/pci@8100/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/ pci@0/pci@1/****@0	
29	PCI#6	/pci@8100/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/ pci@0/pci@10/****@0	
30	PCI#7	/pci@8100/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/ pci@0/pci@11/****@0	
31	PCI#8	/pci@8100/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/ pci@0/pci@0/****@0	
32	PCI#9	/pci@8100/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/ pci@0/pci@1/****@0	
33	PCI#10	/pci@8100/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/ pci@0/pci@10/****@0	
34	PCI#11	/pci@8100/pci@4/pci@0/pci@1/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/ pci@0/pci@11/****@0	
35	PCI#2	/pci@8100/pci@4/pci@0/pci@9/****@0	20
Unité d'extension PCI sous PCI#2			
36	PCI#1	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0	
37	PCI#2	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0	
38	PCI#3	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0	
39	PCI#4	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/ pci@0/pci@0/****@0	
40	PCI#5	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/ pci@0/pci@1/****@0	
41	PCI#6	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/ pci@0/pci@10/****@0	
42	PCI#7	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/ pci@0/pci@11/****@0	
43	PCI#8	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/ pci@0/pci@0/****@0	
44	PCI#9	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/ pci@0/pci@1/****@0	

Tableau A-12 Chemins d'accès au périphérique d'E/S du châssis du SPARC M10-1 et sur côté unité d'extension PCI (suite)

Instance Priorité	Périphérique	Chemin d'accès de périphériques	Nombre dans schéma
45	PCI#10	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/ pci@0/pci@10/****@0	
46	PCI#11	/pci@8100/pci@4/pci@0/pci@9/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/ pci@0/pci@11/****@0	

Figure A-6 Schéma fonctionnel du SPARC M10-1



A.5 Chemins d'accès de périphériques SPARC M10-4

Les chemins d'accès de périphériques reconnus par le SPARC M10-4 et le schéma fonctionnel du matériel correspondant aux chemins d'accès de périphériques sont comme suit.

A.5.1 Pour une configuration à 2 processeurs au moment de l'installation initiale

Les chemins d'accès de périphériques pour une configuration à 2 processeurs à l'installation initiale, ainsi que le schéma fonctionnel du matériel correspondant aux chemins d'accès de périphériques sont comme suit.

Remarque : si vous désactivez la reconfiguration de bus E/S (ioreconfigure) avec la commande setpparmode, les chemins d'accès de périphériques suivants s'appliquent également aux installations passant d'une configuration à 2 processeur à une configuration à 4 processeurs. Dans ce cas, vous n'avez pas besoin de reconfigurer les domaines logiques, réinstallez Oracle Solaris, puis configurez-le à nouveau.

Si vous activez la reconfiguration de bus E/S (ioreconfigure) et étendez une configuration à 2 processeur en configuration à 4 processeurs, les chemins d'accès de périphériques passent à ceux pour la configuration à 4 processeurs ([Tableau A-16](#)) lors de la réinitialisation de PPAR. À ce moment, le système passe en configuration d'usine par défaut. Dans ce cas, les domaines logiques doivent être reconfigurés.

De plus, il est possible que vous deviez réinstaller Oracle Solaris et le configurer à nouveau. Si vous souhaitez conserver la configuration de domaine logique, désactivez la reconfiguration de bus E/S et étendez la configuration.

Chemins d'accès de périphériques d'E/S du châssis du SPARC M10-4

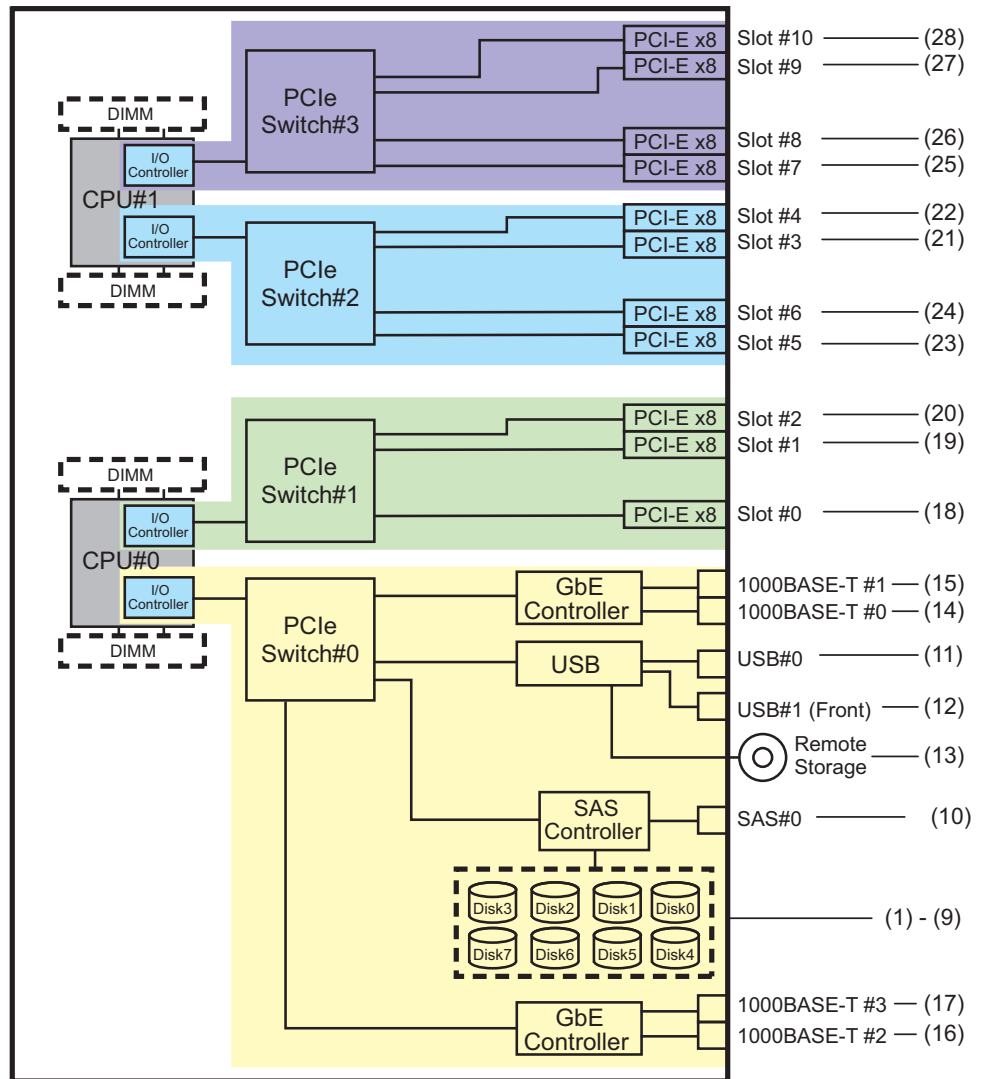
Tableau A-13 Chemins d'accès de périphériques d'E/S du châssis du SPARC M10-4 (au moment de l'installation initiale : 2 processeurs)

Instance Priorité	Périphérique	Chemin d'accès de périphériques	Nombre dans schéma
1	LSB#0	SAS interne /pci@8000/pci@4/pci@0/pci@0/scsi@0	1
-		HDD#0 interne /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p0	2
-		HDD#1 interne /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p1	3
-		HDD#2 interne /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p2	4
-		HDD#3 interne /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p3	5
-		HDD#4 interne /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p4	6
-		HDD#5 interne /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p5	7
-		HDD#6 interne /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p6	8
-		HDD#7 interne /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p7	9
-		SAS externe /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p5xx	10
2	Port USB interne (arrière : USB 1.1)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4/****@1	11

Tableau A-13 Chemins d'accès de périphériques d'E/S du châssis du SPARC M10-4 (au moment de l'installation initiale : 2 processeurs) (*suite*)

Instance Priorité	Périphérique	Chemin d'accès de périphériques	Nombre dans schéma
3	Port USB interne (arrière : USB 2.0)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/****@1	11
4	Port USB interne (avant : USB 1.1/2.0)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/****@1	12
5	Stockage à distance	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3	13
6	LAN#0 interne	/pci@8000/pci@4/pci@0/pci@9/network@0	14
7	LAN#1 interne	/pci@8000/pci@4/pci@0/pci@9/network@0,1	15
8	LAN#2 interne	/pci@8000/pci@4/pci@0/pci@a/network@0	16
9	LAN#3 interne	/pci@8000/pci@4/pci@0/pci@a/network@0,1	17
10	PCI#0	/pci@8100/pci@4/pci@0/pci@0/****@0	18
11	PCI#1	/pci@8100/pci@4/pci@0/pci@8/****@0	19
12	PCI#2	/pci@8100/pci@4/pci@0/pci@9/****@0	20
13	PCI#3	/pci@8200/pci@4/pci@0/pci@0/****@0	21
14	PCI#4	/pci@8200/pci@4/pci@0/pci@8/****@0	22
15	PCI#5	/pci@8200/pci@4/pci@0/pci@9/****@0	23
16	PCI#6	/pci@8200/pci@4/pci@0/pci@11/****@0	24
17	PCI#7	/pci@8300/pci@4/pci@0/pci@0/****@0	25
18	PCI#8	/pci@8300/pci@4/pci@0/pci@8/****@0	26
19	PCI#9	/pci@8300/pci@4/pci@0/pci@9/****@0	27
20	PCI#10	/pci@8300/pci@4/pci@0/pci@11/****@0	28

Figure A-7 Schéma fonctionnel du SPARC M10-4 (2 processeurs)



Chemins d'accès de périphériques d'E/S sur le côté de l'unité d'extension PCI

Si l'emplacement du serveur PCI possédant une carte de liaison connectée à l'unité d'extension PCI est PCI#X, les chemins d'accès de périphériques suivants sont créés avec le vvvv et le u correspondants indiqués dans le chemin d'accès de périphériques de PCI#X /pci@vvvv/pci@4/pci@0/pci@u/****@0 dans [Tableau A-13](#).

Tableau A-14 Chemins d'accès de périphériques d'E/S sur le côté de l'unité d'extension PCI (au moment de l'installation initiale : 2 processeurs)

Instance Priorité	Périphérique	Chemin d'accès de périphériques
	Unité d'extension PCI sous PCI#X	
1	PCI#1	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0
2	PCI#2	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0
3	PCI#3	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0
4	PCI#4	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@0/****@0
5	PCI#5	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@1/****@0
6	PCI#6	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@10/****@0
7	PCI#7	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@11/****@0
8	PCI#8	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@0/****@0
9	PCI#9	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@1/****@0
10	PCI#10	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@10/****@0
11	PCI#11	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@11/****@0

A.5.2 Pour une configuration à 4 processeur au moment de l'installation initiale

Les chemins d'accès de périphériques pour une configuration à 4 processeurs à l'installation initiale, ainsi que le schéma fonctionnel du matériel correspondant aux chemins d'accès de périphériques sont comme suit.

Remarque : si vous désactivez la reconfiguration de bus E/S (ioreconfigure) avec la commande setpparmode, les chemins d'accès de périphériques suivants s'appliquent également aux retraits passant d'une configuration à 4 processeurs à une configuration à 2 processeurs. Dans ce cas, vous n'avez pas besoin de reconfigurer les domaines logiques, réinstallez Oracle Solaris, puis configurez-le à nouveau.

Si vous activez la reconfiguration de bus E/S (ioreconfigure) et réduisez une configuration à 4 processeurs en configuration à 2 processeur, les chemins d'accès de périphériques passent à ceux pour la configuration à 2 processeur (Tableau A-13) lors de la réinitialisation de PPAR. À ce moment, le système passe en configuration d'usine par défaut. Dans ce cas, les domaines logiques doivent être reconfigurés.

De plus, il est possible que vous deviez réinstaller Oracle Solaris et le configurer à nouveau. Si vous souhaitez conserver la configuration de domaine logique, désactivez la reconfiguration de bus E/S et réduisez la configuration.

Périphériques d'E/S du châssis du SPARC M10-4

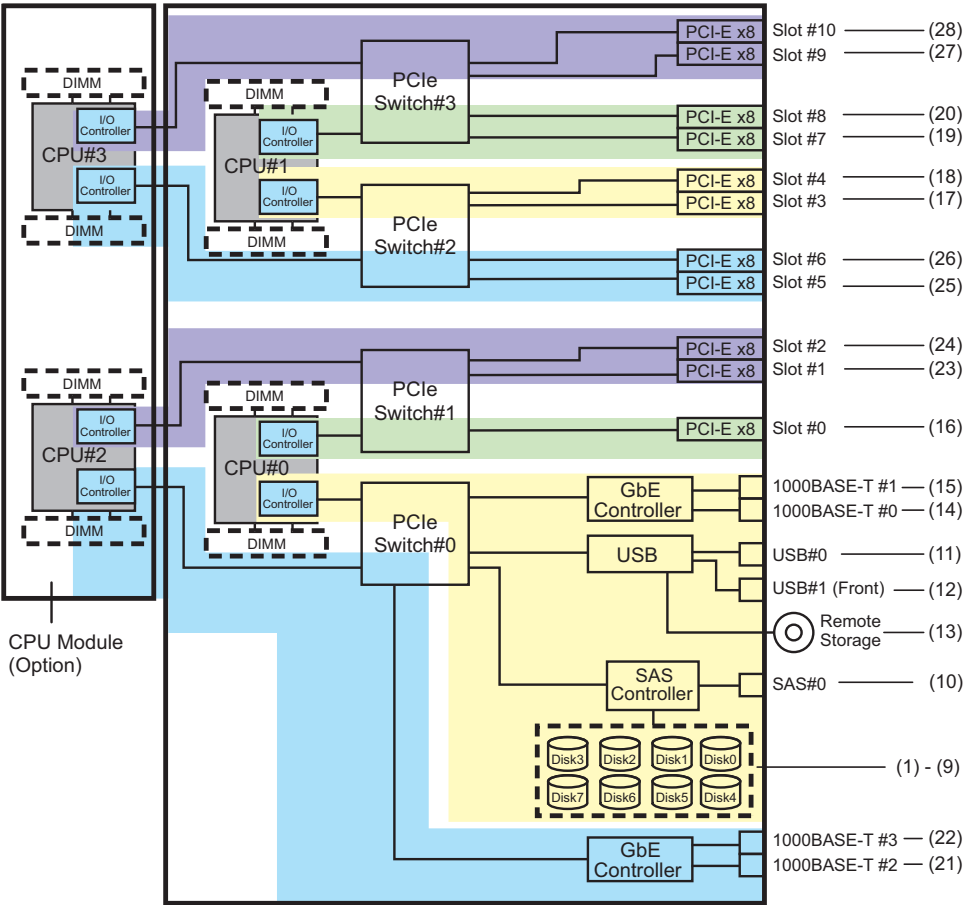
Tableau A-15 Chemins d'accès de périphériques d'E/S du châssis du SPARC M10-4 (au moment de l'installation initiale : 4 processeurs)

Instance Priorité	Périphérique	Chemin d'accès de périphériques	Nombre dans schéma
1	LSB#0	SAS interne	1
-		HDD#0 interne	2
-		HDD#1 interne	3
-		HDD#2 interne	4
-		HDD#3 interne	5
-		HDD#4 interne	6
-		HDD#5 interne	7
-		HDD#6 interne	8
-		HDD#7 interne	9
-		SAS externe	10
2	Port USB interne (arrière : USB 1.1)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4/****@1	11
3	Port USB interne (arrière : USB 2.0)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/****@1	11
4	Port USB interne (avant : USB 1.1/2.0)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/****@1	12
5	Stockage à distance	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3	13
6	LAN#0 interne	/pci@8000/pci@4/pci@0/pci@9/network@0	14
7	LAN#1 interne	/pci@8000/pci@4/pci@0/pci@9/network@0,1	15
8	PCI#0	/pci@8100/pci@4/pci@0/pci@0/****@0	16
9	PCI#3	/pci@8200/pci@4/pci@0/pci@0/****@0	17
10	PCI#4	/pci@8200/pci@4/pci@0/pci@8/****@0	18
11	PCI#7	/pci@8300/pci@4/pci@0/pci@0/****@0	19
12	PCI#8	/pci@8300/pci@4/pci@0/pci@8/****@0	20
13	LAN#2 interne	/pci@8400/pci@4/pci@0/pci@a/network@0	21
14	LAN#3 interne	/pci@8400/pci@4/pci@0/pci@a/network@0,1	22

Tableau A-15 Chemins d'accès de périphériques d'E/S du châssis du SPARC M10-4 (au moment de l'installation initiale : 4 processeurs) (suite)

Instance Priorité	Périphérique	Chemin d'accès de périphériques	Nombre dans schéma
15	PCI#1	/pci@8500/pci@4/pci@0/pci@8/****@0	23
16	PCI#2	/pci@8500/pci@4/pci@0/pci@9/****@0	24
17	PCI#5	/pci@8600/pci@4/pci@0/pci@9/****@0	25
18	PCI#6	/pci@8600/pci@4/pci@0/pci@11/****@0	26
19	PCI#9	/pci@8700/pci@4/pci@0/pci@9/****@0	27
20	PCI#10	/pci@8700/pci@4/pci@0/pci@11/****@0	28

Figure A-8 Schéma fonctionnel du SPARC M10-4 (4 processeurs)



Périphériques d'E/S sur le côté de l'unité d'extension PCI

Si l'emplacement du serveur PCI possédant une carte de liaison connectée à l'unité d'extension PCI est PCI#X, les chemins d'accès de périphériques suivants sont créés avec le vvvv et le u correspondants indiqués dans le chemin d'accès de périphériques de PCI#X /pci@vvvv/pci@4/pci@0/pci@u/****@0 dans [Tableau A-15](#).

Tableau A-16 Chemins d'accès de périphériques d'E/S sur le côté de l'unité d'extension PCI (au moment de l'installation initiale : 4 processeurs)

Instance Priorité	Périphérique	Chemin d'accès de périphériques
Unité d'extension PCI sous PCI#X		
1	PCI#1	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0
2	PCI#2	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0
3	PCI#3	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0
4	PCI#4	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@0/****@0
5	PCI#5	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@1/****@0
6	PCI#6	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@10/****@0
7	PCI#7	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@11/****@0
8	PCI#8	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@0/****@0
9	PCI#9	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@1/****@0
10	PCI#10	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@10/****@0
11	PCI#11	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@11/****@0

A.6 Chemins d'accès de périphériques SPARC M10-4S

Les chemins d'accès de périphériques reconnus par le SPARC M10-4S et le schéma fonctionnel du matériel correspondant aux chemins d'accès de périphériques sont comme suit.

A.6.1 Pour une configuration à 2 processeurs au moment de l'installation initiale

Les chemins d'accès de périphériques pour une configuration à 2 processeurs à l'installation initiale, ainsi que le schéma fonctionnel du matériel correspondant aux chemins d'accès de périphériques sont comme suit.

Remarque : si vous réglez la reconfiguration de bus E/S (ioreconfigure) sur l'état désactivé (par défaut) avec la commande setpparmode, les chemins d'accès de périphériques suivants s'appliquent également aux installations passant d'une configuration à 2 processeurs à une configuration à 4 processeurs. Dans ce cas, vous n'avez pas besoin de reconfigurer les domaines logiques, réinstallez Oracle Solaris, puis configurez-le à nouveau.

Si vous activez la reconfiguration de bus E/S (ioreconfigure) et étendez une configuration à 2 processeur en configuration à 4 processeurs, les chemins d'accès de périphériques passent à ceux pour la configuration à 4 processeurs ([Tableau A-20](#)) lors de la réinitialisation de PPAR. À ce moment, le système passe en configuration d'usine par défaut. Dans ce cas, les domaines logiques doivent être reconfigurés.

De plus, il est possible que vous deviez réinstaller Oracle Solaris et le configurer à nouveau. Si vous souhaitez conserver la configuration de domaine logique, désactivez la reconfiguration de bus E/S et étendez la configuration.

Chemins d'accès de périphériques d'E/S du châssis du SPARC M10-4S

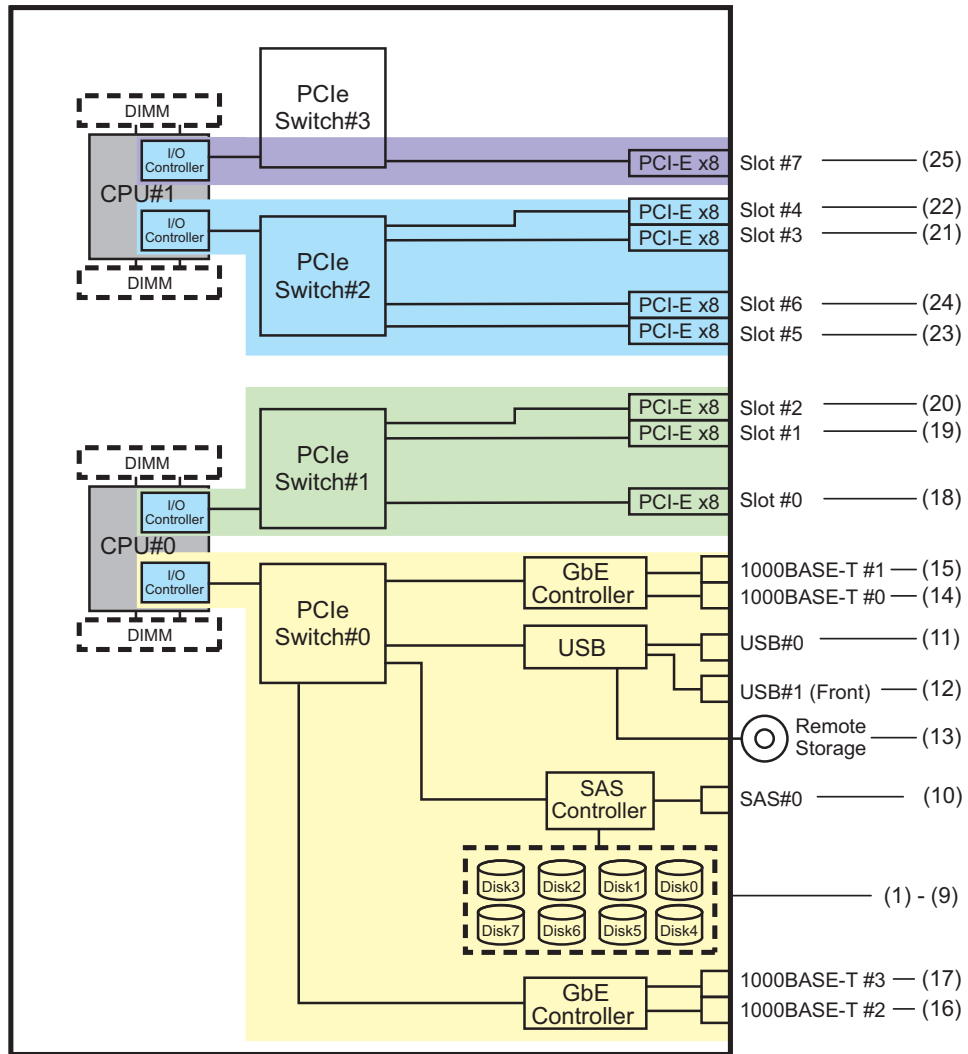
Tableau A-17 Chemins d'accès de périphériques d'E/S du châssis du SPARC M10-4S (au moment de l'installation initiale : 2 processeurs)

Instance Priorité	Périphérique	Chemin d'accès de périphériques	Nombre dans schéma
1	LSB#0	SAS interne /pci@8000/pci@4/pci@0/pci@0/scsi@0	1
-		HDD#0 interne /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p0	2
-		HDD#1 interne /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p1	3
-		HDD#2 interne /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p2	4
-		HDD#3 interne /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p3	5
-		HDD#4 interne /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p4	6
-		HDD#5 interne /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p5	7
-		HDD#6 interne /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p6	8
-		HDD#7 interne /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p7	9
-		SAS externe /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p5xx	10
2	Port USB interne (arrière : USB 1.1)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4/****@1	11
3	Port USB interne (arrière : USB 2.0)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/****@1	11
4	Port USB interne (avant : USB 1.1/2.0)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/****@1	12
5	Stockage à distance	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3	13

Tableau A-17 Chemins d'accès de périphériques d'E/S du châssis du SPARC M10-4S (au moment de l'installation initiale : 2 processeurs) (*suite*)

Instance Priorité	Périphérique	Chemin d'accès de périphériques	Nombre dans schéma
6	LAN#0 interne	/pci@8000/pci@4/pci@0/pci@9/network@0	14
7	LAN#1 interne	/pci@8000/pci@4/pci@0/pci@9/network@0,1	15
8	LAN#2 interne	/pci@8000/pci@4/pci@0/pci@a/network@0	16
9	LAN#3 interne	/pci@8000/pci@4/pci@0/pci@a/network@0,1	17
10	PCI#0	/pci@8100/pci@4/pci@0/pci@0/****@0	18
11	PCI#1	/pci@8100/pci@4/pci@0/pci@8/****@0	19
12	PCI#2	/pci@8100/pci@4/pci@0/pci@9/****@0	20
13	PCI#3	/pci@8200/pci@4/pci@0/pci@0/****@0	21
14	PCI#4	/pci@8200/pci@4/pci@0/pci@8/****@0	22
15	PCI#5	/pci@8200/pci@4/pci@0/pci@9/****@0	23
16	PCI#6	/pci@8200/pci@4/pci@0/pci@11/****@0	24
17	PCI#7	/pci@8300/pci@4/pci@0/pci@0/****@0	25

Figure A-9 Schéma fonctionnel du SPARC M10-4S (2 processeurs)



Chemins d'accès de périphériques d'E/S sur le côté de l'unité d'extension PCI

Si l'emplacement du serveur PCI possédant une carte de liaison connectée à l'unité d'extension PCI est PCI#X, les chemins d'accès de périphériques suivants sont créés avec le vvvv et le u correspondants indiqués dans le chemin d'accès de périphériques de PCI#X/pci@vvvv/pci@4/pci@0/pci@u/****@0 dans [Tableau A-17](#).

Tableau A-18 Chemins d'accès de périphériques d'E/S sur le côté de l'unité d'extension PCI (au moment de l'installation initiale : 2 processeurs)

Instance Priorité	Périphérique	Chemin d'accès de périphériques
Unité d'extension PCI sous PCI#X		
1	PCI#1	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0
2	PCI#2	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0
3	PCI#3	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0
4	PCI#4	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@0/****@0
5	PCI#5	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@1/****@0
6	PCI#6	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@10/****@0
7	PCI#7	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@11/****@0
8	PCI#8	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@0/****@0
9	PCI#9	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@1/****@0
10	PCI#10	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@10/****@0
11	PCI#11	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@11/****@0

Chemins d'accès de périphériques d'E/S des cartes de système logique

Les chemins d'accès de périphériques pour LSB#1 à LSB#15 ont la priorité d'instance en ordre croissant de LSB#, comme LSB#0. Les nœuds de périphériques ([Tableau A-18/pci@vvvv](#)) au début deviennent ceux indiqués dans [Tableau A-19](#). Les autres nœuds de périphérique sont les mêmes que ceux dans [Tableau A-18](#).
À titre d'exemple, pour LSB#1, interprétez les valeurs de nœud dans [Tableau A-19](#) comme indiqué ci-dessous. De la même manière, interprétez également la valeur en un nœud pour LSB#2 à LSB#15.
/pci@8000->/pci@8800, /pci@8100->/pci@8900, /pci@8200->/pci@8a00, /pci@8300->/pci@8b00, /pci@8400->/pci@8c00, /pci@8500->/pci@8d00, /pci@8600->/pci@8e00, /pci@8700->/pci@8f00

Tableau A-19 Chemins d'accès de périphériques d'E/S de LSB#1 à LSB#15 (au moment de l'installation initiale : 2 processeurs)

Numéro de LSB	Chemin d'accès de périphériques
LSB#1	/pci@8800/ ...
	/pci@8900/ ...
	/pci@8a00/ ...
	/pci@8b00/ ...
LSB#2	/pci@9000/ ...
	/pci@9100/ ...
	/pci@9200/ ...
	/pci@9300/ ...

Tableau A-19 Chemins d'accès de périphériques d'E/S de LSB#1 à LSB#15 (au moment de l'installation initiale : 2 processeurs) (*suite*)

Numéro de LSB	Chemin d'accès de périphériques
LSB#3	/pci@9800/ ... /pci@9900/ ... /pci@9a00/ ... /pci@9b00/ ...
LSB#4	/pci@a000/ ... /pci@a100/ ... /pci@a200/ ... /pci@a300/ ...
LSB#5	/pci@a800/ ... /pci@a900/ ... /pci@aa00/ ... /pci@ab00/ ...
LSB#6	/pci@b000/ ... /pci@b100/ ... /pci@b200/ ... /pci@b300/ ...
LSB#7	/pci@b800/ ... /pci@b900/ ... /pci@ba00/ ... /pci@bb00/ ...
LSB#8	/pci@c000/ ... /pci@c100/ ... /pci@c200/ ... /pci@c300/ ...
LSB#9	/pci@c800/ ... /pci@c900/ ... /pci@ca00/ ... /pci@cb00/ ...
LSB#10	/pci@d000/ ... /pci@d100/ ... /pci@d200/ ... /pci@d300/ ...
LSB#11	/pci@d800/ ... /pci@d900/ ... /pci@da00/ ... /pci@db00/ ...
LSB#12	/pci@e000/ ... /pci@e100/ ... /pci@e200/ ... /pci@e300/ ...
LSB#13	/pci@e800/ ... /pci@e900/ ... /pci@ea00/ ... /pci@eb00/ ...

Tableau A-19 Chemins d'accès de périphériques d'E/S de LSB#1 à LSB#15 (au moment de l'installation initiale : 2 processeurs) (suite)	
Numéro de LSB	Chemin d'accès de périphériques
LSB#14	/pci@f000/...
	/pci@f100/...
	/pci@f200/...
	/pci@f300/...
LSB#15	/pci@f800/...
	/pci@f900/...
	/pci@fa00/...
	/pci@fb00/...

A.6.2 Pour une configuration à 4 processeur au moment de l'installation initiale

Les chemins d'accès de périphériques pour une configuration à 4 processeurs à l'installation initiale, ainsi que le schéma fonctionnel du matériel correspondant aux chemins d'accès de périphériques sont comme suit.

Remarque : si vous désactivez la reconfiguration de bus E/S (ioreconfigure) avec la commande setpparmode, les chemins d'accès de périphériques suivants s'appliquent également aux retraits passant d'une configuration à 4 processeurs à une configuration à 2 processeurs. Dans ce cas, vous n'avez pas besoin de reconfigurer les domaines logiques, réinstallez Oracle Solaris, puis configurez-le à nouveau.

Si vous activez la reconfiguration de bus E/S (ioreconfigure) et réduisez une configuration à 4 processeurs en configuration à 2 processeur, les chemins d'accès de périphériques passent à ceux pour la configuration à 2 processeur ([Tableau A-17](#)) lors de la réinitialisation de PPAR. À ce moment, le système passe en configuration d'usine par défaut. Dans ce cas, les domaines logiques doivent être reconfigurés.

De plus, il est possible que vous deviez réinstaller Oracle Solaris et le configurer à nouveau. Si vous souhaitez conserver la configuration de domaine logique, désactivez la reconfiguration de bus E/S et réduisez la configuration.

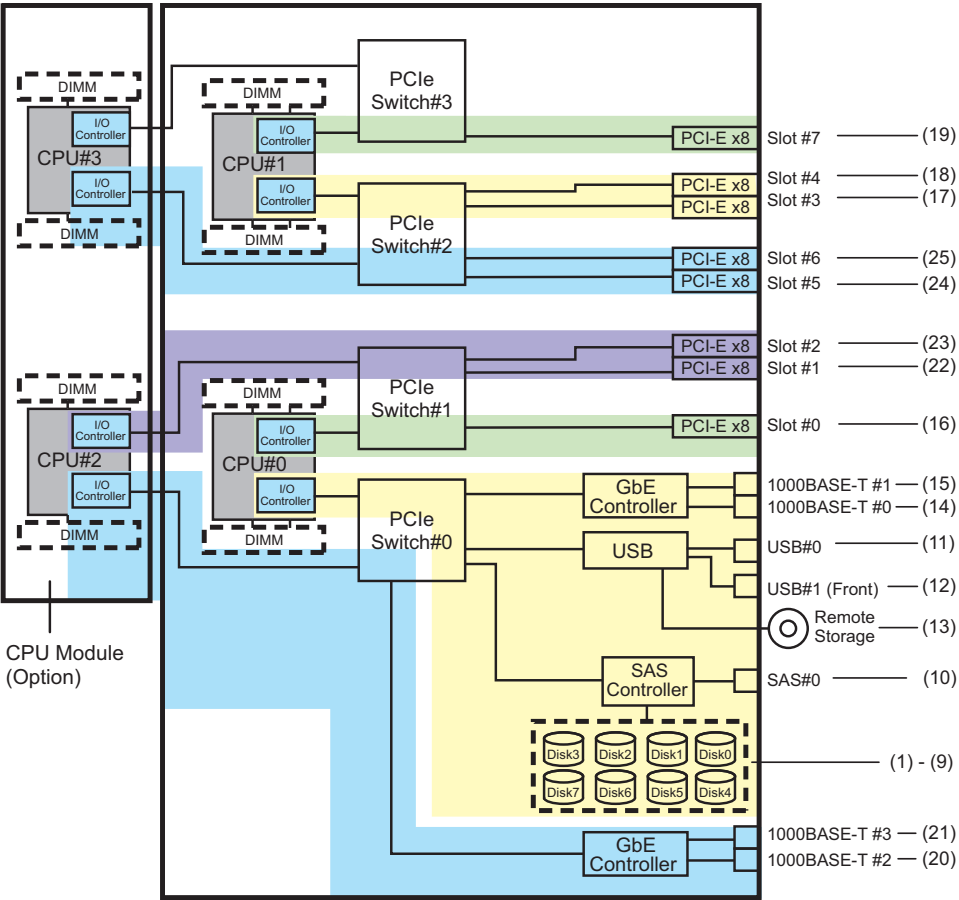
Périphériques d'E/S du châssis du SPARC M10-4S

Tableau A-20 Chemins d'accès de périphériques d'E/S du châssis du SPARC M10-4S (au moment de l'installation initiale : 4 processeurs)				
Instance	Périphérique	Chemin d'accès de périphériques		Nombre dans schéma
Priorité				
1	LSB#0	SAS interne	/pci@8000/pci@4/pci@0/pci@0/scsi@0	1
-		HDD#0 interne	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p0	2
-		HDD#1 interne	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p1	3
-		HDD#2 interne	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p2	4

Tableau A-20 Chemins d'accès de périphériques d'E/S du châssis du SPARC M10-4S (au moment de l'installation initiale : 4 processeurs) *(suite)*

Instance Priorité	Périphérique	Chemin d'accès de périphériques	Nombre dans schéma
-	HDD#3 interne	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p3	5
-	HDD#4 interne	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p4	6
-	HDD#5 interne	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p5	7
-	HDD#6 interne	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p6	8
-	HDD#7 interne	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p7	9
-	SAS externe	/pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p5xx	10
2	Port USB interne (arrière : USB 1.1)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4/****@1	11
3	Port USB interne (arrière : USB 2.0)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/****@1	11
4	Port USB interne (avant : USB 1.1/2.0)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/****@1	12
5	Stockage à distance	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3	13
6	LAN#0 interne	/pci@8000/pci@4/pci@0/pci@9/network@0	14
7	LAN#1 interne	/pci@8000/pci@4/pci@0/pci@9/network@0,1	15
8	PCI#0	/pci@8100/pci@4/pci@0/pci@0/****@0	16
9	PCI#3	/pci@8200/pci@4/pci@0/pci@0/****@0	17
10	PCI#4	/pci@8200/pci@4/pci@0/pci@8/****@0	18
11	PCI#7	/pci@8300/pci@4/pci@0/pci@0/****@0	19
12	LAN#2 interne	/pci@8400/pci@4/pci@0/pci@a/network@0	20
13	LAN#3 interne	/pci@8400/pci@4/pci@0/pci@a/network@0,1	21
14	PCI#1	/pci@8500/pci@4/pci@0/pci@8/****@0	22
15	PCI#2	/pci@8500/pci@4/pci@0/pci@9/****@0	23
16	PCI#5	/pci@8600/pci@4/pci@0/pci@9/****@0	24
17	PCI#6	/pci@8600/pci@4/pci@0/pci@11/****@0	25

Figure A-10 Schéma fonctionnel du SPARC M10-4S (4 processeurs)



Périphériques d'E/S sur le côté de l'unité d'extension PCI

Si l'emplacement du serveur PCI possédant une carte de liaison connectée à l'unité d'extension PCI est PCI#X, les chemins d'accès de périphériques suivants sont créés avec le vvvv et le u correspondants indiqués dans le chemin d'accès de périphériques de PCI#X /pci@vvvv/pci@4/pci@0/pci@u/****@0 dans [Tableau A-20](#).

