SPARC Enterprise M3000/M4000/M5000/ M8000/M9000 Servers

XSCF Reference Manual for XCP Version 1101

Part No. E21466-01,
Manual Code: C120-E645-01EN
February 2011

Copyright © 2011, Oracle and/or its affiliates and FUJITSU LIMITED. All rights reserved.

Oracle and/or its affiliates provided technical input and review on portions of this material.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related software documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS. Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). FUJITSU LIMITED, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa-ken 211-8588, Japan and Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065 and FUJITSU LIMITED, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa-ken 211-8588, Japan.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates and FUJITSU LIMITED disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Fujitsu and the Fujitsu logo are registered trademarks of Fujitsu Limited.

AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. UNIX is a registered trademark licensed through X/Open Company, Ltd.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates and FUJITSU LIMITED are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates FUJITSU LIMITED will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Copyright © 2011, Oracle et/ou ses affiliés. Tous droits réservés.

Entrée et revue tecnical fournies par Oracle et ses affiliés sur des parties de ce matériel.

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf disposition de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, breveter, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs,Oracle Corporation et FUJITSU LIMITED ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

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 RIGHTS. Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). FUJITSU LIMITED, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa-ken 211-8588, Japan et Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065 et FUJITSU LIMITED, 1-1, Kamikodanaka 4-chome, Nakahara-ku, Kawasaki-shi, Kanagawa-ken 211-8588, Japan.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer des dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour ce type d'applications.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés.Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

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

AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. Intel et Intel Xeon sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. UNIX est une marque déposée concédée sous licence par X/Open Company, Ltd.

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés et FUJITSU LIMITED déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers. En aucun cas, Oracle Corporation et ses affiliés et FUJITSU LIMITED ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation.

Please
Recycle

Adobe PostScript™

Contents

Preface ix

User and System Administration Commands 1

Intro 3

User Commands 13

exit 15
man 17
who 19

System Administration 21

addboard 23
addcodactivation 27
addcodlicense 29
addfru 31
adduser 33
applynetwork 35
cfgdevice 41
clockboard 47
console 49
deleteboard 51
deletecodactivation 55
deletecodlicense 57

deletefru 59
deleteuser 61
disableuser 63
dumpconfig 65
enableuser 71
flashupdate 73
fmadm 77
fmdump 79
fmstat 87
getflashimage 91
ioxadm 97
moveboard 107
nslookup 111
password 113
ping 117
poweroff 119
poweron 123
prtfru 127
rebootxscf 131
replacefru 133
reset 135
resetdateoffset 139
restoreconfig 141
restoredefaults 147
sendbreak 153
setad 155
setaltitude 163
setarchiving 165
setaudit 169
setautologout 175
setcod 177
setdate 181
setdcl 185
setdomainmode 191

setdomparam 199
setdscp 201
setdualpowerfeed 205
setemailreport 207
sethostname 211
sethttps 213
setldap 219
setldapssl 223
setlocale 231
setlocator 233
setloginlockout 235
setlookup 237
setnameserver 239
setnetwork 243
setntp 249
setpacketfilters 253
setpasswordpolicy 259
setpowerupdelay 263
setprivileges 265
setroute 269
setshutdowndelay 273
setsmtp 275
setsnmp 279
setsnmpusm 287
setsnmpvacm 291
setssh 295
setsunmc 301
settelnet 303
settimezone 305
setupfru 313
setupplatform 315
showad 319
showaltitude 323
showarchiving 325

showaudit 329
showautologout 333
showboards 335
showcod 341
showcodactivation 343
showcodactivationhistory 345
showcodlicense 347
showcodusage 349
showconsolepath 355
showdate 357
showdateoffset 359
showdcl 363
showdevices 369
showdomainmode 375
showdomainstatus 379
showdscp 381
showdualpowerfeed 385
showemailreport 387
showenvironment 389
showfru 395
showhardconf 397
showhostname 409
showhttps 411
showldap 413
showldapssl 415
showlocale 419
showlocator 421
showloginlockout 423
showlogs 425
showlookup 439
showmonitorlog 441
shownameserver 443
shownetwork 445
shownotice 451

showntp 453
showpacketfilters 457
showpasswordpolicy 459
showpowerupdelay 461
showresult 463
showroute 465
showshutdowndelay 469
showsmtp 471
showsnmp 473
showsnmpusm 475
showsnmpvacm 477
showssh 479
showstatus 483
showsunmc 485
showtelnet 487
showtimezone 489
showuser 495
snapshot 497
switchscf 505
testsb 507
traceroute 513
unlockmaintenance 517
version 519
viewaudit 523

Preface

This manual contains the man pages for the XSCF firmware for the SPARC Enterprise M3000/M4000/M5000/M8000/M9000 servers from Oracle and Fujitsu.

Some references to server names and document names are abbreviated for readability. For example, if you see a reference to the M9000 server, note that the full product name is the SPARC Enterprise M9000 server. And if you see a reference to the *XSCF Reference Manual*, note that the full document name is the *SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers XSCF Reference Manual*.

Before reading this document, you should read the overview guide for your server the *SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers Administration Guide*, and the *SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers XSCF User's Guide*.

At publication of this document, servers described herein were shipping with XCP 1101 firmware supported or installed. That might no longer be the latest available version, or the version now installed. Always see the Product Notes that apply to the firmware on your server, and those that apply to the latest firmware release.

This chapter includes the following sections:

- "Audience" on page x
- "Related Documentation" on page x
- "Text Conventions" on page xii
- "Syntax of the Command-Line Interface (CLI)" on page xiii
- "Documentation Feedback" on page xiii

Audience

This manual is written for experienced system administrators with working knowledge of computer networks and advanced knowledge of the Oracle Solaris Operating System (Oracle Solaris OS).

Related Documentation

All documents for your sever are available online at the following locations:

- Sun Oracle software-related manuals (Oracle Solaris OS, and so on): (http://www.oracle.com/technetwork/documentation/index.html)
- Fujitsu documents: (http://www.fujitsu.com/sparcenterprise/manual/)
- Oracle M3000/M4000/M5000/M8000/M9000 server software documents: (http://www.oracle.com/pls/topic/lookup?ctx=E19867-01&id=homepage)
- Oracle M3000 server hardware documents: (http://www.oracle.com/pls/topic/lookup?ctx=E19855-01&id=homepage)
- Oracle M4000 server hardware documents: (http://www.oracle.com/pls/topic/lookup?ctx=E19855-01&id=homepage)
- Oracle M5000 server hardware documents: (http://www.oracle.com/pls/topic/lookup?ctx=E19580-01&id=homepage)
- Oracle M8000 server hardware documents: (http://www.oracle.com/pls/topic/lookup?ctx=E19170-01&id=homepage)
- Oracle M9000 server hardware documents: (http://www.oracle.com/pls/topic/lookup?ctx=E19415-01&id=homepage)

Related SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers Documents
SPARC Enterprise M3000 Server Site Planning Guide
SPARC Enterprise M4000/M5000 Servers Site Planning Guide
SPARC Enterprise M8000/M9000 Servers Site Planning Guide
SPARC Enterprise Equipment Rack Mounting Guide
SPARC Enterprise M3000 Server Getting Started Guide[*]
SPARC Enterprise M4000/M5000 Servers Getting Started Guide[*]
SPARC Enterprise M8000/M9000 Servers Getting Started Guide[*]
SPARC Enterprise M3000 Server Overview Guide
SPARC Enterprise M4000/M5000 Servers Overview Guide
SPARC Enterprise M8000/M9000 Servers Overview Guide
SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers Important Legal and Safety Information[*]
SPARC Enterprise M3000 Server Safety and Compliance Guide
SPARC Enterprise M4000/M5000 Servers Safety and Compliance Guide
SPARC Enterprise M8000/M9000 Servers Safety and Compliance Guide
External I/O Expansion Unit Safety and Compliance Guide
SPARC Enterprise M4000 Server Unpacking Guide[*]
SPARC Enterprise M5000 Server Unpacking Guide[*]
SPARC Enterprise M8000/M9000 Servers Unpacking Guide[*]
SPARC Enterprise M3000 Server Installation Guide
SPARC Enterprise M4000/M5000 Servers Installation Guide
SPARC Enterprise M8000/M9000 Servers Installation Guide
SPARC Enterprise M3000 Server Service Manual
SPARC Enterprise M4000/M5000 Servers Service Manual
SPARC Enterprise M8000/M9000 Servers Service Manual
External I/O Expansion Unit Installation and Service Manual
SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers Administration Guide
SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers XSCF User's Guide
SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers XSCF Reference Manual
SPARC Enterprise M4000/M5000/M8000/M9000 Servers Dynamic Reconfiguration (DR) User's Guide
SPARC Enterprise M4000/M5000/M8000/M9000 Servers Capacity on Demand (COD) User's Guide

Related SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers Documents
SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers Product Notes†
SPARC Enterprise M3000 Server Product Notes
SPARC Enterprise M4000/M5000 Servers Product Notes
SPARC Enterprise M8000/M9000 Servers Product Notes
External I/O Expansion Unit Product Notes
SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers Glossary

* This is a printed document

† Beginning with the XCP 1100 release

Text Conventions

This manual uses the following fonts and symbols to express specific types of information.

Font/symbol	Meaning	Example
AaBbCc123	What you type, when contrasted with on-screen computer output. This font represents the example of command input in the frame.	XSCF> **adduser jsmith**
AaBbCc123	The names of commands, files, and directories; on-screen computer output. This font represents the example of command output in the frame.	XSCF> **showuser -P** User Name: jsmith Privileges: useradm auditadm
Italic	Indicates the name of a reference manual, a variable, or user-replaceable text.	See the *SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers XSCF User's Guide*
" "	Indicates names of chapters, sections, items, buttons, or menus.	See Chapter 2, "System Features."

Syntax of the Command-Line Interface (CLI)

The command syntax is as follows:

- A variable that requires input of a value must be put in Italics.
- An optional element must be enclosed in [].
- A group of options for an optional keyword must be enclosed in [] and delimited by |.

Documentation Feedback

If you have any comments or requests regarding this document, go to the following web sites:

- For Oracle users:

  (http://www.oraclesurveys.com/se.ashx?s=25113745587BE578)

  Include the title and part number of your document with your feedback:

  SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers XSCF Reference Manual, part number E21466-01.

- For Fujitsu users, refer to this SPARC Enterprise contact:

  (http://www.fujitsu.com/global/contact/computing/sparce_index.html)

R E F E R E N C E

User and System Administration Commands

NAME

Intro - list the commands provided by the XSCF firmware

DESCRIPTION

This Intro page lists the user commands (`exit`(1), `man`(1), and `who`(1)) and system administration commands (all the others, beginning with `addboard`(8)) provided by the XSCF firmware of the SPARC Enterprise M3000/M4000/M5000/M8000/M9000 servers. Some XSCF commands have the same name as their Oracle Solaris OS counterpart, but function slightly differently. For details, refer to the man page for each command.

The following commands are supported:

`exit`	exit the XSCF shell
`man`	display manual pages of specified XSCF shell command
`who`	display a list of the user accounts who are logged in to the XSCF
`addboard`	configure an eXtended System Board (XSB) into the domain configuration or assign it to the domain configuration
`addcodactivation`	add a Capacity on Demand (COD) hardware activation key (COD key) to the COD database
`addcodlicense`	add a Capacity on Demand (COD) right-to-use (RTU) license key to the COD license database
`addfru`	add a Field Replaceable Unit (FRU)
`adduser`	create an XSCF user account
`applynetwork`	apply XSCF network information to the XSCF
`cfgdevice`	connect the CD-RW/DVD-RW drive unit and the tape drive unit to the port, disconnect it from the port, or display the status of the drive
`clockboard`	set or display the clock control unit used at system startup
`console`	connect to a domain console
`deleteboard`	disconnect an eXtended System Board (XSB) from the domain configuration

`deletecodactivation`	remove a Capacity on Demand (COD) hardware activation key (COD key) from the COD database
`deletecodlicense`	remove a Capacity on Demand (COD) right-to-use (RTU) license key from the COD license database
`deletefru`	delete a Field Replaceable Unit (FRU)
`deleteuser`	delete an XSCF user account
`disableuser`	disable an XSCF user account
`dumpconfig`	save system configuration information to a file
`enableuser`	enable an XSCF user account
`flashupdate`	update the firmware
`fmadm`	fault management configuration tool
`fmdump`	view fault management logs
`fmstat`	report fault management module statistics
`getflashimage`	download a firmware image file
`ioxadm`	manage External I/O Expansion Units and add-in cards that contain Energy Storage Modules and are attached to the host system
`moveboard`	move an eXtended System Board (XSB) from the current domain to another
`nslookup`	refer to the DNS server for the host
`password`	manage user passwords and expiration settings
`ping`	send the ICMP ECHO_REQUEST packets to the network host or the network device
`poweroff`	turn off the power to the specified domain
`poweron`	turn on the power to the specified domain
`prtfru`	display FRUID data on the system and External I/O Expansion Unit