Tableau A-21 Chemins d'accès de périphériques d'E/S sur le côté de l'unité d'extension PCI (au moment de l'installation initiale : 4 processeurs)

Instance Priorité	Périphérique	Chemin d'accès de périphériques
Unité d'extension PCI sous PCI#X		
1	PCI#1	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@0/****@0
2	PCI#2	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@1/****@0
3	PCI#3	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@8/****@0

Tableau A-21 Chemins d'accès de périphériques d'E/S sur le côté de l'unité d'extension PCI (au moment de l'installation initiale : 4 processeurs) (suite)

Instance Priorité	Périphérique	Chemin d'accès de périphériques
4	PCI#4	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@0/****@0
5	PCI#5	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@1/****@0
6	PCI#6	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@10/****@0
7	PCI#7	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@10/pci@0/pci@11/****@0
8	PCI#8	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@0/****@0
9	PCI#9	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@1/****@0
10	PCI#10	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@10/****@0
11	PCI#11	/pci@vvvv/pci@4/pci@0/pci@u/pci@0/pci@0/pci@0/pci@1/pci@0/pci@11/pci@0/pci@11/****@0

Périphériques d'E/S des cartes de système logique

Pour les chemins d'accès de périphériques d'E/S de LSB#1 à LSB#15, les nœuds de périphériques (/pci@vvvv) au début du chemin d'accès de périphériques d'E/S dans [Tableau A-20](#) deviennent ceux indiqués dans [Tableau A-22](#). Les autres nœuds de périphérique sont les mêmes que ceux dans [Tableau A-20](#).
À titre d'exemple, pour LSB#1, interprétez les valeurs de nœud dans [Tableau A-20](#) comme indiqué ci-dessous. De la même manière, interprétez également la valeur en un nœud pour LSB#2 à LSB#15.

/pci@8000->/pci@8800, /pci@8100->/pci@8900, /pci@8200->/pci@8a00, /pci@8300->/pci@8b00
/pci@8400->/pci@8c00, /pci@8500->/pci@8d00, /pci@8600->/pci@8e00

Tableau A-22 Chemins d'accès de périphériques d'E/S de LSB#1 à LSB#15 (au moment de l'installation initiale : 4 processeurs)

Numéro de LSB	Chemin d'accès de périphériques
LSB#1	/pci@8800/ ... /pci@8900/ ... /pci@8a00/ ... /pci@8b00/ ... /pci@8c00/... /pci@8d00/... /pci@8e00/...
LSB#2	/pci@9000/ ... /pci@9100/ ... /pci@9200/ ... /pci@9300/ ... /pci@9400/... /pci@9500/... /pci@9600/...

Tableau A-22 Chemins d'accès de périphériques d'E/S de LSB#1 à LSB#15 (au moment de l'installation initiale : 4 processeurs) *(suite)*

Numéro de LSB	Chemin d'accès de périphériques
LSB#3	/pci@9800/ ...
	/pci@9900/ ...
	/pci@9a00/ ...
	/pci@9b00/ ...
	/pci@9c00/...
	/pci@9d00/...
	/pci@9e00/...
LSB#4	/pci@a000/ ...
	/pci@a100/ ...
	/pci@a200/ ...
	/pci@a300/ ...
	/pci@a400/...
	/pci@a500/...
	/pci@a600/...
LSB#5	/pci@a800/ ...
	/pci@a900/ ...
	/pci@aa00/ ...
	/pci@ab00/ ...
	/pci@ac00/...
	/pci@ad00/...
	/pci@ae00/...
LSB#6	/pci@b000/ ...
	/pci@b100/ ...
	/pci@b200/ ...
	/pci@b300/ ...
	/pci@b400/...
	/pci@b500/...
	/pci@b600/...
LSB#7	/pci@b800/ ...
	/pci@b900/ ...
	/pci@ba00/ ...
	/pci@bb00/ ...
	/pci@bc00/...
	/pci@bd00/...
	/pci@be00/...
LSB#8	/pci@c000/ ...
	/pci@c100/ ...
	/pci@c200/ ...
	/pci@c300/ ...
	/pci@c400/...
	/pci@c500/...
	/pci@c600/...

Tableau A-22 Chemins d'accès de périphériques d'E/S de LSB#1 à LSB#15 (au moment de l'installation initiale : 4 processeurs) (*suite*)

Numéro de LSB	Chemin d'accès de périphériques
LSB#9	/pci@c800/ ... /pci@c900/ ... /pci@ca00/ ... /pci@cb00/ ... /pci@cc00/... /pci@cd00/... /pci@ce00/...
LSB#10	/pci@d000/ ... /pci@d100/ ... /pci@d200/ ... /pci@d300/ ... /pci@d400/... /pci@d500/... /pci@d600/...
LSB#11	/pci@d800/ ... /pci@d900/ ... /pci@da00/ ... /pci@db00/ ... /pci@dc00/... /pci@dd00/... /pci@de00/...
LSB#12	/pci@e000/ ... /pci@e100/ ... /pci@e200/ ... /pci@e300/ ... /pci@e400/... /pci@e500/... /pci@e600/...
LSB#13	/pci@e800/ ... /pci@e900/ ... /pci@ea00/... /pci@eb00/... /pci@ec00/... /pci@ed00/... /pci@ee00/...
LSB#14	/pci@f000/... /pci@f100/... /pci@f200/... /pci@f300/... /pci@f400/... /pci@f500/... /pci@f600/...

Tableau A-22 Chemins d'accès de périphériques d'E/S de LSB#1 à LSB#15 (au moment de l'installation initiale : 4 processeurs) *(suite)*

Numéro de LSB	Chemin d'accès de périphériques
LSB#15	/pci@f800/...
	/pci@f900/...
	/pci@fa00/...
	/pci@fb00/...
	/pci@fc00/...
	/pci@fd00/...
	/pci@fe00/...

Identifier un périphérique SAS2 en fonction de WWN

Cette annexe décrit comment identifier le périphérique SAS2 en fonction d'une valeur WWN.

- Syntaxe World Wide Name (WWN)
- Présentation du résultat de la commande probe-scsi-all
- Identification de l'emplacement d'un disque à l'aide de la commande probe-scsi-all
- Identification de l'emplacement d'un disque

B.1 Syntaxe World Wide Name (WWN)

Oracle Solaris utilise désormais la syntaxe World Wide Name (WWN) pour les noms de périphérique logique. Cette section décrit comment mapper un nom de périphérique basé sur WWN vers un périphérique SCSI spécifique.

Par exemple, un périphérique de démarrage s'utilise pour afficher les différences de notation entre d' anciens noms de périphérique (tn, ID de cible) et des noms de périphérique basés sur WWN.

Tableau B-1 Différence de notation entre les noms de périphérique

Nom du périphérique de démarrage utilisant la valeur WWN	Ancien nom du périphérique de démarrage (utilisant l'ID de cible)
c#tWWNd# WWN est un nombre hexadécimal totalement unique pour ce périphérique. Le fabricant attribue ce numéro au périphérique.	c0t0d0

Une valeur WWN ne se conforme pas à l'ancienne structure du nom du périphérique logique. Il est ainsi impossible d'identifier directement le périphérique cible à partir d'une valeur c#tWWNd#.

Pour mapper un nom de périphérique basé sur WWN vers le périphérique physique

spécifique, utilisez la commande `probe-scsi-all` d'OpenBoot PROM. Pour plus de détails, consultez « [B.3 Identification de l'emplacement d'un disque à l'aide de la commande `probe-scsi-all`](#) ».

B.2 Présentation du résultat de la commande `probe-scsi-all`

Les résultats de la commande `probe-scsi-all` d'OpenBoot PROM affichent une liste de tous les périphériques SCSI du système et les informations de base de chaque périphérique. Les tableau suivant liste les éléments affichés.

Tableau B-2 Configuration de la commande `probe-scsi-all`

Nom de l'entité	Description
Target	ID cible unique attribué à chaque périphérique SAS
SASDeviceName	Valeur WWN attribuée à un périphérique SAS par le fabricant. Oracle Solaris le reconnaît.
SASAddress	Valeur WWN reconnue par le microprogramme OpenBoot PROM et attribuée à un périphérique SCSI
PhyNum	ID de nombre hexadécimal du port de contrôleur connecté au lecteur cible
VolumeDeviceName (lors de la configuration d'un volume RAID)	Valeur WWN reconnue par Oracle Solaris et attribuée à un volume RAID. Elle remplace <code>SASDeviceName</code> pour chaque périphérique SCSI inclus dans le volume RAID.
VolumeWWID (lors de la configuration d'un volume RAID)	Valeur WWN reconnue par le microprogramme OpenBoot PROM et attribuée à un volume RAID. Elle remplace <code>SASAddress</code> pour chaque périphérique SCSI inclus dans le volume RAID.

B.3 Identification de l'emplacement d'un disque à l'aide de la commande `probe-scsi-all`

Cette section décrit comment identifier l'emplacement d'un disque à l'aide de la commande `probe-scsi-all` d'OpenBoot PROM. Cela peut associer l'emplacement de disque avec la valeur WWN correspondante.

B.3.1 Exemple d'identification de l'emplacement d'un disque à l'aide de la commande probe-scsi-all (SPARC M12-1/M12-2/M12-2S/M10-1/M10-4/M10-4S)

Cette section décrit la correspondance entre PhyNum, connecté au contrôleur SAS embarqué, et les emplacements de disque.

Dans le SPARC M12-1/M12-2/M12-2S/M10-1/M10-4/M10-4S, le contrôleur SAS est connecté au fond de panier du disque dur. Le tableau suivant indique le mappage entre le PhyNum du backplane du disque dur et les emplacements de disque.

Tableau B-3 Mappage de PhyNum et des emplacements de disque (SPARC M12-1/M10-1/M10-4/M10-4S)

PhyNum	Emplacement de disque
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Tableau B-4 Mappage de PhyNum et des emplacements de disque (SPARC M12-2/M12-2S)

PhyNum	Numéro de contrôleur SAS	Emplacement de disque
0	0	0
1		1
2		2
3		3
4	1	4
5		5
6		6
7		7

Remarque : pour les positions physiques des emplacements de disques dans le SPARC M12-1/M12-2/M12-2S/M10-1/M10-4/M10-4S, consultez « Maintaining the Internal Storage » dans le *Service Manual* pour votre serveur.

Exemple de résultat de la commande probe-scsi-all

La procédure pour identifier l'emplacement d'un disque est décrite ci-dessous dans un cas où huit lecteurs de disque internes sont montés dans le SPARC M12-2S/M10-1.

1. Exécutez la commande probe-scsi-all.

Dans l'exemple suivant du SPARC M10-1, le PhyNum du lecteur de disque interne monté sur l'emplacement de disque 0 est 0. Le lecteur de disque interne est attribué à Target a et la valeur de SASDeviceName est 50000393c813ae74.

Exemple du SPARC M10-1

```
{0} ok probe-scsi-all
/pci@8000/pci@4/pci@0/pci@0/scsi@0 <---- Contrôleur SAS

FCode Version 1.00.56, MPT Version 2.00, Firmware Version 13.00.57.00

Target a
  Unit 0   Disk   TOSHIBA   MBF2300RC           3706   585937500 Blocks, 300 GB
    SASDeviceName 50000393c813ae74 SASAddress 50000393c813ae76 PhyNum 0
Target b
  Unit 0   Disk   TOSHIBA   MBF2300RC           3706   585937500 Blocks, 300 GB
    SASDeviceName 50000393b81b24ec SASAddress 50000393b81b24ee PhyNum 1
Target c
  Unit 0   Disk   TOSHIBA   MBF2300RC           3706   585937500 Blocks, 300 GB
    SASDeviceName 50000393b81af47c SASAddress 50000393b81af47e PhyNum 2
Target d
  Unit 0   Disk   TOSHIBA   MBF2300RC           3706   585937500 Blocks, 300 GB
    SASDeviceName 50000393b81af3c0 SASAddress 50000393b81af3c2 PhyNum 3
Target e
  Unit 0   Disk   TOSHIBA   MBF2300RC           3706   585937500 Blocks, 300 GB
    SASDeviceName 50000393b81b0f58 SASAddress 50000393b81b0f5a PhyNum 4
Target f
  Unit 0   Disk   TOSHIBA   MBF2300RC           3706   585937500 Blocks, 300 GB
    SASDeviceName 50000393b81b130c SASAddress 50000393b81b130e PhyNum 5
Target 10
  Unit 0   Disk   TOSHIBA   MBF2300RC           3706   585937500 Blocks, 300 GB
    SASDeviceName 50000393b81b2420 SASAddress 50000393b81b2422 PhyNum 6
Target 11
  Unit 0   Disk   TOSHIBA   MBF2300RC           3706   585937500 Blocks, 300 GB
    SASDeviceName 50000393b81acc84 SASAddress 50000393b81acc86 PhyNum 7
Target 12
  Unit 0   Encl Serv device FUJITSU   NBBEXP           0d32
    SASAddress 500000e0e04d003d PhyNum 14
{0} ok
```

Exemple du SPARC M12-2S

```
{0} ok probe-scsi-all
/pci@8500/pci@4/pci@0/pci@0/scsi@0 <---- Contrôleur SAS 1
```

```

FCode Version 1.00.56, MPT Version 2.00, Firmware Version 20.00.06.00

Target a
Unit 0    Disk    TOSHIBA  AL13SEB600AL14SE 3702    1172123568 Blocks, 600 GB
SASDeviceName 5000039678332cc5 SASAddress 5000039678332cc6 PhyNum 4
Target b
Unit 0    Disk    TOSHIBA  AL13SEB600AL14SE 3702    1172123568 Blocks, 600 GB
SASDeviceName 5000039678332ca9 SASAddress 5000039678332caa PhyNum 5
Target c
Unit 0    Disk    TOSHIBA  AL13SEB600AL14SE 3702    1172123568 Blocks, 600 GB
SASDeviceName 5000039678332c59 SASAddress 5000039678332c5a PhyNum 6
Target d
Unit 0    Disk    TOSHIBA  AL13SEB600AL14SE 3702    1172123568 Blocks, 600 GB
SASDeviceName 5000039678332c55 SASAddress 5000039678332c56 PhyNum 7
Target e
Unit 0    Encl Serv device FUJITSU  BBEXP          0d32
SASAddress 500000e0e0b0103d PhyNum 14

/pci@8100/pci@4/pci@0/pci@0/scsi@0 <---- Contrôleur SAS 0
FCode Version 1.00.56, MPT Version 2.00, Firmware Version 20.00.06.00

Target a
Unit 0    Disk    TOSHIBA  AL13SEB600AL14SE 3702    1172123568 Blocks, 600 GB
SASDeviceName 5000039698002565 SASAddress 5000039698002566 PhyNum 0
Target b
Unit 0    Disk    TOSHIBA  AL13SEB600AL14SE 3702    1172123568 Blocks, 600 GB
SASDeviceName 50000396980024b9 SASAddress 50000396980024ba PhyNum 1
Target c
Unit 0    Disk    TOSHIBA  AL13SEB600AL14SE 3702    1172123568 Blocks, 600 GB
SASDeviceName 5000039698002495 SASAddress 5000039698002496 PhyNum 2
Target d
Unit 0    Disk    TOSHIBA  AL13SEB600AL14SE 3702    1172123568 Blocks, 600 GB
SASDeviceName 5000039678332cd1 SASAddress 5000039678332cd2 PhyNum 3
Target e
Unit 0    Encl Serv device FUJITSU  BBEXP          0d32
SASAddress 500000e0e0b0103d PhyNum 14

```

Remarque : la méthode ci-dessus peut également identifier l'emplacement d'un disque dans le SPARC M12-1/M12-2/M10-4/M10-4S.

B.4 Identification de l'emplacement d'un disque

Pour effectuer le remplacement actif d'un stockage interne, il est nécessaire de connaître le nom de périphérique physique ou logique du lecteur devant être installé ou supprimé. Si une erreur de disque se produit sur le système, il est généralement possible de vérifier le message indiquant le disque sur lequel une panne peut se

produire ou le disque en panne. Ces informations sont également enregistrées dans le fichier /var/adm/messages.

Ce message indique généralement le lecteur de disque interne en panne par son nom de périphérique physique ou logique. Le numéro d'emplacement du disque peut également être reporté selon l'application.

Les procédures de vérification des informations de l'emplacement d'installation des HDD varie selon la version d'Oracle Solaris.

- **Dans le cas d'Oracle Solaris 11**

Pour plus de détails, consultez « [B.4.1 Utilisation de la commande de formatage \(Oracle Solaris 11\)](#) » ou « [B.4.2 Utilisation de la commande diskinfo \(Oracle Solaris 11\)](#) ».

- **Dans le cas d'Oracle Solaris 10**

Pour plus de détails, consultez « [B.4.3 Utilisation de la commande diskinfo \(Oracle Solaris 10\)](#) ».

B.4.1 Utilisation de la commande de formatage (Oracle Solaris 11)

1. **Exécutez la commande showhardconf et vérifiez le numéro de série du CMUL du châssis dont l' information de l'emplacement d'installation est affichée.**

```
XSCF> showhardconf
SPARC M10-4S;
+ Serial:2081238017; Operator_Panel_Switch:Service;
+ System_Power:Off; System_Phase:Cabinet Power Off;
Partition#0 PPAR_Status:Powered Off;
Partition#1 PPAR_Status:Powered Off;
BB#00 Status:Normal; Role:Master; Ver:2044h; Serial:2081238017;
+ FRU-Part-Number:CA07361-D202 A1 ;
+ Power_Supply_System: ;
+ Memory_Size:256 GB;
CMUL Status:Normal; Ver:0101h; Serial:PP123001Y1 ;
* Numéro de série de la CMUL BB#00
+ FRU-Part-Number:CA07361-D941 C3 /7060911 ;
+ Memory_Size:128 GB;
CPU#0 Status:Normal; Ver:4142h; Serial:00321144;
+ Freq:3.000 GHz; Type:0x10;
+ Core:16; Strand:2;
CPU#1 Status:Normal; Ver:4142h; Serial:00322957;
+ Freq:3.000 GHz; Type:0x10;
+ Core:16; Strand:2;
-----Omis-----
BB#01 Status:Normal; Role:Standby; Ver:2044h; Serial:2081230011;
+ FRU-Part-Number:CA07361-D202 A1 ;
+ Power_Supply_System: ;
+ Memory_Size:256 GB;
CMUL Status:Normal; Ver:0101h; Serial:PP123203N0 ;
* Numéro de série de la CMUL BB#01
```



```

+ FRU-Part-Number:CA07361-D941 C3 /7060911 ;
+ Memory_Size:128 GB;
CPU#0 Status:Normal; Ver:4142h; Serial:00320804;
+ Freq:3.000 GHz; Type:0x10;
+ Core:16; Strand:2;
CPU#1 Status:Normal; Ver:4142h; Serial:00321030;
+ Freq:3.000 GHz; Type:0x10;
+ Core:16; Strand:2;
MEM#00A Status:Normal;
+ Code:2c800118KSF1G72PZ-1G6E1 4531-1A94229F;
+ Type:04; Size:8 GB;
-----Omis-----

```

2. Exécutez la commande de formatage et vérifiez l'emplacement physique du disque.

Dans les exemples suivants, (1) à (5) indiquent ce qui suit :

- (1) : Nom du chemin d'accès logique du disque
- (2) : Le disque est installé à l'emplacement HDD00 de BB#01
- (3) : Le disque est installé à l'emplacement HDD01 de BB#01
- (4) : Le disque est installé à l'emplacement HDD00 de BB#00
- (5) : Le disque est installé à l'emplacement HDD01 de BB#00

```

# format
Searching for disks...done

AVAILABLE DISK SELECTIONS:
  0. c2t50000394281B5312d0 <TOSHIBA-MBF2600RC-3706 cyl 64986 alt 2 hd 27 sec
668> <-- (1)
      /pci@8800/pci@4/pci@0/pci@0/scsi@0/iport@f/disk@w50000394281b5312,0
      /dev/chassis/FUJITSU-BBEXP.500000e0e06d31bf/03N0_HDD00/disk <-- (2)
                                     * 4 derniers chiffres du
numéro de série de BB#1_CMUL
                                     * HDD00
  1. c2t50000394281B59D6d0 <TOSHIBA-MBF2600RC-3706 cyl 64986 alt 2 hd 27 sec
668> <-- (1)
      /pci@8800/pci@4/pci@0/pci@0/scsi@0/iport@f/disk@w50000394281b59d6,0
      /dev/chassis/FUJITSU-BBEXP.500000e0e06d31bf/03N0_HDD01/disk <-- (3)
                                     * HDD01
  2. c0t500003942823C8C6d0 <TOSHIBA-MBF2600RC-3706 cyl 64986 alt 2 hd 27 sec
668> <-- (1)
      /pci@8000/pci@4/pci@0/pci@0/scsi@0/iport@f/disk@w500003942823c8c6,0
      /dev/chassis/FUJITSU-BBEXP.500000e0e06d237f/01Y1_HDD00/disk <-- (4)
                                     * 4 derniers chiffres du
numéro de série de BB#0_CMUL
                                     * HDD00
  3. c0t50000394281B517Ad0 <TOSHIBA-MBF2600RC-3706 cyl 64986 alt 2 hd 27 sec
668> <-- (1)
      /pci@8000/pci@4/pci@0/pci@0/scsi@0/iport@f/disk@w50000394281b517a,0
      /dev/chassis/FUJITSU-BBEXP.500000e0e06d237f/01Y1_HDD01/disk <-- (5)
                                     * HDD01

Specify disk (enter its number):

```

B.4.2 Utilisation de la commande diskinfo (Oracle Solaris 11)

1. **Exécutez la commande showhardconf et vérifiez le numéro de série du CMUL du châssis dont l'information de l'emplacement d'installation est affichée.**

```
XSCF> showhardconf
SPARC M10-4S;
+ Serial:2081238017; Operator_Panel_Switch:Service;
+ System_Power:Off; System_Phase:Cabinet Power Off;
Partition#0 PPAR_Status:Powered Off;
Partition#1 PPAR_Status:Powered Off;
BB#00 Status:Normal; Role:Master; Ver:2044h; Serial:2081238017;
+ FRU-Part-Number:CA07361-D202 A1 ;
+ Power_Supply_System: ;
+ Memory_Size:256 GB;
CMUL Status:Normal; Ver:0101h; Serial:PP123001Y1 ;
* Numéro de série de la CMUL BB#00
+ FRU-Part-Number:CA07361-D941 C3 /7060911 ;
+ Memory_Size:128 GB;
CPU#0 Status:Normal; Ver:4142h; Serial:00321144;
+ Freq:3.000 GHz; Type:0x10;
+ Core:16; Strand:2;
CPU#1 Status:Normal; Ver:4142h; Serial:00322957;
+ Freq:3.000 GHz; Type:0x10;
+ Core:16; Strand:2;
-----Omis-----
BB#01 Status:Normal; Role:Standby; Ver:2044h; Serial:2081230011;
+ FRU-Part-Number:CA07361-D202 A1 ;
+ Power_Supply_System: ;
+ Memory_Size:256 GB;
CMUL Status:Normal; Ver:0101h; Serial:PP123203N0 ;
* Numéro de série de la CMUL BB#01
+ FRU-Part-Number:CA07361-D941 C3 /7060911 ;
+ Memory_Size:128 GB;
CPU#0 Status:Normal; Ver:4142h; Serial:00320804;
+ Freq:3.000 GHz; Type:0x10;
+ Core:16; Strand:2;
CPU#1 Status:Normal; Ver:4142h; Serial:00321030;
+ Freq:3.000 GHz; Type:0x10;
+ Core:16; Strand:2;
MEM#00A Status:Normal;
+ Code:2c800118KSF1G72PZ-1G6E1 4531-1A94229F;
+ Type:04; Size:8 GB;
-----Omis-----
```

2. **Exécutez la commande diskinfo et vérifiez l'emplacement physique du disque.**
Dans les exemples suivants, (1) à (4) indiquent ce qui suit :
(1) : Le nom du périphérique et du chemin d'accès logique du disque installé dans HDD 0 de BB#01

- (2) : Le nom du périphérique et du chemin d'accès logique du disque installé dans HDD 1 de BB#01
- (3) : Le nom du périphérique et du chemin d'accès logique du disque installé dans HDD 0 de BB#00
- (4) : Le nom du périphérique et du chemin d'accès logique du disque installé dans HDD 1 de BB#00

```
# diskinfo
D:devchassis-path c:occupant-compdev
-----
/dev/chassis/SYS/BB0/CMUL/HDD0 -
/dev/chassis/SYS/BB0/CMUL/HDD1 -
/dev/chassis/SYS/BB0/CMUL/HDD2 -
/dev/chassis/SYS/BB0/CMUL/HDD3 -
/dev/chassis/SYS/BB0/CMUL/HDD4 -
/dev/chassis/SYS/BB0/CMUL/HDD5 -
/dev/chassis/SYS/BB0/CMUL/HDD6 -
/dev/chassis/SYS/BB0/CMUL/HDD7 -
/dev/chassis/SYS/BB1/CMUL/HDD0 -
/dev/chassis/SYS/BB1/CMUL/HDD1 -
/dev/chassis/SYS/BB1/CMUL/HDD2 -
/dev/chassis/SYS/BB1/CMUL/HDD3 -
/dev/chassis/SYS/BB1/CMUL/HDD4 -
/dev/chassis/SYS/BB1/CMUL/HDD5 -
/dev/chassis/SYS/BB1/CMUL/HDD6 -
/dev/chassis/SYS/BB1/CMUL/HDD7 -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d31bf/03N0_HDD00/disk
c4t50000394281B5312d0 <-- (1)
* 4 derniers chiffres du numéro de série de
BB#01_CMUL
/dev/chassis/FUJITSU-BBEXP.500000e0e06d31bf/03N0_HDD01/disk
c4t50000394281B59D6d0 <-- (2)
/dev/chassis/FUJITSU-BBEXP.500000e0e06d31bf/03N0_HDD02 -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d31bf/03N0_HDD03 -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d31bf/03N0_HDD04 -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d31bf/03N0_HDD05 -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d31bf/03N0_HDD06 -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d31bf/03N0_HDD07 -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d237f/01Y1_HDD00/disk
c2t500003942823C8C6d0 <-- (3)
* 4 derniers chiffres du numéro de série de
BB#00_CMUL
/dev/chassis/FUJITSU-BBEXP.500000e0e06d237f/01Y1_HDD01/disk
c2t50000394281B517Ad0 <-- (4)
/dev/chassis/FUJITSU-BBEXP.500000e0e06d237f/01Y1_HDD02 -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d237f/01Y1_HDD03 -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d237f/01Y1_HDD04 -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d237f/01Y1_HDD05 -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d237f/01Y1_HDD06 -
/dev/chassis/FUJITSU-BBEXP.500000e0e06d237f/01Y1_HDD07 -
```

B.4.3 Utilisation de la commande diskinfo (Oracle Solaris 10)

1. **Exécutez la commande diskinfo et vérifiez l'emplacement physique du disque et de la carte de système logique.**
Dans les exemples suivants, (1) à (4) indiquent ce qui suit :
- (1) : Le nom du chemin d'accès logique du disque installé dans HDD 0.
 - (2) : Les chemins d'accès de périphériques du disque installé dans HDD 0 de LSB#00
 - (3) : Le nom du chemin d'accès logique du disque installé dans HDD 1.
 - (4) : Les chemins d'accès de périphériques du disque installé dans HDD 1 de LSB#00

```
# diskinfo -ap

Enclosure path:      2081210007-physical-hba-0
Chassis Serial Number: 2081210007-physical-hba-0
Chassis Model:      ORCL,SPARC64-X

Enclosure path:      /dev/es/ses0
Chassis Serial Number: 500000e0e06d233f
Chassis Model:      FUJITSU-BBEXP

Label      Disk name      Vendor      Product      Vers
-----
HDD_0      c0t50000393D8289180d0    TOSHIBA     MBF2600RC     3706 <-- (1)
Physical path
-----
0: /pci@8000/pci@4/pci@0/pci@0/scsi@0/iport@f/disk@w50000393D8289180,0<-- (2)
* LSB#0
HDD_1      c0t50000393D82891D0d0    TOSHIBA     MBF2600RC     3706 <-- (3)
Physical path
-----
0: /pci@8000/pci@4/pci@0/pci@0/scsi@0/iport@f/disk@w50000393D82891D0,0<-- (4)
* LSB#0
```

Le format de notation du chemin d'accès de périphérique d'un disque affiché par la commande diskinfo est le suivant.

<SAS controller device path>/iport@f/disk@wXXXXXXXX,Y:Z

Le chemin d'accès de périphériques varie selon le modèle ou la configuration du système. Pour plus de détails, consultez « [Annexe A Listes des chemins d'accès de périphériques des systèmes SPARC M12/M10](#) ».

Liste des pages de XSCF Web

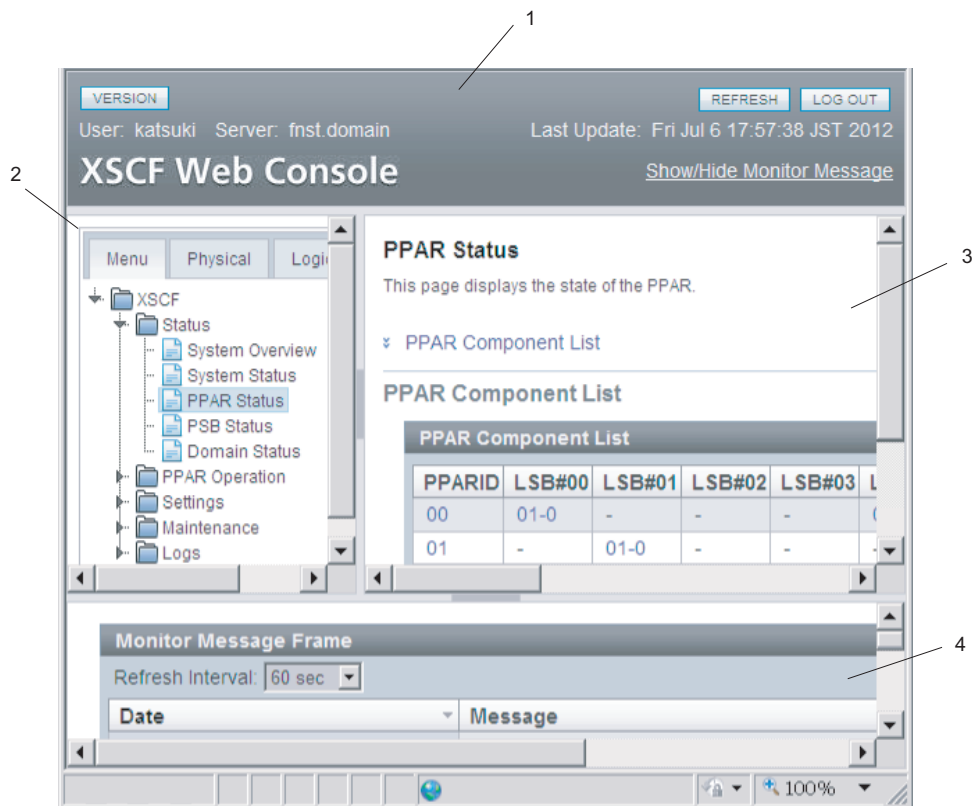
Cette annexe fournit un aperçu de chacune des pages de XSCF Web. Pour plus de détails sur la façon de se connecter ou se déconnecter de XSCF Web, consultez « [Chapitre 2 Connexion à / Déconnexion de XSCF](#) ».

- [Aperçu des pages](#)
- [Comprendre la configuration du menu](#)
- [Pages disponibles](#)

C.1 Aperçu des pages

[Figure C-1](#) montre la fenêtre de la console XSCF Web qui s'affiche après la connexion.

Figure C-1 Fenêtre de la console XSCF Web



-
- 1 Cadre d'en-tête
 - 2 Cadre du menu (arborescence)
 - 3 Cadre principal
 - 4 Cadre d'événement
-

La console XSCF Web affichée après la connexion est composée de quatre cadres. Sélectionner un élément de menu dans le cadre de gauche permet d'afficher ses informations dans le cadre de droite. Cela permet à l'utilisateur d'utiliser et/ou de gérer le serveur.

Tableau C-1 répertorie les types de cadres de la console XSCF Web et fournit un aperçu de chaque cadre.

Tableau C-1 Aperçus des cadres

Type de cadre	Aperçu
Cadre d'en-tête	Page en haut de la fenêtre (1 sur Figure C-1). Ce cadre affiche le nom du compte d'utilisateur indiqué lors de la connexion, le nom de l'hôte connecté et d'autres informations. À la déconnexion du cadre, l'utilisateur est redirigé vers la page de connexion.
Cadre du menu (arborescence)	Page à gauche de la fenêtre (2 sur Figure C-1). Lorsqu'un élément de menu y est sélectionné, le cadre principal, situé sur la droite, peut afficher les informations correspondantes. Le cadre comprend trois onglets. Chaque menu apparaît sous forme d'arborescence. - Menu : permet d'afficher un menu montrant divers réglages, opérations et affichages d'état. - Physique : permet d'afficher la configuration des composants physiques du système. - Logique : permet d'afficher la configuration des composants logiques, par partition physique.
Cadre principal	Page à droite de la fenêtre (3 sur Figure C-1). Sélectionner un élément de menu dans l'arborescence permet d'afficher la page correspondante.
Cadre d'événement (cadre des messages de surveillance)	Page en bas de la fenêtre (4 sur Figure C-1). Les événements du système complet sont affichés sous forme de messages de surveillance. Ce cadre est actualisé régulièrement. La valeur de l'intervalle peut être modifiée dans le même cadre. L'intervalle d'actualisation par défaut est de 60 secondes.

[Tableau C-2](#) répertorie les fonctions et fournit des aperçus des principales pages affichées par la console XSCF Web.

Tableau C-2 Aperçu des principale pages

Fonction de la page	Aperçu
Page de connexion	Il s'agit de la page de connexion de la console XSCF Web. Connectez-vous à l'aide d'un compte d'utilisateur XSCF sur la page de connexion.
Affichage de l'état du serveur	Cette page affiche l'état du système complet, des partitions physiques ainsi que des domaines logiques. Cela comprend également l'état de l'unité d'extension PCI. Dans l'onglet [Menu], sélectionnez [Status].
Faire fonctionner une partition physique	Cette page est utilisée pour faire fonctionner une partition physique et des domaines logiques. Ces opérations incluent l'alimentation électrique de la partition physique et la gestion de la configuration de la carte système (PSB). Dans l'onglet [Menu], sélectionnez [PPAR Operation].

Tableau C-2 Aperçu des principale pages (*suite*)

Fonction de la page	Aperçu
Configuration du serveur	Plusieurs réglages pour le système complet et le XSCF sont réalisés sur cette page. Dans l'onglet [Menu], sélectionnez [Settings].
Maintenance du serveur	Les opérations réalisables sur cette page comprennent la sauvegarde/restauration de données, la mise à jour du microprogramme, le redémarrage et la commutation du XSCF, le service de maintenance à distance et la sauvegarde des journaux. Dans l'onglet [Menu], sélectionnez [Maintenance].
Affichage d'un journal	Les journaux affichés comprennent le journal d'erreur, le journal d'alimentation, le journal des événements et le journal de la console. Dans l'onglet [Menu], sélectionnez [Logs].
Page du côté en veille	Cette page s'affiche après une connexion au XSCF de veille. Elle peut commuter le XSCF, sauvegarder des journaux, etc.

C.2 Comprendre la configuration du menu

Cette section décrit la configuration du menu.