`rebootxscf`	reset the XSCF
`replacefru`	replace a field replaceable unit (FRU)
`reset`	reset the specified domain
`resetdateoffset`	reset time of domains to match system time
`restoreconfig`	restore the system configuration information previously saved by dumpconfig
`restoredefaults`	restore factory settings of the server or XSCF unit
`sendbreak`	send a break signal to the specified domain
`setad`	configure Active Directory
`setaltitude`	set the altitude of the system or whether or not the air filter installed
`setarchiving`	configure the log archiving functionality
`setaudit`	manage the system auditing functionality
`setautologout`	set the session timeout time of the XSCF shell
`setcod`	set up the Capacity on Demand (COD) resources used for domains
`setdate`	set the date and time of XSCF
`setdcl`	set a domain component list (DCL)
`setdomainmode`	set the modes of operation for the specified domain
`setdomparam`	forcibly rewrite OpenBoot PROM environment variables
`setdscp`	set the IP address assignments for the Domain to Service Processor Communications Protocol (DSCP)
`setdualpowerfeed`	set dual power feed mode
`setemailreport`	set up the email report configuration data
`sethostname`	set a host name and a DNS domain name for an XSCF unit

`sethttps`	start or stop the HTTPS service, which is used in the XSCF network. This command also performs authentication-related settings
`setldap`	configure the Service Processor as a Lightweight Directory Access Protocol (LDAP) client
`setldapssl`	configure LDAP/SSL
`setlocale`	set the default locale of the XSCF
`setlocator`	control the blinking of the CHECK LED on the operator panel
`setloginlockout`	enable or disable login lockout feature
`setlookup`	enable or disable the use of the Lightweight Directory Access Protocol (LDAP) server for authentication and privilege lookup
`setnameserver`	set the domain name system (DNS) servers and the DNS search paths used in the XSCF network
`setnetwork`	set or remove an XSCF network interface
`setntp`	set the NTP servers used on the XSCF network, the stratum value, the preferred server and the clock address of the local clock of XSCF
`setpacketfilters`	set the IP packet filtering rules to be used in the XSCF network
`setpasswordpolicy`	manage the system password policy
`setpowerupdelay`	set the warm-up time of the system and wait time before system startup
`setprivileges`	assign user privileges
`setroute`	set routing information for an XSCF network interface
`setshutdowndelay`	set the shutdown wait time at power interruption of the uninterruptible power supply (UPS)
`setsmtp`	set up the Simple Mail Transfer Protocol (SMTP) settings

setsnmp	manage the SNMP agent
setsnmpusm	specify the SNMPv3 agent's User-based Security Model (USM) configuration
setsnmpvacm	modify the SNMPv3 agent's View-based Access Control Model (VACM) configuration
setssh	configure the settings for the Secure Shell (SSH) service used in the XSCF network
setsunmc	start or stop the Sun Management Center agent and make changes to its configuration
settelnet	start or stop the Telnet service used in the XSCF network
settimezone	set the time zone and Daylight Saving Time of XSCF
setupfru	set up device hardware
setupplatform	set up platform specific settings
showad	show Active Directory configuration and messages
showaltitude	display the altitude of the system and whether the air filter installed
showarchiving	display log archiving configuration and status
showaudit	display the current auditing system state
showautologout	display the session timeout time of the XSCF shell
showboards	display information on an eXtended System Board (XSB)
showcod	display Capacity on Demand (COD) information
showcodactivation	display the current Capacity on Demand (COD) hardware activation permits (COD permits) stored in the COD database
showcodactivationhistory	show Capacity on Demand (COD) activation log

`showcodlicense`	display the current Capacity on Demand (COD) right-to-use (RTU) licenses stored in the COD license database
`showcodusage`	display the current usage statistics for Capacity on Demand (COD) resources
`showconsolepath`	displays information on the domain console that is currently connected
`showdate`	display the date and time of XSCF
`showdateoffset`	display the time differences between the time of the system and the time of the domains
`showdcl`	display the current domain component list (DCL)
`showdevices`	display current information on an eXtended System Board (XSB)
`showdomainmode`	display the modes of operation for the specified domain
`showdomainstatus`	display the current domain component list (DCL)
`showdscp`	display the IP addresses assigned to the Domain to Service Processor Communications Protocol (DSCP)
`showdualpowerfeed`	display the current setting of dual power feed mode
`showemailreport`	display the email report configuration data
`showenvironment`	display the airflow volume, intake air temperature and humidity, temperature sensor, voltage sensor, fan speed, and power consumption information in the server
`showfru`	display the hardware settings of specified device
`showhardconf`	display information about field replaceable unit (FRU) installed in the system
`showhostname`	display the current host name for the XSCF unit

`showhttps`	display the status of the HTTPS service set for the XSCF network
`showldap`	display the Lightweight Directory Access Protocol (LDAP) configuration for the Service Processor
`showldapssl`	show LDAP/SSL configuration and messages
`showlocale`	display the current setting for the XSCF locale
`showlocator`	display the state of the CHECK LED on the operator panel
`showloginlockout`	display the account lockout setting
`showlogs`	display the specified log
`showlookup`	display the configuration for authentication and privileges lookup
`showmonitorlog`	display the contents of monitoring messages in real time
`shownameserver`	display the registered domain name system (DNS) servers and the DNS search paths specified on the XSCF network
`shownetwork`	display information of network interfaces for XSCF
`shownotice`	display copyright and license information for the XSCF Control Package (XCP)
`showntp`	display the NTP information which currently set for XSCF
`showpacketfilters`	show the IP packet filtering rules that are set in the XSCF network
`showpasswordpolicy`	display the current password settings
`showpowerupdelay`	display the current settings for the warm-up time of the system and wait time before system startup
`showresult`	display the exit status of the most recently executed command

`showroute`	display routing information for an XSCF network interface
`showshutdowndelay`	display the shutdown wait time at power interruption of the uninterruptible power supply (UPS)
`showsmtp`	display the Simple Mail Transfer Protocol (SMTP) configuration information
`showsnmp`	display the configuration information and current status of the SNMP agent
`showsnmpusm`	display the current User-based Security Model (USM) information for the SNMP agent
`showsnmpvacm`	display the current View-based Access Control Access (VACM) information for the SNMP agent
`showssh`	display the settings of the Secure Shell (SSH) service that configured for the XSCF network
`showstatus`	display the degraded Field Replaceable Units (FRUs)
showsunmc	show setup information and status of Sun Management Center agent
`showtelnet`	display the current status of the Telnet service for the XSCF network
`showtimezone`	display the XSCF time zone and Daylight Saving Time information of current settings
`showuser`	display user account information
`snapshot`	collect and transfer environment, log, error, and FRUID data
`switchscf`	switch the XSCF unit between the active and standby states
`testsb`	perform an initial diagnosis of the specified physical system board (PSB)
`traceroute`	display the route packets take to the specified network host or the network device

`unlockmaintenance`	forcibly release the locked status of XSCF
`version`	display firmware version
`viewaudit`	display audit records

R E F E R E N C E

User Commands

NAME

exit - exit the XSCF shell

SYNOPSIS

`exit`

DESCRIPTION

The `exit`(1) command exits and closes the XSCF shell.