La configuration affichée lorsque l'onglet [Menu] est sélectionné dans le cadre de menu est présentée ci-dessous.

```

Menu
+ XSCF
  + Status
    - System Overview
    - System Status
    - PPAR Status
    - PSB Status
    - Domain Status
  + PPAR Operation
    - PPAR Power
    - PPAR Mode Configuration
    - PPAR Configuration
    - PSB Configuration
    - Domain Configuration
    - PPAR Parameter
    - Verified Boot
  + Settings
    + Network
      - Current
      - Reserve
    + Service
      - Service State
  
```


- HTTPS
- SSH
- Telnet
- NTP
- SMTP
- SNMP
- SNMP Security
- + User Manager
 - Account
 - LDAP
 - LDAP/SSL
 - Active Directory
- Autologout
- CoD Reservation
- CoD Activation
- Audit
- Email Reporting
- Time
- Power Capping
- Power Schedule
- Add-In Card Manager
- PCIBOX DIO
- Remote Storage
- + Maintenance
 - + Network Tools
 - Ping
 - Traceroute
 - Nslookup
 - Configuration Management
 - Firmware Update
 - Reboot XSCF
 - Switch Over
 - Snapshot
 - ASR
- + Logs
 - Error Log
 - Power Log
 - Event Log
 - Console Log
 - Panic Log
 - Environment Log
 - IPL Message Log
 - Monitor Message Log
 - Audit Log

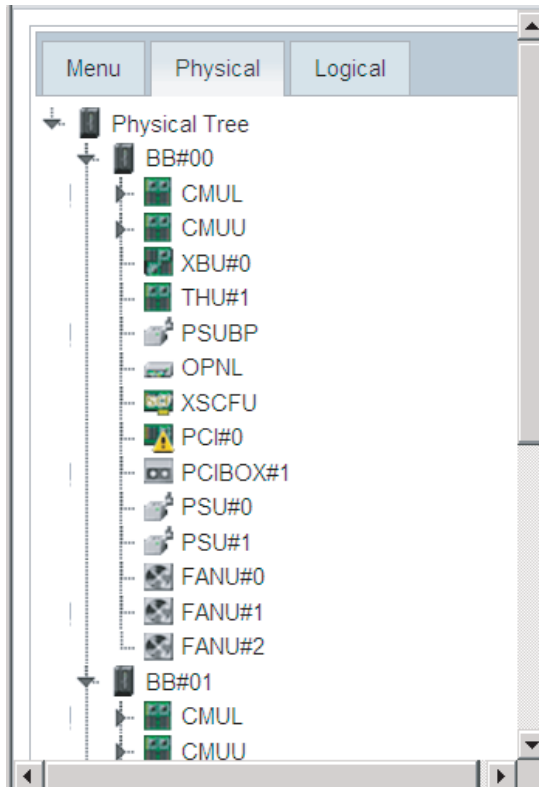
Remarque : chaque élément de menu peut être modifié afin d'en améliorer le fonctionnement ou pour d'autres raisons. De plus, les éléments de menu peuvent varier en fonction du modèle ou des conditions.

La sélection d'un élément de menu affiche la page correspondante dans le cadre principal.

Dans des systèmes comportant plusieurs XSCF, l'élément de menu [Switch Over] est disponible et permet de passer de l'un à l'autre. Pour un aperçu de chaque page correspondant à un élément de menu, consultez « [C.3 Pages disponibles](#) ».

Figure C-2 montre un exemple d'écran affiché lorsque l'onglet [Physical] est sélectionné dans le cadre de menu.

Figure C-2 Arborescence des composants physiques



Remarque : la disposition de la fenêtre et le contenu affiché indiqués dans ce manuel constituent un exemple et peuvent être modifiés afin d'en améliorer le fonctionnement ou pour d'autres raisons.

En sélectionnant l'onglet [Physical], les composants du système s'affichent sous forme d'arborescence. Le cadre principal montre les informations et/ou l'état du composant sélectionné dans cette arborescence.

Si l'onglet [Logical] est sélectionné, les composants logiques appartenant à la partition physique sont affichés sous forme d'arborescence. Le cadre principal montre les informations et/ou l'état du composant logique sélectionné dans cette arborescence et appartenant à la partition physique.

L'affichage d'état du composant est le suivant.

Tableau C-3 Affichage d'état du composant

Affichage	Aperçu
	Fonctionne normalement
	Ne fonctionne pas du fait d'une panne
	L'un des états suivants - Continue de fonctionner bien que certains composant soient défectueux ou dégradés - Bien que l'état du composant soit normal, il est en fait dégradé car d'autres composants sont défectueux ou dégradés - Composant sur lequel une maintenance est effectuée

C.3 Pages disponibles

Cette section fournit un aperçu des pages disponibles dans le cadre principal. Les fonctions de chaque page sont les mêmes que celles des commandes du shell XSCF. Pour des informations plus détaillées sur chaque fonction, consultez « [Chapitre 3 Configuration du système](#) », les chapitres traitant des commandes correspondantes ou le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

C.3.1 Pages indiquant l'état du système, les partitions physiques et les domaines logiques

[Tableau C-4](#) répertorie les fonctions disponibles pour afficher les informations relatives au système. Sélectionnez [Menu] - [Status] - [System Overview].

Tableau C-4 Informations du système

Élément	Aperçu	Commande correspondante
Nom du produit	Affiche le nom du serveur.	showhardconf(8)
Numéro de série	Affiche le numéro de série du système.	
État du commutateur de mode du système	Affiche l'état du commutateur de mode sur le panneau de commande.	
Type d'alimentation en entrée	Affiche le type d'alimentation en entrée.	
État de l'alimentation	Affiche l'état activé/désactivé (on/off) de l'alimentation en entrée.	
Phase d'alimentation	Affiche la phase d'alimentation du système.	

Tableau C-4 Informations du système (*suite*)

Élément	Aperçu	Commande correspondante
Version de XSCF	Affiche la version du microprogramme du XSCF.	version(8)
État du châssis	Indique quels sont les châssis maître et de veille.	showbbstatus(8)
Heure du système	Affiche l'heure du système.	showdate(8)
Composants en panne	Affiche les composants défectueux ou dégradés.	showstatus(8)
Température	Affiche la température de l'air d'admission du châssis.	showenvironment(8)
Évacuation d'air	Affiche la quantité d'air évacué du châssis.	showenvironment(8)
État de la limitation de l'alimentation	Indique si la fonction de limitation de l'alimentation, qui permet de réduire la consommation électrique du système, est activée ou désactivée.	showpowercapping(8)

Tableau C-5 répertorie les fonctions disponibles permettant d'afficher l'état de chaque composant du système. Sélectionnez [Menu] - [Status] - [System Status].

Tableau C-5 État du composant

Élément	Aperçu	Commande correspondante
Consommation électrique Température Tension Informations sur le ventilateur	Affiche la consommation électrique, la température de l'air évacué, la tension et la vitesse du ventilateur de chaque composant.	showenvironment(8)

Tableau C-6 répertorie les fonctions disponibles permettant d'afficher l'état de chaque partition physique. Sélectionnez [Menu] - [Status] - [PPAR Status].

Tableau C-6 État de la partition physique

Élément	Aperçu	Commande correspondante
Affichage sous forme de liste de la configuration de PPAR	Affiche les numéros de carte système physique (PSB) correspondant aux numéros de carte de système logique (LSB) de chaque PPAR sous forme de tableau.	showpcl(8)
État de la PPAR	Affiche l'état de fonctionnement de la PPAR et sa stratégie de configuration.	showpcl(8)
Informations de PSB	Affiche les informations relatives à la carte système physique (PSB).	showboards(8)

Tableau C-7 répertorie les fonctions disponibles permettant d'afficher l'état de la carte système physique (PSB). Sélectionnez [Menu] - [Status] - [PSB Status].

Tableau C-7 État de la PSB

Élément	Aperçu	Commande correspondante
État de la PSB	Affiche une liste d'états détaillée comprenant les ID de chaque PPAR auxquelles des PSB sont intégrées.	showboards(8)

Tableau C-8 répertorie les fonctions disponibles permettant d'afficher l'état du domaine logique. Sélectionnez [Menu] - [Status] - [Domain Status].

Tableau C-8 État du domaine logique

Élément	Aperçu	Commande correspondante
État du domaine logique	Affiche l'état de fonctionnement de chaque domaine logique appartenant à la PPAR spécifiée.	showdomainstatus(8) showpparstatus(8)

C.3.2 Pages permettant d'utiliser une partition physique

Tableau C-9 répertorie les fonctions disponibles permettant de gérer l'alimentation des partitions physiques. Sélectionnez [Menu] - [PPAR Operation] - [PPAR Power].

Tableau C-9 Opérations d'alimentation de la partition physique

Élément	Aperçu	Commande correspondante
Mise sous/hors tension du système	Indique s'il faut mettre le système (toutes les partitions physiques) sous ou hors tension.	showpparstatus(8) poweron(8) poweroff(8)
Mise sous/hors tension ou réinitialisation de la PPAR	Effectue les opérations suivantes sur la PPAR spécifiée : - Mise sous/hors tension - Mise hors tension forcée - por : réinitialisation de la PPAR - panic : instruction de panique aux domaines logiques - sir : réinitialisation du domaine logique - xir : réinitialisation du processeur - Envoi d'un signal d'arrêt	showpparstatus(8) poweron(8) poweroff(8) reset(8) sendbreak(8)

Tableau C-10 répertorie les fonctions disponibles permettant de paramétrer le mode de fonctionnement d'une partition physique. Sélectionnez [Menu] - [PPAR Operation] - [PPAR Mode Configuration].

Tableau C-10 Mode de fonctionnement d'une partition physique

Élément	Aperçu	Commande correspondante
Affichage/ configuration du mode de la PPAR	Affiche/configure les modes suivants pour la PPAR spécifiée : - ID de l'hôte - Niveau du diagnostic matériel - Niveau des messages de diagnostic - Fonction de vérification d'activité activée/désactivée - Opération lors de l'expiration de la surveillance d'hôte - Suppression de l'envoi d'un signal d'arrêt - Fonction de démarrage automatique de domaine logique activée/désactivée - Fonctionnement en consommation réduite activé/désactivé - Réorganisation du chemin d'E/S - Fonction DR actuellement activée/désactivée - Fonction DR activée/désactivée lors du prochain démarrage - Adresse Ethernet de la PPAR (adresse mac)	showpparmode(8) setpparmode(8)

Remarque : pour des informations complémentaires concernant les fonctions de vérification d'activité et DR entre le XSCF et le superviseur, consultez les dernières *Notes de produit* pour votre serveur.

Tableau C-11 répertorie les fonctions disponibles permettant de configurer les partitions physiques. Sélectionnez [Menu] - [PPAR Operation] - [PPAR Configuration].

Tableau C-11 Paramètres de partition physique

Élément	Aperçu	Commande correspondante
Affichage sous forme de liste de la configuration de PPAR	Affiche la PCL de la carte système (PSB) PPAR spécifiée. Cette fonction affiche/paramètre également la stratégie de configuration de la PPAR. Sur le SPARC M12-1/M12-2/M10-1/M10-4, elle peut uniquement afficher des informations et définir la stratégie de configuration de PPAR-ID 00.	showpcl(8) setpcl(8)
Configuration de la liste de configuration de la partition physique (PCL)	Paramètre la PCL. Cette fonction associe une LSB de PPAR à une PSB et définit les informations de configuration d'une LSB. Le SPARC M12-1/M12-2/M10-1/M10-4 ne prend pas cette fonction en charge.	showpcl(8) setpcl(8)

Tableau C-11 Paramètres de partition physique (*suite*)

Élément	Aperçu	Commande correspondante
Ajout, suppression ou paramétrage de PSB	Donne des instructions permettant de modifier la configuration d'une PSB pour une PPAR de la manière suivante : - Mettre de côté ou intégrer une PSB (BB) à une PPAR - Retirer une PSB (BB) d'une PPAR - Déplacer une PSB (BB) d'une PPAR à une autre Effectuez les opérations mentionnées ci-dessus en suivant les procédures décrites dans le <i>Guide de configuration du domaine Fujitsu SPARC M12 et Fujitsu M10/SPARCM10</i>. Le SPARC M12-1/M12-2/M10-1/M10-4 ne prend pas cette fonction en charge.	addboard(8) deleteboard(8)

Tableau C-12 répertorie les fonctions disponibles permettant de configurer le mode de mise en miroir de la mémoire. Sélectionnez [Menu] - [PPAR Operation] - [PSB Configuration].

Tableau C-12 Paramètres de la carte système

Élément	Aperçu	Commande correspondante
Affichage/paramétrage des informations de mode de mise en miroir de la mémoire	Affiche/paramètre les informations de mode de mise en miroir de la mémoire pour les processeurs d'une carte système (PSB).	showfru(8) setupfru(8)

Tableau C-13 répertorie les fonctions disponibles permettant de définir la configuration d'un domaine logique. Sélectionnez [Menu] - [PPAR Operation] - [Domain Configuration].

Tableau C-13 Paramètres du domaine logique

Élément	Aperçu	Commande correspondante
Affichage des informations de configuration d'un domaine logique	Affiche les informations de configuration d'un domaine logique de la PPAR spécifiée. Les informations de configuration comportent les éléments suivants : - Nom de la configuration - Nombre des domaines logiques composant une PPAR - Date de la configuration Cette fonction affiche également le nom de configuration du domaine logique actuellement en fonctionnement dans la PPAR ainsi que le nom de configuration du domaine logique suivant à fonctionner.	showdomainconfig(8)

Tableau C-13 Paramètres du domaine logique (*suite*)

Élément	Aperçu	Commande correspondante
Définition de la configuration du domaine logique	Définit une configuration de domaine logique. Cette fonction définit la configuration du prochain domaine logique programmé pour entrer en activité dans la PPAR spécifiée.	setdomainconfig(8)

Tableau C-14 répertorie les fonctions disponibles permettant d'écraser des variables d'environnement OpenBoot PROM pour le domaine de commande d'une partition physique. Sélectionnez [Menu] - [PPAR Operation] - [PPAR Parameter].

Remarque : pour des informations complémentaires sur [PPAR Parameter], consultez les dernières *Notes de produit*.

Tableau C-14 Configuration des variables d'environnement OpenBoot PROM

Élément	Aperçu	Commande correspondante
Affichage/ paramétrage des variables d'environnement OpenBoot PROM de la PPAR	Affiche/écrase les paramètres des variables d'environnement OpenBoot PROM suivantes pour la PPAR spécifiée. - use-nvramrc - security-mode - bootscript	showpparparam(8) setpparparam(8)

Tableau C-15 répertorie les fonctions disponibles pour configurer le démarrage vérifié pour chaque partition physique. Sélectionnez [Menu] - [PPAR Operation] - [Verified Boot].

Tableau C-15 Configuration du démarrage vérifié

Élément	Aperçu	Commande correspondante
Réglage/Affichage de la stratégie	Affiche/Règle la stratégie de démarrage ou de module pour le démarrage vérifié.	showvbootconfig(8) setvbootconfig(8)
Affichage du certificat par défaut du système	Affiche le certificat de clé publique X.509 pré-installé sur le système.	showvbootcerts(8)
Enregistrement/ suppression/ activation/ désactivation d'un certificat de clé publique X.509	Enregistre/supprime un certificat de clé publique X.509 spécifié par un utilisateur. Active/désactive/affiche un certificat de clé publique X.509 spécifié par un utilisateur.	addvbootcerts(8) deletevbootcerts(8) showvbootconfig(8) setvbootconfig(8)

C.3.3 Pages permettant de configurer le serveur

Paramètres du réseau XSCF

Tableau C-16 répertorie les fonctions disponibles permettant de configurer un réseau XSCF. Sélectionnez [Menu] - [Setting] - [Network] - [Current]. Sinon, sélectionnez [Menu] - [Setting] - [Network] - [Reserve]. Les paramètres du réseau sont accessibles depuis le menu [Current] ou [Reserve]. Le menu [Current] affiche les informations relatives au réseau XSCF actuellement utilisé. Vous pouvez vérifier les informations paramétrées sur le menu [Reserve].

Une fois le réseau configuré à l'aide du menu [Current], une transition automatique s'opère vers le menu [Reserve]. Après avoir configuré le réseau, diffusez les paramètres en cliquant sur [Apply] dans le menu [Reserve], puis sur le bouton [Reboot].

Tableau C-16 Paramètres du réseau XSCF

Menu	Élément	Aperçu	Commande correspondante
[Current]	Affichage de l'état/des informations du réseau XSCF, Paramètres du réseau XSCF	Affiche les informations et l'état du réseau XSCF actuellement utilisé. Cette fonction définit également chaque nom d'hôte, nom de domaine, adresse IP et masque de réseau pour les interfaces de réseau XSCF et détermine s'il fait les activer ou les désactiver. Vous pouvez configurer le réseau en cliquant sur le bouton [Edit] pour passer au menu [Reserve]. Vous pouvez vérifier les informations paramétrées à l'aide du menu [Reserve].	shownetwork(8) showhostname (8)
	Affichage/paramétrage de l'accès	Affiche les accès actuels. Cette fonction permet également de les paramétrer. Vous pouvez configurer un accès en cliquant sur le bouton [Edit] pour passer au menu [Reserve]. Vous pouvez vérifier les informations paramétrées à l'aide du menu [Reserve].	shownameserver(8) setnameserver (8)
	Affichage/paramétrage de DNS	Affiche les serveurs de nom actuellement utilisés ainsi que les chemins de recherche. Cette fonction permet également de configurer les serveurs de nom et les chemins de recherche. Vous pouvez configurer le DNS en cliquant sur le bouton [Edit] pour passer au menu [Reserve]. Vous pouvez vérifier les informations paramétrées à l'aide du menu [Reserve].	shownameserver(8) setnameserver (8)

Tableau C-16 Paramètres du réseau XSCF (*suite*)

Menu	Élément	Aperçu	Commande correspondante
[Reserve]	Affichage des informations de configuration du réseau XSCF, Paramètres du réseau XSCF	Affiche les informations de configuration du réseau XSCF. Cette fonction définit également chaque nom d'hôte, nom de domaine, adresse IP et masque de réseau pour les interfaces de réseau XSCF et détermine s'il faut les activer ou les désactiver. Vous pouvez afficher les informations actuellement utilisées pour le fonctionnement en cliquant sur le bouton [Current Status] pour passer au menu [Current].	applynetwork(8) setnetwork(8) sethostname(8)
	Paramétrage des accès/affichage des informations de paramétrage des accès	Affiche les informations de paramétrage des accès. Cette fonction permet également de les paramétrer. Vous pouvez afficher les informations actuellement utilisées pour le fonctionnement en cliquant sur le bouton [Current Status] pour passer au menu [Current].	applynetwork(8) setroute(8)
	Paramétrage du DNS/affichage des informations de paramétrage du DNS	Affiche les informations de paramétrage du serveur de nom et du chemin de recherche. Cette fonction permet également de configurer les serveurs de nom et les chemins de recherche. Vous pouvez afficher les informations actuellement utilisées pour le fonctionnement en cliquant sur le bouton [Current Status] pour passer au menu [Current].	applynetwork(8) setnameserver(8)
	Application des paramètres du réseau	Affiche/diffuse les paramètres du réseau. Une fois les paramètres sauvegardés, un redémarrage du XSCF est nécessaire pour finaliser la procédure.	applynetwork(8) rebootxscf(8)

Remarque : les adresses de liaison SSCP ne peuvent pas être paramétrées/affichées sur XSCF Web. Utilisez les commandes setsscp et showsscp pour paramétrer/afficher ces adresses.

Remarque : les règles de filtrage des paquets IP ne peuvent pas être paramétrées/affichées sur XSCF Web. Utilisez les commandes setpacketfilters et showpacketfilters pour paramétrer/afficher ces règles de filtrage.

Paramètres des fonctions de service individuelles

Tableau C-17 répertorie les fonctions disponibles permettant d'activer/désactiver les fonctions de service individuelles. Sélectionnez [Settings] - [Service] - [Service State].

Tableau C-17 Paramétrage de l'activation/désactivation d'une fonction de service individuelle

Élément	Aperçu	Commande correspondante
Affichage d'état de fonction de service Activation/ désactivation	Affiche sous forme de liste l'état des fonctions de service suivantes. Cette fonction permet également d'activer/désactiver les fonctions de service. - Service HTTPS - Service SNMPv3 - Service SSH - Service Telnet - Service de serveur NTP L'activation/désactivation du service SNMPv3 fait passer l'affichage au menu de configuration SNMP sur lequel vous pouvez configurer l'agent SNMP. En outre, en sélectionnant le service de serveur NTP, vous pouvez activer/désactiver le fonctionnement du XSCF en tant que serveur NTP.	showhttps(8) sethttps(8) showsnmp(8) setsnmp(8) showssh(8) setssh(8) showtelnet(8) settelnet(8) showntp(8) setntp(8)

Tableau C-18 répertorie les fonctions disponibles permettant d'activer/désactiver la fonction de service HTTP. Sélectionnez [Settings] - [Service] - [HTTPS].

Tableau C-18 Paramétrage de l'activation/désactivation de la fonction de service HTTP

Élément	Aperçu	Commande correspondante
Paramétrage de l'activation/ désactivation du service HTTP	Indique si le service HTTPS est activé ou non ou active/désactive ce même service.	showhttps(8) sethttps(8)

Remarque : XSCF Web ne peut être utilisé lorsque le service HTTPS est désactivé. Pour activer le service HTTPS, utilisez la commande sethttps.

Tableau C-19 répertorie les fonctions disponibles permettant d'activer/désactiver la fonction de service SSH. Sélectionnez [Settings] - [Service] - [SSH].

Tableau C-19 Paramétrage de l'activation/désactivation de la fonction de service SSH

Élément	Aperçu	Commande correspondante
Paramétrage de l'activation/désactivation du service SSH	Indique si le service SSH est activé ou non ou active/désactive ce même service.	showssh(8) setssh(8)

Remarque : XSCF Web ne prend pas en charge la génération d'une clé d'hôte, l'enregistrement/suppression d'une clé publique d'utilisateur et les paramètres d'expiration du shell XSCF. Utilisez les commandes showssh et setssh pour paramétrer ces fonctions.

Tableau C-20 répertorie les fonctions disponibles permettant d'activer/désactiver la fonction de service Telnet. Sélectionnez [Settings] - [Service] - [Telnet].

Tableau C-20 Paramétrage de l'activation/désactivation de la fonction de service Telnet

Élément	Aperçu	Commande correspondante
Paramétrage de l'activation/désactivation du service Telnet	Indique si le service Telnet est activé ou non ou active/désactive ce même service.	showtelnet(8) settelnet(8)

Tableau C-21 répertorie les fonctions disponibles permettant de configurer la fonction de service NTP du XSCF. Sélectionnez [Settings] - [Service] - [NTP].

Tableau C-21 Paramètres de la fonction de service NTP

Élément	Aperçu	Commande correspondante
Affichage/paramétrage de l'activation/désactivation du serveur NTP	Indique/définit si le fonctionnement du XSCF en tant que serveur NTP est activé ou non.	showntp(8) setntp(8)
Affichage/paramétrage de l'activation/désactivation du client NTP	Indique/définit si le fonctionnement du XSCF en tant que client NTP est activé ou non.	
Paramètres du serveur NTP	Affiche/définit les éléments suivants pour les paramètres du serveur NTP utilisé par le réseau XSCF : - Serveurs NTP (jusqu'à trois) - Priorité du serveur (préférence) - Valeur de couche (stratum) - Pour finaliser le paramètre de l'adresse d'horloge locale du XSCF, il est nécessaire de redémarrer le XSCF. Un redémarrage du XSCF est nécessaire pour finaliser la procédure de réglage.	

Tableau C-22 répertorie les fonctions disponibles permettant de configurer la fonction de service SMTP du XSCF. Sélectionnez [Settings] - [Service] - [SMTP].

Tableau C-22 Paramètres de la fonction de service SMTP

Élément	Aperçu	Commande correspondante
Affichage/ paramétrage du serveur SMTP	Affiche/configure l'adresse du serveur SMTP, l'algorithme d'authentification, l'adresse du serveur POP, l'adresse de destination des e-mails d'erreur ainsi que d'autres informations relatives au serveur SMTP.	showsmtp(8) setsmtp(8)

Tableau C-23 répertorie les fonctions disponibles permettant de configurer la fonction d'agent SNMP du XSCF. Sélectionnez [Settings] - [Service] - [SNMP].

Tableau C-23 Paramètres de la fonction d'agent SNMP

Élément	Aperçu	Commande correspondante
Affichage/ paramétrage de l'agent SNMPv3	Indique/définit si l'agent SNMPv3 est activé ou non. Cette fonction affiche/configure également un fichier de définition de la MIB, les informations de gestion du système, etc.	showsnmp(8) setsnmp(8)
Affichage/ paramétrage de l'agent SNMPv1/v2c	Indique/définit si l'agent SNMPv1/v2c est activé ou non. Cette fonction affiche/configure également les chaînes de communauté.	
Affichage/ paramétrage d'hôte d'interruption	Affiche sous forme de liste les hôtes d'interruption de SNMPv1/v2c et SNMPv3. Cette fonction permet également d'afficher/configurer les noms d'hôtes de destination d'interruption, les numéros de port et d'autres informations sur l'hôte.	

Tableau C-24 répertorie les fonctions disponibles permettant de configurer la fonction de sécurité pour SNMPv3. Sélectionnez [Settings] - [Service] - [SNMP Security].

Tableau C-24 Paramètres de la fonction de sécurité SNMP

Élément	Aperçu	Commande correspondante
Affichage/ paramétrage des informations de gestion USM	Affiche/paramètre les informations de gestion USM telles que l'algorithme d'authentification de l'utilisateur. Pour plus de détails sur les informations de gestion USM, consultez Tableau 10-5 .	showsnmpusm(8) setsnmpusm(8)
Affichage/ paramétrage de l'agent SNMPv1/v2c	Affiche/configure les informations de gestion VACM comme les groupes de contrôle d'accès et les visualisations de contrôle d'accès. Pour plus de détails sur les informations de gestion VACM, consultez Tableau 10-5 .	showsnmpvacm(8) setsnmpvacm(8)

Paramètres du compte d'utilisateur

Tableau C-25 répertorie les fonctions disponibles permettant de configurer des comptes d'utilisateurs locaux de XSCF. Sélectionnez [Settings] - [User Manage] - [Account].

Tableau C-25 Paramètres du compte d'utilisateur

Élément	Aperçu	Commande correspondante
Affichage des informations du compte d'utilisateur	Affiche les informations et l'état des comptes d'utilisateurs actuellement enregistrés ; le privilège useradm est requis.	showuser(8)
Ajout/suppression de compte d'utilisateur	Ajoute/supprime des comptes d'utilisateurs. Le privilège useradm est requis.	adduser(8) deleteuser(8)
Activation/désactivation de compte d'utilisateur	Désactive des comptes d'utilisateurs actuellement enregistrés et les réactive. Le privilège useradm est requis.	disableuser(8) enableuser(8)
Affichage/modification des informations du compte d'utilisateur	Affiche les informations relatives à un compte d'utilisateur donné et modifie le mot de passe, les privilèges d'utilisateur ainsi que la stratégie de mot de passe. Le privilège useradm est requis.	showuser(8) password(8) setprivileges(8)
Affichage des informations du compte d'utilisateur local/modification du mot de passe	Avec tout autre privilège que useradm, vous pouvez afficher les informations relatives à un compte d'utilisateur local et modifier le mot de passe.	showuser(8) password(8)
Affichage/paramétrage de la stratégie de mot de passe du système	Affiche la stratégie de mot de passe actuelle du système. Cette fonction définit également la stratégie de mot de passe du système à appliquer ultérieurement.	showpasswordpolicy(8) setpasswordpolicy(8)

Remarque : XSCF Web ne prend pas en charge la fonction de verrouillage, qui bloque l'accès à un compte d'utilisateur après trois échecs d'identification successifs. Utilisez les commandes setloginlockout et showloginlockout pour la fonction de verrouillage du shell XSCF.

Paramètres du service LDAP

Tableau C-26 répertorie les fonctions disponibles permettant de configurer un client LDAP. Sélectionnez [Settings] - [User Manage] - [LDAP].

Tableau C-26 Paramètres du service LDAP

Élément	Aperçu	Commande correspondante
Affichage/enregistrement d'un serveur LDAP	Affiche/enregistre un serveur LDAP avec le XSCF configuré comme un client LDAP.	showldap(8) setldap(8)

Tableau C-26 Paramètres du service LDAP (*suite*)

Élément	Aperçu	Commande correspondante
Affichage/ importation d'un certificat	Affiche/importe le certificat du serveur LDAP.	

Paramètres du service LDAP sur SSL

[Tableau C-27](#) répertorie les fonctions disponibles permettant de configurer un client LDAP sur SSL. Sélectionnez [Settings] - [User Manage] - [LDAP/SSL].

Tableau C-27 Paramètres du service LDAP sur SSL

Élément	Aperçu	Commande correspondante
Affichage/ enregistrement du serveur LDAP sur SSL	Affiche/enregistre un serveur LDAP sur SSL avec le XSCF configuré comme un client LDAP sur SSL.	showldapssl(8) setldapssl(8)
Affichage/ paramétrage de usermap	Affiche/définit le usermap.	
Affichage/ paramétrage de certificat	Affiche/charge/supprime les certificats du serveur LDAP sur SSL.	
Affichage/ paramétrage de defaultrole	Affiche/définit les privilèges attribués à tous les utilisateurs authentifiés via LDAP sur SSL.	
Affichage/ paramétrage des serveurs alternatifs	Affiche/définit jusqu'à cinq serveurs LDAP sur SSL alternatifs.	
Affichage/ paramétrage des groupes	Affiche/définit le groupe d'administrateurs, le groupe d'opérateurs et le groupe d'utilisateurs.	
Affichage/ paramétrage du domaine d'utilisateur	Affiche/définit jusqu'à cinq domaines d'utilisateur.	

Paramètres du service Active Directory

[Tableau C-28](#) répertorie les fonctions disponibles permettant de configurer un client Active Directory. Sélectionnez [Settings] - [User Manage] - [Active Directory].

Tableau C-28 Paramètres du service Active Directory

Élément	Aperçu	Commande correspondante
Affichage/ paramétrage du serveur Active Directory	Active/désactive Active Directory avec le XSCF configuré comme client. Affiche/définit le serveur, le mode, le délai de déconnexion, le journal, les paramètres par défaut, etc.	showad(8) setad(8)
Affichage/ paramétrage de certificat	Affiche/charge/supprime les certificats du serveur Active Directory.	
Affichage/ paramétrage de defaultrole	Affiche/définit les privilèges attribués à tous les utilisateurs authentifiés via Active Directory.	
Affichage/ paramétrage des serveurs alternatifs	Affiche/définit jusqu'à cinq serveurs Active Directory alternatifs, et affiche/charge/supprime les certificats de serveur.	
Affichage/ paramétrage des groupes	Affiche/définit le groupe d'administrateurs, le groupe d'opérateurs et le groupe d'utilisateurs.	
Affichage/ paramétrage du domaine d'utilisateur	Affiche/définit jusqu'à cinq domaines d'utilisateur.	
Affichage/ paramétrage de requête d'index DNS	Affiche/définit jusqu'à cinq requêtes d'index DNS.	

Paramétrage de la déconnexion automatique

Tableau C-29 répertorie les fonctions disponibles permettant de configurer l'expiration de la session XSCF Web (déconnexion automatique). Sélectionnez [Settings] - [Autologout] - [Account]. Lorsque le délai de déconnexion automatique (en minutes) est défini et que des utilisateurs se connectent à XSCF Web, ils sont déconnectés automatiquement s'ils n'y accèdent pas pendant le délai défini.

Tableau C-29 Paramétrage de la déconnexion automatique

Élément	Aperçu	Commande correspondante
Affichage/ paramétrage du délai de déconnexion automatique	Affiche le délai de déconnexion automatique actuellement défini (en minutes) ou en définit un. La valeur par défaut est 10 minutes. Vous pouvez indiquer une valeur comprise entre 1 et 255.	Cela est uniquement pris en charge par XSCF Web.

Remarque : XSCF Web ne prend pas en charge le paramétrage de délai de déconnexion automatique du shell XSCF. Utilisez les commandes showautologout et setautologout.

Paramétrage d'activation du processeur (CPU)

Tableau C-30 répertorie les fonctions disponibles permettant de définir une activation du processeur. Sélectionnez [Settings] - [CoD Reservation].

Tableau C-30 Paramétrage d'activation du processeur (CPU)

Élément	Aperçu	Commande correspondante
Utilisation des ressources de cœur de processeur	Affiche l'utilisation des ressources de cœur de processeur. L'affichage s'opère comme suit : - Ressource (processeur) - Partitions physiques (PPAR) individuelles	showcodusage(8)
Affichage/paramétrage de l'attribution d'activation du processeur	Affiche l'état d'attribution d'activation de processeur pour chaque PPAR. Cette fonction détermine également quelle PPAR voit augmenter ou réduire le nombre d'activations de processeur pour les ressources.	showcod(8) setcod(8)

Tableau C-31 répertorie les fonctions disponibles permettant d'enregistrer une clé d'activation du processeur. Sélectionnez [Settings] - [CoD Activation].

Tableau C-31 Enregistrement de la clé d'activation de processeur

Élément	Aperçu	Commande correspondante
Affichage/paramétrage des informations de clé d'activation de processeur	Affiche les informations relatives à la clé d'activation de processeur actuellement enregistrée.	showcodactivation(8)
Ajout/suppression de clé d'activation de processeur	Ajoute/supprime des clés d'activation de processeur.	addcodactivation(8) deletecodactivation(8)
Historique d'enregistrement de clé d'activation de processeur	Affiche les données d'historique concernant l'ajout et la suppression de clés d'activation de processeur.	showcodactivationhistory(8)

Paramètres de l'audit

Tableau C-32 répertorie les fonctions disponibles permettant de configurer les paramètres d'audit de XSCF. Sélectionnez [Settings] - [Audit].

Tableau C-32 Paramètres de l'audit

Élément	Aperçu	Commande correspondante
État d'utilisation du journal d'audit (pistes d'audit) / archivage de données / suppression de données	Affiche la capacité d'utilisation d'un journal d'audit. Cette fonction archive également un journal d'audit (*1) et supprime les fichiers secondaires.	showaudit(8) setaudit(8)
Activation/désactivation de l'audit	Indique/définit si l'audit est activé ou non.	
Affichage/paramétrage de la stratégie d'audit	Affiche/détermine la stratégie appliquée lorsque le journal d'audit atteint la pleine capacité (*2), le seuil d'avertissement pour la quantité de journaux d'audit locaux (en %) ainsi que l'adresse de destination des e-mails d'avertissement.	
Affichage/paramétrage de la stratégie d'utilisateur globale	Détermine si la stratégie d'utilisateur globale doit ou non être activée.	
Affichage/ajout/modification de la stratégie de génération d'enregistrements d'audit d'utilisateur	Affiche sous forme de liste les stratégies de génération d'enregistrements d'audit propres à l'utilisateur (génération d'enregistrement d'audit activée/désactivée). Cette fonction ajoute également des stratégies de génération d'enregistrements d'audit pour les utilisateurs. Avec les stratégies ajoutées, la stratégie d'utilisateur globale est désactivée pour ces utilisateurs. La stratégie de génération d'enregistrements d'audit est activée/désactivée par l'utilisateur spécifié, qui indique s'il y a lieu d'activer la stratégie d'utilisateur globale.	
Affichage/paramétrage de la classe/de l'évènement d'audit	Affiche les événements et les classes d'audit. Cette fonction détermine également si les événements et classes d'audit doivent être activés ou non.	

*1 L'archivage des journaux d'audit n'est pas pris en charge actuellement.

*2 Lorsqu'un journal d'audit atteint la pleine capacité, seule la stratégie d'audit « count », qui supprime les enregistrements d'audit, est actuellement prise en charge. Par conséquent, ne spécifiez pas « suspend ».

Paramètres d'e-mail

Tableau C-33 répertorie les fonctions disponibles permettant de configurer les paramètres d'e-mail de XSCF. Sélectionnez [Settings] - [Email Reporting].

Tableau C-33 Paramètres d'e-mail

Élément	Aperçu	Commande correspondante
Affichage/ paramétrage de la fonction de notification par e-mail	Affiche/paramètre les informations de configuration de la fonction de notification par e-mail. Cette fonction active/désactive la fonction de notification par e-mail et affiche/définit l'adresse de destination des notifications par e-mail envoyées à l'administrateur système.	showemailreport(8) setemailreport(8)

Paramètres de l'heure

Tableau C-34 répertorie les fonctions disponibles permettant de paramétrer l'heure et le fuseau horaire du système. Sélectionnez [Settings] - [Time].

Tableau C-34 Paramètres de l'heure

Élément	Aperçu	Commande correspondante
Affichage/réglage de l'heure du système	Affiche/paramètre l'heure et le fuseau horaire actuels du système. Une fois le réglage effectué, le XSCF est redémarré. Connectez-vous à nouveau. Si l'heure du système est synchronisée sur un serveur NTP, elle ne peut pas être modifiée.	showdate(8) setdate(8) showtimezone(8) settimezone(8)

Remarque : l'heure d'été ne peut pas être paramétrée sur XSCF Web. Utilisez les commandes showtimezone et settimezone pour effectuer ce réglage.

Paramètres de consommation électrique

Tableau C-35 répertorie les fonctions disponibles permettant de définir une limite de consommation électrique du système. Sélectionnez [Settings] - [Power Capping].

Tableau C-35 Paramètres de consommation électrique

Élément	Aperçu	Commande correspondante
Affichage/définition de la limite de consommation électrique	Affiche le paramètre de limitation de la consommation électrique. Cette fonction permet également d'activer/désactiver cette limitation, d'en définir la valeur maximale, etc.	showpowercapping(8) setpowercapping(8)

Paramétrage de la planification d'alimentation

Tableau C-36 répertorie les fonctions disponibles permettant de configurer une planification d'alimentation. Sélectionnez [Settings] - [Power Schedule].