Privileges

No privileges are required to run this command.

Refer to `setprivileges`(8) for more information.

NAME

man - display manual pages of specified XSCF shell command

SYNOPSIS

man *command_name...*

man -h

DESCRIPTION

man(1) displays manual pages of specified XSCF shell command.

Privileges

No privileges are required to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following option is supported:

-h	Displays usage statement. When used with other options or operands, an error occurs.

OPERANDS

The following operand is supported:

command_name	Specifies the command name whose manual page is displayed. Multiple *command_name* can be specified by delimited the spaces.

EXTENDED DESCRIPTION

- If the relevant manual page is too long, the page is divided into pages that each can fit on one screen. In such cases, the following key operations are available:

Key	Description
Enter	Displays the next line.
space	Displays the next page.
b	Goes back half a page.
q	Quits display of the page in the manual.

- If intro is specified for *command_name*, a list of XSCF shell commands is displayed.

EXAMPLES

EXAMPLE 1 Displays the manual page of the addboard(8) command.

```
XSCF> man addboard
```

EXAMPLE 2 Displays a list of XSCF shell commands.

```
XSCF> man intro
```

EXIT STATUS

The following exit values are returned:

0	Successful completion
>0	An error occurred.

NAME

who - display a list of the user accounts who are logged in to the XSCF

SYNOPSIS

who

who -h

DESCRIPTION

who(1) displays a list of the user accounts who are logged in to the XSCF.

The following information is displayed:

- XSCF user account name
- Terminal used
- Idle time
- Login time
- Remote host name

Privileges

No privileges are required to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following option is supported:

-h Displays usage statement.

EXAMPLES

EXAMPLE 1 Displays a list of the user accounts who are logged in to the XSCF.

```
XSCF> who
USER        TTY      IDLE      FROM            HOST
scf         pts/0    00:00m    Dec 21 13:57    JJJJ.ggg.Company.com
```

EXIT STATUS

The following exit values are returned:

0 Successful completion.

>0 An error occurred.

R E F E R E N C E

System Administration

NAME

addboard - configure an eXtended System Board (XSB) into the domain configuration or assign it to the domain configuration

SYNOPSIS

addboard [[-q] -{y|n}] [-f] [-v] [-c configure] -d *domain_id xsb* [*xsb*...]

addboard [[-q] -{y|n}] [-f] [-v] [-c assign] -d *domain_id xsb* [*xsb*...]

addboard [[-q] -{y|n}] [-f] [-v] [-c reserve] -d *domain_id xsb* [*xsb*...]

addboard -h

DESCRIPTION

The addboard(8) command, based on domain component list (DCL), configures a XSB into the domain configuration or assigns it to the domain configuration.

The addboard(8) command is not available on the M3000 server.

One of the following configuration methods can be specified:

configure	Configures an XSB into the specified domain configuration. The incorporated XSB can be accessed from the Oracle Solaris OS.
assign	Assigns an XSB to the specified domain. The assigned XSB is reserved for the specified domain and cannot be configured in or assigned to other domains. The assigned XSB is configured in the domain by reboot or execution of the addboard(8) command with "-c configure".
reserve	Reserves incorporation of an XSB into the domain configuration. The action of "reserve" is the same as "assign."

Privileges

You must have one of the following privileges to run this command:

platadm	Can run this command for all domains.
domainadm	Can run this command only for your managed domains.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-c assign	Assigns an XSB to the domain configuration. If the -c option is omitted, "-c configure" is used.
-c configure	Configures an XSB in the domain configuration. If the -c option is omitted, "-c configure" is used.
-c reserve	Reserves incorporation of an XSB into the domain configuration. If the -c option is omitted, "-c configure" is used.

`-d` *domain_id*	Specifies the ID of the domain in which an XSB is to be configured or to which it is to be assigned. *domain_id* can be 0–23 depending on the system configuration.
`-f`	Forcibly incorporates into a domain an XSB. **Caution -** If the `-f` option is used to forcibly add an XSB to a domain, all the added hardware resources may not work normally. For this reason, use of the `-f` option is not recommended in normal operation. If the `-f` option must be specified, verify the status of every added XSB and device.
`-h`	Displays usage statement. When used with other options or operands, an error occurs.
`-n`	Automatically answers "`n`" (no) to all prompts.
`-q`	Suppresses all messages to stdout, including prompts.
`-v`	Displays a detailed message. If this option is specified with the `-q` option, the `-v` option is ignored.
`-y`	Automatically answers "`y`" (yes) to all prompts.

OPERANDS

The following operand is supported:

xsb	Specifies the XSB number to be configured or assigned. Multiple *xsb* operands are permitted, separated by spaces. The following xsb form is accepted: *x*–y where: *x* — An integer from `00–15`. *y* — An integer from `0–3`.

EXTENDED DESCRIPTION

- You can execute the `addboard`(8) command on a domain that is not running. When the domain is running, the `addboard`(8) command with "`-c configure`" will succeed only if the following Oracle Solaris Service Management Facility (SMF) services are active on that domain:
  - Domain SP Communication Protocol (dscp)
  - Domain Configuration Server (dcs)
  - Oracle Sun Cryptographic Key Management Daemon (sckmd)
- When the command is executed, a prompt to confirm execution of the command with the specified options is displayed. Enter "`y`" to execute the command or "`n`" to cancel the command.

- If "`-c configure`" is specified when either the domain power has been turned off or the Oracle Solaris OS is not running, an error occurs.
- When "`-c configure`" is specified, hardware diagnosis is performed on the XSB before it is incorporated into the domain. Therefore, command execution may take time.
- To use the `addboard`(8) command to configure or assign an XSB, DCL must be set up in advance using the `setdcl`(8) command.
- If the `addboard`(8) command is executed under the progress of power-on or power-off processing, the busy status is returned. After that processing in the domain is completed, reexecute the command.
- See the `setdcl`(8) and `showdcl`(8) commands for DCL.

EXAMPLES

EXAMPLE 1 Configures XSB#00-0, #01-0, #02-0, and #03-0 into domain ID 0.

```
XSCF> addboard -y -c assign -d 0 00-0 01-0 02-0 03-0
```

EXAMPLE 2 Configures XSB#00-0, #01-0, #02-0, and #03-0 forcibly into domain ID 2.

```
XSCF> addboard -f -d 2 00-0 01-0 02-0 03-0
```

EXIT STATUS

The following exit values are returned:

`0`	Successful completion.
`>0`	An error occurred.

SEE ALSO

deleteboard`(8)`, **moveboard**`(8)`, **replacefru**`(8)`, **setdcl**`(8)`, **setdomainmode**`(8)`, **setupfru**`(8)`, **showboards**`(8)`,**showdcl**`(8)`, **showdevices**`(8)`, **showdomainstatus**`(8)`, **showfru**`(8)`, **testsb**`(8)`

NAME

addcodactivation - add a Capacity on Demand (COD) hardware activation key (COD key) to the COD database

SYNOPSIS

addcodactivation *key_signature*

addcodactivation -h

DESCRIPTION

addcodactivation(8) adds the specified COD key to the COD database on the Service Processor.

This command is not available on the M3000 server.

When the COD key is added, the quantity of headroom is reduced by the quantity provided by the key. The quantity of headroom cannot be lower than 0.

Note – Before you run this command, you must obtain a COD key. To obtain a COD key, contact your sales representative. For details on COD keys, refer to the *SPARC Enterprise M4000/M5000/M8000/M9000 Servers Capacity on Demand (COD) User's Guide*.

Privileges

You must have platadm privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following option is supported:

-h Displays usage statement.

When used with other options or operands, an error occurs.

OPERANDS

The following operand is supported:

key_signature Specifies the key to be added to the COD database.

EXAMPLES

EXAMPLE 1 Adding a Key

```
XSCF> addcodactivation \
01:84000000:104:0301010100:3:00000000:xxxxxxxxxxxxxxxxxxxxxx
```

EXIT STATUS

The following exit values are returned:

0 Successful completion.

>0 An error occurred.

SEE ALSO

SPARC Enterprise M4000/M5000/M8000/M9000 Servers Capacity on Demand (COD) User's Guide

NAME

addcodlicense - add a Capacity on Demand (COD) right-to-use (RTU) license key to the COD license database

SYNOPSIS

addcodlicense *license-signature*

addcodlicense -h

DESCRIPTION

addcodlicense(8) adds the COD RTU specified license key to the COD license database on the Service Processor.

The addcodlicense(8) command is not available on the M3000 server.

When the license key is added, the quantity of headroom is reduced by the quantity provided by the license key. The quantity of headroom cannot be lower than 0.

Note – Before you run this command, you must obtain a COD license key. To obtain a license key, contact your sales representative. For details on COD RTU license keys, refer to the *SPARC Enterprise M4000/M5000/M8000/M9000 Servers Capacity on Demand (COD) User's Guide*.

Privileges

You must have platadm privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following option is supported:

-h Displays usage statement.

When used with other options or operands, an error occurs.

OPERANDS

The following operand is supported:

license-signature Specifies the COD RTU license key to be added to the COD license database.

EXAMPLES

EXAMPLE 1 Adding a COD RTU License Key

```
XSCF> addcodlicense \
01:84000000:104:0301010100:3:00000000:xxxxxxxxxxxxxxxxxxxxxx
```

EXIT STATUS

The following exit values are returned:

0 Successful completion.

>0 An error occurred.

SEE ALSO

SPARC Enterprise M4000/M5000/M8000/M9000 Servers Capacity on Demand (COD) User's Guide

NAME

addfru - add a Field Replaceable Unit (FRU)

SYNOPSIS

addfru

addfru -h

DESCRIPTION

The addfru(8) command adds an FRU.

The addfru(8) command enables the user to make the settings that are required for FRU addition and related to selecting, confirming, and mounting FRUs, interactively using menus.

The following FRUs can be added by the addfru(8) command:

- CPU/Memory Board unit (CMU)
- I/O unit (IOU)
- Fan unit (FANU)
- Power supply unit (PSU)

Privileges

You must have fieldeng privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following option is supported:

-h Displays usage statement.

EXIT STATUS

The following exit values are returned:

0 Successful completion.

>0 An error occurred.

SEE ALSO

deletefru(8), **replacefru**(8), **setupfru**(8), **showfru**(8), **showhardconf**(8), **testsb**(8), **unlockmaintenance**(8)

NAME

adduser - create an XSCF user account

SYNOPSIS

adduser [-u *UID*] *user*

adduser -h

DESCRIPTION

adduser(8) creates a new local XSCF user account. This account is used to configure, operate, manage and administer the XSCF firmware. Initially, this account has no password. It cannot be used for login until either the password is set (using password(8)) or Secure Shell (SSH) public key authentication is set for the user. The new account will be locked but not disabled. The system can support up to 100 local users with an average length of 10 characters for the *user* operand.

If the Service Processor is configured to use Lightweight Directory Access Protocol (LDAP), Active Directory, or LDAP/SSL for user account data, the user name and UID (if specified) must not already be in use locally or in LDAP, Active Directory, or LDAP/SSL.

When a user is created, adduser(8) command stores the current password policy values in a file for the user. For more information on setting password policy see, setpasswordpolicy(8).

Privileges

You must have useradm privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported.

-h — Displays usage statement.

When used with other options or operands, an error occurs.

-u *UID* — Creates a new user with the given user identifier (UID). If specified, the UID must be between 100 and 60000, inclusive. If not specified, a UID is automatically assigned with a minimum value of 100.

OPERANDS

The following operand is supported:

user — Specifies a valid user name to be added. The maximum length of the user name is 31 characters. A new local XSCF user account name can be a combination of lowercase letters, numbers, "-", or "_". Do not use uppercase letters. The first character must be a letter. Examples of acceptable names include jsmith, j_smith, and j_smith-0123.

EXAMPLES

EXAMPLE 1 Creating a New User

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

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

deleteuser(8), **disableuser**(8), **enableuser**(8), **password**(8), **setad**(8), **setldap**(8), **setldapssl**(8), **setpasswordpolicy**(8), **showad**(8), **showldap**(8), **showldapssl**(8), **showpasswordpolicy**(8), **showuser**(8)

NAME

applynetwork - apply XSCF network information to the XSCF

SYNOPSIS

applynetwork [[-q] -{y|n}] [-M]

applynetwork -h

DESCRIPTION

applynetwork(8) command applies XSCF network information that has been set to the XSCF.

Setting network information on XSCF is a three-step process:

1. Set the information with the following commands:

- sethostname(8) - Set XSCF host name and a DNS domain name
- setnameserver(8) - Set a DNS server name and a DNS search path
- setnetwork(8) - Set IP address and netmask of XSCF network interface
- setroute(8) - Set routing information of XSCF network interface

2. Execute the applynetwork(8) command to apply the settings to XSCF.

3. Execute the rebootxscf(8) command to make the changes to the XSCF permanent.

Note – If XSCF is reset without executing the applynetwork(8) command, network information that is set is not applied in XSCF. Also, information that is set is deleted.

Privileges

You must have platadm privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-h	Displays usage statement. When used with other options or operands, an error occurs.
-M	Displays text by page.
-n	Automatically answers "n" (no) to all prompts.
-q	Suppresses all messages to stdout, including prompts.
-y	Automatically answers "y" (yes) to all prompts.