Tableau C-36 Paramétrage de la planification d'alimentation

Élément	Aperçu	Commande correspondante
Affichage d'état du paramétrage de planification d'alimentation	Affiche sous forme de liste l'état des planifications d'alimentation d'une PPAR.	showpowerschedule(8)
Paramétrage de la planification d'alimentation	Définit une planification d'alimentation. Cette fonction active/désactive la planification et permet d'effectuer des réglages concernant : - Partitions physiques (PPAR) individuelles - Toutes les PPAR	setpowerschedule(8)
Affichage des informations de planification d'alimentation	Affiche les prochaines heures de mise sous/hors tension par PPAR.	showpowerschedule(8)
Informations détaillées sur la planification d'alimentation	Affiche /paramètre les détails concernant les informations de planification d'alimentation. Cette fonction affiche/ajoute/modifie/supprime les planifications pour : - Partitions physiques (PPAR) individuelles - Toutes les PPAR	showpowerschedule(8) setpowerschedule(8) addpowerschedule(8) deletepowerschedule(8)

Paramètres de périphérique

Tableau C-37 répertorie les fonctions disponibles permettant de définir les informations de l'unité d'extension PCI et les informations sur les cartes connectées aux serveurs. Sélectionnez [Settings] - [Add-In Card Manager].

Tableau C-37 Paramétrage des informations sur l'unité d'extension PCI

Élément	Aperçu	Commande correspondante
Affichage des informations du capteur de carte/unité d'extension PCI	Cette fonction affiche sous forme de liste les informations du capteur par : - Carte PCI (connectée au serveur) - Unité d'extension PCI - FRU dans l'unité d'extension PCI	ioxadm(8)
Affichage des informations du périphérique/paramétrage de l'alimentation	Affiche sous forme de liste les informations sur les périphériques comme les cartes PCI, les unités d'extension PCI et les cartes de liaison. Cette fonction donne également des instructions de mise sous/hors tension aux unités d'alimentation électrique dans l'unité d'extension PCI.	
Initialisation des composants de surveillance	Initialise les composants de surveillance de l'unité d'extension PCI.	

Tableau C-37 Paramétrage des informations sur l'unité d'extension PCI (*suite*)

Élément	Aperçu	Commande correspondante
Mise à jour du microprogramme	Vérifie, enregistre et met à jour le microprogramme de l'unité d'extension PCI et de la carte de liaison.	
Affichage/paramétrage des états des DEL de l'unité d'extension PCI	Affichage/paramétrage de l'état des DEL de localisation de FRU dans l'unité d'extension PCI.	

Remarque : si les deux unités d'alimentation électrique de l'unité d'extension PCI sont mises hors tension, l'unité d'extension PCI ne peut plus être mise sous tension via XSCF Web ou le shell XSCF. Pour la remettre sous tension, vous devez appuyer sur le bouton d'alimentation physique POWER.

Paramétrage de la fonction d'E/S directe de l'unité d'extension PCI

Tableau C-38 répertorie les fonctions disponibles pour configurer la fonction d'E/S directe de l'unité d'extension PCI. Sélectionnez [Settings] - [PCIBOX DIO].

Tableau C-38 Paramétrage de la fonction d'E/S directe de l'unité d'extension PCI

Élément	Aperçu	Commande correspondante
Activation/désactivation de la fonction d'E/S directe.	Affiche/définit si la fonction d'E/S directe de l'unité d'extension PCI est activée ou désactivée pour chaque emplacement PCI du châssis du SPARC M12/M10.	showpciboxdio(8) setpciboxdio(8)

Paramètres du stockage à distance

Tableau C-39 répertorie les fonctions disponibles permettant de configurer le stockage à distance. Sélectionnez [Settings] - [Remote Storage].

Tableau C-39 Paramètres du stockage à distance

Élément	Aperçu	Commande correspondante
Démarrage du serveur de stockage à distance	Démarrez Java Runtime Environment pour démarrer le serveur de stockage à distance.	Non

Tableau C-39 Paramètres du stockage à distance (*suite*)

Élément	Aperçu	Commande correspondante
Affichage/définition du statut de la connexion au stockage à distance	Affiche les informations de connexion au stockage à distance dans une liste. - Interface XSCF-LAN - XSCF-LAN, adresse IP, masque de réseau, passerelle - Statut de connexion/adresse IP du terminal de gestion du système Sélectionnez également l'interface XSCF-LAN et connectez-vous au support/déconnectez le support/spécifiez une adresse IP/configurez un XSCF esclave pour le terminal de gestion du système.	setremotestorage(8) showremotestorage(8)

C.3.4 Pages relatives à la maintenance du serveur

Informations sur la connexion réseau

Tableau C-40 répertorie les fonctions disponibles pour afficher les informations relatives à la connexion réseau. Sélectionnez [Maintenance] - [Network Tools]. Les menus [Ping], [Traceroute], et [Nslookup], lorsque sélectionnés, affichent respectivement le temps de réponse de l'hôte, l'itinéraire réseau vers l'hôte, et les informations sur le nom d'hôte.

Tableau C-40 Affichage des informations sur la connexion réseau

Élément	Aperçu	Commande correspondante
Affichage du temps de réponse de l'hôte	Affiche l'état de la réponse réseau entre le XSCF et l'hôte spécifié.	ping(8)
Affichage de l'itinéraire réseau	Affiche des informations sur l'itinéraire réseau vers l'hôte ou le périphérique spécifié.	traceroute(8)
Affichage des informations de nom d'hôte	Affiche des informations sur le nom de l'hôte spécifié.	nslookup(8)

Sauvegarde/restauration des informations des réglages de XSCF

Tableau C-41 répertorie les fonctions disponibles permettant de sauvegarder/restaurer les informations des réglages de XSCF. Sélectionnez [Maintenance] - [Configuration Management].

Tableau C-41 Sauvegarde/restauration des informations des réglages de XSCF

Élément	Aperçu	Commande correspondante
Sauvegarde/ restauration des informations de réglage	Les informations des réglages de XSCF ou les clés d'activation de processeur sont sauvegardées/restaurées. Le XSCF est redémarré lorsque ces informations sont sauvegardées/restaurées à l'aide du bouton [Run]. Connectez-vous à nouveau.	dumpconfig(8) restoreconfig(8) dumpcodactivation(8) restorecodactivation(8)

Mise à jour du microprogramme

Tableau C-42 répertorie les fonctions disponibles permettant de mettre à jour le microprogramme XCP. Sélectionnez [Maintenance] - [Firmware Update].

Tableau C-42 Mise à jour du microprogramme

Élément	Aperçu	Commande correspondante
Affichage de version	Affiche les versions du microprogramme suivantes : - Version de XCP - Version du microprogramme XSCF - Version du microprogramme CMU	version(8)
Importation de XCP	Indique parmi les fichiers de microprogramme suivants ceux qui permettent d'importer le microprogramme sur le serveur : - Fichier de microprogramme XCP - Fichier de microprogramme de l'unité d'extension PCI	getflashimage(8)
Mise à jour du microprogramme	Effectue une mise à jour de XCP. À ce moment-là, le XSCF a redémarré, connectez-vous donc de nouveau au XSCF.	flashupdate(8)
Concordance des versions (pour les systèmes comprenant plusieurs XSCF)	Fait concorder les versions de microprogramme XCP dans un système comprenant plusieurs XSCF. Utilisez cette fonction après le remplacement d'une unité XSCF, d'une CMU, d'un châssis ou d'un autre composant.	flashupdate(8)

Redémarrage de XSCF

Tableau C-43 répertorie les fonctions disponibles permettant de redémarrer le XSCF. Sélectionnez [Maintenance] - [Reboot XSCF].

Tableau C-43 Redémarrage de XSCF

Élément	Aperçu	Commande correspondante
Redémarrage de XSCF	Redémarre le XSCF local.	rebootxscf(8)
Redémarrage du XSCF cible (pour les systèmes comprenant plusieurs XSCF)	Indique le BB-ID du châssis disposant de XSCF pour redémarrer le châssis. - Tous les châssis - Châssis spécifié	showbbstatus(8) rebootxscf(8)

Basculement de XSCF

Tableau C-44 répertorie la fonction disponible permettant de basculer entre les XSCF dans un système avec plusieurs XSCF. Sélectionnez [Maintenance] - [Switch Over].

Tableau C-44 Basculement de XSCF

Élément	Aperçu	Commande correspondante
Passage d'un XSCF à l'autre (pour les systèmes comprenant plusieurs XSCF)	Bascule le XSCF du maître au boîtier de veille ou inversement.	switchscf(8)

Sauvegarde des informations du serveur

Tableau C-45 répertorie les fonctions disponibles permettant de recueillir des informations sur le serveur et d'analyser/résoudre les problèmes du système. Sélectionnez [Maintenance] - [Switch Over].

Tableau C-45 Sauvegarde des informations du serveur

Élément	Aperçu	Commande correspondante
Sauvegarde des informations du serveur/ sauvegarde des informations du châssis cible (pour les systèmes comprenant plusieurs XSCF)	Indique le BB-ID cible pour recueillir des données comme la configuration du serveur, les journaux de système commun ainsi que de châssis, et sauvegarder les données sur un fichier. - Tous les châssis - Châssis spécifié	snapshot(8)

Remarque : dans les systèmes comprenant plusieurs XSCF, vous pouvez sauvegarder les informations du serveur sur la page affichée après la connexion au XSCF de veille.

Paramètres de la fonction ASR

Tableau C-46 Paramètres de la fonction ASR

Élément	Aperçu	Commande correspondante
Activation/ désactivation de la fonction ASR (étiquette de service) (*1)	Indique/définit si l'étiquette de service est activée ou non.	showservicetag(8) setservicetag(8)
Test d'activité	Génère des erreurs fictives dans le Ops Center et le gestionnaire ASR, ou vérifie s'ils sont en activité.	

*1 La fonction ASR est un service de maintenance à distance qui utilise le logiciel Oracle Auto Service Request fourni par l'entreprise Oracle. Pour plus d'informations sur la fonction ASR, consultez le *Oracle Auto Service Request Installation and Operations Guide* relatif à la version du logiciel que vous utilisez.

C.3.5 Pages d'affichage des journaux

Tableau C-47 répertorie les fonctions disponibles permettant de consulter les informations des journaux. Sélectionnez [Logs]. Sélectionnez le journal souhaité.

Tableau C-47 Informations des journaux

Élément	Aperçu	Commande correspondante
Affichage du journal d'erreur	Affiche le journal d'erreur. Vous pouvez effectuer une recherche dans ce journal.	showlogs(8) error option
Affichage du journal d'alimentation	Affiche le journal d'alimentation. Vous pouvez effectuer une recherche dans ce journal.	showlogs(8) power option
Affichage du journal des événements	Affiche le journal des événements. Vous pouvez effectuer une recherche dans ce journal.	showlogs(8) event option
Affichage du journal de la console	Affiche le journal de la console. Vous pouvez effectuer une recherche dans ce journal.	showlogs(8) console option
Affichage du journal de panique	Affiche le journal de panique. Vous pouvez effectuer une recherche dans ce journal.	showlogs(8) panic option
Affichage du journal de l'historique de température (journal d'environnement)	Indique le BB-ID du châssis pour lequel le journal de l'historique de température est affiché. Vous pouvez effectuer une recherche dans ce journal.	showlogs(8) env option
Affichage du journal des messages IPL	Indique la PPAR pour laquelle le journal IPL est affiché. Vous pouvez effectuer une recherche dans ce journal.	showlogs(8) ipl option

Tableau C-47 Informations des journaux (*suite*)

Élément	Aperçu	Commande correspondante
Affichage du journal des messages de surveillance	Affiche le journal des messages de surveillance. Vous pouvez effectuer une recherche dans ce journal.	showlogs(8) monitor option
Affichage du journal d'audit	Affiche le journal d'audit. Il vous est possible de spécifier une période, une date, un utilisateur et une classe pour vous y référer dans le journal.	viewaudit(8)

Informations sur la MIB de XSCF

Cette annexe résume la base d'informations de gestion (MIB) étendue de XSCF, prise en charge par la fonction de l'agent SNMP de XSCF. Pour plus de détails sur la fonction de l'agent SNMP, consultez « [10.3 Surveillance/Gestion de l'état du système avec l'agent SNMP](#) ».

- [Identification d'objet MIB](#)
- [MIB standard](#)
- [MIB étendue](#)
- [Traps](#)

D.1 Identification d'objet MIB

Cette section affiche des exemples d'identifiants d'objets MIB (OID) pris en charge par XSCF.

Internet	OBJECT IDENTIFIER ::=	{ iso org(3) dod(6) 1 }
directory	OBJECT IDENTIFIER ::=	{ internet 1 }
mgmt	OBJECT IDENTIFIER ::=	{ internet 2 }
experimental	OBJECT IDENTIFIER ::=	{ internet 3 }
private	OBJECT IDENTIFIER ::=	{ internet 4 }
mib-2	OBJECT IDENTIFIER ::=	{ mgmt 1 }
system	OBJECT IDENTIFIER ::=	{ mib-2 1 }
interfaces	OBJECT IDENTIFIER ::=	{ mib-2 2 }
at	OBJECT IDENTIFIER ::=	{ mib-2 3 }
ip	OBJECT IDENTIFIER ::=	{ mib-2 4 }

icmp	OBJECT IDENTIFIER ::=	{ mib-2 5 }
tcp	OBJECT IDENTIFIER ::=	{ mib-2 6 }
udp	OBJECT IDENTIFIER ::=	{ mib-2 7 }
snmp	OBJECT IDENTIFIER ::=	{ mib-2 11 }
enterprises	OBJECT IDENTIFIER ::=	{ private 1 }
fujitsu	OBJECT IDENTIFIER ::=	{ enterprises 211 }
product	OBJECT IDENTIFIER ::=	{ fujitsu 1 }
solaris	OBJECT IDENTIFIER ::=	{ product 15 }
sparc	OBJECT IDENTIFIER ::=	{ solaris 4 }
xscfSpMIB	OBJECT IDENTIFIER ::=	{ sparc 1 }
scfObjects	OBJECT IDENTIFIER ::=	{ xscfSpMIB 1 }
scfInfo	OBJECT IDENTIFIER ::=	{ scfObjects 1 }
scfState	OBJECT IDENTIFIER ::=	{ scfObjects 2 }
scfMonitorInfo	OBJECT IDENTIFIER ::=	{ scfObjects 3 }
scfSystemInfo	OBJECT IDENTIFIER ::=	{ scfObjects 4 }
scfPPARInfo	OBJECT IDENTIFIER ::=	{ scfObjects 5 }
scfPsbInfo	OBJECT IDENTIFIER ::=	{ scfObjects 6 }
scfLsbInfo	OBJECT IDENTIFIER ::=	{ scfObjects 7 }
scfBoardInfo	OBJECT IDENTIFIER ::=	{ scfObjects 8 }
scfCpuInfo	OBJECT IDENTIFIER ::=	{ scfObjects 9 }
scfMemoryInfo	OBJECT IDENTIFIER ::=	{ scfObjects 10 }
scfPciBoxInfo	OBJECT IDENTIFIER ::=	{ scfObjects 11 }
scfComponentInfo	OBJECT IDENTIFIER ::=	{ scfObjects 12 }
scfDomainInfo	OBJECT IDENTIFIER ::=	{ scfObjects 13 }
scfMIBTraps	OBJECT IDENTIFIER ::=	{ xscfSpMIB 2 }
scfMIBTrapPrefix	OBJECT IDENTIFIER ::=	{ scfMIBTraps 0 }
scfMIBTrapData	OBJECT IDENTIFIER ::=	{ scfMIBTraps 1 }
scfMIBConformances	OBJECT IDENTIFIER ::=	{ xscfSpMIB 3 }
scfMIBCompliances	OBJECT IDENTIFIER ::=	{ scfMIBConformances 1 }
scfMIBGroups	OBJECT IDENTIFIER ::=	{ scfMIBConformances 2 }
scfMIBObjectGroups	OBJECT IDENTIFIER ::=	{ scfMIBGroups 1 }

scfMIBNotifGroups	OBJECT IDENTIFIER ::=	{ scfMIBGroups 2 }
scfHwCtrlMIB	OBJECT IDENTIFIER ::=	{ sparceEnterprise 2 }
scfHwCtrlMIBObjects	OBJECT IDENTIFIER ::=	{ scfHwCtrlMIB 1 }
scfHwCtrlPowerMgmt	OBJECT IDENTIFIER ::=	{ scfHwCtrlMIBObjects 1 }

D.2 MIB standard

La MIB standard prise en charge par XSCF se conforme aux RFC suivants (voir remarque). Pour plus d'informations sur le fichier de définition de la MIB standard, consultez les documents RFC généraux.

Exemples de protocoles et de RFC

MIB II	RFC1213
User-based Security Model (USM)	RFC3414
View-based Access Control Model (VACM)	RFC3415
SNMPv2-MIB	RFC3418

Remarque : RFC correspond à Request For Comments. Les RFC sont des spécifications techniques publiées par l'IETF (Internet Engineering Task Force), qui est une organisation permettant d'établir des normes techniques liées à Internet.

D.3 MIB étendue

Le XSCF des systèmes SPARC M12/M10 fournit les informations suivantes, à partir de la MIB étendue de XSCF :

- Informations sur le système, versions du matériel / microprogramme et informations sur la configuration du système
- Informations environnementales (températures, tensions, vitesse du ventilateur, et ainsi de suite)
- États des partitions physiques et informations sur la configuration des partitions physiques

- Informations sur les pannes de composants du système
- Informations relatives aux valeurs d'alimentation du système

Remarque : pour savoir comment obtenir et installer le fichier de définition de la MIB étendue de XSCF, consultez « [10.3 Surveillance/Gestion de l'état du système avec l'agent SNMP](#) ».

D.3.1 Objets de la MIB étendue de XSCF

Cette section décrit les informations de chaque groupe d'objets principaux de la MIB étendue de XSCF.

scfObjects

- Groupe scfInfo
Ce groupe donne des informations générales sur XSCF, telles que sur le XSCF maître, ainsi que des informations sur le XSCF-LAN.
- Groupe scfState
Ce groupe donne des informations sur l'état de XSCF, l'état du commutateur de mode du panneau de commande, etc.
- Groupe scfMonitorInfo
Ce groupe donne des informations sur l'environnement de différents composants du système. Ces informations concernent le nom du composant, la température, la tension et la vitesse du ventilateur.
- Groupe scfSystemInfo
Ce groupe offre les informations suivantes à propos du système :
 - Nom d'hôte, numéro de série, nombre de processeurs montés et autres informations sur les produits du système
 - Informations sur l'état des DEL
 - Informations sur l'environnement du système, telles que la consommation électrique, l'évacuation d'air et la température de l'admission d'air
- Groupe scfPPARInfo
Ce groupe offre les informations suivantes à propos de la partition physique :
 - ID de la PPAR, nombre de processeurs montés, capacité de la mémoire, et d'autres informations sur le matériel de la partition physique
 - Versions d'OpenBoot PROM, de POST et du superviseur
 - Informations sur Oracle Solaris
 - État fonctionnel de la partition physique, stratégie de configuration
- Groupe scfPsbInfo
Ce groupe donne des informations sur la PSB (BB), telles que le numéro de la PSB, l'état d'alimentation de la PSB et l'état d'attribution/incorporation de la PSB dans une partition physique.

- Groupe scfLsbInfo
Ce groupe donne des informations sur la LSB, telles que le numéro de la LSB, l'ID de la PPAR à laquelle la LSB appartient et des informations sur la PCL.
- Groupe scfBoardInfo
Ce groupe donne des informations sur la CMU telles que le nom de la mémoire CPU (CMUL, CMUU), son numéro et l'état fonctionnel.
- Groupe scfCpuInfo
Ce groupe donne des informations sur le module CPU, telles que le numéro, la fréquence et l'état fonctionnel du processeur.
- Groupe scfMemoryInfo
Ce groupe donne des informations telles que le numéro, la capacité et l'état de fonctionnement de l'unité de la mémoire.
- Groupe scfPciBoxInfo
Ce groupe donne des informations sur les unités d'extension PCI et les composants qui les constituent. Les composants typiques sont les cartes d'E/S, les cartes PCI, les cartes de liaison, les unités d'alimentation, les unités de ventilation et les capteurs. Pour plus de détails sur les pièces, consultez « Chapitre 2 Understanding the PCI Expansion Unit Components » dans le *PCI Expansion Unit for Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 Service Manual*.
- Groupe scfComponentInfo
Ce groupe donne des informations sur les FRU et les états de tous les composants du système.
- Groupe scfDomainInfo
Ce groupe donne des informations sur les domaines logiques, tels que l'ID de la PPAR à laquelle ils appartiennent, le nom et l'état du domaine logique.

D.4 Traps

Les interruptions peuvent être standard ou étendues. Les interruptions standards sont des interruptions générales destinées aux périphériques individuels définis pour SNMP. Pour plus de détails sur les interruptions standards, consultez la documentation générale. Dans ce manuel, les interruptions permettant d'identifier des événements spécifiques à ces systèmes sont appelées interruptions étendues. Les interruptions étendues offrent différents types d'informations pour l'objet scfMIBTRap. Pour un aperçu sur les interruptions étendues, consultez « [10.3 Surveillance/Gestion de l'état du système avec l'agent SNMP](#) ».

Fonctions spécifiques du système SPARC M12/M10 pour Oracle VM Server pour SPARC

Cette annexe décrit et fournit des informations supplémentaires sur les fonctions d'Oracle VM Server pour SPARC spécifiques aux systèmes SPARC M12/M10. Pour plus de détails sur logiciel de gestion d'Oracle VM Server pour SPARC, consultez le *Oracle VM Server for SPARC Administration Guide* de la version correspondante.

- Arrêt commandé des domaines logiques
- Prise en charge de l'activation du processeur
- Vérification des ressources en panne
- Remplacement automatique du réglage des processeurs en erreur
- Vidage du superviseur
- Fonction de connexion de la console du domaine
- Restrictions du socket du processeur

E.1 Arrêt commandé des domaines logiques

Dans les systèmes SPARC M12/M10, vous pouvez effectuer un arrêt commandé de tous les domaines logiques depuis le XSCF. Pour plus de détails, consultez « [8.7 Arrêt commandé des domaines logiques](#) ».

E.2 Prise en charge de l'activation du processeur

L'activation du processeur est prise en charge sur les systèmes SPARC M12/M10. Vous pouvez afficher une liste d'information sur l'activation du processeur en

E.3 Vérification des ressources en panne

Les systèmes SPARC M12/M10 détectent et dégradent automatiquement les ressources de mémoire et de processeur défectueuses. La commande ldm(1M) peut être utilisé pour afficher les statuts des ressources de mémoire et de processeur. Pour plus de détails, consultez « [10.6 Vérification des ressources matérielles en panne](#) ».

E.3.1 Confirmation de panne ou d'absence de panne de la mémoire ou du processeur en utilisant la commande list-domain sub

1. **Affiche les informations détaillées du domaine logique dans la partition physique ainsi que les informations concernant la panne ou l'absence de panne de la mémoire ou du processeur.**

```
primary# ldm list-domain -l -S
```

E.3.2 Affichage de panne ou d'absence de panne de la mémoire ou du processeur en utilisant la commande list-device sub

1. **Affiche les informations des ressources de la mémoire disponible et du processeur dans la partition physique ainsi que les informations concernant la panne ou l'absence de panne de la mémoire ou du processeur.**

```
primary# ldm list-devices -S memory cpu
```

E.4 Remplacement automatique du réglage des processeurs en erreur

Les systèmes SPARC M12/M10 détectent et mettent hors ligne automatiquement les

processeurs défectueux. Vous pouvez configurer Oracle VM Server pour SPARC afin que le processeur défectueux soit automatiquement remplacé en cas de processeur libre ou d'activation de processeur disponible. Pour plus de détails, consultez « [10.7 Configuration d'une substitution automatique de cœurs du processeur en panne](#) ».

E.5 Vidage du superviseur

Le superviseur peut être interrompu en cas de détection d'une incohérence dans la partition physique. Dans ce cas, le microprogramme conserve le contenu de la mémoire du superviseur et le système est redémarré avec la configuration d'usine par défaut. Pour plus de détails, consultez « [8.13 Collecte d'un fichier de vidage du superviseur](#) ».

E.6 Fonction de connexion de la console du domaine

Dans un environnement de domaine logique, la destination de sortie de la console du domaine de commande est XSCF. La destination de sortie de la console de tous les autres domaines est le domaine de service ayant démarré la collecte du terminal de console virtuelle et l'unité de distribution (vcc). Dans Oracle Solaris 11.1 et les versions ultérieures, les domaines de service prennent en charge la fonction de connexion de la console des domaines logiques. Pour plus de détails, consultez « [8.10 Fonction de connexion de la console du domaine](#) ».

E.7 Restrictions du socket du processeur

Pour le système SPARC M12/M10 avec Oracle VM Server pour SPARC 3.3 ou version ultérieure, la configuration du domaine logique peut être gérée en fonction du socket physique du processeur. Pour plus de détails, consultez « [8.14 Gestion des ressources des domaines logiques associées aux sockets de processeur](#) ».

Exemples d'affichage de la commande d'utilitaire SAS2IRCU

Cette annexe comporte des exemples d'affichage de commandes d'utilitaire SAS2IRCU typiques pour configurer et gérer des volumes de RAID matériel du système SPARC M12/M10 à l'aide de l'utilitaire de configuration intégré RAID SAS-2 (SAS2IRCU) (appelé ci-dessous utilitaire SAS2IRCU) version 14.00.00.00 ou plus récente de Broadcom Limited.

Pour plus de détails sur l'utilitaire SAS2IRCU, consultez le site web de Broadcom Limited décrit dans « [14.2 Configuration du RAID matériel](#) ». Pour plus de détails concernant l'utilitaire SAS2IRCU et la façon de l'utiliser, consultez *SAS-2 Integrated RAID Configuration Utility User Guide* sur ce même site web.

L'utilitaire de configuration RAID intégré SAS-2 (SAS2IRCU) est l'œuvre protégée de Broadcom Limited et de ses sociétés affiliées.

- [Affichage d'une liste des contrôleurs SAS reconnus par sas2ircu](#)
- [Affichage des informations d'un volume RAID matériel](#)
- [Ajout d'un volume RAID matériel](#)
- [Affichage de l'état de configuration d'un volume RAID matériel](#)
- [Création d'un composant de rechange à chaud d'un volume RAID matériel](#)
- [Suppression d'un composant de rechange à chaud d'un volume RAID matériel](#)
- [Suppression d'un volume RAID matériel](#)
- [Identification du lecteur de disque défaillant d'un volume RAID matériel](#)

F.1 Affichage d'une liste des contrôleurs SAS reconnus par sas2ircu

Pour afficher une liste des contrôleurs SAS reconnus par sas2ircu, utilisez la commande `list` de sas2ircu.

L'exemple suivant montre que `Adapter Type = SAS2308_2` est un contrôleur SAS interne.

Vérifiez le numéro d'index affiché pour le contrôleur SAS interne.

Vous trouverez ci-dessous un exemple du SPARC M12-2.

Remarque : dans les systèmes SPARC M12-2/M12-2S ou une configuration de système avec plusieurs unités SPARC M12-2S/M10-4S, plusieurs contrôleurs SAS sont affichés, mais vous ne pouvez pas identifier leurs emplacements d'installation à l'aide du numéro d'index. Les emplacements d'installation des contrôleurs SAS peuvent être identifiés à l'aide des informations sas2ircu DISPLAY. Pour plus de détails sur sas2ircu DISPLAY, consultez « [F.2 Affichage des informations d'un volume RAID matériel](#) ».

./sas2ircu LIST
LSI Corporation SAS2 IR Configuration Utility.
Version 20.00.00.00 (2014.09.18)
Copyright (c) 2008-2014 LSI Corporation. All rights reserved.

Index	Adapter Type	Vendor ID	Device ID	Pci Address	SubSys Ven ID	SubSys Dev ID
0	SAS2308_2	1000h	87h	00h:03h:00h:00h	10cfh	187eh

Index	Adapter Type	Vendor ID	Device ID	Pci Address	SubSys Ven ID	SubSys Dev ID
1	SAS2308_2	1000h	87h	00h:03h:00h:00h	10cfh	187eh

F.2 Affichage des informations d'un volume RAID matériel

Pour afficher les informations des volumes RAID matériels et des lecteurs de disques configurées dans le système, utilisez la commande DISPLAY de sas2ircu.

L'exemple suivant montre le volume RAID 1 (miroir) équipé d'un lecteur de disque dans l'emplacement 0 comme lecteur primaire et d'un autre lecteur de disque dans l'emplacement 1 comme lecteur secondaire ainsi que de lecteurs de disque non adaptés au RAID matériel dans les emplacements 2, 3, 4 et 5 pour le contrôleur SAS (*1) avec Index=1.

*1 Ceci peut être vérifié à l'aide de la commande list de sas2ircu. Consultez « [F.1 Affichage d'une liste des contrôleurs SAS reconnus par sas2ircu](#) ».

Dans les exemples suivants, (1) à (4) indiquent ce qui suit :

(1) : Informations du contrôleur SAS

(2) : Informations du volume RAID

(2-1) : Informations du volume RAID n°1

Vous pouvez obtenir les informations suivantes (extrait partiel).

- L'ID du volume RAID est 286

- Le nom du volume RAID est RAID1-SYS

- L'état du volume RAID est normal (Okay (OKY))
 - Le niveau de RAID est RAID1 (effet miroir)
 - Le disque (2:0) de l'emplacement interne 0 du SPARC M12/M10 est installé sur PHY[0] (primaire)
 - Le disque (2:1) de l'emplacement interne 1 du SPARC M12/M10 est installé sur PHY[1] (secondaire)
- (3) : Informations de périphérique physique
- (3-1) : État du lecteur de disque (Drive Type=SAS_HDD) de l'emplacement interne 0 du SPARC M12/M10 (Enclosure#:2,Slot#:0)
Il est optimisé en tant que partie des volumes RAID. (State:Optimal (OPT))
- (3-2) : État du périphérique de services d'enceinte (Device Type= Enclosure services device) de l'emplacement de disque interne 0 du SPARC M12/M10 (Enclosure#:2,Slot#:0)
Ceci représente un autre périphérique qu'un disque dur. Bien que l'état de veille soit montré, l'affichage est normal. (State:Standby (SBY))
- (3-3) : État du lecteur de disque (Drive Type=SAS_HDD) de l'emplacement interne 2 du SPARC M12/M10 (Enclosure#:2,Slot#:2)
Ceci représente un lecteur de disque qui n'est pas en configuration RAID. Cet état indique qu'il peut être intégré à un volume RAID et à un échange à chaud. (State:Ready (RDY))
- (4) : Informations de châssis du SPARC M12/M10
- (4-1) : Adresse SAS du contrôleur SAS

Remarque : vous pouvez trouver le chemin d'accès du périphérique et l'emplacement d'installation du contrôleur SAS en vérifiant au préalable sur OBP l'adresse SAS du contrôleur SAS et en la comparant à sas2ircu DISPLAY. Pour plus de détails sur la manière d'obtenir les informations du contrôleur SAS sur OBP, consultez « [14.2.4 Préparation avant utilisation du RAID matériel](#) ».

```

root# ./sas2ircu 0 DISPLAY
LSI Corporation SAS2 IR Configuration Utility.
Version 17.00.00.00 (2013.07.19)
Copyright (c) 2009-2013 LSI Corporation. All rights reserved.

Read configuration has been initiated for controller 0
-----
Controller information <-- (1)
-----
Controller type           : SAS2308_2
BIOS version              : 0.00.00.00
Firmware version         : 13.00.66.00
Channel description       : 1 Serial Attached SCSI
Initiator ID              : 0
Maximum physical devices  : 255
Concurrent commands supported : 3072
Slot                      : Unknown
Segment                   : 0
Bus                       : 3
Device                    : 0
Function                  : 0

```

RAID Support : Yes

IR Volume information <-- (2)

IR volume 1 <-- (2-1)

Volume ID : 286
Volume Name : RAID1-SYS
Status of volume : Okay (OKY)
Volume wwid : 0aa6d102f1bf517a
RAID level : RAID1
Size (in MB) : 571250
Physical hard disks :
PHY[0] Enclosure#/Slot# : 2:0
PHY[1] Enclosure#/Slot# : 2:1

Physical device information <-- (3)

Initiator at ID #0

Device is a Hard disk <-- (3-1)

Enclosure # : 2
Slot # : 0
SAS Address : 5000039-4-281b-51e2
State : Optimal (OPT)
Size (in MB)/(in sectors) : 572325/1172123567
Manufacturer : TOSHIBA
Model Number : MBF2600RC
Firmware Revision : 3706
Serial No : EA25PC7007NC
GUID : 50000394281b51e0
Protocol : SAS
Drive Type : SAS_HDD

Device is a Enclosure services device <-- (3-2)

Enclosure # : 2
Slot # : 0
SAS Address : 500000e-0-e049-073d
State : Standby (SBY)
Manufacturer : FUJITSU
Model Number : NBBEXP
Firmware Revision : 0d32
Serial No : x3625413500
GUID : N/A
Protocol : SAS
Device Type : Enclosure services device

Device is a Hard disk

Enclosure # : 2
Slot # : 1
SAS Address : 5000039-4-281b-549a
State : Optimal (OPT)
Size (in MB)/(in sectors) : 572325/1172123567
Manufacturer : TOSHIBA


```

Model Number                : MBF2600RC
Firmware Revision           : 3706
Serial No                   : EA25PC7007PT
GUID                        : 50000394281b5498
Protocol                    : SAS
Drive Type                  : SAS_HDD

Device is a Hard disk <-- (3-3)
Enclosure #                 : 2
Slot #                     : 2
SAS Address                 : 5000039-4-281a-8ad2
State                       : Ready (RDY)
Size (in MB)/(in sectors)  : 572325/1172123567
Manufacturer                : TOSHIBA
Model Number               : MBF2600RC
Firmware Revision          : 3706
Serial No                  : EA25PC7007G7
GUID                       : 50000394281a8ad0
Protocol                   : SAS
Drive Type                 : SAS_HDD

Device is a Hard disk
Enclosure #                 : 2
Slot #                     : 3
SAS Address                 : 5000039-4-281b-5dc2
State                       : Ready (RDY)
Size (in MB)/(in sectors)  : 572325/1172123567
Manufacturer                : TOSHIBA
Model Number               : MBF2600RC
Firmware Revision          : 3706
Serial No                  : EA25PC7007T3
GUID                       : 50000394281b5dc0
Protocol                   : SAS
Drive Type                 : SAS_HDD

Device is a Hard disk
Enclosure #                 : 2
Slot #                     : 4
SAS Address                 : 5000039-4-281b-58b2
State                       : Ready (RDY)
Size (in MB)/(in sectors)  : 572325/1172123567
Manufacturer                : TOSHIBA
Model Number               : MBF2600RC
Firmware Revision          : 3706
Serial No                  : EA25PC7007RA
GUID                       : 50000394281b58b0
Protocol                   : SAS
Drive Type                 : SAS_HDD

Device is a Hard disk
Enclosure #                 : 2
Slot #                     : 5
SAS Address                 : 5000039-4-281b-502e
State                       : Ready (RDY)
Size (in MB)/(in sectors)  : 572325/1172123567

```

```

Manufacturer          : TOSHIBA
Model Number          : MBF2600RC
Firmware Revision     : 3706
Serial No             : EA25PC7007LR
GUID                  : 50000394281b502c
Protocol              : SAS
Drive Type            : SAS_HDD

```

```

-----
Enclosure information <-- (4)
-----

```

```

Enclosure#           : 1
Logical ID            : 500000e0:e046ff10 <-- (4-1)
Numslots              : 8
StartSlot             : 0
Enclosure#           : 2
Logical ID            : 500000e0:e049073f
Numslots              : 9
StartSlot             : 0
-----

```

```

SAS2IRCUC: Command DISPLAY Completed Successfully.
SAS2IRCUC: Utility Completed Successfully.

```

F.3 Ajout d'un volume RAID matériel

Utilisez la commande CREATE de sas2ircu pour ajouter un volume RAID matériel au système.