EXTENDED DESCRIPTION

- When the command is executed, a prompt to confirm execution of the command with the specified options is displayed. Enter "**y**" to execute the command or "**n**" to cancel the command.

- Use the appropriate network commands to specify the following settings, then execute the `applynetwork`(8) command. All these settings must be present and proper or the XSCF network settings will not be applied.
  - XSCF host name (`sethostname`(8))
  - DNS domain name (`sethostname`(8))
  - IP address and netmask of XSCF network interface (`setnetwork`(8))
- On M8000/M9000 servers, use the `sethostname`(8) command to set host names to both xscf#0 and xscf#1.
- On M3000/M4000/M5000 servers, use the `setnetwork`(8) command to set xscf#0-lan#0 and xscf#0-lan#1 so that at least one is up. If both are up, they must use different subnets.
- On M8000/M9000 servers, if xscf#0-lan#0, xscf#1-lan#0, xscf#0-lan#1, and xscf#1-lan#1 are all in down status, an error results.
- On M8000/M9000 servers, if the network interface which is in the up status has the following settings, it results in an error. Use the `setnetwork`(8) command to set up correctly.
  - If the subnet of xscf#0-lan#0, xscf#1-lan#0, and the takeover IP address lan#0 are different
  - If the subnet of xscf#0-lan#1, xscf#1-lan#1, and the takeover IP address lan#1 are different
  - If the subnet of ISN is different
  - If the subnet of xscf#0-lan#0, xscf#0-lan#1, and xscf#0-if are the same
  - If the subnet of xscf#1-lan#0, xscf#1-lan#1, and xscf#1-if are the same
- In case the total number of the characters of the DNS domain name that you set by using the `sethostname`(8) command and of the search path that you set by using the `setnameserver`(8) command exceeds 256, it results in an error.
- In the `setnameserver`(8) command, if you do not set the DNS server but set the search path alone, an error results.
- On M8000/M9000 servers, do not execute the `applynetwork`(8) command during XSCF failover.

EXAMPLES

EXAMPLE 1 Applies the information that has been set for the XSCF network.

On M3000/M4000/M5000 servers:

```
XSCF> applynetwork
The following network settings will be applied:
 xscf#0 hostname  :hostname-0
 DNS domain name  :example.com
 nameserver       :10.23.4.3
```

```
 interface        :xscf#0-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        :xscf#0-lan#1
 status           :down
 IP address       :
 netmask          :
 route            :

Continue? [y|n] :y
Please reset the XSCF by rebootxscf to apply the network settings.
Please confirm that the settings have been applied by executing
showhostname, shownetwork, showroute and shownameserver after rebooting
the XSCF.
```

On M8000/M9000 servers:

```
XSCF> applynetwork
The following network settings will be applied:
 xscf#0 hostname  :hostname-0
 xscf#1 hostname  :hostname-1
 DNS domain name  :example.com
 nameserver       :10.23.4.3

 interface        :xscf#0-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        :xscf#0-lan#1
 status           :down
 IP address       :
 netmask          :
 route            :

 interface        :xscf#0-if
 status           :down
 IP address       :10.24.100.1
 netmask          :255.255.255.0

 interface        :lan#0
```

```
 status           :down
 IP address       :
 netmask          :

 interface        :xscf#1-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        :xscf#1-lan#1
 status           :down
 IP address       :
 netmask          :
 route            :

 interface        :xscf#1-if
 status           :down
 IP address       :10.24.100.2
 netmask          :255.255.255.0

 interface        :lan#1
 status           :down
 IP address       :
 netmask          :

Continue? [y|n] :y
Please reset the XSCF by rebootxscf to apply the network settings.
Please confirm that the settings have been applied by executing
showhostname, shownetwork, showroute and shownameserver after rebooting
the XSCF.
```

EXAMPLE 2 Applies the information that has been set for the XSCF network, on M3000/M4000/M5000 servers. Automatically answers "y" to all prompts.

```
XSCF> applynetwork -y
The following network settings will be applied:
 xscf#0 hostname  :hostname-0
 DNS domain name  :example.com
 nameserver       :10.23.4.3

 interface        :xscf#0-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        :xscf#0-lan#1
 status           :down
 IP address       :
 netmask          :
 route            :

Continue? [y|n] :y
Please reset the XSCF by rebootxscf to apply the network settings.
Please confirm that the settings have been applied by executing
showhostname, shownetwork, showroute and shownameserver after rebooting
the XSCF.
```

EXAMPLE 3 Applies the information that has been set for the XSCF network. Suppresses prompts, and automatically answers "y" to all prompts.

```
XSCF> applynetwork -q -y
```

EXAMPLE 4 Sets the name server and the search path and then applies the XSCF network settings.

```
XSCF> applynetwork
The following network settings will be applied:
 xscf#0 hostname  :hostname-0
 DNS domain name  :example.com
 nameserver       :10.23.4.3
 nameserver       :10.24.144.3
 nameserver       :10.24.131.7
 search           :example1.com
 search           :example2.com
 search           :example3.com
 search           :example4.com
 search           :example5.com

 interface        :xscf#0-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        :xscf#0-lan#1
 status           :down
 IP address       :
 netmask          :
 route            :
```

```
Continue? [y|n] :y
Please reset the XSCF by rebootxscf to apply the network settings.
Please confirm that the settings have been applied by executing
showhostname, shownetwork, showroute and shownameserver after rebooting
the XSCF.
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

rebootxscf(8), **sethostname**(8), **setnameserver**(8), **setnetwork**(8), **setroute**(8)

NAME

cfgdevice - connect the CD-RW/DVD-RW drive unit and the tape drive unit to the port, disconnect it from the port, or display the status of the drive

SYNOPSIS

cfgdevice [[-q] -{y|n}] -c attach -p *port_no*

cfgdevice [[-q] -{y|n}] -c detach -p *port_no*

cfgdevice -l [-M]

cfgdevice -h

DESCRIPTION

The cfgdevice(8) connects the CD-RW/DVD-RW drive unit and the tape drive unit to the specified port, disconnects it from the domain, or displays the current status.

The cfgdevice(8) command is available only for the M8000/M9000 servers.

To connect the CD-RW/DVD-RW drive unit and the tape drive unit, the port number which is a PCI slot number on the I/O unit which installed IOU Onboard Device Card A (IOUA) needs to specify. Executing the cfgdevice(8) command, the CD-RW/DVD-RW drive unit and the tape drive unit is connected to specified port by the built-in switching unit.

The current status of the drive that is displayed with this command includes the following types of status information:

`port_no` Port number of the port where the IOUA is installed and that can be connected to the CD-RW/DVD-RW drive unit and the tape drive unit. It is displayed in the "*IOU number-PCI slot number*" format.

`IOU/SAS-status` Connection status between IOUA and built-in switching unit. It is changed by specifying "`attach`" or "`detach`."

- `enable/disable`: Setting status of the `cfgdeive`(8) command
  `enable`: Connected with "`-c attach`."
  `disable`: Not connected.
- `up/down`: Logical connection between IOUA and built-in switching unit.
  `up`: Connected.
  `down`: Not connected.

`SAS-status` Connection status between I/O unit and the system.

- `enable/disable`: Connection setting between I/O unit and the system. When starting a domain with no I/O unit, the "`disable`" may be displayed.
  `enable`: Yes
  `disable`: No
- `up/down`: Logical connection between I/O unit and the system.
  `up`: Connected.
  `down`: Not connected.

Privileges

You must have `platadm` or `fieldeng` privileges to run this command.

Refer to `setprivileges`(8) for more information.

OPTIONS

The following options are supported:

`-c attach` Connects the CD-RW/DVD-RW drive unit and the tape drive unit to the specified port.

`-c detach` Disconnects the CD-RW/DVD-RW drive unit and the tape drive unit from the specified port.

`-h` Displays usage statement. When used with other options or operands, an error occurs.

`-l` Displays the current status of the CD-RW/DVD-RW drive unit and the tape drive unit currently set up.

`-M` Displays text by page. This option provides a function that is the same as that of the `more` command.

`-n`	Automatically answers "`n`" (no) to all prompts.
`-p` *port_no*	Specifies the number of the port, in the specified domain, to which the CD-RW/DVD-RW drive unit and the tape drive unit is to be connected. *port_no* can be specified in the '*IOU number-PCI slot number*' format. The `-p` option cannot be omitted.
`-q`	Suppresses all messages to stdout, including prompts.
`-y`	Automatically answers "`y`" (yes) to all prompts.

EXTENDED DESCRIPTION

- When the command is executed, a prompt to confirm execution of the command with the specified options is displayed. Enter "`y`" to execute the command or "`n`" to cancel the command.
- When all domains are powered off, "`-c attach`" reserves attachment and "`-c detach`" reserves detachment. When the the status of the power is in any state other than off, the setting will be immediately applied after the `cfgdevice`(8) command is executed.

  To verify that all domains are powered off, execute the `showlogs power` command and look for the value `System Power Off`.
- The CD-RW/DVD-RW and the tape connection is maintained even if the domain configuration is changed, or a CPU/Memory Board unit (CMU) or I/O unit (IOU) is replaced with a connected CD-RW/DVD-RW drive unit and the tape drive unit.
- The CD-RW/DVD-RW and the tape connection is maintained even if the domain power is turned off or the system is rebooted.
- The CD-RW/DVD-RW drive unit and the tape drive unit is mounted in each of the base and expansion cabinets in the M9000 server that has the expansion cabinet. In such cases, each CD-RW/DVD-RW drive unit and the tape drive unit can be connected only to a domain within the cabinet in which the drive is mounted. Settings for connection must be made for both the base cabinet and expansion cabinet.

```
XSCF> cfgdevice -l
Current connection for DVD/DAT:
  Main chassis:      port 0-0
  Expansion chassis: port 8-0
Expander status
Port No. IOU/SAS-status SAS-status
-----------------------------------
 0-0     enable  up     enable  up
 0-2     disable down   enable  up
 0-4     disable down   enable  up
 0-6     disable down   enable  up
```

```
 1-0     disable down   enable  up
 1-2     disable down   enable  up
 1-4     disable down   enable  up
 1-6     disable down   enable  up
 2-0     disable down   enable  up
 2-2     disable down   enable  up
 2-4     disable down   enable  up
 2-6     disable down   enable  up
 8-0     enable  up     enable  up
 8-2     disable down   enable  up
 8-4     disable down   enable  up
 8-6     disable down   enable  up
```

EXAMPLES

EXAMPLE 1 When the system is being powered off, reserves the connection of the CD-RW/DVD-RW drive unit and the tape drive unit to the port 0-0.

```
XSCF> cfgdevice -c attach -p 0-0
Are you sure you want to attach the device [y|n] :y
Completed.( Reservation )
```

EXAMPLE 2 When the system is being powered on, connects the CD-RW/DVD-RW drive unit and the tape drive unit to port 0-0.

```
XSCF> cfgdevice -c attach -p 0-0
Are you sure you want to attach the device [y|n] :y
Completed.
```

EXAMPLE 3 Disconnects the CD-RW/DVD-RW drive unit and the tape drive unit from the port 0-0.

```
XSCF> cfgdevice -f -c detach -p 0-0
Are you sure you want to detach the device [y|n] :y
Completed.
```

EXAMPLE 4 Displays the status of individual CD-RW/DVD-RW drive unit and the tape drive unit set on the M8000 server and the M9000 server without the expansion cabinet.

```
XSCF> cfgdevice -l
Current connection for DVD/DAT: port 0-0
Expander status
Port No. IOU/SAS-status SAS-status
-----------------------------------
 0-0     enable  up     enable  up
 0-2     disable down   enable  up
```

EXAMPLE 5 Displays the status of individual CD-RW/DVD-RW drive unit and the tape drive unit set on the M9000 server with the expansion cabinet.

```
XSCF> cfgdevice -l
Current connection for DVD/DAT: port 0-0
  Main chassis:      port 0-0
  Expansion chassis: port 8-0
Expander status
Port No. IOU/SAS-status SAS-status
-----------------------------------
 0-0     enable  up     enable  up
 0-2     disable down   enable  up
 0-4     disable down   enable  up
 0-6     disable down   enable  up
 1-0     disable down   enable  up
 1-2     disable down   enable  up
 1-4     disable down   enable  up
 1-6     disable down   enable  up
 2-0     disable down   enable  up
 2-2     disable down   enable  up
 2-4     disable down   enable  up
 2-6     disable down   enable  up
 8-0     enable  up     enable  up
 8-2     disable down   enable  up
 8-4     disable down   enable  up
 8-6     disable down   enable  up
```

EXAMPLE 6 Connects the CD-RW/DVD-RW drive unit and the tape drive unit to port 0-0 when the system is being powered on. Automatically answers "y" to all prompts.

```
XSCF> cfgdevice -y -c attach -p 0-0
Are you sure you want to attach the device [y|n] :y
Completed.
```

EXAMPLE 7 Connects the CD-RW/DVD-RW drive unit and the tape drive unit to port 0-0 when the system is being powered on. Automatically answers "y" to all prompts without displaying messages.

```
XSCF> cfgdevice -q -y -c attach -p 0-0
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

NAME

clockboard - set or display the clock control unit used at system startup

SYNOPSIS

clockboard

clockboard -s *CLKU_B-number*

clockboard -h

DESCRIPTION

The clockboard(8) command specifies the clock control unit used when the system power is turned on, or it displays the clock control unit that is currently used and the clock control unit used at the next system startup.