Dans l'exemple suivant, un volume RAID1E (effet miroir étendu) nommé « RAID1E-VOL » est créé pour les lecteurs de disque installés dans les emplacements 2, 3 et 4 (zones entières de disques) du SPARC M10-1.

```

root# ./sas2ircu 0 CREATE RAID1E MAX 2:2 2:3 2:4 RAID1E-VOL
LSI Corporation SAS2 IR Configuration Utility.
Version 17.00.00.00 (2013.07.19)
Copyright (c) 2009-2013 LSI Corporation. All rights reserved.
You are about to create an IR volume.
WARNING: Proceeding with this operation may cause data loss or data
corruption. Are you sure you want to proceed (YES/NO)? YES
WARNING: This is your last chance to abort this operation. Do you wish
to abort (YES/NO)? NO
Please wait, may take up to a minute...
Jan 20 16:20:15 1S-341-D0 scsi: /pci@8000/pci@4/pci@0/pci@0/scsi@0 (mpt_sas0):
Jan 20 16:20:15 1S-341-D0      Volume 0 is now , enabled, inactive
Jan 20 16:20:15 1S-341-D0 scsi: /pci@8000/pci@4/pci@0/pci@0/scsi@0 (mpt_sas0):
Jan 20 16:20:15 1S-341-D0      Volume 0 is now , enabled, active
Jan 20 16:20:15 1S-341-D0 scsi: /pci@8000/pci@4/pci@0/pci@0/scsi@0 (mpt_sas0):
Jan 20 16:20:15 1S-341-D0      Volume 0 is now , enabled, active, data scrub
in progress

```

```

Jan 20 16:20:15 1S-341-D0 scsi: /pci@8000/pci@4/pci@0/pci@0/scsi@0 (mpt_sas0):
Jan 20 16:20:15 1S-341-D0          Volume 0 is now , enabled, active, background
initialization in progress, data scrub in progress
Jan 20 16:20:15 1S-341-D0 scsi: WARNING: /scsi_vhci/disk@g50000394281b5dc0
(sd0):
Jan 20 16:20:15 1S-341-D0          Command failed to complete...Device is gone
SAS2IRCU: Volume created successfully.
SAS2IRCU: Command CREATE Completed Successfully.
SAS2IRCU: Utility Completed Successfully.

```

Après ajout d'un volume RAID matériel, vérifiez celui-ci et les informations de lecteur de disque en exécutant la commande DISPLAY de sas2ircu.

Vérifiez les informations suivantes.

(1) : Informations du volume IR

(1-1) : Vérifiez que le nouveau volume RAID volume (volume ID:285) a été créé tel qu'il a été défini par la commande CREATE de sas2ircu et que l'état du volume RAID est « Okay (OKY). »

(2) : Informations de périphérique physique

(2-1) (2-2) (2-3) : Vérifiez que l'état des lecteurs de disque des emplacements 2, 3 et 4 tout juste intégrés au volume RAID est bien « Optimal (OPT) ».

■ Résultats de l'exécution de la commande DISPLAY de sas2ircu (extrait partiel)

```

root# ./sas2ircu 0 DISPLAY
-----
IR Volume information    <-- (1)
-----
IR volume 1    <-- (1-1)
  Volume ID                      : 285
  Volume Name                    : RAID1E-VOL
  Status of volume               : Okay (OKY)
  Volume wwid                    : 00c354402fc35418
  RAID level                     : RAID1E
  Size (in MB)                  : 856875
  Physical hard disks           :
  PHY[0] Enclosure#/Slot#       : 2:2
  PHY[1] Enclosure#/Slot#       : 2:3
  PHY[2] Enclosure#/Slot#       : 2:4
IR volume 2
  Volume ID                      : 286
  Volume Name                    : RAID1-SYS
  Status of volume               : Okay (OKY)
  Volume wwid                    : 0aa6d102f1bf517a
  RAID level                     : RAID1
  Size (in MB)                  : 571250
  Physical hard disks           :
  PHY[0] Enclosure#/Slot#       : 2:0
  PHY[1] Enclosure#/Slot#       : 2:1
-----
Physical device information <-- (2)
-----
Device is a Hard disk    <-- (2-1)
  Enclosure #              : 2
  Slot #                   : 2

```

```

SAS Address          : 5000039-4-281a-8ad2
State                : Optimal (OPT)
Size (in MB)/(in sectors) : 572325/1172123567
Manufacturer         : TOSHIBA
Model Number         : MBF2600RC
Firmware Revision    : 3706
Serial No            : EA25PC7007G7
GUID                 : 50000394281a8ad0
Protocol             : SAS
Drive Type           : SAS_HDD
Device is a Hard disk <-- (2-2)
Enclosure #          : 2
Slot #               : 3
SAS Address          : 5000039-4-281b-5dc2
State                : Optimal (OPT)
Size (in MB)/(in sectors) : 572325/1172123567
Manufacturer         : TOSHIBA
Model Number         : MBF2600RC
Firmware Revision    : 3706
Serial No            : EA25PC7007T3
GUID                 : 50000394281b5dc0
Protocol             : SAS
Drive Type           : SAS_HDD
Device is a Hard disk <-- (2-3)
Enclosure #          : 2
Slot #               : 4
SAS Address          : 5000039-4-281b-58b2
State                : Optimal (OPT)
Size (in MB)/(in sectors) : 572325/1172123567
Manufacturer         : TOSHIBA
Model Number         : MBF2600RC
Firmware Revision    : 3706
Serial No            : EA25PC7007RA
GUID                 : 50000394281b58b0
Protocol             : SAS
Drive Type           : SAS_HDD

```

F.4 Affichage de l'état de configuration d'un volume RAID matériel

Utilisez la commande STATUS de sas2ircu pour afficher l'état du volume RAID matériel créé.

Dans les exemples suivants, l'état de configuration du volume RAID matériel nouvellement créé (ID:285) est affiché. Il indique que le taux de progression s'élève à 0,14 % à l'aide de l'état d'initialisation d'arrière-plan.

Remarque : « Current Operation:Background Init » indique que la configuration du volume

RAID est en cours. Lorsque « Pourcentage complet » (taux de progression) atteint 100 %, l'état passe à « Current Operation:None » et le volume RAID peut être utilisé en toute sécurité.

Dans les exemples ci-dessous, les mentions (1) à (2) ont les significations suivantes :

(1) : Informations du volume RAID n°1

- L'ID du volume RAID est 285
- RAID mène actuellement une initialisation d'arrière-plan et le taux de progression de cette opération s'élève à 0,14 %
- Le volume RAID est activé et optimisé

(2) : Informations du volume RAID n°2

- L'ID du volume RAID est 286
- Aucune opération RAID actuellement
- Le volume RAID est activé et optimisé

```
root# ./sas2ircu 0 STATUS
LSI Corporation SAS2 IR Configuration Utility.
Version 17.00.00.00 (2013.07.19)
Copyright (c) 2009-2013 LSI Corporation. All rights reserved.

Background command progress status for controller 0...

IR Volume 1 <-- (1)
  Volume ID                      : 285
  Current operation               : Background Init
  Volume status                  : Enabled
  Volume state                   : Optimal
  Volume wwid                    : 00c354402fc35418
  Physical disk I/Os             : Not quiesced
  Volume size (in sectors)       : 1754880000
  Number of remaining sectors    : 1752440704
  Percentage complete            : 0.14%

IR Volume 2 <-- (2)
  Volume ID                      : 286
  Current operation               : None
  Volume status                  : Enabled
  Volume state                   : Optimal
  Volume wwid                    : 0aa6d102f1bf517a
  Physical disk I/Os             : Not quiesced
SAS2IRCU: Command STATUS Completed Successfully.
SAS2IRCU: Utility Completed Successfully.
```

F.5 Création d'un composant de rechange à chaud d'un volume RAID matériel

Utilisez la commande HOTSPARE de sas2ircu pour créer un composant de rechange

à chaud du volume RAID matériel.

Dans les exemples suivants, un composant de rechange à chaud du lecteur de disque installé dans l'emplacement 5 du SPARC M10-1 est créé.

```
root# ./sas2ircu 0 HOTSPARE 2:5
LSI Corporation SAS2 IR Configuration Utility.
Version 17.00.00.00 (2013.07.19)
Copyright (c) 2009-2013 LSI Corporation. All rights reserved.

WARNING: Proceeding with this operation may cause data loss or data
corruption. Are you sure you want to proceed (YES/NO)? YES

WARNING: This is your last chance to abort this operation. Do you wish
to abort (YES/NO)? NO
Please wait, may take up to a minute...
SAS2IRCU: Hot Spare disk created successfully.
SAS2IRCU: Command HOTSPARE Completed Successfully.
SAS2IRCU: Utility Completed Successfully.
```

Après création d'un composant de rechange à chaud, vérifiez les éléments suivants à l'aide de la commande DISPLAY de sas2ircu.

(1) Informations de périphérique physique

(1-1) Si le champ « State » du lecteur de disque dans l'emplacement 5 affiche
« HotSpare (HSP) »

■ Résultats de l'exécution de la commande DISPLAY de sas2ircu (extrait partiel)

```
root# ./sas2ircu 0 DISPLAY
-----
Physical device information <-- (1)
-----
Device is a Hard disk <-- (1-1)
Enclosure #           : 2
Slot #                : 5
SAS Address           : 5000039-4-281b-5022
State                 : Hot Spare (HSP)
Size (in MB)/(in sectors) : 572325/1172123567
Manufacturer          : TOSHIBA
Model Number          : MBF2600RC
Firmware Revision     : 3706
Serial No             : EA25PC7007LM
GUID                  : 50000394281b5020
Protocol              : SAS
Drive Type             : SAS_HDD
```

F.6 Suppression d'un composant de rechange à chaud d'un volume RAID matériel

Utilisez la commande HOTSPARE de sas2ircu pour supprimer un composant de rechange à chaud du volume RAID matériel.

Dans les exemples suivants, un composant de rechange à chaud du lecteur de disque installé dans l'emplacement 5 du SPARC M10-1 est supprimé.

```
root# ./sas2ircu 0 HOTSPARE DELETE 2:5
LSI Corporation SAS2 IR Configuration Utility.
Version 17.00.00.00 (2013.07.19)
Copyright (c) 2009-2013 LSI Corporation. All rights reserved.

WARNING: Proceeding with this operation may cause data loss or data
corruption. Are you sure you want to proceed (YES/NO)? YES

WARNING: This is your last chance to abort this operation. Do you wish
to abort (YES/NO)? NO
SAS2IRCU: Hot Spare disk deleted successfully.
SAS2IRCU: Command HOTSPARE Completed Successfully.
SAS2IRCU: Utility Completed Successfully.
```

Après suppression d'un composant de rechange à chaud, vérifiez les éléments suivants à l'aide de la commande DISPLAY de sas2ircu.

(1) Informations de périphérique physique

(1-1) Si le champ « State » du lecteur de disque dans l'emplacement 5 affiche « Ready (RDY) »

■ Résultats de l'exécution de la commande DISPLAY de sas2ircu (extrait partiel)

```
root# ./sas2ircu 0 DISPLAY
-----
Physical device information <-- (1)
-----
Device is a Hard disk <-- (1-1)
Enclosure #           : 2
Slot #                : 5
SAS Address           : 5000039-4-281b-5022
State                 : Ready (RDY)
Size (in MB)/(in sectors) : 572325/1172123567
Manufacturer          : TOSHIBA
Model Number          : MBF2600RC
Firmware Revision     : 3706
Serial No             : EA25PC7007LM
GUID                  : 50000394281b5020
Protocol              : SAS
Drive Type            : SAS_HDD
```

F.7 Suppression d'un volume RAID matériel

Utilisez la commande `DELETEVOLUME` de `sas2ircu` pour supprimer un volume RAID matériel du système.

L'exemple suivant montre la suppression du volume RAID disposant de l'ID:285 sur le SPARC M10.

```
root# ./sas2ircu 0 DELETEVOLUME 285
LSI Corporation SAS2 IR Configuration Utility.
Version 17.00.00.00 (2013.07.19)
Copyright (c) 2009-2013 LSI Corporation. All rights reserved.

You are about to delete an existing RAID Volume on a controller. This command
will delete the specified RAID volume and associated HotSpare drive(s).

WARNING: Proceeding with this operation may cause data loss or data
corruption. Are you sure you want to proceed (YES/NO)? YES

WARNING: This is your last chance to abort this operation. Do you wish
to abort (YES/NO)? NO
Please wait, may take up to a minute...
SAS2IRCUC: Volume deleted successfully.
SAS2IRCUC: Command DELETEVOLUME Completed Successfully.
SAS2IRCUC: Utility Completed Successfully.
```

Après suppression d'un volume RAID matériel, vérifiez celui-ci et les éléments de lecteur de disque ci-dessous en exécutant la commande `DISPLAY` de `sas2ircu`.

(1) Informations du volume IR

(1-1) Si le volume RAID disposant de l'ID:285 est supprimé et que seules restent les informations du volume ID:286

(2) Informations de périphérique physique

(2-1) (2-2) (2-3) Si le champ « State » des lecteurs de disque des emplacements 2, 3 et 4 intégrés au volume RAID disposant de l'ID:285 supprimé affiche « Ready (RDY) ».

- Résultats de l'exécution de la commande `DISPLAY` de `sas2ircu` (extrait partiel)

```
root# ./sas2ircu 0 DISPLAY
-----
IR Volume information <-- (1)
-----
IR volume 1 <-- (1-1)
  Volume ID                : 286
  Volume Name              : RAID1-SYS
  Status of volume         : Okay (OKY)
  Volume wwid              : 0aa6d102f1bf517a
  RAID level               : RAID1
```



```

Size (in MB)                : 571250
Physical hard disks          :
PHY[0] Enclosure#/Slot#     : 2:0
PHY[1] Enclosure#/Slot#     : 2:1

```

Physical device information <-- (2)

Device is a Hard disk <-- (2-1)

```

Enclosure #                  : 2
Slot #                       : 2
SAS Address                   : 5000039-4-281a-8ad2
State                         : Ready (RDY)
Size (in MB)/(in sectors)    : 572325/1172123567
Manufacturer                  : TOSHIBA
Model Number                  : MBF2600RC
Firmware Revision             : 3706
Serial No                     : EA25PC7007G7
GUID                          : 50000394281a8ad0
Protocol                      : SAS
Drive Type                    : SAS_HDD

```

Device is a Hard disk <-- (2-2)

```

Enclosure #                  : 2
Slot #                       : 3
SAS Address                   : 5000039-4-281b-5dc2
State                         : Ready (RDY)
Size (in MB)/(in sectors)    : 572325/1172123567
Manufacturer                  : TOSHIBA
Model Number                  : MBF2600RC
Firmware Revision             : 3706
Serial No                     : EA25PC7007T3
GUID                          : 50000394281b5dc0
Protocol                      : SAS
Drive Type                    : SAS_HDD

```

Device is a Hard disk <-- (2-3)

```

Enclosure #                  : 2
Slot #                       : 4
SAS Address                   : 5000039-4-281b-58b2
State                         : Ready (RDY)
Size (in MB)/(in sectors)    : 572325/1172123567
Manufacturer                  : TOSHIBA
Model Number                  : MBF2600RC
Firmware Revision             : 3706
Serial No                     : EA25PC7007RA
GUID                          : 50000394281b58b0
Protocol                      : SAS
Drive Type                    : SAS_HDD

```

F.8 Identification du lecteur de disque défaillant d'un volume RAID matériel

Afin d'identifier le volume RAID matériel et le lecteur de disque défaillants, utilisez la commande DISPLAY de sas2ircu.

Dans l'exemple suivant, le lecteur de disque dans l'emplacement 1 du SPARC M10-1 est défaillant.

Dans les exemples ci-dessous, les mentions (1) à (2) ont les significations suivantes :

(1) : Informations du volume RAID

(1-1) : Informations du volume RAID n°2

Vous pouvez obtenir les informations suivantes (extrait partiel).

- L'ID du volume RAID est 286
- L'état du volume RAID est dégradé (Degraded (DGD))
- Le niveau de RAID est RAID1 (effet miroir)
- Le disque (2:0) de l'emplacement interne 0 du SPARC M12/M10 est installé sur PHY[0] (primaire)
- PHY[1] (secondaire) ne possède aucune information sur le disque (0:0)

(2) : Informations de périphérique physique

(2-1) : État du lecteur de disque (Drive Type=SAS_HDD) ne disposant d'aucune information sur le lieu d'installation (Enclosure#:0,Slot#:0 = existait auparavant en tant que Enclosure#:2,Slot#:1, mais n'était pas accessible lorsque cette commande était exécutée)

Cela indique que le lecteur de disque est hors service. (State:Failed (FLD))

```
root# ./sas2ircu 0 DISPLAY
LSI Corporation SAS2 IR Configuration Utility.
Version 17.00.00.00 (2013.07.19)
Copyright (c) 2009-2013 LSI Corporation. All rights reserved.

Read configuration has been initiated for controller 0
-----
Controller information
-----
Controller type           : SAS2308_2
BIOS version             : 0.00.00.00
Firmware version         : 13.00.66.00
Channel description      : 1 Serial Attached SCSI
Initiator ID             : 0
Maximum physical devices : 255
Concurrent commands supported : 3072
Slot                     : Unknown
Segment                  : 0
Bus                      : 3
Device                   : 0
Function                  : 0
RAID Support              : Yes
-----
```

IR Volume information <-- (1)

IR volume 1

Volume ID : 285
Volume Name : RAID1E-VOL
Status of volume : Okay (OKY)
Volume wwid : 0fd4f41e8cd673de
RAID level : RAID1E
Size (in MB) : 856875
Physical hard disks :
PHY[0] Enclosure#/Slot# : 2:2
PHY[1] Enclosure#/Slot# : 2:3
PHY[2] Enclosure#/Slot# : 2:4

IR volume 2 <-- (1-1)

Volume ID : 286
Volume Name : RAID1-SYS
Status of volume : Degraded (DGD)
Volume wwid : 0aa6d102f1bf517a
RAID level : RAID1
Size (in MB) : 571250
Physical hard disks :
PHY[0] Enclosure#/Slot# : 2:0
PHY[1] Enclosure#/Slot# : 0:0

Physical device information <-- (2)

Initiator at ID #0

Device is a Hard disk <-- (2-1)

Enclosure # : 0
Slot # : 0
SAS Address : 00000000-0-0000-0000
State : Failed (FLD)
Manufacturer : TOSHIBA
Model Number : MBF2600RC
Firmware Revision : 3706
Serial No : EA25PC700855
GUID : N/A
Protocol : SAS
Drive Type : SAS_HDD

Device is a Enclosure services device

Enclosure # : 2
Slot # : 0
SAS Address : 500000e-0-e049-073d
State : Standby (SBY)
Manufacturer : FUJITSU
Model Number : NBBEXP
Firmware Revision : 0d32
Serial No : x3625413500
GUID : N/A
Protocol : SAS
Device Type : Enclosure services device

```

Device is a Hard disk
Enclosure #           : 2
Slot #               : 0
SAS Address          : 5000039-4-281b-6466
State                : Optimal (OPT)
Size (in MB)/(in sectors) : 572325/1172123567
Manufacturer         : TOSHIBA
Model Number        : MBF2600RC
Firmware Revision   : 3706
Serial No           : EA25PC7007UE
GUID                : 50000394281b6464
Protocol            : SAS
Drive Type          : SAS_HDD

```

```

Device is a Hard disk
Enclosure #           : 2
Slot #               : 2
SAS Address          : 5000039-4-281a-8ad2
State                : Optimal (OPT)
Size (in MB)/(in sectors) : 572325/1172123567
Manufacturer         : TOSHIBA
Model Number        : MBF2600RC
Firmware Revision   : 3706
Serial No           : EA25PC7007G7
GUID                : 50000394281a8ad0
Protocol            : SAS
Drive Type          : SAS_HDD

```

```

Device is a Hard disk
Enclosure #           : 2
Slot #               : 3
SAS Address          : 5000039-4-281b-5dc2
State                : Optimal (OPT)
Size (in MB)/(in sectors) : 572325/1172123567
Manufacturer         : TOSHIBA
Model Number        : MBF2600RC
Firmware Revision   : 3706
Serial No           : EA25PC7007T3
GUID                : 50000394281b5dc0
Protocol            : SAS
Drive Type          : SAS_HDD

```

```

Device is a Hard disk
Enclosure #           : 2
Slot #               : 4
SAS Address          : 5000039-4-281b-502e
State                : Optimal (OPT)
Size (in MB)/(in sectors) : 572325/1172123567
Manufacturer         : TOSHIBA
Model Number        : MBF2600RC
Firmware Revision   : 3706
Serial No           : EA25PC7007LR
GUID                : 50000394281b502c
Protocol            : SAS

```

```

Drive Type                               : SAS_HDD
-----
Enclosure information
-----
Enclosure#                               : 1
Logical ID                               : 500000e0:e046ff10
Numslots                                 : 8
StartSlot                                : 0
Enclosure#                               : 2
Logical ID                               : 500000e0:e049073f
Numslots                                 : 9
StartSlot                                : 0
-----
SAS2IRCU: Command DISPLAY Completed Successfully.
SAS2IRCU: Utility Completed Successfully.
root#

```

Remarque : il se peut que le message suivant s'affiche sur Oracle Solaris après avoir utilisé un volume RAID pour créer ou supprimer un volume RAID, supprimer un composant de rechange à chaud, etc. Cela indique qu'il n'y pas d'informations d'étiquette sur le volume RAID ou le lecteur de disque. Dans cet état, le volume RAID ou le lecteur de disque ne peuvent pas être utilisés sur Oracle Solaris. Ils seront utilisables sur Oracle Solaris uniquement après exécution de la commande format en sélectionnant le volume RAID ou le lecteur de disque approprié, puis en l'étiquetant.

■ Exemple de message de sortie

```

Jan 20 15:55:07 1S-341-D0 cmlb: WARNING: /scsi_vhci/disk@g50000394281a8ad0
(sd1):
Jan 20 15:55:07 1S-341-D0          Corrupt label; wrong magic number

```

■ Exemple d'exécution de la commande format

```

root@solaris:/root# format
Searching for disks...
Jan 20 15:55:07 1S-341-D0 cmlb: WARNING: /scsi_vhci/disk@g50000394281a8ad0
(sd1):
Jan 20 15:55:07 1S-341-D0          Corrupt label; wrong magic number
Jan 20 15:55:07 1S-341-D0 cmlb: WARNING: /scsi_vhci/disk@g50000394281a8ad0
(sd1):
Jan 20 15:55:07 1S-341-D0          Corrupt label; wrong magic number
Jan 20 15:55:07 1S-341-D0 cmlb: WARNING: /scsi_vhci/disk@g50000394281b58b0
(sd3):
Jan 20 15:55:07 1S-341-D0          Corrupt label; wrong magic number
Jan 20 15:55:07 1S-341-D0 cmlb: WARNING: /scsi_vhci/disk@g50000394281b58b0
(sd3):
Jan 20 15:55:07 1S-341-D0          Corrupt label; wrong magic number
Jan 20 15:55:07 1S-341-D0 cmlb: WARNING: /scsi_vhci/disk@g50000394281b5dc0
(sd0):
Jan 20 15:55:07 1S-341-D0          Corrupt label; wrong magic number
Jan 20 15:55:08 1S-341-D0 cmlb: WARNING: /scsi_vhci/disk@g50000394281b5dc0

```

```

(sd0):
Jan 20 15:55:08 1S-341-D0          Corrupt label; wrong magic number
done
c0t50000394281A8AD0d0: configured with capacity of 558.89GB
c0t50000394281B5DC0d0: configured with capacity of 558.89GB
c0t50000394281B58B0d0: configured with capacity of 558.89GB
AVAILABLE DISK SELECTIONS:
    0. c0t50000394281A8AD0d0 <TOSHIBA-MBF2600RC-3706 cyl 64986 alt 2 hd 27
sec 668>
        /scsi_vhci/disk@g50000394281a8ad0
        /dev/chassis/SYS/HDD02/disk
    1. c0t50000394281B5DC0d0 <TOSHIBA-MBF2600RC-3706 cyl 64986 alt 2 hd 27
sec 668>
        /scsi_vhci/disk@g50000394281b5dc0
        /dev/chassis/SYS/HDD03/disk
    2. c0t50000394281B58B0d0 <TOSHIBA-MBF2600RC-3706 cyl 64986 alt 2 hd 27
sec 668>
        /scsi_vhci/disk@g50000394281b58b0
        /dev/chassis/SYS/HDD04/disk
    3. c0t50000394281B5020d0 <LSI-Logical Volume-3000 cyl 24998 alt 2 hd 16
sec 128>
        /scsi_vhci/disk@g50000394281b5020
        /dev/chassis/SYS/HDD05/disk
    4. c2t3AA6D102F1BF517Ad0 <LSI-Logical Volume-3000 cyl 65533 alt 2 hd 32
sec 557>
        /pci@8000/pci@4/pci@0/pci@0/scsi@0/ipro@v0/disk@w3aa6d102f1bf517a,0
Specify disk (enter its number): 0
[disk formatted]
Disk not labeled.  Label it now? yes

```

Fonction de mode de démarrage du XSCF SPARC M12-1/M10-1

Cette annexe décrit la fonction de mode de démarrage du XSCF, qui peut être utilisée pour réduire le temps de démarrage du SPARC M12-1/M10-1.

- [Présentation de la fonction](#)
- [Restrictions et remarques](#)
- [Procédure de configuration](#)

G.1 Présentation de la fonction

G.1.1 Qu'est-ce que la fonction de mode de démarrage du XSCF ?

La fonction de mode de démarrage du XSCF a été introduite dans les versions de XCP 2220 et supérieures pour les systèmes SPARC M12-1/M10-1.

La commande `xscfstartupmode` est utilisée pour modifier le comportement du XSCF au démarrage. Elle permet à l'utilisateur de choisir entre le mode « normal » (par défaut) et le mode « fast ».

Le mode « fast » permet au système SPARC M12-1/M10-1 de démarrer automatiquement la partition physique lorsque le système est mis sous tension (AC ON) et que le XSCF a démarré. En mode « fast », il n'y a pas besoin de lancer la commande `poweron` pour démarrer la partition physique.

Pour les systèmes SPARC M12-1/M10-1 ayant une version de XCP antérieure à 2220, ou pour les les systèmes SPARC M12-1/M10-1 ayant une version 2220 ou supérieure mais `xscfstartupmode` configuré à « normal », la commande XSCF `poweron` doit être utilisée pour démarrer la partition physique après la mise sous tension du système (AC ON).

Pour démarrer automatiquement la partition physique, configurez le mode de démarrage à « fast », le commutateur de mode du panneau de commande à

« Locked », et mettez le système sous tension (AC ON). Si le système est mis sous tension (AC ON) lorsque le commutateur de mode du panneau de commande est configuré à « Service », le mode de démarrage repasse à « normal », et la partition physique n'est donc pas démarrée automatiquement.

Pour fonctionner temporairement en mode « normal », configurez le commutateur de mode du panneau de commande à « Service » et mettez le système sous tension (AC ON).

La fonction de mode de démarrage du XSCF est spécifique au SPARC M12-1/M10-1 uniquement et n'est pas présente sur le M12-2/M12-2S/M10-4/M10-4S.

G.1.2 Conditions d'utilisation

Les conditions suivantes s'appliquent lors de l'utilisation de la fonction de mode de démarrage du XSCF.

- Si le mode de démarrage est défini comme « fast » avec la commande `xscfstartupmode`, et que l'alimentation est activée avec le commutateur de mode du panneau de commande configuré à « Locked », le système démarrera en mode « fast ». Cependant, même si le mode de démarrage est changé en « fast », si le commutateur de mode du panneau de commande passe de « Service » à « Locked » après la mise sous tension, le système démarrera en mode « normal » et non en mode « fast ».
- Lorsque le mode de démarrage est changé à « fast », un redémarrage du XSCF ne génère pas de démarrage automatique de la partition physique. L'activation automatique de la partition physique ne fonctionne que lors de la mise sous tension.
- Le mode de démarrage du système ne peut pas être modifié uniquement en exécutant la commande `rebootxscf` après avoir modifié la configuration du mode de démarrage. Mettre le système hors tension puis sous tension est nécessaire pour que la modification de configuration du mode de démarrage soit effective.
- La configuration du mode de démarrage est enregistrée dans le XSCF sur l'unité de carte mère (MBU), mais aucune sauvegarde interne sur l'unité de backplane PSU (PSUBP) n'est effectuée. Si la MBU est remplacée, le mode de démarrage peut repasser à sa configuration par défaut. Après un remplacement de la MBU, assurez-vous de vérifier le mode de démarrage, et, si nécessaire, de le modifier pour la configuration de votre choix.
- Lorsque le système est démarré en mode « fast », vous ne devez pas modifier pas la configuration de XSCF, effectuer de détérioration ou restauration, configurer les paramètres d'environnement d'OpenBoot PROM, ni sauvegarder les informations de configuration des domaines logiques. N'effectuez ces opérations que dans le mode « normal ». Si vous les effectuez alors que le système a été démarré en mode « fast », les configurations et modifications seront sauvegardées dans le XSCF sur la MBU, mais aucune sauvegarde interne sur le PSUBP ne sera effectuée. Si la MBU est remplacée, les informations de configuration ne pourront pas être récupérées de la sauvegarde interne du PSUBP, et le système pourrait ne pas pouvoir démarrer.

En plus de la configuration « fast » de la fonction de mode de démarrage du XSCF,

le temps pris entre la mise sous tension du système et le démarrage d'Oracle Solaris / Oracle VM Server pour SPARC peut être réduit davantage par :

- L'utilisation de stockage interne SSD comme périphériques de démarrage (au lieu de disques SAS)
- Le paramétrage du niveau de diagnostic POST à off (au lieu de la valeur par défaut de min)

Remarque : lorsque vous modifiez le niveau de diagnostic POST, assurez-vous de modifier le paramètre après avoir vérifié le contenu de « [G.2.2 Restrictions et remarques pendant le fonctionnement du système](#) ».

G.2 Restrictions et remarques

G.2.1 Restrictions et remarques au moment de l'installation du système

- Les opérations d'installation du système doivent être effectuées avec le mode de démarrage XSCF « normal », ensuite seulement le mode de démarrage peut être modifié en « fast ». L'état du mode de démarrage peut être référencé par la commande `xscfstartupmode -d`, décrite dans « [G.3 Procédure de configuration](#) ». Les informations de configuration matérielle du système et de configuration XSCF ne sont enregistrées que sur le XSCF (aucune sauvegarde interne n'est effectuée) lorsque le mode de démarrage XSCF est « fast ». S'il existe une différence entre les informations enregistrées dans le XSCF et les informations matérielles du système, des problèmes comme des défaillances du processus XSCF et une incapacité des partitions physiques à fonctionner correctement peuvent se produire.
- Si le système est configuré pour effectuer des opérations programmées avec la commande `setpowerschedule`, et que le mode de démarrage est « fast », le système démarrera dans le mode « fast » au moment programmé.
- Si la restauration d'alimentation est configurée en « off » ou en « auto » avec la commande `setpowerschedule`, et que le mode de démarrage est « fast », le système ignorera les paramètres « off » ou « auto » et démarrera en mode « fast » lorsque l'alimentation arrivera (AC ON).

G.2.2 Restrictions et remarques pendant le fonctionnement du système

- En mode de démarrage XSCF « fast », les connexions à XSCF des utilisateurs par telnet ou ssh sont limitées à un maximum de 10.
- La commande `xscfstartupmode` elle-même ne sera pas auditée, mais d'autres audits sont affectés par la configuration du mode de démarrage XSCF.
- Lorsque la partition physique est démarrée dans le mode « fast », le champ « Cause » du journal d'alimentation de XSCF contiendra « power recover ».
- Si le niveau de diagnostic POST est défini à « off », les diagnostics du processeur, de la mémoire et des E/S par POST ne sont pas effectués lors de la mise sous tension de la partition physique. Par conséquent, sauf dans le cas où POST lui-même cesse de fonctionner, la détection des anomalies et la détérioration subséquente des composants défectueux par le diagnostic POST n'est pas effectuée. À la place, « Hypervisor Abort » ou « OS PANIC » peuvent se produire lorsque l'anomalie du processeur, de la mémoire ou des E/S est détectée.
- Si le niveau de diagnostic POST est défini à « min/max », un diagnostic du processeur, de la mémoire et des E/S est effectué, mais le temps de démarrage est augmenté du temps nécessaire pour cette opération.
- Lorsque vous modifiez les informations de configuration de XSCF, faites-le après avoir démarré XSCF en mode de démarrage « normal ». Pour utiliser temporairement le mode « normal », configurez le commutateur de mode du panneau de commande sur « Service », mettez le XSCF hors tension puis sous tension pour le redémarrer, puis modifiez les informations de configuration de XSCF.
- Lorsque vous créez ou modifiez les informations de configuration de domaines logiques, faites-le après avoir démarré XSCF en mode de démarrage « normal ». Pour utiliser temporairement le mode « normal », configurez le commutateur de mode du panneau de commande sur « Service », mettez le XSCF hors tension puis sous tension pour le redémarrer, puis créez ou modifiez les informations de configurations des domaines logiques pendant que la partition physique fonctionne, et assurez-vous d'exécuter la commande « `ldm add-spconfig` » pour sauvegarder les informations de configuration des domaines logiques dans le XSCF.

G.2.3 Restrictions lors de la maintenance

- Les défaillances matérielles peuvent être confirmées par les marques de défaillance (signalées par « * ») dans la sortie générée par les commandes XSCF `showhardconf` ou `showstatus`. Lorsque le mode de démarrage est défini à « fast » et qu'une défaillance matérielle a été détectée dans le système, si l'alimentation est interrompue et rétablie même une seule fois, toutes les marques de défaillance (signalées par « * ») pour les composants concernés sont effacées au prochain démarrage du système. Avant de remplacer les composants défectueux, prenez note des informations de défaillances avec les commandes XSCF `showhardconf` ou

showstatus. Puis, référez-vous aux informations FRU dans les journaux d'erreur pour remplacer les composants.

- Lorsque vous sauvegardez ou restaurez des informations de configuration avec les commandes dumpconfig ou restoreconfig, faites-le après avoir démarré XSCF en mode « normal ». Pour utiliser temporairement le mode « normal », configurez le commutateur de mode du panneau de commande sur « Service », mettez le XSCF hors tension puis sous tension pour le redémarrer, puis effectuez ces opérations.
- Le paramètre de mode de démarrage n'est pas inclus dans les informations sauvegardées ou restaurées lors de l'utilisation des commandes XSCF dumpconfig ou restoreconfig. Par conséquent, il convient de réinitialiser le mode de démarrage après la restauration des informations de configuration avec la commande restoreconfig après un remplacement de la MBU. Si la commande restoreconfig est exécutée sur un système pour lequel la MBU n'a pas été remplacée, elle ne supprime pas les informations de configuration existantes.
- Le matériel ne peut pas être remplacé avec la commande replacefru lorsque le système est démarré en mode « fast ». Remplacez le matériel avec l'alimentation hors tension. Après ceci, configurez le commutateur de mode du panneau de commande sur « Service » et allumez l'alimentation, et attendez que XSCF démarre. De cette manière les informations de configuration matérielle et les informations de configuration XSCF sont enregistrées dans XSCF. Après le démarrage de XSCF, éteignez l'alimentation et configurez le commutateur de mode du panneau de commande sur « Locked ». Lorsqu'ensuite le système est mis sous tension, il démarrera en mode « fast ».
- Le mode de démarrage n'est pas initialisé lorsque le système est initialisé aux valeurs d'usine au moyen de la commande restoredefaults. Assurez-vous de changer le mode de démarrage à « normal » et de mettre le système hors tension puis sous tension avant d'exécuter la commande restoredefaults.
- Lorsque vous mettez à jour le microprogramme XSCF, faites-le après avoir démarré XSCF en mode « normal ».

G.3 Procédure de configuration

Cette section décrit les tâches permettant de configurer la fonction de mode de démarrage de XSCF.

1. **Effectuez les tâches d'installation comme la mise à jour du microprogramme, la configuration du ou des réseau(x) et des utilisateurs XSCF, l'activation de cœurs de processeur, etc.**

Pour plus de détails, consultez les dernières *Notes de produit* pour votre serveur.

Remarque : ne configurez pas le mode de démarrage à « fast » lors de l'installation du système.

Remarque : le mode de démarrage XSCF est pris en charge à partir de XCP 2220. Si le

microprogramme du système est antérieur à XCP 2220, suivez les manuels ou les notes de produit pour obtenir et mettre à jour un microprogramme plus récent.

2. Mettez sous tension la partition physique.

- a. Vérifiez que les informations de configuration des domaines logiques sont « factory defaults » avec la commande `showdomainconfig`.
- b. Exécutez la commande `poweron` pour démarrer la partition physique.

Remarque : ne configurez pas le mode de démarrage à « fast » lors de l'installation du système.

3. Installez les logiciels comme Oracle Solaris or Oracle VM Server pour SPARC, etc., et/ou configurez les domaines logiques.

Concernant l'installation du logiciel, reportez-vous à « [4.5 Connexion d'un lecteur de DVD](#) ». Pour plus de détails sur la configuration des domaines logiques, consultez le *Guide de configuration du domaine Fujitsu SPARC M12 et Fujitsu M10/SPARCM10*.

Remarque : ne configurez pas le mode de démarrage à « fast » lors de l'installation du système.

Remarque : si les informations de configurations des domaines logiques ont été créées, assurez-vous de les enregistrer dans le XSCF en exécutant la commande `ldm « add-spconfig »`.

4. Utilisez la commande `poweroff` pour mettre la partition physique hors tension.

5. Configurez le mode de démarrage XSCF à « fast ».

- a. Connectez-vous à XSCF avec le privilège « platadm ».
- b. Vérifiez la valeur actuelle du mode de démarrage.
Pour plus de détails sur la commande `xscfstartupmode(8)`, consultez *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

```
XSCF> xscfstartupmode -d
Setting Mode: normal
Current Mode: normal
```

- c. Configurez le mode de démarrage à « fast ».

```
XSCF> xscfstartupmode -m fast
```

- d. Vérifiez que le mode de démarrage est bien défini à « fast ».

```
XSCF> xscfstartupmode -d
Setting Mode: fast [need AC OFF/ON]
Current Mode: normal
```

6. **Définissez le niveau de diagnostic POST à « OFF »** (si vous souhaitez annuler le diagnostic POST lors de la mise sous tension pour réduire encore le temps de démarrage du système).
 - a. Vérifiez le niveau de diagnostic POST actuel.

```
XSCF> showpparmode -p 0
Host-ID                :9007002b
Diagnostic Level        :min
Message Level          :normal
Alive Check            :on
Watchdog Reaction      :reset
Break Signal           :on
Autoboot (Guest Domain) :on
Elastic Mode           :off
IOreconfigure          :false
CPU Mode               :auto
PPAR DR (Current)      :-
PPAR DR (Next)         :off
```

- b. Configurez le niveau de diagnostic POST à « OFF ».

```
XSCF> setpparmode -p 0 -m diag=off
```

- c. Vérifiez l'état du niveau de diagnostic POST.

```
XSCF> showpparmode -p 0
Host-ID                :9007002b
Diagnostic Level        :off
Message Level          :normal
Alive Check            :on
Watchdog Reaction      :reset
Break Signal           :on
Autoboot (Guest Domain) :on
Elastic Mode           :off
IOreconfigure          :false
CPU Mode               :auto
PPAR DR (Current)      :-
PPAR DR (Next)         :off
```

7. **Éteignez l'alimentation.**
8. **Configurez le commutateur de mode du panneau de commande à « Locked ».**
9. **Allumez l'alimentation pour démarrer la partition physique.**
10. **Vérifiez que le mode de démarrage a bien été défini à « fast ».**
Pour plus de détails sur la commande `xscfstartupmode(8)`, consultez *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

```
XSCF> xscfstartupmode -d  
Setting Mode: fast  
Current Mode: fast
```

Variables d'environnement et commandes d'OpenBoot PROM

Cette annexe décrit les commandes d'OpenBoot PROM spécifiques au système SPARC M12/M10, ainsi que les commandes et les variables d'environnement d'OpenBoot PROM qui ne sont pas prises en charge par les systèmes SPARC M12/M10, et le comportement avec le mode de sécurité activé.

Pour plus de détails sur des points non décrits dans cette annexe, consultez l'explication eeprom dans le manuel de référence d'Oracle Solaris et le *OpenBoot 4.x Command Reference Manual* d'Oracle Corporation.

- [Affichage des périphériques SCSI](#)
- [Variables d'environnement d'OpenBoot PROM non prises en charge](#)
- [Commandes d'OpenBoot PROM non prises en charge](#)
- [Comportement avec le mode de sécurité activé](#)

H.1 Affichage des périphériques SCSI

Pour afficher tous les périphériques sur le bus SCSI, utilisez la commande `probe-scsi-all`.

```
{0} ok probe-scsi-all
```

H.2 Variables d'environnement d'OpenBoot PROM non prises en charge

Dans les systèmes SPARC M12/M10, les variables d'environnement d'OpenBoot PROM suivantes ne peuvent pas être utilisées.

- `diag-device`
- `diag-file`

- diag-level
- os-root-device

Pour configurer/afficher le niveau de diagnostic Power-On Self-Test (POST) approprié pour diag-level, utilisez les commandes setpparmode ou showpparmode du microprogramme XSCF.

H.3 Commandes d'OpenBoot PROM non prises en charge

Dans les systèmes SPARC M12/M10, les commandes d'OpenBoot PROM suivantes ne peuvent pas être utilisées.

- cache-off
- cache-on
- callback
- clear-cache
- ecdatal
- ecdatal@
- ectagl
- ectagl@
- eject floppy
- firmware-version
- flush-cache
- help dump
- iomap?
- iomap-page
- iomap-pages
- iopgmap@
- iopgmap!
- map-region
- map-segments
- obdiag
- pgmap?
- rmap!
- rmap@
- sbus
- segmentsize
- smap!

- smap?
- smap@
- test-all
- .ver
- %f0 à %f31

H.4 Comportement avec le mode de sécurité activé

Lorsque le mode de sécurité de la variable d'environnement OpenBoot PROM est réglée sur « command » ou « full » et une chaîne de caractères affichables de un à huit caractères est réglé comme mot de passe de sécurité, le mode de sécurité d'OpenBoot PROM est activé et le mot de passe est requis pour les opérations et les commandes.

(1) Lorsque le mode de sécurité est réglé sur « command »

La commande boot et la commande go ne requièrent pas le mot de passe, mais toutes les autres commandes requièrent le mot de passe. Notez que le système démarre automatiquement lorsque « auto-boot? = true » est spécifié.

(2) Lorsque le mode de sécurité est réglé sur « full »

Toute action, y compris les opérations ordinaires telles que la commande boot requiert le mot de passe pour l'exécution, à l'exception de la commande go. Le mot de passe est requis au lancement du démarrage même lorsque « auto-boot? = true » est spécifié.

Lorsque le mode de sécurité est activé, l'invite d' OpenBoot PROM passe de « ok » au mode d'invite de sécurité avec > déclenché par l'une des options suivantes et le mot de passe est requis pour les cas (1) et (2) ci-dessus.

- La commande logout est exécutée.
- La console de domaine est déconnectée et reconnectée lorsque OpenBoot PROM est en fonctionnement (2340 XCP ou version ultérieure).
- Un signal d'interruption est envoyé.
- Le domaine est redémarré.
- Une erreur s'est produite pendant l'exécution d'une commande OpenBoot PROM.

Pour plus de détails sur le mode de sécurité de la variable d'environnement OpenBoot PROM, consultez le manuel d'Oracle.

Comment spécifier le périphérique de démarrage

Cette annexe décrit comment spécifier un stockage interne comme périphérique de démarrage dans l'OpenBoot PROM d'un domaine logique dans le système SPARC M12/M10.

- [Chemin d'accès de périphérique du stockage interne](#)
- [Méthode de spécification avec un numéro PHY](#)
- [Méthode de spécification avec un ID cible](#)
- [Méthode de spécification avec une adresse SAS](#)
- [Méthode de spécification avec un nom de périphérique de volume](#)

I.1 Chemin d'accès de périphérique du stockage interne

Pour spécifier un stockage interne comme périphérique de démarrage, ajoutez les informations d'identification du disque à la fin du chemin d'accès de périphérique du stockage interne. Le chemin d'accès de périphérique du stockage interne varie selon le modèle ou le nombre de processeurs montés. Pour plus de détails, consultez « [Annexe A Listes des chemins d'accès de périphériques des systèmes SPARC M12/M10](#) ».

Il existe quatre méthodes pour identifier un stockage interne, c'est-à-dire pour spécifier un stockage interne comme périphérique de démarrage. [Tableau I-1](#) décrit ces quatre méthodes. Notez que les méthodes de spécification qui peuvent être utilisées diffèrent entre un disque dur autonome intégré et un volume RAID intégré.

Tableau I-1 Méthodes de spécification du stockage interne comme périphérique de démarrage

Méthode de spécification	Résumé	Type de stockage interne applicable
Avec un numéro PHY	Cette méthode de spécification utilise le numéro PHY correspondant à l'emplacement de disque sur lequel le disque intégré est installé. Elle est aussi utilisée en tant que devalias dans OpenBoot PROM.	Disque dur autonome
Avec un ID cible	Cette méthode de spécification utilise l'ID cible unique attribué au disque intégré. L'ID cible peut varier en fonction de l'ordre d'installation des disques.	Disque dur autonome
Avec une adresse SAS	Cette méthode de spécification utilise l'adresse SAS unique attribuée au disque intégré. L'adresse SAS est changée lorsque le disque est remplacé.	Disque dur autonome
Avec un nom de périphérique de volume	Cette méthode de spécification utilise le nom de périphérique de volume RAID matériel.	RAID matériel

I.2 Méthode de spécification avec un numéro PHY

Cette méthode utilise le numéro PHY correspondant à l'emplacement de montage d'un disque intégré pour identifier le disque utilisé comme périphérique de démarrage.

Vous pouvez utiliser cette méthode de spécification lorsque vous choisissez un disque dur autonome intégré comme périphérique de démarrage. Cependant, vous ne pouvez pas l'utiliser pour spécifier un RAID matériel intégré.

[Tableau I-2](#) répertorie les numéros PHY correspondants aux emplacements de disques.

Tableau I-2 Numéros PHY correspondant aux emplacements de disques

Emplacement de disque	Numéro PHY
Emplacement de disque intégré #0	100 ou 0
Emplacement de disque intégré #1	101 ou 1
Emplacement de disque intégré #2	102 ou 2
Emplacement de disque intégré #3	103 ou 3
Emplacement de disque intégré #4	104 ou 4
Emplacement de disque intégré #5	105 ou 5
Emplacement de disque intégré #6	106 ou 6
Emplacement de disque intégré #7	107 ou 7

Pour trouver le numéro de disque du disque de démarrage, exécutez la commande `probe-scsi-all` dans OpenBoot PROM, et vérifiez la valeur `PhyNum`.

```
{0} ok probe-scsi-all
/pci@8000/pci@4/pci@0/pci@0/scsi@0
FCode Version 1.00.56, MPT Version 2.00, Firmware Version 13.00.54.00
Target a
Unit 0 Disk TOSHIBA MBF2300RC 3706 585937500 Blocks, 300 GB
SASDeviceName 50000393d82891d0 SASAddress 50000393d82891d2 PhyNum 0
                                                    Numéro PHY
Target b
Unit 0 Disk TOSHIBA MBF2300RC 3706 585937500 Blocks, 300 GB
SASDeviceName 50000393d8289180 SASAddress 50000393d8289182 PhyNum 1
Target e
Unit 0 Encl Serv device FUJITSU BBEXP 0d32
SASAddress 500000e0e06d233d PhyNum 14
```

Notation de périphérique de démarrage

<Chemin d'accès du contrôleur SAS>/disk@pX,Y:Z

Ici, remplacez le X après « disk@p » par le numéro PHY correspondant à l'emplacement de montage du disque. D'autre part, indiquez le numéro d'unité logique (LUN) et le numéro de tranche du stockage interne, respectivement pour Y et Z.

Remarque : vous pouvez omettre les numéros d'unité logique (LUN) et de tranche. Dans ce cas, le numéro LUN est considéré comme « 0 » et le numéro de tranche « a ». Si un stockage interne est utilisé comme périphérique de démarrage, un LUN de « 0 » et un numéro de tranche « a » sont spécifiés, ces numéros sont donc identiques aux valeurs prises lorsqu'ils sont omis. Par conséquent, dans l'exemple d'utilisation, la notation est dans une forme qui les omet.

Exemple d'utilisation

Indiquez la valeur suivante, où « 0 » est le numéro PHY du disque de démarrage.

```
{0} ok boot /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@p0
```

I.3 Méthode de spécification avec un ID cible

Cette méthode utilise l'ID cible unique attribué à chaque disque pour identifier le disque utilisé comme périphérique de démarrage.

Vous pouvez utiliser cette méthode de spécification lorsque vous choisissez un disque dur autonome intégré comme périphérique de démarrage. Vous ne pouvez pas par contre l'utiliser pour spécifier un RAID matériel intégré.

Pour trouver l'ID cible du disque de démarrage, exécutez la commande `probe-scsi-all` dans OpenBoot PROM, et vérifiez la valeur Target.

```
{0} ok probe-scsi-all
/pci@8000/pci@4/pci@0/pci@0/scsi@0
FCode Version 1.00.56, MPT Version 2.00, Firmware Version 13.00.54.00
Target a
  ID cible
Unit 0 Disk TOSHIBA MBF2300RC 3706 585937500 Blocks, 300 GB
SASDeviceName 50000393d82891d0 SASAddress 50000393d82891d2 PhyNum 0
Target b
Unit 0 Disk TOSHIBA MBF2300RC 3706 585937500 Blocks, 300 GB
SASDeviceName 50000393d8289180 SASAddress 50000393d8289182 PhyNum 1
Target e
Unit 0 Encl Serv device FUJITSU BBEXP 0d32
SASAddress 500000e0e06d233d PhyNum 14
```

Notation de périphérique de démarrage

```
<Chemin d'accès du contrôleur SAS>/disk@X,Y:Z
```

Ici, remplacez le *X* après « `disk@` » par l'ID cible. D'autre part, indiquez le numéro d'unité logique (LUN) et le numéro de tranche du stockage interne, respectivement pour *Y* et *Z*.

Remarque : vous pouvez omettre les numéros d'unité logique (LUN) et de tranche. Dans ce cas, le numéro LUN est considéré comme « 0 » et le numéro de tranche « a ». Si un stockage interne est utilisé comme périphérique de démarrage, un LUN de « 0 » et un numéro de tranche « a » sont spécifiés, ces numéros sont donc identiques aux valeurs prises lorsqu'ils sont omis. Par conséquent, dans l'exemple d'utilisation, la notation est dans une forme qui les omet.

Exemple d'utilisation

Indiquez la valeur suivante, où « *a* » est l'ID cible du disque de démarrage.

```
{0} ok boot /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@a
```

I.4 Méthode de spécification avec une adresse SAS

Cette méthode utilise l'adresse SAS unique d'un lecteur de disque pour indiquer le périphérique de démarrage.

Pour le stockage interne, chaque lecteur de disque dispose d'une adresse SAS attribuée unique, qui est changée lorsque le disque est remplacé. Après un remplacement de disque, le nom de périphérique indiqué lors du démarrage change en conséquence.

Vous pouvez utiliser cette méthode de spécification lorsque vous choisissez un disque dur autonome intégré comme périphérique de démarrage. Vous ne pouvez pas par contre l'utiliser pour spécifier un RAID matériel intégré.

Pour trouver l'adresse SAS cible du disque de démarrage, exécutez la commande `probe-scsi-all` dans OpenBoot PROM, et vérifiez la valeur `SASAddress`.

```
{0} ok probe-scsi-all
/pci@8000/pci@4/pci@0/pci@0/scsi@0
FCode Version 1.00.56, MPT Version 2.00, Firmware Version 13.00.54.00
Target a
Unit 0 Disk TOSHIBA MBF2300RC 3706 585937500 Blocks, 300 GB
SASDeviceName 50000393d82891d0 SASAddress 50000393d82891d2 PhyNum 0
                               Adresse SAS
Target b
Unit 0 Disk TOSHIBA MBF2300RC 3706 585937500 Blocks, 300 GB
SASDeviceName 50000393d8289180 SASAddress 50000393d8289182 PhyNum 1
Target e
Unit 0 Encl Serv device FUJITSU BBEXP 0d32
SASAddress 500000e0e06d233d PhyNum 14
```

Notation de périphérique de démarrage

```
<Chemin d'accès du contrôleur SAS>/disk@wXXXXXXXX, Y:Z
```

Ici, remplacez le XXXXXXXX après « `disk@w` » par l'adresse SAS. D'autre part, indiquez le numéro d'unité logique (LUN) et le numéro de tranche du stockage interne, respectivement pour Y et Z.

Remarque : vous pouvez omettre les numéros d'unité logique (LUN) et de tranche. Dans ce cas, le numéro LUN est considéré comme « 0 » et le numéro de tranche « a ». Si un stockage interne est utilisé comme périphérique de démarrage, un LUN de « 0 » et un numéro de tranche « a » sont spécifiés, ces numéros sont donc identiques aux valeurs prises lorsqu'ils sont omis. Par conséquent, dans l'exemple d'utilisation, la notation est dans une forme qui les omet.

Exemple d'utilisation

Indiquez la valeur suivante, où « 50000393d82891d2 » est l'adresse SAS du disque de démarrage.

```
{0} ok boot /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@w50000393d82891d2
```

I.5 Méthode de spécification avec un nom de périphérique de volume

Cette méthode utilise le nom de périphérique de volume d'un RAID matériel intégré pour indiquer le périphérique de démarrage. Le nom de périphérique de volume est attribué à chaque volume configuré dans le RAID.

Vous pouvez utiliser cette méthode lorsque vous choisissez un RAID matériel intégré comme périphérique de démarrage.

Pour trouver le nom de périphérique de volume du disque de démarrage, exécutez la commande `probe-scsi-all` dans OpenBoot PROM, et vérifiez la valeur `VolumeDeviceName`.

```
{0} ok probe-scsi-all
/pci@8000/pci@4/pci@0/scsi@0
FCode Version 1.00.56, MPT Version 2.00, Firmware Version 13.00.54.00
Target 11e Volume 0
Unit 0 Disk LSI Logical Volume 3000 10485760 Blocks, 5368 MB
VolumeDeviceName 3eb2fdbd4c32058f VolumeWWID 0eb2fdbd4c32058f
Nom de périphérique de volume
```

Dans XCP 2070 ou les versions antérieures, il se peut que `VolumeDeviceName` ne soit pas affiché. Dans ce cas, exécutez la commande `show-volumes`, qui affichera un volume WWID. Remplacez le premier caractère du WWID par « 3 » pour obtenir le nom de périphérique de volume.

```
{0} ok select /pci@8000/pci@4/pci@0/pci@0/scsi@0
{0} ok show-volumes
Volume 0 Target 11e Type RAID1 (Mirroring)
Name raid1-volume WWID 0eb2fdbd4c32058f
WWID du volume RAID
Optimal Enabled Data Scrub In Progress
2 Members 1169920000 Blocks, 598 GB
Disk 1
Primary Optimal
Target a TOSHIBA MBF2300RC 3706
Disk 0
Secondary Optimal
```



```
Target b TOSHIBA MBF2300RC 3706
{0} ok
```

Notation de périphérique de démarrage

```
<Chemin d'accès du contrôleur SAS>/disk@wXXXXXXXX, Y:Z
```

Ici, remplacez le XXXXXXXX après « disk@w » par le nom de périphérique de volume. D'autre part, indiquez le numéro d'unité logique (LUN) et le numéro de tranche RAID matériel intégré, respectivement pour Y et Z.

Remarque : vous pouvez omettre les numéros d'unité logique (LUN) et de tranche. Dans ce cas, le numéro LUN est considéré comme « 0 » et le numéro de tranche « a ». Si un RAID matériel intégré est utilisé comme périphérique de démarrage, un LUN de « 0 » et un numéro de tranche « a » sont spécifiés, ces numéros sont donc identiques aux valeurs prises lorsqu'ils sont omis. Par conséquent, dans l'exemple d'utilisation, la notation est dans une forme qui les omet.

Exemple d'utilisation

Indiquez la valeur suivante, où « 3eb2fdbd4c32058f » est le nom de périphérique de volume du périphérique de démarrage.

```
{0} ok boot /pci@8000/pci@4/pci@0/pci@0/scsi@0/disk@w3eb2fdbd4c32058f
```


Listes des alias des lecteurs DVD

Cette annexe décrit les alias des lecteurs DVD.

- [Alias des lecteurs DVD externes](#)
- [Alias des lecteurs DVD de stockage à distance](#)

J.1 Alias des lecteurs DVD externes

Cette section répertorie les alias des lecteurs DVD externes dans les systèmes SPARC M12/M10.

J.1.1 Alias des lecteurs DVD externes SPARC M12-1

Tableau J-1 Alias des lecteurs DVD externes SPARC M12-1

Alias	Chemin d'accès de périphériques
cdrom (avant)	/pci@8100/pci@4/pci@0/pci@8/usb@0/cdrom@6/disk@0 (USB2.0/1.1)
cdrom0-30 (arrière)	/pci@8100/pci@4/pci@0/pci@8/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom0 (arrière)	/pci@8100/pci@4/pci@0/pci@8/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom1 (avant)	/pci@8100/pci@4/pci@0/pci@8/usb@0/cdrom@6/disk@0 (USB2.0/1.1)

J.1.2 Alias des lecteurs DVD externes SPARC M12-2

Pour une configuration à 1 processeur (CMUL) ou 2 processeurs à l'installation initiale

Tableau J-2 Alias des lecteurs DVD externes SPARC M12-2 (au moment de l'installation initiale : 1 processeur ou 2 processeurs)

Alias	Chemin d'accès de périphériques
cdrom (avant)	/pci@8100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom00-0-30 (arrière)	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom00-0 (arrière)	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom00-1 (avant)	/pci@8100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)

J.1.3 Alias des lecteurs DVD externes SPARC M12-2S

Pour une configuration à 1 processeur (CMUL) ou 2 processeurs à l'installation initiale

Tableau J-3 Alias des lecteurs DVD externes SPARC M12-2S (au moment de l'installation initiale : 1 processeur ou 2 processeurs)

Alias	Chemin d'accès de périphériques
cdrom (avant)	/pci@8100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom00-0-30 (arrière)	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom00-0 (arrière)	/pci@8100/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom00-1 (avant)	/pci@8100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom01-0-30 (arrière)	/pci@8900/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom01-0 (arrière)	/pci@8900/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)

Tableau J-3 Alias des lecteurs DVD externes SPARC M12-2S (au moment de l'installation initiale : 1 processeur ou 2 processeurs) (*suite*)

Alias	Chemin d'accès de périphériques
cdrom01-1 (avant)	/pci@8900/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom02-0-30 (arrière)	/pci@9100/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom02-0 (arrière)	/pci@9100/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom02-1 (avant)	/pci@9100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom03-0-30 (arrière)	/pci@9900/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom03-0 (arrière)	/pci@9900/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom03-1 (avant)	/pci@9900/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom04-0-30 (arrière)	/pci@a100/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom04-0 (arrière)	/pci@a100/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom04-1 (avant)	/pci@a100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom05-0-30 (arrière)	/pci@a900/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom05-0 (arrière)	/pci@a900/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom05-1 (avant)	/pci@a900/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom06-0-30 (arrière)	/pci@b100/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom06-0 (arrière)	/pci@b100/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom06-1 (avant)	/pci@b100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom07-0-30 (arrière)	/pci@b900/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom07-0 (arrière)	/pci@b900/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom07-1 (avant)	/pci@b900/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom08-0-30 (arrière)	/pci@c100/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)

Tableau J-3 Alias des lecteurs DVD externes SPARC M12-2S (au moment de l'installation initiale : 1 processeur ou 2 processeurs) *(suite)*

Alias	Chemin d'accès de périphériques
cdrom08-0 (arrière)	/pci@c100/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom08-1 (avant)	/pci@c100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom09-0-30 (arrière)	/pci@c900/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom09-0 (arrière)	/pci@c900/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom09-1 (avant)	/pci@c900/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom10-0-30 (arrière)	/pci@d100/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom10-0 (arrière)	/pci@d100/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom10-1 (avant)	/pci@d100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom11-0-30 (arrière)	/pci@d900/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom11-0 (arrière)	/pci@d900/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom11-1 (avant)	/pci@d900/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom12-0-30 (arrière)	/pci@e100/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom12-0 (arrière)	/pci@e100/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom12-1 (avant)	/pci@e100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom13-0-30 (arrière)	/pci@e900/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom13-0 (arrière)	/pci@e900/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom13-1 (avant)	/pci@e900/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)
cdrom14-0-30 (arrière)	/pci@f100/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom14-0 (arrière)	/pci@f100/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@1/disk@0 (USB2.0/1.1)
cdrom14-1 (avant)	/pci@f100/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)

Tableau J-3 Alias des lecteurs DVD externes SPARC M12-2S (au moment de l'installation initiale : 1 processeur ou 2 processeurs) (*suite*)

Alias	Chemin d'accès de périphériques
cdrom15-0-30 (arrière)	/pci@f900/pci@4/pci@0/pci@1/usb@0/hub@1/cdrom@1/disk@0 (USB3.0)
cdrom15-0 (arrière)	/pci@f900/pci@4/pci@0/pci@1/usb@0/hub@5/cdrom@6/disk@0 (USB2.0/1.1)
cdrom15-1 (avant)	/pci@f900/pci@4/pci@0/pci@1/usb@0/cdrom@6/disk@0 (USB3.0/2.0/1.1)

J.1.4 Alias des lecteurs DVD externes SPARC M10-1

Tableau J-4 Alias des lecteurs DVD externes SPARC M10-1

Alias	Chemin d'accès de périphériques
cdrom (avant)	/pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/cdrom@2/disk@0
cdrom0 (arrière)	/pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/cdrom@1/disk@0
cdrom1 (avant)	/pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/cdrom@2/disk@0

J.1.5 Alias des lecteurs DVD externes SPARC M10-4

Pour une configuration à 2 processeurs (CMUL) ou 4 processeurs à l'installation initiale

Tableau J-5 Alias des lecteurs DVD externes SPARC M10-4 (au moment de l'installation initiale : 2 processeurs ou 4 processeurs)

Alias	Chemin d'accès de périphériques
cdrom (avant)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom00-0 (arrière)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom00-1 (avant)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a

J.1.6 Alias des lecteurs DVD externes SPARC M10-4S

[Tableau J-6](#) répertorie les alias des lecteurs DVD externes, où les cartes système logiques (LSB) sont numérotées de 0 à 15.

Pour une configuration à 2 processeurs (CMUL) ou 4 processeurs à l'installation initiale

Tableau J-6 Alias des lecteurs DVD externes SPARC M10-4S (au moment de l'installation initiale : 2 processeur ou 4 processeurs)

Alias	Chemin d'accès de périphériques
cdrom (avant)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom00-0 (arrière)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom00-1 (avant)	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom01-0 (arrière)	/pci@8800/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom01-1 (avant)	/pci@8800/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom02-0 (arrière)	/pci@9000/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom02-1 (avant)	/pci@9000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom03-0 (arrière)	/pci@9800/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom03-1 (avant)	/pci@9800/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom04-0 (arrière)	/pci@a000/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom04-1 (avant)	/pci@a000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom05-0 (arrière)	/pci@a800/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom05-1 (avant)	/pci@a800/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom06-0 (arrière)	/pci@b000/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom06-1 (avant)	/pci@b000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom07-0 (arrière)	/pci@b800/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom07-1 (avant)	/pci@b800/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom08-0 (arrière)	/pci@c000/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom08-1 (avant)	/pci@c000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom09-0 (arrière)	/pci@c800/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom09-1 (avant)	/pci@c800/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom10-0 (arrière)	/pci@d000/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom10-1 (avant)	/pci@d000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom11-0 (arrière)	/pci@d800/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom11-1 (avant)	/pci@d800/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom12-0 (arrière)	/pci@e000/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom12-1 (avant)	/pci@e000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom13-0 (arrière)	/pci@e800/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom13-1 (avant)	/pci@e800/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom14-0 (arrière)	/pci@f000/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a

Tableau J-6 Alias des lecteurs DVD externes SPARC M10-4S (au moment de l'installation initiale : 2 processeur ou 4 processeurs) (*suite*)

Alias	Chemin d'accès de périphériques
cdrom14-1 (avant)	/pci@f000/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a
cdrom15-0 (arrière)	/pci@f800/pci@4/pci@0/pci@1/pci@0/usb@4,1/cdrom@1/disk@0,0:a
cdrom15-1 (avant)	/pci@f800/pci@4/pci@0/pci@1/pci@0/usb@4,1/hub@2/cdrom@1/disk@0,0:a

J.2 Alias des lecteurs DVD de stockage à distance

Cette section répertorie les alias des lecteurs DVD de stockage à distance dans les systèmes SPARC M12/M10.

J.2.1 Alias des lecteurs DVD de stockage à distance SPARC M12-1

Tableau J-7 Alias des lecteurs DVD de stockage à distance SPARC M12-1

Alias	Chemin d'accès de périphériques
rcdrom	/pci@8100/pci@4/pci@0/pci@8/usb@0/storage@7/disk@0

J.2.2 Alias des lecteurs DVD de stockage à distance SPARC M12-2

Pour une configuration à 1 processeur (CMUL) ou 2 processeurs à l'installation initiale

Tableau J-8 Alias des lecteurs DVD de stockage à distance SPARC M12-2 (au moment de l'installation initiale : 1 processeur ou 2 processeurs)

Alias	Chemin d'accès de périphériques
rcdrom	/pci@8100/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom00	/pci@8100/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0

J.2.3

Alias des lecteurs DVD de stockage à distance
SPARC M12-2S

Pour une configuration à 1 processeur (CMUL) ou 2 processeurs à l'installation initiale

Tableau J-9 Alias des lecteurs DVD de stockage à distance SPARC M12-2S (au moment de l'installation initiale : 1 processeur ou 2 processeurs)

Alias	Chemin d'accès de périphériques
rcdrom	/pci@8100/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom00	/pci@8100/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom01	/pci@8900/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom02	/pci@9100/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom03	/pci@9900/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom04	/pci@a100/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom05	/pci@a900/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom06	/pci@b100/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom07	/pci@b900/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom08	/pci@c100/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom09	/pci@c900/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom10	/pci@d100/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom11	/pci@d900/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom12	/pci@e100/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom13	/pci@e900/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom14	/pci@f100/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0
rcdrom15	/pci@f900/pci@4/pci@0/pci@1/usb@0/storage@7/disk@0

J.2.4

Alias des lecteurs DVD de stockage à distance
SPARC M10-1

Tableau J-10 Alias des lecteurs DVD de stockage à distance SPARC M10-1

Alias	Chemin d'accès de périphériques
rcdrom	/pci@8000/pci@4/pci@0/pci@2/pci@0/usb@4,1/storage@3/disk@0

J.2.5 Alias des lecteurs DVD de stockage à distance SPARC M10-4

Pour une configuration à 2 processeurs (CMUL) ou 4 processeurs à l'installation initiale

Tableau J-11 Alias des lecteurs DVD de stockage à distance SPARC M10-4 (au moment de l'installation initiale : 2 processeurs ou 4 processeurs)

Alias	Chemin d'accès de périphériques
rcdrom	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom00	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a

J.2.6 Alias des lecteurs DVD de stockage à distance SPARC M10-4S

Tableau J-12 répertorie les alias des lecteurs DVD pour stockage à distance, où les cartes système logiques (LSB) sont numérotées de 0 à 15.

Pour une configuration à 2 processeurs (CMUL) ou 4 processeurs à l'installation initiale

Tableau J-12 Alias des lecteurs DVD de stockage à distance SPARC M10-4S (au moment de l'installation initiale : 2 processeurs ou 4 processeurs)

Alias	Chemin d'accès de périphériques
rcdrom	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom00	/pci@8000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom01	/pci@8800/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom02	/pci@9000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom03	/pci@9800/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom04	/pci@a000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom05	/pci@a800/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom06	/pci@b000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom07	/pci@b800/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom08	/pci@c000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom09	/pci@c800/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom10	/pci@d000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a

Tableau J-12 Alias des lecteurs DVD de stockage à distance SPARC M10-4S (au moment de l'installation initiale : 2 processeurs ou 4 processeurs) *(suite)*

Alias	Chemin d'accès de périphériques
rcdrom11	/pci@d800/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom12	/pci@e000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom13	/pci@e800/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom14	/pci@f000/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a
rcdrom15	/pci@f800/pci@4/pci@0/pci@1/pci@0/usb@4,1/storage@3/disk@0,0:a

Permis temporaire d'activation de processeur

Cette annexe décrit le permis temporaire d'activation de processeur. L'utilisation d'un permis temporaire d'activation de processeur permet, avant d'ajouter et d'obtenir un nombre suffisant d'activations de processeur, d'utiliser les ressources de cœur de processeur supplémentaires.

- [Qu'est-ce que le permis temporaire d'activation de processeur ?](#)
- [Conditions d'utilisation du permis temporaire d'activation de processeur et précautions](#)
- [Commandes liées](#)
- [Étapes et procédures d'utilisation d'un permis temporaire d'activation de processeur](#)
- [Notification d'événement d'un permis temporaire d'activation de processeur](#)
- [Autres notes importantes](#)

K.1 Qu'est-ce que le permis temporaire d'activation de processeur ?

L'activation du processeur est une fonction SPARC M12/M10 qui vous permet d'optimiser votre opération.

En enregistrant des clés d'activation de processeur supplémentaires avec votre SPARC M12/M10, des cœurs de processeur supplémentaires peuvent être ajoutés dynamiquement sans interruption des charges de travail de production. Cette fonction SPARC M12/M10 vous permet d'optimiser votre investissement de serveur.

Cependant, le processus d'achat d'une activation de processeur peut prendre plus d'un d'un jour, bien que vous pourriez déjà avoir besoin de vos ressources de cœurs du processeur supplémentaires. La fonction SPARC M12/M10 du permis temporaire d'activation de CPU résout ce problème.

Pour activer un permis temporaire d'activation de processeur, vous n'avez pas besoin d'ajouter de clé d'activation de processeur. Une fois que le permis temporaire est activé, tous les cœurs physiques disponibles dans la partition physique (PPAR) ou le

SPARC M12/M10 peuvent être utilisés pendant 30 jours.

Le permis temporaire d'activation de processeur vous permet d'utiliser immédiatement les ressources de cœur du processeur même lorsqu'aucune clé d'activation de processeur supplémentaire achetée n'est à portée de main.

K.2 Conditions d'utilisation du permis temporaire d'activation de processeur et précautions

Vous pouvez utiliser le permis temporaire d'activation de processeur en exécutant les commandes du microprogramme XSCF. [Tableau K-1](#) indique les versions de microprogramme XSCF nécessaires pour chaque système, afin d'utiliser le permis temporaire d'activation de processeur. La version listée du microprogramme dans [Tableau K-1](#) doit être installée sur votre système pour utiliser un permis temporaire d'activation de processeur.

Tableau K-1 Modèles pris en charge pour le permis temporaire d'activation de processeur

Modèle	Version XCP	Modalités d'utilisation
SPARC M10-1/M10-4 (*1)	XCP 232x	Un permis temporaire d'activation de processeur peut être utilisé une seule fois pour le SPARC M10-1/M10-4. (*2)
	XCP 2330 ou version ultérieure	Un permis temporaire d'activation de processeur peut être utilisé plus d'une fois, sous certaines conditions. (*3)
SPARC M12-1/M12-2/ M12-2S/M10-4S	XCP 2330 ou version ultérieure	Un permis temporaire d'activation de processeur peut être utilisé pour chaque PPAR. Un permis temporaire d'activation de processeur peut être utilisé plus d'une fois, sous certaines conditions. (*3)

- *1 Le SPARC M10-1 et le SPARC M10-4 prennent en charge un permis temporaire d'activation de processeur avec XCP 2320 et version ultérieure. Cependant, nous recommandons d'utiliser un permis temporaire d'activation de processeur avec XCP 2330 ou version ultérieure, ce qui vous permet de réactiver un permis temporaire d'activation de processeur sous les conditions appropriées.
- *2 Une fois que vous avez utilisé le permis temporaire d'activation de processeur, vous ne pouvez plus utiliser cette fonction à nouveau même après la mise à jour vers XCP 2330 ou une version ultérieure.
- *3 Pour utiliser le permis temporaire d'activation de processeur, vous devez d'abord enregistrer les clés d'activation du processeur supplémentaires achetées et paramétrer pour ajouter les activations de processeur achetées à la partition physique (pour le SPARC M12-2S/M10-4S) ou sur le système (pour le SPARC M12-1/M12-2/M10-1/M10-4). Si l'enregistrement d'activations de processeur supplémentaires achetées et le paramétrage pour attribuer les ressources de cœur de processeur supplémentaires à la partition physique (pour le SPARC M12-2S/M10-4S) ou le système (pour le SPARC M12-1/M12-2/M10-1/M10-4) n'ont pas été réalisés depuis la dernière activation du permis temporaire d'activation de processeur, vous ne pouvez pas activer à nouveau le permis temporaire d'activation de processeur. Pour plus de détails, consultez « [Activation à plusieurs reprises du permis temporaire d'activation de processeur](#) ».

Précautions

- Un permis temporaire d'activation de processeur peut être utilisé pendant 30 jours. Veillez à ajouter la clé d'activation de processeur déjà achetée dans cette période. Si le permis temporaire d'activation de CPU expire alors que le nombre de cœurs du processeur utilisés par Oracle VM Server pour SPARC est supérieur ou égal la quantité sous les activations de processeur achetées installées, Oracle VM Server pour SPARC supprime automatiquement les cœurs du processeur en trop.
- Lorsque le permis temporaire d'activation de processeur est activé, tous les cœurs de processeur du système (une partition physique dans le cas du SPARC M12-2S/M10-4S) sont activés. Ainsi, la fonction de remplacement automatique de processeur ne fonctionne pas lorsqu'une défaillance de cœur du processeur survient.
- Les coûts de la licence de certains types de logiciels varient selon le nombre de cœurs utilisés. Confirmez les conditions de la licence du logiciel lors de l'ajout de cœurs du processeur pour une utilisation avec un permis temporaire d'activation de CPU.

K.3 Commandes liées

Cette section décrit les commandes liées au permis temporaire d'activation de processeur.

K.3.1 Commandes pour l'utilisation d'un permis temporaire d'activation de processeur

Tableau K-2 répertorie les commandes XSCF pour l'utilisation d'un permis temporaire d'activation de processeur.

Tableau K-2 Commandes XSCF pour l'utilisation d'un permis temporaire d'activation de processeur

Utilisation	Commande
Pour activer/désactiver le permis temporaire d'activation de processeur	setinterimpermit(8)
Pour afficher les informations de réglage/l'état du permis temporaire d'activation de processeur	showinterimpermit(8)
Utilisation du cœur de processeur d'un permis temporaire d'activation de processeur	showinterimpermitusage(8) (*1)

*1 XCP 232x ne prend pas en charge la commande showinterimpermitusage(8).

Pour plus de détails sur chaque commande, consultez le *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF Reference Manual*.

K.3.2 Commandes liées à l'utilisation d'un permis temporaire d'activation de processeur

Les commandes suivantes sont utilisées pour gérer (enregistrer/supprimer) les activations de processeur achetées ou pour afficher l'état des cœurs de processeur. Elles sont également utilisées pendant l'utilisation d'un permis temporaire d'activation de processeur.

- addcodactivation
- deletecodactivation
- showcodactivation
- setcod
- showcod
- showcodusage
- showcodactivationhistory

Ces commandes n'affichent pas les réglages du permis temporaire d'activation de processeur ni l'état d'utilisation des ressources de cœur de processeur disponibles lorsque le permis temporaire d'activation de processeur est activé.

Lorsque le permis temporaire d'activation de CPU est activé, les clés d'activation de CPU ne sont pas utilisées pour gérer les ressources de cœur du processeur (vérification de la présence d'une violation d'utilisation). Cependant, même dans ce cas, vous pouvez changer le nombre de cœurs de processeur attribués au système en ajoutant ou supprimant des clés d'activation de processeur pour anticiper l'expiration du permis temporaire d'activation de processeur.

Pour vérifier si un permis temporaire d'activation de processeur est activé ou désactivé, vérifiez le journal des événements XSCF en exécutant la commande `showlogs event` du XSCF.

K.4 Étapes et procédures d'utilisation d'un permis temporaire d'activation de processeur

Cette section décrit les étapes et procédures d'utilisation d'un permis temporaire d'activation de processeur. Avant l'utilisation d'un permis temporaire d'activation de processeur, lisez attentivement les descriptions des étapes et procédures présentes dans cette section.

Cette section décrit également la situation dans laquelle la période de validité est écoulée lorsque les cœurs du processeur sont utilisés avec un permis temporaire d'activation de processeur activé, et quand le permis temporaire d'activation de processeur est désactivé.

K.4.1 Flux et procédures pour XCP 2330 et version ultérieure

Flux de fonctionnement pour XCP 2330 et version ultérieure

Le flux d'opérations est le suivant.

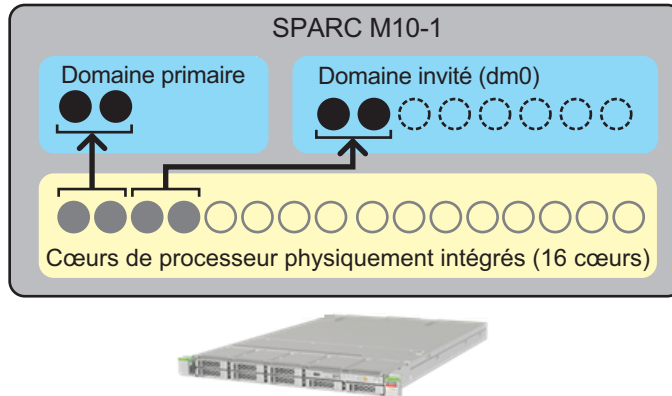
1. **Confirmez que des cœurs de processeur supplémentaires sont requis, puis démarrez le processus d'achat des activations de processeur requises.**
2. **Activez un permis temporaire d'activation de processeur.**
3. **Enregistrez les clés d'activation de processeur obtenues dans le système.**
4. **Désactivez le permis temporaire d'activation de processeur.**

Exemple de configuration

La description de « [Procédure de fonctionnement pour XCP 2330 et version ultérieure](#) » utilise la configuration suivante comme exemple.

- Le SPARC M10-1 à un seul socket de processeur avec 16 cœurs de processeur physiques est utilisé.
- Les activations de processeur pour activer les 4 cœurs de processeur ont été achetées et enregistrées sur le système.
- Le système est composé de deux domaines logiques en exécution.
 - Deux cœurs de processeur sont attribués au domaine de commande (domaine primaire).
 - Deux cœurs de processeur sont attribués au domaine invité (dm0).
- Pour répondre à une augmentation de charge, le domaine invité (dm0) requiert six cœurs de CPU supplémentaires.

Figure K-1 Exemple de configuration pour XCP 2330 ou version ultérieure (SPARC M10-1)



- : Cœur de processeur attribué au domaine logique
- (noir pointillé) : Cœur de processeur à attribuer au domaine logique
- (gris) : Cœur de processus activé par une clé d'activation de processeur achetée
- (blanc) : Cœur de processus physiquement intégré mais pas activé par une clé d'activation de processeur achetée

Remarque : les clés d'activation de processeur enregistrées dans le système activent un nombre défini de cœurs de processeur. Ils n'activent pas les cœurs du processeur en spécifiant le socket de CPU et l'emplacement physique de chaque cœur du processeur. Pour la facilité de compréhension, des cœurs du processeur spécifique sont activés et attribués aux domaines logiques dans [Figure K-1](#).

Remarque : dans un système SPARC M12-2S/M10-4S, le permis temporaire d'activation de processeur est activé/désactivé pour chaque PPAR.

Procédure de fonctionnement pour XCP 2330 et version ultérieure

La procédure de fonctionnement est la suivante.

1. **Confirmez que des cœurs de processeur supplémentaires sont requis, puis démarrez le processus d'achat des activations de processeur requises.**
Assurez-vous de vérifier ce qui suit avant de procéder à l'achat.
 - a. Déterminez si des cœurs de processeur supplémentaires sont requis à partir d'une analyse de la charge ou évaluez la manipulation pour l'ensemble du système, dans le cas d'un système M12-1/M12-2/M10-1/M10-4, ou pour la partition physique cible (PPAR), dans le cas d'un système SPARC M12-2S/M10-4S.
 - b. Un permis temporaire d'activation de processeur peut être utilisé pendant 30 jours. Nous vous recommandons de vérifier à l'avance combien de temps les clés d'activation de CPU prendront pour parvenir dans votre région. Pour ces

informations, contactez votre représentant commercial local.

2. Activez un permis temporaire d'activation de processeur.

Effectuez les opérations suivantes.

- a. Exécutez la commande `showinterimpermitsusage` du XSCF pour vérifier l'utilisation actuelle des cœurs de processeur du système.

```
XSCF> showinterimpermitsusage
```

```
PPAR-ID: 0
```

```
Installed Cores:                16
Purchased Cores Assigned to PPAR: 4
Cores In Use by Ldoms:          4
Interim Assignable Cores:        0
In Use Interim Cores:            0
```

Note:

Please confirm the value of "Cores In Use by Ldoms" using the Oracle VM Server for SPARC `ldm` command.
The XSCF may take up to 20 minutes to reflect the "Cores In Use by Ldoms" of logical domains.

Dans le cas du SPARC M12-1/M12-2/M10-1/M10-4, seules les informations pour PPAR-ID 0 sont affichées. Dans le cas d'un SPARC M12-2S/M10-4S, les informations de toutes les PPAR ou d'une PPAR spécifiée sont affichées. Vérifiez l'utilisation des cœurs de processeur de la PPAR cible pour laquelle le permis temporaire d'activation de processeur est utilisé.

[Tableau K-3](#) indique la signification des valeurs affichées par la commande `showinterimpermitsusage`.

Tableau K-3 Signification de `showinterimpermitsusage`

Affichage de colonne	Description	Signification des valeurs de l'exemple de commande
Installed Cores	Nombre de cœurs de processeur physiques montés sur le système ou la PPAR	« 16 » : le système dispose de 16 cœurs de processeur physiques.
Purchased Cores Assigned to PPAR	Nombre d'activations de processeur attribuées à la PPAR	« 4 » : les activations de processeur pour activer 4 cœurs de processeur sont attribuées à ce système.
Cores In Use by Ldoms	Nombre de ressources du cœur de processeur actuellement utilisées dans les domaines logiques	« 4 » : 4 cœurs de processeur sont actuellement utilisés dans les domaines logiques.
Interim Assignable Cores	Nombre de cœurs de processeur supplémentaires rendus disponibles lors de l'activation d'un permis temporaire d'activation de processeur	« 0 » : aucun cœur de processeur supplémentaire disponible pour le moment. Référence - 12 : 12 cœurs de processeur supplémentaires sont disponibles.

Tableau K-3 Signification de showinterimpermitusage (suite)

Affichage de colonne	Description	Signification des valeurs de l'exemple de commande
In Use Interim Cores	Nombre de cœurs de processeur utilisés dans les domaines logiques, parmi les cœurs de processeur rendus disponibles lors de l'activation d'un permis temporaire d'activation de processeur	« 0 » : aucun cœur de processeur supplémentaire disponible utilisé dans les domaines logiques.

Si le nombre de « Purchased Cores Assigned to PPAR » est supérieur ou égal à celui de « Installed Cores », cela indique que les clés d'activation de processeur pour tous les cœurs de processeur physiquement intégrés ont bien été enregistrées. Dans ce cas, le permis temporaire d'activation de processeur n'est pas requis. N'activez pas la fonction.

- b. Exécutez la commande setinterimpermit du XSCF pour activer le permis temporaire d'activation de processeur.
Dans le cas du SPARC M12-1/M12-2/M10-1/M10-4, le PPAR-ID spécifié par la commande setinterimpermit est fixé à 0. Tous les cœurs de processeur des puces de processeur montées sur la partition physique (fixée sur PPAR 0) sont rendus disponibles par l'exécution de cette commande.
Dans le cas d'un système SPARC M12-2S/M10-4S, activez le permis temporaire d'activation de processeur en spécifiant une partition physique (PPAR). Dans ce cas, tous les cœurs de processeur dans toutes les puces de processeur montées sur chaque bloc de construction (SPARC M12-2S/M10-4S) qui compose la PPAR spécifiée sont rendus disponibles.

```
XSCF> setinterimpermit -p 0 -c enable

Note:
  Please add CPU Activation(s) within 30 days of enabling the Interim Permit.

The Interim Permit for the PPAR will be changed to enabled.
Continue? [y|n] :y

Completed.
```

- c. Exécutez la commande showinterimpermitusage du XSCF pour vérifier le nombre de cœurs de processeur supplémentaires rendus disponibles par l'utilisation du permis temporaire d'activation de processeur.

```
XSCF> showinterimpermitusage

PPAR-ID: 0
  Installed Cores:                16
  Purchased Cores Assigned to PPAR: 4
  Cores In Use by Ldoms:          4
  Interim Assignable Cores:       12
  In Use Interim Cores:           0
```

Note:

Please confirm the value of "Cores In Use by Ldoms" using the Oracle VM Server for SPARC ldm command.
The XSCF may take up to 20 minutes to reflect the "Cores In Use by Ldoms" of logical domains.

Cet exemple montre que « Interim Assignable Cores » est « 12 », ce qui signifie que 12 cœurs de processeur supplémentaires ont été mis à disposition par l'activation du permis temporaire d'activation de processeur. Dans ce cas, 12 cœurs de processeur supplémentaires peuvent être utilisés au maximum dans les domaines logiques pendant 30 jours.

Plutôt que d'utiliser tous les cœurs du processeur supplémentaires rendus disponibles, attribuez simplement les cœurs du processeur correspondant au nombre d'activations CPU que vous envisagez d'acheter pour les domaines logiques.

Par exemple, si vous souhaitez acheter et ajouter deux cœurs du processeur, nous recommandons vivement d'attribuer seulement deux cœurs du processeur supplémentaires au domaine logique. Si vous attribuez quatre cœurs de processeur aux domaines logiques puis que vous achetez une activation de processeur pour activer seulement deux cœurs de processeur supplémentaires, le total sera réduit de deux cœurs de processeur. Cela risque d'entraîner un problème de performance si vous désactivez le permis temporaire d'activation de processeur.

- d. Si vous exécutez la commande `showcodusage` du XSCF sans les options à ce stade, le message suivant s'affiche.

```
XSCF> showcodusage
Resource In Use Installed CoD Permitted Status
-----
PROC          4         16          4 OK: 0 cores available
PPAR-ID/Resource In Use Installed Assigned
-----
0 - PROC          4         16          4 cores
Unused - PROC     0          0          0 cores
```

Veuillez noter que si vous exécutez la commande `showcodusage` du XSCF à ce stade, le contenu affiché avant et après l'activation du permis temporaire d'activation de processeur ne change pas, même si le nombre de cœurs de processeur disponibles a augmenté par l'utilisation de la fonction.

[Tableau K-4](#) répertorie les significations des valeurs affichées par la commande `showcodusage`.

Tableau K-4 Significations de showcodusage

Affichage de colonne	Description	Signification des valeurs de l'exemple de commande
In Use	Nombre de cœurs de processeur utilisés actuellement dans les domaines logiques de l'ensemble du système ou dans chaque PPAR, parmi les cœurs de processeur disponibles lorsqu'ils sont gérés via le nombre d'activations de processeur achetées	« 4 » : 4 cœurs de processeur sont actuellement utilisés dans les domaines logiques de l'ensemble du système et dans la PPAR 0.
Installed	Nombre de cœurs de processeur physiques montés sur l'ensemble du système ou sur chaque PPAR	« 16 » : 16 cœurs de processeur physiques sont montés sur l'ensemble du système et sur la PPAR 0.
CoD Permitted	Nombre d'activations de processeur achetées et enregistrées dans le système	« 4 » : les activations de processeur pour activer 4 cœurs de processeur sont attribuées à ce système.
Status	Nombre d'activations de processeur qui ne sont pas actuellement utilisées dans les domaines logiques du système (toutes les PPAR) (différence entre « CoD Permitted » et « In Use »)	« OK » : la valeur obtenue par la soustraction de la valeur de « In Use » à celle de « CoD Permitted » est supérieure ou égale à 0, ce qui signifie l'absence de violation. Référence - « VIOLATION » : la valeur obtenue par la soustraction de la valeur de « In Use » à celle de « CoD Permitted » est inférieure à 0, ce qui signifie la présence d'une violation.
Unused- Assigned	Nombre d'activations de processeur qui ne sont pas actuellement utilisées dans les domaines logiques du système (toutes les PPAR). Une valeur négative désigne le nombre de cœurs de processeur actuellement utilisés en violation.	« 0 » : les cœurs de processeur correspondant au nombre d'activations de processeur attribuées au système (toutes les PPAR) sont actuellement utilisés. Référence - « -12 » : 12 cœurs de processeur de plus que le nombre d'activations de processeur attribuées sont actuellement utilisés, ce qui est synonyme de violation.

La commande showcodusage est utilisée pour gérer le nombre de cœurs du processeur actuellement utilisés dans les domaines logiques et le nombre d'activations de processeur enregistrées (achetées). Ainsi, le contenu affiché par la commande showcodusage n'est pas affectée par l'activation/la désactivation du permis temporaire d'activation de processeur. Le champ « CoD Permitted », qui désigne le nombre d'activation de CPU achetées et enregistrées, ainsi que « In Use », qui désigne le nombre de cœurs du processeur utilisés dans les domaines logiques, affichent les valeurs actuelles telles qu'elles sont.

Dans cet exemple, aucun cœur du processeur supplémentaire n'a encore été attribué aux domaines logiques. La valeur de « CoD Permitted », qui indique le nombre d'activations de processeur enregistrées dans le système,

est de « 4 » et la valeur du champ « Installed », qui indique le nombre de cœurs de processeur physiques, est de « 16 ». Cela signifie qu'il existe un manque d'activations de processeur pour les 12 cœurs de processeur physiques. Cependant, les 12 cœurs de processeur peuvent être utilisés pendant 30 jours car le permis temporaire d'activation de processeur est activé.

Si par exemple, vous attribuez les 12 cœurs de processeur à des domaines logiques alors que le permis temporaire d'activation de processeur est activé, « Status » affiche « VIOLATION: 12 cores in excess ». Dans ce cas, « VIOLATION » n'indique pas une urgence. Cela alerte qu'une violation d'activation de processeur surviendra lorsque le permis temporaire d'activation de processeur expirera ou sera désactivé.

Dans le champ Assigned de la ligne Unused, vous pouvez vérifier le nombre de cœurs de processeur qui n'ont pas encore été utilisés dans les domaines logiques du système (toutes les partitions physiques (PPAR)) par rapport aux activations de processeur achetées. Ces cœurs du processeur non utilisés sont utilisés par la fonction de remplacement automatique de CPU en cas de défaillance d'un cœur du processeur en cours d'utilisation.

- e. Exécutez la commande `showinterimpermit` du XSCF pour vérifier l'état du permis temporaire d'activation de processeur.

L'exemple suivant vous montre que le permis temporaire d'activation de processeur est activé et qu'il reste 29 jours avant son expiration.

```
XSCF> showinterimpermit -p 0
Interim permit for PPAR 0: enabled [29 days remaining]
```

- f. Pour commencer à utiliser les cœurs du processeur supplémentaires dans un ou plusieurs domaines logiques, exécutez la commande `ldm add-core` depuis le domaine de commande (domaine primaire). L'exemple suivant montre que six cœurs de processeur sont ajoutés au domaine logique.

```
# ldm add-core 6 dm0
```

- g. Exécutez la commande `showcodusage` du XSCF.

L'exemple suivant montre que la valeur de « In Use » a augmenté de « 4 » à « 10 », car six cœurs de processeur ont été ajoutés et utilisés dans les domaines logiques. Comme la différence entre les champs « In Use » et « CoD Permitted » est de six, « VIOLATION: 6 cores in excess » s'affiche, ce qui signifie que six cœurs de processeur sont temporairement en violation. Comme mentionné ci-dessus, cette « VIOLATION » n'indique pas une urgence.

```
XSCF> showcodusage -p resource
Resource In Use Installed CoD Permitted Status
-----
PROC          10         16          4 VIOLATION: 6 cores in excess
```

Remarque : L'application des informations sur l'utilisation du cœur du processeur des domaines logiques peut prendre jusqu'à 20 minutes. Ainsi, il est possible que la commande `showcodusage` n'affiche pas le changement résultant de l'utilisation de la commande `ldm` pendant une durée allant jusqu'à 20 minutes.

- h. Si vous souhaitez vérifier le nombre de cœurs du processeur utilisé dans les domaines logiques immédiatement après avoir changé l'attribution des cœurs du processeur, exécutez la commande `ldm list-permits` à partir du domaine de commande.

```
# ldm list-permits CPU CORE
PERMITS (PERMANENT) IN USE REST
16      (16)      10      0
```

- i. Si le permis temporaire d'activation de processeur est activé alors que tous les domaines logiques sont hors tension, il est possible que la commande `ldm` ne soit pas requise pour l'ajout de cœurs de processeur aux domaines logiques. Si l'exécution de la commande `showdomainconfig` du XSCF affiche « `factory-default` » dans « `Booting config` » comme indiqué ci-dessous, tous les cœurs de processeur disponibles seront automatiquement utilisés dans le domaine de commande (domaine primaire) lors du prochain démarrage du domaine. Dans le cas où le domaine de commande est en mode par défaut (indiqué comme « `factory-default` »), cela est dû au fait que toutes les ressources matérielles disponibles sont attribuées au domaine lorsque ce dernier est sous tension.

```
XSCF> showdomainconfig -p 0
PPAR-ID      :0
Booting config
(Current)    :factory-default
(Next)       :factory-default
```

Si « `Booting config` » n'est pas « `factory-default` », exécutez la commande `ldm` pour attribuer des cœurs de processeur supplémentaires après le démarrage du domaine de commande. Après l'exécution de la commande `ldm`, enregistrez les informations de configuration du domaine modifiées en utilisant la commande « `ldm add-spconfig` ». Cela garantit que les dernières informations de configuration du domaine logique sont utilisées plus tard lorsque le domaine est redémarré.

Nous recommandons vivement l'utilisation d'un nom différent du nom actuellement utilisé comme nom de configuration du domaine logique, comme indiqué dans l'exemple suivant.

```
XSCF> showdomainconfig -p 0
PPAR-ID      :0
Booting config
(Current)    :before-IPermit
(Next)       :IPermit-enabled
```


- j. Exécutez la commande `showinterimpermitsusage` du XSCF pour vérifier l'utilisation actuelle des ressources des cœurs de processeur.

```
XSCF> showinterimpermitsusage
```

```
PPAR-ID: 0
```

```
  Installed Cores:                16
  Purchased Cores Assigned to PPAR:  4
  Cores In Use by Ldoms:           10
  Interim Assignable Cores:         12
  In Use Interim Cores:             6
```

```
Note:
```

```
Please confirm the value of "Cores In Use by Ldoms" using the Oracle VM
Server for SPARC ldm command.
The XSCF may take up to 20 minutes to reflect the "Cores In Use by Ldoms"
of logical domains.
```

Cet exemple montre que « Cores In Use by Ldoms » affiche « 10 », ce qui signifie que le nombre de cœurs de processeur actuellement utilisés dans les domaines logiques est passé de 4 à 10. De plus, « In Use Interim Cores » affiche « 6 », ce qui signifie que 6 des 12 cœurs de processeur disponibles dans « Interim Assignable Cores » sont utilisés de manière supplémentaire dans les domaines logiques.

3. **Enregistrez les clés d'activation de processeur obtenues dans le système.** Effectuez les opérations suivantes.
- a. Après la réception des clés d'activation de processeur récemment achetées, enregistrez-les avec le système en utilisant la commande `addcodactivation` du XSCF.

```
XSCF> addcodactivation
Product: SPARC M10-1 SequenceNumber: 1
Cpu: noExpiration 2
Text-Signature-SHA256-RSA2048:
U1VOVyxTUEFSQylFbnRlcnByaXNlAA.....
Above Key will be added, Continue?[y|n]: y
XSCF>
```

- b. Réglez le nombre d'activations de CPU pour la partition physique en utilisant la commande `setcod`.

```
XSCF> setcod -p 0 -s cpu -c set 10
PROC Permits assigned for PPAR 1 : 4 -> 10

PROC Permits assigned for PPAR will be changed.
Continue? [y|n] :y

Completed.
```

- c. Vérifiez l'état des cœurs de processeur en utilisant la commande `showcodusage`.

L'exemple suivant montre que dix cœurs de processeur sont disponibles au total, car six nouvelles activations de processeur sont enregistrées et ajoutées à quatre activations, et les paramètres sont configurés pour la partition physique.

```
XSCF> showcodusage
Resource In Use Installed CoD Permitted Status
-----
PROC          10          16          10 OK: 0 cores available
PPAR-ID/Resource In Use Installed Assigned
-----
0 - PROC          10          16          10 cores
Unused - PROC          0          0          0 cores
```

- d. Exécutez la commande `showinterimpermitsusage` du XSCF pour vérifier l'utilisation actuelle des ressources des cœurs du processeur.

```
XSCF> showinterimpermitsusage

PPAR-ID: 0
  Installed Cores:          16
  Purchased Cores Assigned to PPAR: 10
  Cores In Use by Ldoms:    10
  Interim Assignable Cores: 6
  In Use Interim Cores:     0

Note:
  Please confirm the value of "Cores In Use by Ldoms" using the Oracle VM
  Server for SPARC ldm command.
  The XSCF may take up to 20 minutes to reflect the "Cores In Use by Ldoms"
  of logical domains.
```

Vous désactiverez le permis temporaire d'activation de processeur lors de l'étape 4. Ainsi, vérifiez attentivement que « In Use Interim Cores » indique « 0 », ce qui signifie que les ressources des cœurs de processeur supplémentaires rendues disponibles par le permis temporaire d'activation de processeur ne sont pas utilisées dans les domaines logiques.

Si le nombre affiché dans le champ « Cores In Use by Ldoms » est supérieur à celui du champ « Purchased Cores Assigned to PPAR », le système a détecté une violation de cœurs de processeur. Pour plus de détails sur le fonctionnement du système lorsqu'une violation est détectée après l'expiration ou la désactivation d'un permis temporaire d'activation de processeur, consultez « [K.4.3 Cas dans lequel la fonction a expiré ou a été désactivée](#) ».

4. Désactivez le permis temporaire d'activation de processeur.

Effectuez les opérations suivantes.

- a. Exécutez la commande `setinterimpermit` à partir du XSCF pour désactiver le permis temporaire d'activation de processeur.

```
XSCF> setinterimpermit -p 0 -c disable
Interim permit will be disabled.
Continue?[y|n] :y

Completed.
```

- b. Exécutez la commande `showcodusage` pour vérifier l'utilisation actuelle des cœurs du processeur.
- Vérifiez que le champ Status est OK, ce qui signifie que l'utilisation de tous les cœurs de processeur en cours d'utilisation est permise par l'intermédiaire des activations de processeur achetées.

```
XSCF> showcodusage -p resource
Resource In Use Installed CoD Permitted Status
-----
PROC          10          16          10 OK: 0 cores available
```

- c. Exécutez la commande `showinterimpermitusage` du XSCF pour vérifier l'utilisation actuelle des ressources des cœurs de processeur.
- Cet exemple montre que « Interim Assignable Cores » est « 0 », ce qui signifie qu'aucun cœur du processeur supplémentaire n'a été rendu disponible par l'activation du permis temporaire d'activation de processeur.

```
XSCF> showinterimpermitusage

PPAR-ID: 0
  Installed Cores:                16
  Purchased Cores Assigned to PPAR: 10
  Cores In Use by Ldoms:          10
  Interim Assignable Cores:        0
  In Use Interim Cores:           0

Note:
  Please confirm the value of "Cores In Use by Ldoms" using the Oracle VM
  Server for SPARC ldm command.
  The XSCF may take up to 20 minutes to reflect the "Cores In Use by Ldoms"
  of logical domains.
```

Activation à plusieurs reprises du permis temporaire d'activation de processeur

Avec XCP 2330 ou version ultérieure, le permis temporaire d'activation de processeur peut être utilisé plus d'une fois. Cependant, pour activer le permis temporaire d'activation de processeur, toutes les conditions suivantes doivent être réunies.

- Condition 1. Désactivez le permis temporaire d'activation de processeur même s'il est activé. (`setinterimpermit(8)`)
- Condition 2. Enregistrez une clé d'activation de processeur supplémentaire achetée avec le système. (`addcodactivation(8)`)

Condition 3. Attribuez les ressources de cœur de processeur à ajouter à la partition physique (PPAR). (setcod(8))

Si l'enregistrement des activations de processeur supplémentaires et les réglages supplémentaires pour la PPAR n'ont pas été effectués depuis la dernière activation du permis temporaire d'activation de processeur, vous ne pouvez pas activer à nouveau le permis temporaire d'activation de processeur.

Remarque : de plus, la période de validité de 30 jours ne sera pas étendue, même si les conditions 2 et 3 ci-dessus sont remplies. Désactivez une fois le permis temporaire d'activation de processeur ici.

Ces conditions peuvent être confirmées de la manière suivante en exécutant la commande `showinterimpermit-v`.

- (1) Si le permis temporaire d'activation de processeur est actuellement activé, il est nécessaire d'exécuter `setinterimpermit(8)` afin de le désactiver pour l'instant. Après l'exécution, le « Status » affiché par l'exécution de la commande `showinterimpermit-v` passe sur « Interim Permit cannot be enabled again (until more Purchased CPU Activations are installed and Purchased cores are assigned to the PPAR) ».
- (2) Il est nécessaire d'augmenter le nombre de clés d'activation de processeur achetées enregistrées dans le système. Il peut être augmenté en exécutant `addcodactivation(8)`.
La valeur de « Registered CPU Activation Keys (in units of cores) » de « Current CPU Activation Information » affichée en exécutant la commande `showinterimpermit-v` doit être supérieure à la valeur de « Registered CPU Activation Keys (in units of cores) » de « CPU Activation Information from the last time Interim Permit was enabled ».
- (3) Le nombre de ressources du cœur de processeur pour la PPAR (pour le système SPARC M12-2S/M10-4S) / le système (pour le système SPARC M12-1/M12-2/M10-1/M10-4) sur lequel vous souhaitez réactiver le permis temporaire d'activation de processeur, doit être augmenté. Il peut être augmenté en exécutant `setcod(8)`.
La valeur de « Purchased Cores Assigned to PPAR » de « Current CPU Activation Information » affichée en exécutant la commande `showinterimpermit-v` doit être supérieure à la valeur de « Purchased Cores Assigned to PPAR » de « CPU Activation Information from the last time Interim Permit was enabled ».

L'exemple suivant montre que la valeur de « Registered CPU Activation Keys (in units of cores) » de « Current CPU Activation Information » a augmenté de 16 et que « Purchased Cores Assigned to PPAR » de « Current CPU Activation Information » a augmenté de 8 et que le message « can be enabled » s'affiche donc. Cela signifie que le permis temporaire d'activation de processeur peut être utilisé à nouveau.

```
XSCF> showinterimpermit -v -p 0
PPAR-ID: 0
Status: Interim Permit is disabled (can be enabled)
```

```
CPU Activation Information from the last time Interim Permit was enabled:
Registered CPU Activation Keys (in units of cores): 16
Purchased Cores Assigned to PPAR: 8

Current CPU Activation Information:
Registered CPU Activation Keys (in units of cores): 32
Purchased Cores Assigned to PPAR: 16
```

Pour utiliser à nouveau le permis temporaire d'activation de processeur, enregistrez les activations de processeur supplémentaires et ajoutez-les à la PPAR en réalisant la même opération décrite à l'étape 3 dans [Procédure de fonctionnement pour XCP 2330 et version ultérieure](#).

Puis, réalisez la même opération décrite à l'étape 2 dans « [Procédure de fonctionnement pour XCP 2330 et version ultérieure](#) » pour activer le permis temporaire d'activation de processeur.

K.4.2 Flux et procédures pour XCP 232x

Avec XCP 232x, un permis temporaire d'activation de CPU peut être utilisé à nouveau pour un système SPARC M10-1/M10-4.

Flux de fonctionnement pour XCP 232x

Le flux d'opérations est le suivant.

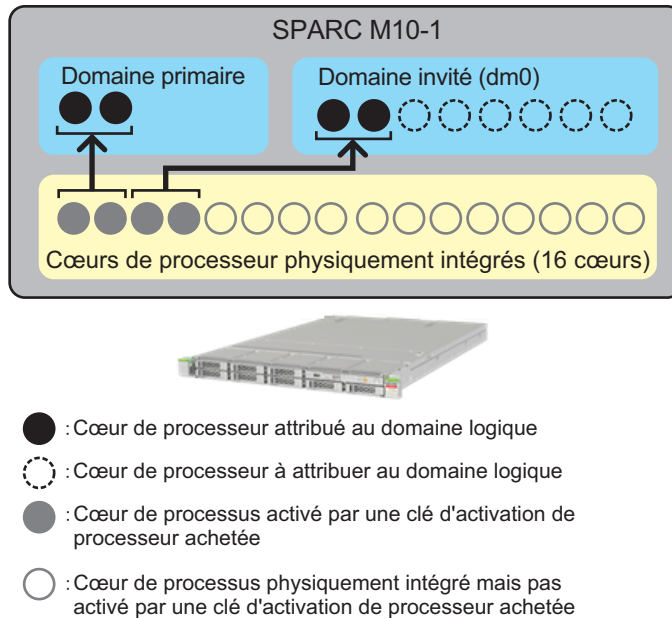
1. **Constatez que des cœurs de processeur supplémentaires sont requis, puis démarrez le processus d'achat des clés d'activation de processeur requises.**
2. **Activez un permis temporaire d'activation de processeur.**
3. **Enregistrez les clés d'activation de processeur obtenues dans le système.**
4. **Désactivez le permis temporaire d'activation de processeur.**

Exemple de configuration

La description de « [Procédure de fonctionnement pour XCP 232x](#) » utilise la configuration suivante comme exemple.

- Le SPARC M10-1 à un seul socket de processeur avec 16 cœurs de processeur physiques est utilisé.
- Les activations de CPU pour activer les 4 cœurs de CPU ont été achetées et enregistrées sur le système.
- Le système est composé de deux domaines logiques en exécution.
 - Deux cœurs de processeur sont attribués au domaine de commande (domaine primaire).
 - Deux cœurs de processeur sont attribués au domaine invité (dm0).
 - Pour répondre à une augmentation de charge, le domaine invité (dm0) requiert six cœurs de processeur supplémentaires.

Figure K-2 Exemple de configuration pour XCP 232x (SPARC M10-1)



Remarque : les clés d'activation de processeur enregistrées dans le système activent un nombre défini de cœurs de processeur. Ils n'activent pas les cœurs du processeur en spécifiant le socket de CPU et l'emplacement physique de chaque cœur du processeur. Pour la facilité de compréhension, des cœurs du processeur spécifique sont activés et attribués aux domaines logiques dans [Figure K-2](#).

Procédure de fonctionnement pour XCP 232x

La procédure de fonctionnement est la suivante.

1. **Confirmez que des cœurs de processeur supplémentaires sont requis, puis démarrez le processus d'achat des clés d'activation de processeur requises.**
Assurez-vous de vérifier ce qui suit avant de procéder à l'achat.
 - a. Déterminez si des cœurs de processeur sont requis à partir d'une analyse de charge ou évaluez la manipulation pour le système.
 - b. Un permis temporaire d'activation de processeur peut être utilisé pendant 30 jours. Nous vous recommandons de vérifier à l'avance combien de temps les clés d'activation de CPU prendront pour parvenir dans votre région. Pour ces informations, contactez votre représentant commercial local.
2. **Activez un permis temporaire d'activation de processeur.**
Effectuez les opérations suivantes.
 - a. Exécutez la commande `showcodusage` du XSCF pour vérifier l'utilisation actuelle des cœurs de processeur du système.

```
XSCF> showcodusage -p resource
Resource In Use Installed CoD Permitted Status
-----
PROC          4          16          4 OK: 0 cores available
```

Tableau K-5 répertorie les significations des valeurs affichées par la commande showcodusage.

Tableau K-5 Significations de showcodusage

Affichage de colonne	Description	Signification des valeurs de l'exemple de commande
In Use	Nombre de cœurs de processeur utilisés actuellement dans les domaines logiques de l'ensemble du système, parmi les cœurs de processeur disponibles lorsqu'ils sont gérés via le nombre d'activations de processeur achetées	« 4 » : 4 cœurs de processeur sont actuellement utilisés dans les domaines logiques de l'ensemble du système.
Installed	Nombre de cœurs de processeur physiques montés sur l'ensemble du système	« 16 » : 16 cœurs de processeur physiques sont montés sur l'ensemble du système.
CoD Permitted	Nombre d'activations de processeur achetées et enregistrées dans le système	« 4 » : les activations de processeur pour activer 4 cœurs de processeur sont attribuées à ce système.
Status	Nombre d'activations de processeur qui ne sont pas actuellement utilisées dans les domaines logiques du système (différence entre « CoD Permitted » et « In Use »)	« OK » : la valeur obtenue par la soustraction de la valeur de « In Use » à celle de « CoD Permitted » est supérieure ou égale à 0, ce qui signifie l'absence de violation. Référence - « VIOLATION » : la valeur obtenue par la soustraction de la valeur de « In Use » à celle de « CoD Permitted » est inférieure à 0, ce qui signifie la présence d'une violation.
Unused- Assigned	Nombre d'activations de processeur qui ne sont pas actuellement utilisées dans les domaines logiques du système. Une valeur négative désigne le nombre de cœurs de processeur actuellement utilisés en violation.	« 0 » : les cœurs de processeur correspondant au nombre d'activations de processeur attribuées au système sont actuellement utilisés. Référence - « -12 » : 12 cœurs de processeur de plus que le nombre d'activations de processeur attribuées sont actuellement utilisés, ce qui est synonyme de violation.

Si la valeur de « Installed » est égale à celle de « CoD Permitted », cela indique que les clés d'activation de processeur pour tous les cœurs de processeur physiquement intégrés ont bien été enregistrées. Dans ce cas, le permis temporaire d'activation de processeur n'est pas requis. N'activez pas la fonction.

- b. Exécutez la commande `setinterimpermit` du XSCF pour activer le permis temporaire d'activation de processeur. Tous les cœurs des puces des processeurs montées sur le système sont rendus disponibles par l'exécution de cette commande.

```
XSCF> setinterimpermit -p 0 -c enable
Note:
  Interim Permit can be used only once.
  Please add CPU activation(s) within 30 days of enabling the Interim Permit.

The Interim Permit for the PPAR will be changed to enabled.
Continue?[y|n] :y

Completed.
```

- c. Exécutez la commande `showcodusage` du XSCF pour vérifier le nombre de cœurs de processeur supplémentaires rendus disponibles.

```
XSCF> showcodusage -p resource
Resource In Use Installed CoD Permitted Status
-----
PROC          4         16          4 OK: 0 cores available
```

Cet exemple montre que « Installed » est « 16 ». La valeur n'a pas changé avant et après l'activation du permis temporaire d'activation de processeur. Cependant, elle montre que 12 cœurs de processeur supplémentaires ont été rendus disponibles par l'activation du permis temporaire d'activation de processeur. Dans ce cas, 12 cœurs de processeur supplémentaires peuvent être utilisés au maximum dans le domaine logique (dm0) pendant 30 jours.

Plutôt que d'utiliser tous les cœurs du processeur supplémentaires rendus disponibles, attribuez simplement les cœurs du processeur correspondant au nombre d'activations CPU que vous envisagez d'acheter pour les domaines logiques.

Par exemple, si vous souhaitez acheter et ajouter deux cœurs du processeur, nous recommandons vivement d'attribuer seulement deux cœurs du processeur supplémentaires au domaine logique. Si vous attribuez quatre cœurs de processeur aux domaines logiques puis que vous achetez une activation de processeur pour activer seulement deux cœurs de processeur supplémentaires, le total sera réduit de deux cœurs de processeur. Cela risque d'entraîner un problème de performance si vous désactivez le permis temporaire d'activation de processeur.

- d. Si vous exécutez la commande `showcodusage` du XSCF sans les options à ce stade, le message suivant s'affiche.

```
XSCF> showcodusage
Resource In Use Installed CoD Permitted Status
-----
PROC          4         16          4 OK: 0 cores available
PPAR-ID/Resource In Use Installed Assigned
```


0 - PROC	4	16	4 cores
Unused - PROC	0	0	0 cores

Veillez noter que si vous exécutez la commande `showdusage` du XSCF à ce stade, le contenu affiché avant et après l'activation du permis temporaire d'activation de processeur ne change pas, même si le nombre de cœurs de processeur disponibles a augmenté par l'utilisation de la fonction.

La commande `showcodusage` est utilisée pour gérer le nombre de cœurs du processeur actuellement utilisés dans les domaines logiques et le nombre d'activations de processeur enregistrées (achetées). Ainsi, le contenu affiché par la commande `showcodusage` n'est pas affectée par l'activation/la désactivation du permis temporaire d'activation de processeur. Le champ « CoD Permitted », qui désigne le nombre d'activation de CPU achetées et enregistrées, ainsi que « In Use, », qui désigne le nombre de cœurs du processeur utilisés dans les domaines logiques, affichent les valeurs actuelles telles qu'elles sont.

Dans cet exemple, aucun cœur du processeur supplémentaire n'a encore été attribué aux domaines logiques. La valeur de « CoD Permitted », qui indique le nombre d'activations de processeur enregistrées dans le système, est de « 4 » et la valeur du champ « Installed », qui indique le nombre de cœurs de processeur physiques, est de « 16 ». Cela signifie qu'il existe un manque d'activations de CPU pour les 12 cœurs du processeur physiques. Cependant, les 12 cœurs du processeur peuvent être utilisés pendant 30 jours car le permis temporaire d'activation de CPU est activé.

Si par exemple, vous attribuez les 12 cœurs de processeur à des domaines logiques alors que le permis temporaire d'activation de processeur est activé, « Status » affiche « VIOLATION: 12 cores in excess ». Dans ce cas, « VIOLATION » n'indique pas une urgence. Cela alerte qu'une violation d'activation de processeur surviendra lorsque le permis temporaire d'activation de processeur expirera ou sera désactivé.

Dans le champ « Assigned » de la ligne « Unused », vous pouvez vérifier que le nombre de cœurs de processeur qui n'ont pas encore été utilisés dans les domaines logiques du système par rapport aux activations de processeur achetées. Ces cœurs du processeur non utilisés sont utilisés par la fonction de remplacement automatique de CPU en cas de défaillance d'un cœur du processeur en cours d'utilisation.

- e. Exécutez la commande `showinterimpermit` du XSCF pour vérifier l'état du permis temporaire d'activation de processeur. L'exemple suivant vous montre que le permis temporaire d'activation de processeur est activé et qu'il reste 29 jours avant son expiration.

```
XSCF> showinterimpermit -p 0
Interim permit for PPAR 0: enabled [29 days remaining]
```

- f. Pour commencer à utiliser les cœurs du processeur supplémentaires dans un ou plusieurs domaines logiques, exécutez la commande `ldm add-core` depuis le domaine de commande (domaine primaire). L'exemple suivant montre que

six cœurs de processeur sont ajoutés au domaine logique.

```
# ldm add-core 6 dm0
```

- g. Exécutez la commande `showcodusage` du XSCF.
- L'exemple suivant montre que la valeur de « In Use » a augmenté de « 4 » à « 10 », car six cœurs de processeur ont été ajoutés et utilisés dans les domaines logiques. Comme la différence entre les champs « In Use » et « CoD Permitted » est de six, « VIOLATION: 6 cores in excess » s'affiche, ce qui signifie que six cœurs de processeur sont temporairement en violation. Comme mentionné ci-dessus, cette « VIOLATION » n'indique pas une urgence.

```
XSCF> showcodusage -p resource
Resource In Use Installed CoD Permitted Status
-----
PROC          10          16          4 VIOLATION: 6 cores in excess
```

Remarque : L'application des informations sur l'utilisation du cœur du processeur des domaines logiques peut prendre jusqu'à 20 minutes. Ainsi, il est possible que la commande `showcodusage` n'affiche pas le changement résultant de l'utilisation de la commande `ldm` pendant une durée allant jusqu'à 20 minutes.

- h. Si vous souhaitez vérifier le nombre de cœurs du processeur utilisé dans les domaines logiques immédiatement après avoir changé l'attribution des cœurs du processeur, exécutez la commande `ldm list-permits` à partir du domaine de commande.

```
# ldm list-permits
```

- i. Si le permis temporaire d'activation de processeur est activé alors que tous les domaines logiques sont hors tension, il est possible que la commande `ldm` ne soit pas requise pour l'ajout de cœurs de processeur aux domaines logiques.
- Si l'exécution de la commande `showdomainconfig` du XSCF affiche « factory-default » dans « Booting config » comme indiqué ci-dessous, tous les cœurs de processeur disponibles seront automatiquement utilisés dans le domaine de commande (domaine primaire) lors du prochain démarrage du domaine. Dans le cas du domaine de commande (« factory-default »), cela est dû au fait que toutes les ressources matérielles disponibles sont attribuées au domaine lorsque ce dernier est sous tension.

```
XSCF> showdomainconfig -p 0
PPAR-ID          :0
Booting config
(Current)        :factory-default
(Next)           :factory-default
```

Si « Booting config » n'est pas « factory-default », exécutez la commande

ldm pour attribuer des cœurs de processeur supplémentaires après le démarrage du domaine de commande. Après l'exécution de la commande ldm, enregistrez les informations de configuration du domaine modifiées en utilisant la commande « ldm add-spconfig ». Cela garantit que les dernières informations de configuration du domaine logique sont utilisées plus tard lorsque le domaine est redémarré.

Nous recommandons vivement l'utilisation d'un nom différent du nom actuellement utilisé comme nom de configuration du domaine logique, comme indiqué dans l'exemple suivant.

```
XSCF> showdomainconfig -p 0
PPAR-ID          :0
Booting config
(Current)        :before-IPermit
(Next)           :IPermit-enabled
```

3. Enregistrez les clés d'activation de processeur obtenues dans le système.

Effectuez les opérations suivantes.

- a. Après la réception des activations du processeur récemment achetées, enregistrez-les avec le système en utilisant la commande addcodactivation du XSCF.

```
XSCF> addcodactivation
Product: SPARC M10-1 SequenceNumber: 1
Cpu: noExpiration 2
Text-Signature-SHA256-RSA2048:
U1VOVyxTUEFSQylFbnRlcnByaXNlAA.....
Above Key will be added, Continue?[y|n]: y
XSCF>
```

- b. Réglez le nombre d'activations de CPU pour la partition physique en utilisant la commande setcod.

```
XSCF> setcod -p 0 -s cpu -c set 10
PROC Permits assigned for PPAR 1 : 4 -> 10

PROC Permits assigned for PPAR will be changed.
Continue? [y|n] :y

Completed.
```

- c. Vérifiez l'état des cœurs de processeur en utilisant la commande showcodusage.

L'exemple suivant montre que dix cœurs de processeur sont disponibles au total, car six nouvelles activations de processeur sont enregistrées et ajoutées à quatre activations, et les paramètres sont configurés pour la partition physique.

```
XSCF> showcodusage -p resource
Resource In Use Installed CoD Permitted Status
-----
PROC          10          16          10 OK:  0 cores available
```

d. Vous désactiverez le permis temporaire d'activation de processeur lors de l'étape 4. Ainsi, vérifiez soigneusement que le nombre de cœurs de processeur requis est affiché dans « CoD Permitted ». Le nombre affiché dans le champ « In Use » doit être égal ou inférieur à celui du champ « CoD Permitted » quand le domaine est en exécution. Si le nombre affiché dans le champ « In Use » est supérieur à celui du champ « CoD Permitted », le système détecte une violation de cœurs de processeur. Pour plus de détails sur le fonctionnement du système lorsqu'une violation est détectée après l'expiration ou la désactivation du permis temporaire d'activation de processeur, consultez « [K.4.3 Cas dans lequel la fonction a expiré ou a été désactivée](#) ».

4. **Désactivez le permis temporaire d'activation de processeur.**

Effectuez les opérations suivantes.

- a. Exécutez la commande `setinterimpermit` à partir du XSCF pour désactiver le permis temporaire d'activation de processeur.

```
XSCF> setinterimpermit -p 0 -c disable
Interim permit will be disabled.
Continue?[y|n] :y

Completed.
```

- b. Exécutez la commande `showcodusage` pour vérifier l'utilisation actuelle des cœurs du processeur. Vérifiez que le champ Status est OK, ce qui signifie que l'utilisation de tous les cœurs de processeur en cours d'utilisation est permise par l'intermédiaire des activations de processeur achetées.

```
XSCF> showcodusage -p resource
Resource In Use Installed CoD Permitted Status
-----
PROC          10          16          10 OK:  0 cores available
```

K.4.3 Cas dans lequel la fonction a expiré ou a été désactivée

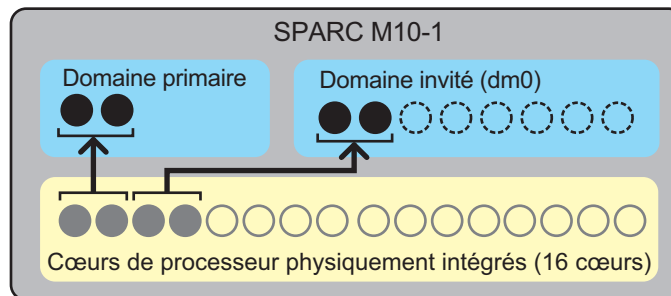
Cette section décrit le fonctionnement et l'action du système à réaliser lorsque le permis temporaire d'activation de processeur a expiré ou est désactivé.

Exemple de configuration

La présente description utilise la configuration suivante comme exemple.

- Le SPARC M10-1 à un seul socket de processeur avec 16 cœurs de processeur physiques est utilisé.
- Les activations de processeur pour activer les 4 cœurs de processeur ont été achetées et enregistrées sur le système.
- Le système est composé de deux domaines logiques en exécution.
 - Deux cœurs de processeur sont attribués au domaine de commande (domaine primaire).
 - Deux cœurs de processeur sont attribués au domaine invité (dm0).
- Pour répondre à une augmentation de charge, le domaine invité (dm0) requiert six cœurs de processeur supplémentaires.
- Le permis temporaire d'activation de processeur est activé et six cœurs du processeur supplémentaires ont été attribués au domaine invité (dm0) en tant qu'action temporaire.

Figure K-3 Exemple de configuration dans le cas où la fonction a expiré ou a été désactivée (SPARC M10-1)



- : Cœur de processeur attribué au domaine logique
- (pointillé) : Cœur de processeur à attribuer au domaine logique
- (gris) : Cœur de processus activé par une clé d'activation de processeur achetée
- (blanc) : Cœur de processus physiquement intégré mais pas activé par une clé d'activation de processeur achetée

Remarque : les clés d'activation de processeur enregistrées dans le système activent un nombre défini de cœurs de processeur. Ils n'activent pas les cœurs du processeur en spécifiant le socket de CPU et l'emplacement physique de chaque cœur du processeur. Pour la facilité de compréhension, des cœurs du processeur spécifique sont activés et attribués aux domaines logiques dans [Figure K-3](#).

Fonctionnement et action du système

Le permis temporaire d'activation de processeur expire 30 jours plus tard, sans tenir compte des clés d'activation de processeur supplémentaires pouvant être enregistrées dans le système. De plus, un permis temporaire d'activation de processeur peut être désactivé involontairement par la commande `setinterimpermit` du XSCF. Une fois que le permis temporaire d'activation de processeur est désactivé, il ne peut pas être réactivé avec XCP 232x. Même avec XCP 2330 et version ultérieure, la fonction ne peut pas être réactivée instantanément sur demande.

Si le permis temporaire d'activation de processeur expire ou est désactivé lorsqu'un cœur de processeur est utilisé en état de violation d'utilisation « VIOLATION », le système fonctionne de la manière suivante.

- Après l'écoulement de 30 minutes après la violation, une notification est envoyée au système, qui essaie de supprimer les cœurs de processeur excessifs des domaines logiques.
- Après l'écoulement de 60 minutes après la violation, le système essaie d'arrêter le domaine de commande.
- Après l'écoulement de 90 minutes après la violation, le système essaie d'arrêter tous les domaines.

Si vous réalisez une des opérations suivantes au cours des 30 minutes qui suivent la détection de la violation, le système ne réalisera pas les opérations a à c ci-dessus.

- Réduction du nombre de cœurs du processeur en cours d'utilisation dans les domaines logiques
- Enregistrez des clés d'activation de processeur achetées supplémentaires à l'aide de la commande `addcodactivation` du XSCF et ajoutez le nombre d'activations de processeur à la partition physique à l'aide de la commande `setcod`.

Si le permis temporaire d'activation de processeur expire et que vous exécutez la commande `showinterimpermit` du XSCF, « expired » s'affichera comme indiqué dans l'exemple suivant.

```
XSCF> showinterimpermit -p 0
Interim permit for PPAR 0: expired
```

Si le permis temporaire d'activation de processeur expire ou est désactivé et que vous exécutez la commande `showcodusage` du XSCF, l'utilisation des cœurs du processeur sera affichée comme indiqué dans l'exemple suivant.

```
XSCF> showcodusage -p resource
Resource In Use Installed CoD Permitted Status
-----
PROC          10          16          4 VIOLATION: 6 cores in excess
```

Dans ce cas, « VIOLATION » s'affiche dans le champs « Status », car le permis temporaire d'activation de processeur a expiré. L'exemple montre que six cœurs de processeur sont utilisés en violation, ce qui avertit en réalité le système d'une urgence. Dans le cas de cet exemple, vous devez immédiatement supprimer au total

six cœurs du processeur des domaines logiques.

Après la détection d'une violation, le système essaie de supprimer les cœurs du processeur des domaines logiques jusqu'à ce que le nombre de cœurs du processeur en cours d'utilisation corresponde au nombre de clés d'activation de CPU achetées et enregistrées. Six cœurs du processeur seront supprimés dans cet exemple.

Le système supprime des cœurs de CPU en commençant par celui avec la valeur CPUID (CID) la plus importante. Il est possible que le système ne soit pas capable de supprimer les cœurs du processeur pour certaines raisons, telles qu'un vcpu appartenant au cœur du processeur qui est associé à un processus spécifique par l'intermédiaire de pbind. Dans ce cas, le cœur de processeur avec la seconde valeur CPU la plus élevée sera supprimé.

Vous pouvez vérifier la valeur CID à l'aide de la commande ldm d'Oracle Solaris, comme indiqué ci-dessous.

```
# ldm list-domain -o core
```

```
NAME
```

```
primary
```

```
CORE
```

CID	CPUSET
0	(0, 1)
4	(8, 9)

```
-----
```

```
NAME
```

```
dm0
```

```
CORE
```

CID	CPUSET
8	(16, 17)
12	(24, 25)

```
<Omis>
```

Une fois que le nombre de cœurs du processeur devient inférieur ou égal à celui de cœurs du processeur dont l'utilisation est permise par les clés d'activations de CPU achetées, l'action ci-dessus n'est pas réalisée.

Comme mentionné ci-dessus, la suppression de cœurs du processeur risque d'échouer. Un échec de la suppression survient lorsqu'un vcpu est associé à un processus spécifique par l'intermédiaire de pbind ou autre moyen, ou lorsque le cœur du processeur à supprimer est le dernier dans un domaine logique. Si le système ne peut pas supprimer suffisamment de cœurs du processeur (six cœurs du processeur dans ce cas), le domaine de commande sera arrêté.

Pour récupérer de la situation mentionnée ci-dessus, réalisée l'une des opérations suivantes.

- Supprimez suffisamment de cœurs du processeur de domaines logiques à l'aide de la commande ldm, ou arrêtez un ou plusieurs domaines logiques.
- Enregistrez un nombre suffisant de clés d'activation de processeur achetées à l'aide de la commande addcodactivation du XSCF et ajoutez le nombre d'activations de processeur à la partition physique à l'aide de la commande setcod.

S'il est impossible de supprimer un nombre suffisant de cœurs de processeur du fait

de l'arrêt du domaine de commande, tous les domaines logiques seront arrêtés.

Si tous les domaines logiques sont arrêtés, les méthodes de récupération possibles sont les suivantes.

- a. Sélectionnez le fichier d'informations de configuration des domaines logiques qui est sauvegardé avant l'activation du permis temporaire d'activation de processeur.
Sélectionnez l'ancien fichier d'informations de configuration des domaines logiques à l'aide de la commande `setdomainconfig` du XSCF, comme indiqué ci-dessous. Puis, démarrez le système.

```
XSCF> setdomainconfig -p 0
PPAR-ID      :0
Booting config
(Current)    :IPermit-enabled
(Next)      :IPermit-enabled
-----
Index       :1
config_name :factory-default
domains     :1
date_created:-
-----
Index       :2
config_name :before-IPermit
domains     :2
date_created:"2015-03-24 19:21:30"
-----
Index       :3
config_name :IPermit-enabled
domains     :2
date_created:"2016-06-16 12:00:30"
Select Index of Using config_name : 2
PPAR-ID of PPARs that will be affected :00
Logical domain config_name will be set to "before-IPermit".
Continue?[y|n] :y
```

- b. Si votre but est de récupérer le domaine de commande, démarrez uniquement le domaine de commande, puis supprimez le nombre nécessaire ressources de cœurs du processeur du domaine de commande.

Remarque : Même si le nombre de cœurs du processeur du domaine de commande est supérieur au nombre de cœurs du processeur permis par l'utilisation des clés d'activation de CPU achetées, le domaine de commande est toujours démarré normalement. La même chose s'applique lorsque le permis temporaire d'activation de processeur a expiré ou a été désactivé. Cependant, si un nombre suffisant de cœurs du processeur ne peut pas être supprimé dans les 30 minutes suivant la détection de la violation, le système démarre à nouveau la suppression automatique de cœurs du processeur selon la procédure indiquée ci-dessus. Une fois que la suppression des ressources de cœurs du processeur a été réalisée avec succès, enregistrez les informations de configuration du domaine logique à l'aide de la commande `ldm add-spconfig`, afin qu'elles puissent être utilisées dans le futur lors du redémarrage du domaine de commande.

- c. Si votre but est de récupérer un domaine invité spécifique, réalisez la procédure suivante.
 - 1. Démarrez uniquement le domaine de commande.
 - 2. Supprimez les cœurs du processeur attribués au domaine invité à partir du domaine de commande, puis enregistrez les informations de configurations du domaine logique corrigées à l'aide de la commande `ldm add-spconfig`.
 - 3. Démarrez le domaine invité.
- d. Enregistrez les clés d'activation de processeur achetées supplémentaires à l'aide de la commande `addcodactivation` du XSCF et ajoutez le nombre d'activations de processeur à la partition physique à l'aide de la commande `setcod`.

Si vous devez récupérer le domaine de commande et le domaine invité sans utiliser l'ancien fichier de configuration des domaines logiques, les opérations b. et c. ci-dessus peuvent être requises.

K.5 Notification d'événement d'un permis temporaire d'activation de processeur

Cette section décrit les notifications d'événements liées au permis temporaire d'activation de processeur.

K.5.1 Types de notification

Les quatre types de notifications d'événement ci-après sont réalisés en connexion avec le permis temporaire d'activation de processeur.

- a. Journal des événements XSCF
Un journal d'événements pouvant être référencé à l'aide de la commande `showlogs event` du XSCF
- b. Messages de la console de domaine (dans le cas de XCP 2330 ou version ultérieure)
Messages enregistrés dans `syslog` et affichés sur la console du domaine primaire
- c. E-mail
E-mail envoyé si la fonction de notification d'e-mail du XSCF est activée (Consultez « [10.2 Réception de notifications par e-mail lorsqu'une panne se produit](#) ».)
- d. Trap SNMP
Un trap SNMP reçu si le système est surveillé par la fonction d'agent SNMP du XSCF (Consultez « [10.3 Surveillance/Gestion de l'état du système avec l'agent SNMP](#) ».)

K.5.2 Exemples de notifications

Démarrant 14 jours avant l'expiration du permis temporaire d'activation de processeur, les notifications sont envoyées toutes les 4 heures jusqu'à ce que le permis temporaire d'activation de processeur soit désactivé ou qu'il expire. Les notifications de chaque événement sont présentées sous ce format : PPAR-ID 0: Interim Permit due to expire in 14 days.

Dès que le permis temporaire d'activation de processeur a expiré, les notifications sont envoyées. Les notifications de chaque événement sont présentées sous ce format : PPAR-ID 0: Interim Permit has expired.

Lorsqu'une violation d'utilisation de cœur de processeur se produit après l'expiration ou la désactivation du permis temporaire d'activation de processeur, une notification est envoyée. Les notifications de chaque événement sont présentées sous ce format : PPAR-ID 0: CoD PROC violation occurred.

De même, lorsqu'une violation d'utilisation de cœur de processeur est résolue, une notification est envoyée. Les notifications de chaque événement sont présentées sous ce format : PPAR-ID 0: CoD PROC violation resolved.

Voici des exemples de notification d'événements.

La description ici utilise des exemples d'événements 14 jours avant l'expiration du permis temporaire d'activation de processeur.

Exemple 1. Journal des événements XSCF

```
XSCF> showlogs event
May 23 18:11:51 JST 2016      PPAR-ID 0: Interim Permit due to expire in 14
days
```

Exemple 2 messages syslog sur la console du domaine primaire (pour XCP 2330 et version ultérieure)

- Exemple de message

```
PPAR-ID 0: Interim Permit due to expire in 14 days
```

- exemple de journal syslog

```
Jul 22 01:10:45 4S-441-D0 SC Alert: [ID 695932 daemon.notice]
PPAR-ID 0: Interim Permit due to expire in 14 days
```

Exemple 3. E-mail

```
From no-reply@xxxx Mon May 23 18:11:51 2016
Date: Mon, 23 May 2016 18:11:51 +0900
From: no-reply@xxxx
Message-Id: <1463994711.2429@xxxx>
To: administrator@m10.org
Subject: Event: M10-1: M10-1: serial# TZ01111111, PPAR-ID 0: Interim Permit
due to expire in 14 days
Content-Length: 200

TYPE: Event, VER: XCP-2320
MODE-SWITCH: Service
SEVERITY: Event
EVENT-TIME: 05-23-2016 18:11:51 JST
CSN: TZ01111111
SERVER-ID: xxxx
FRU: -
DIAGCODE: -
MSG: PPAR-ID 0: Interim Permit due to expire in 14 days
```

Exemple 4. piège SNMP

Le piège SNMP d'OID 1.3.6.1.4.1.211.1.15.4.1.2.0.5 est envoyé. Ce piège contient .1.3.6.1.4.1.211.1.15.4.1.2.1.1.0 (scfTrapEventType.0), qui est un objet dont la valeur indique le type d'événement.

Pour plus de détails sur l'OID, consultez *Fujitsu SPARC M12 and Fujitsu M10/SPARC M10 XSCF MIB and Trap Lists*.

K.6 Autres notes importantes

Cette section décrit les remarques liées à l'utilisation d'un permis temporaire d'activation de processeur.

K.6.1 PPAR DR et permis temporaire d'activation de processeur

Le permis temporaire d'activation de processeur peut être utilisé simultanément avec la reconfiguration dynamique de la partition physique (PPAR DR).

Remarque : pendant l'exécution de PPAR DR à l'aide de la commande `addboard` ou `deleteboard`, le changement de mode du permis temporaire d'activation de processeur échouera. Autrement dit, un conflit entre la commande `setinterimpermit` et la commande `addboard/deleteboard` entraînera l'échec de chaque commande.

Par exemple, supposons que vous allez utiliser la PPAR DR pour ajouter BB#4 à une PPAR pour laquelle le permis temporaire d'activation de processeur est activé. Dans ce cas, tous les cœurs de processeur dans chaque puce de processeur montée sur BB#4 sont rendus disponibles lorsque l'ajout de la PPAR DR est terminé.

Cependant, si la configuration du domaine logique de cette PPAR n'est pas « factory-default », vous devez utiliser la commande `ldm` d'Oracle Solaris pour intégrer les cœurs de processeur ajoutés aux domaines logiques.

À l'inverse, supposons que vous allez utiliser la PPAR DR pour supprimer BB#4 de la PPAR pour laquelle un permis temporaire d'activation de processeur est activé. Dans ce cas, tous les cœurs du processeur sur les puces de CPU montées sur BB#4 sont automatiquement supprimés de la PPAR, dans le cadre du processus de suppression de la PPAR DR. Ainsi, vous devez supprimer les ressources de cœurs de processeur des domaines logiques à l'avance avant de les supprimer de la PPAR.

K.6.2 Lors de la tentative d'utiliser le permis temporaire d'activation de processeur (pour XCP 232x uniquement)

Si vous essayez d'activer à nouveau un permis temporaire d'activation de processeur pour un système pour lequel la fonction a déjà été utilisée, à l'aide de la commande `setinterimpermit` du XSCF, la commande échouera.

L'exemple suivant montre un cas d'échec de la commande.

```

XSCF> showinterimpermit -p 0
Interim permit for PPAR 0: disabled
XSCF> setinterimpermit -p 0 -c enable
Note:
    Interim Permit can be used only once.
    Please add CPU activation(s) within 30 days of enabling the Interim Permit.

The Interim Permit for the PPAR will be changed to enabled.
Continue?[y|n] :y

The Interim Permit cannot be enabled because it has already been used once.
XSCF> showinterimpermit -p 0
Interim permit for PPAR 0: disabled

```

Si XCP 232x est utilisé, cela ne constitue pas une défaillance car un permis temporaire d'activation de processeur peut être activé une seule fois pour chaque système.

Si tous les éléments suivants s'appliquent à vous, contactez votre représentant commercial local.

- Vous avez utilisé votre permis temporaire d'activation de processeur pour un système sur lequel XCP 232x a été installé.
- Puis, vous avez mis à jour le microprogramme vers XCP 2330 ou une version ultérieure.
- Vous avez acheté des clés d'activation de processeur supplémentaires, les avez enregistrées avec le système et attribué les ressources de cœur de processeur à la PPAR.
- Vous souhaitez réutiliser le permis temporaire d'activation de processeur.

K.6.3 Déplacement des clés d'activation de processeur (suppression/déplacement)

Le déplacement (suppression/déplacement) d'une ou plusieurs clés d'activation de processeur depuis un SPARC M12/M10 vers un autre lorsque le permis temporaire d'activation de processeur est activé n'affecte pas le processus de déplacement.

Utilisez la commande `deletecodactivation` du XSCF pour en supprimer et la commande `addcodactivation` pour en ajouter.

Avant la suppression d'une clé d'activation de processeur d'un SPARC M12/M10 à l'aide de la commande `deletecodactivation`, assurez-vous d'enregistrer de manière externe la clé d'activation de processeur sous forme de fichier texte, etc. à l'aide de la commande `showcodactivation`.

La clé d'activation de processeur enregistrée peut être ajoutée à un autre SPARC M12/M10 à l'aide de la commande `addcodactivation`.

Les permis temporaires d'activation de processeur ne sont pas affectés par le processus de déplacement d'activations de processeur. Veuillez noter, cependant, que le nombre de cœurs de processeur utilisés ne doit pas dépasser le nombre d'attributions d'activations de processeur achetées après le processus de déplacement dans un

système pour lequel le permis temporaire d'activation de processeur n'est pas activé.

Pendant que le permis temporaire d'activation de processeur est activé, toutes les clés d'activation de processeur achetées peuvent être supprimées du système et le système continue à fonctionner, même après la suppression. Cependant, une fois que le permis temporaire d'activation de processeur est désactivé ou expire, le système ne fonctionne pas tant qu'une clé d'activation de processeur achetée n'est pas enregistrée dans le système.

K.6.4 Résultat de la commande ldm

Si vous utilisez la commande ldm d'Oracle Solaris lors de l'activation du permis temporaire d'activation de processeur, « PERMANENT » s'affiche pour les cœurs de processeur disponibles supplémentaires, même lorsqu'ils ne sont pas réellement permanents.

En tant qu'exemple, supposons que quatre cœurs de processeur sont présents dans le domaine primaire d'un SPARC M12/M10 et leur utilisation est permise par les clés d'activation de processeur achetées. L'exécution de « ldm list-domain -l » lorsqu'un permis temporaire d'activation de processeur est activé affiche les informations suivantes.

```
# ldm list-domain -l
NAME          STATE      FLAGS    CONS    VCPU    MEMORY    UTIL    NORM    UPTIME
primary       active    -n-c--   UART      8     63744M    0.0%    0.0%    16d 21h
  6m
<Omis>
CPU CORE
PERMITS (PERMANENT)  IN USE    REST
16      (16)        16        0
<Omis>
```

En réalité, seuls quatre cœurs du processeur sont disponibles de manière permanente (c'est à dire disponible par l'intermédiaire des clés d'activation de CPU achetées). Cependant, tous les 16 cœurs de processeur intégrés physiquement sont affichés comme étant permanents dans les résultats de la commande lorsque le permis temporaire d'activation de processeur est activé.

Index

A

Activation de processeur, 251
active directory, compte d'utilisateur XSCF,
gestion, 83
adresse IP de reprise, 149
adresse SAS, spécification, méthode de, 713
agent SNMP, 354
alias des lecteurs DVD de stockage à distance, 723
alias des lecteurs DVD externes, 717
alimentation sans interruption, 501
altitude du système, paramétrage/vérification,
189
arrêt commandé, 308
audit, 176

C

certificats de clé publique X.509, 503
chemins d'accès de périphériques SPARC M10-1,
605
chemins d'accès de périphériques SPARC M10-4,
608
chemins d'accès de périphériques SPARC M10-4S
, 615
chemins d'accès de périphériques SPARC M12-2,
586
chemins d'accès de périphériques SPARC M12-2S
, 593
clé d'activation du processeur, 253
commandes d'OpenBoot PROM, 706

communication inter-processeur, protocole, SSCP
, 149
composant, définition de configuration
redondante, 381
configuration de la mémoire, modification, 523
configuration du système, vérification, 405
configuration réseau, 17
Connexion, 29
connexion (shell XSCF), 38
connexion (XSCF Web), 43
console, basculer, 305
console, passage, 304
consommation électrique, 197
correspondance de la version du
microprogramme, 565

D

déconnexion (XSCF Web), 46
démarrage du système, contrôle, 191
démarrage SAN, utilisation, 488
dépannage, 575
disque dur, contenu, restauration, 397
disque dur, contenu, sauvegarde, 397
domaine logique, arrêt, 307
domaine logique, configuration, 301
domaine logique, démarrage, 306
domaine logique, modification de la
configuration, 320
domaine logique, panique, 398
domaine logique, réinitialisation, 397

domaine logique, taille de page maximale, 339
domaines logiques, 4
domaines logiques, arrêt des, 675
domaines logiques, contrôle, 301

É

état du système, vérification, 405
état, vérifier, 405

F

FAQ, 580
fichier de journal du XSCF, 429
fichier de vidage d'incident, 404
fonction de connexion de la console du domaine, 317, 677
fonction de gestion de l'alimentation à distance, 489
fonction de mode de démarrage du XSCF, remarques relatives à, 699
fonction de mode de démarrage du XSCF, restrictions relatives à, 699
fonction de notification par e-mail, 349
fonctions spécifiques du système, 675
fuseau horaire, 122

H

heure/date XSCF, réglage, 120
Host watchdog, 372

I

ID cible, spécification, méthode de, 711
identification d'objet MIB, 669
informations de configuration du domaine logique, restauration (XML), 390
informations de configuration du domaine logique, restauration (XSCF), 385
informations de configuration du domaine logique, sauvegarde (XML), 390
informations de configuration du domaine logique, sauvegarde (XSCF), 385
informations des réglages de XSCF, restauration, 381
informations sur la MIB de XSCF, 669

interface réseau XSCF, 150
iSCSI, utilisation, 488

J

journal, consultation, 429

L

l'activation de processeur, remarques importantes au sujet de, 272
LDAP sur SSL, compte utilisateur XSCF, gestion, 101
LDAP, compte d'utilisateur XSCF, gestion, 76
lecteur DVD, connexion, 205

M

mécanisme de détérioration, 374
message, consultation, 429
messages d'avertissement et de notification, vérification, 448
MIB étendue, 356, 671
MIB étendue de XSCF, 672
MIB standard, 356, 671
microprogramme XCP, mise à jour, 535
microprogramme XSCF, 5
microprogramme, mise à jour, 544
mise à jour du microprogramme, 543, 559
mise en miroir de la mémoire, configuration, 461
mode de fonctionnement du processeur, 286
mode de récupération, configuration, 380
mode Service, 455
mode Verrouillé, 455

N

nom de périphérique de volume, spécification, méthode de, 714
numéro PHY, spécification, méthode de, 710

O

OpenBoot PROM, 26
Oracle Solaris, démarrage, empêcher, 283
Oracle Solaris, mise à jour, 573
Oracle VM Server pour SPARC, 25

P

- pages de manuel, 55
- pages de XSCF Web, aperçu de, 639
- pages disponibles, 645
- partition physique, configuration, 285
- partition physique, mise hors tension, 297
- partition physique, mise sous tension, 296
- partition physique, modification de la configuration, 298
- partition physique, reconfiguration, 400
- partition physique, vérification, 419
- partitions physiques, 4, 285
- périphérique de démarrage, spécification, 709
- périphérique SAS2 par WWN, 629
- périphériques de destination PCIe, 525
- permis temporaire d'activation de processeur, 727
- permis temporaire d'activation de processeur, commandes liées au, 729
- permis temporaire d'activation de processeur, notes relatives au, 758
- prise en charge de l'activation du processeur, 675
- privège d'utilisateur, 65
- problèmes du système, 581
- processeurs virtuels, 521

R

- RAID matériel, 463
- réseau de contrôle du système, 17
- réseau utilisateur, 17
- réseau XSCF, 17
- réseau XSCF, 148
- ressources des domaines logiques, gestion des, 325
- ressources du cœur du processeur, attribution, 261
- ressources du cœur du processeur, déplacement, 264
- ressources en panne, vérification, 676
- ressources matérielles en panne, vérification, 375

S

- serveur, restauration de l'état aux valeurs d'usine

- à l'expédition, 402
- service HTTPS, 142
- service LDAP, utilisation, 488
- service SSH/Telnet, 136
- SSCP, 149, 154, 162
- superviseur, 25
- syntaxe World Wide Name (WWN), 629
- système, arrêt, 280
- système, configuration, 49
- système, démarrage, 275
- système, redémarrage, 283
- système, surveillance, 372

T

- terminal de gestion du système, 29
- trap, 673

U

- unité d'extension PCI, 529
- utilisateur XSCF, 62
- utilitaire FCode, 463
- utilitaire SAS2IRCU, 463

V

- variables d'environnement d'OpenBoot PROM, 705
- variables d'environnement d'OpenBoot PROM, réglage, 312
- vidage du superviseur, 321
- volume RAID matériel, suppression, 690

W

- WWN, 629

X

- XSCF Web, 639
- XSCF, configuration (shell XSCF), 56
- XSCF, configuration (XSCF Web), 61
- XSCF, problèmes possibles, 575
- XSCF, procédures de dépannage, 348

Z

- zone noyau d'Oracle Solaris, 302