The clockboard(8) command is available only for the M8000/M9000 servers.

The number 0 or 1 is used to specify or display a clock control unit. When the clockboard(8) command is executed with no options, the clock control unit that is currently used and the one used at the next system startup are displayed.

Privileges

You must have fieldeng privilege to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-h	Displays usage statement. When used with other options or operands, an error occurs.
-s *CLKU_B-number*	Specifies the clock control unit to be used the next time the system power is turned on. Either 0 or 1 can be specified for *CLKU_B-number*.

EXAMPLES

EXAMPLE 1 Displays the clock control unit that is currently used and the one used at the next system startup.

```
XSCF> clockboard
current CLKU_B number    :0
next CLKU_B number    :1
```

EXAMPLE 2 Specifies the clock control unit used at the next system startup.

```
XSCF> clockboard -s 1
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

NAME

console - connect to a domain console

SYNOPSIS

console [[-q] -{y|n}] -d *domain_id* [-f |-r] [-s *escapeChar*]

console -h

DESCRIPTION

The console(8) command connects the XSCF shell console to the console of the specified domain (domain console).

Domain consoles include a writable console and read-only console. Only one writable console and multiple read-only consoles can be connected to one domain. An attempt to set up a connection to another writable console while one writable console is already connected results in an error. Even in this case, however, a user with the platadm or domainadm privilege can forcibly establish a connection to a writable console, in which case the currently connected writable console is disconnected.

To exit the domain console and return to the XSCF shell console, press the Enter key and then enter "**#**" and "**.**" (period).

Note – When you return to XSCF shell console without logging out from the domain, the return causes automatically logging out from the domain.

Privileges

You must have one of the following privileges to run this command:

platadm, platop, fieldeng

Can run this command for all domains.

domainadm, domainmgr, domainop

Can run this command only for your accessible domains.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported.

-d *domain_id*	Specifies only one ID of the domain to which to connect to a domain console. *domain_id* can be 0–23 depending on the system configuration.
-f	Forcibly connects to a writable console. The currently connected writable console is disconnected. Only users who belong to the platadm or domainadm privilege can specify this option.
-h	Displays usage statement. When used with other options or operands, an error occurs.
-n	Automatically answers "n" (no) to all prompts.

`-q`	Suppresses all messages to stdout, including prompts.
`-r`	Sets up a connection to a read-only console.
`-s` *escapeChar*	Specifies an escape character. The default is "`#`" . The character specified for *escapeChar* must be enclosed in "`"`" (double quotation). The following symbols can be specified for *escapeChar*: "`#`", "`@`", "`^`", "`&`", "`?`", "`*`", "`=`", "`.`", "`|`" Specified escape character is available only in the session that executed the `console`(8) command.
`-y`	Automatically answers "`y`" (yes) to all prompts.

EXTENDED DESCRIPTION

- When the command is executed, a prompt to confirm execution of the command with the specified options is displayed. Enter "**y**" to execute the command or "**n**" to cancel the command.
- The domain console regards "#" used at the beginning of a line as an escape character. An escape character is specified to instruct the console to perform special processing. Examples of processing that can be specified in combination with "#" are as follows.

"#" and "?"	Outputs a status message.
"#" and "." (period)	Disconnects the console.

- To enter "`#`" at the beginning of a line, enter "`#`" twice.
- To display information on the currently connected domain console, use the `showconsolepath`(8) command.

EXIT STATUS

The following exit values are returned:

`0`	Successful completion.
`>0`	An error occurred.

SEE ALSO

sendbreak`(8)`, **showconsolepath**`(8)`

NAME

deleteboard - disconnect an eXtended System Board (XSB) from the domain configuration

SYNOPSIS

deleteboard [[-q] -{y|n}] [-f] [-v] [-c disconnect] *xsb* [*xsb*...]

deleteboard [[-q] -{y|n}] [-f] [-v] -c unassign *xsb* [*xsb*...]

deleteboard [[-q] -{y|n}] [-f] [-v] -c reserve *xsb* [*xsb*...]

deleteboard -h

DESCRIPTION

The deleteboard(8) command disconnects an XSB from the domain configuration in which it has been configured.

The deleteboard(8) command is not available on the M3000 server.

One of the following disconnection methods can be specified:

disconnect	Disconnects the XSB from the domain configuration but keeps it assigned. Because the XSB thus remains assigned to the domain configuration, it can be configured again in the domain by reboot the domain or execution of the addboard(8) command.
unassign	Completely disconnects the XSB from the main configuration and puts it in the system board pool. The XSB in the system board pool can be incorporated into or assigned to other domain configurations.
reserve	Does not immediately disconnects the XSB from the domain configuration but only reserves detachment. When the domain power is shut down, the reserved XSB is disconnected from the domain configuration and put in the system board pool.

Privileges

You must have one of the following privileges to run this command:

platadm	Can run this command for all domains.
domainadm	Can run this command only for your managed domains.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported.

`-c disconnect` Detaches the XSB from the domain configuration and keeps it assigned. If the `-c` option is omitted, "`-c disconnect`" is used.

`-c reset` Reserves disconnect of an XSB. If the `-c` option is omitted, "`-c disconnect`" is used.

`-c unassign` Disconnects the XSB completely from the domain configuration and puts it in the system board pool. If the `-c` option is omitted, "`-c disconnect`" is used.

`-f` Forcibly detaches the specified XSB.

Caution - If the `-f` option is used to forcibly add a system board to a domain, all the added hardware resources may not work normally. For this reason, use of the `-f` option is not recommended in normal operation. If the `-f` option must be specified, verify the status of every added system board and device.

`-h` Displays usage statement. When used with other options or operands, an error occurs.

`-n` Automatically answers "`n`" (no) to all prompts.

`-q` Suppresses all messages to stdout, including prompts.

`-v` Displays a detailed message. If this option is specified with the `-q` option, the `-v` option is ignored.

`-y` Automatically answers "`y`" (yes) to all prompts.

OPERANDS

The following operand is supported:

xsb Specifies the XSB number to be disconnected. Multiple *xsb* operands are permitted, separated by spaces. The following xsb form is accepted:

x–y

where:

x An integer from `00`–`15`.

y An integer from `0`–`3`.

EXTENDED DESCRIPTION

- You can execute the `deleteboard`(8) command on a domain that is not running. When the domain is running, the `deleteboard`(8) command with "`-c disconnect`" or "`-c unassign`" will succeed only if the following Oracle Solaris Service Management Facility (SMF) services are active on that domain:
  - Domain SP Communication Protocol (dscp)

  - Domain Configuration Server (dcs)
  - Orcacle Sun Cryptographic Key Management Daemon (sckmd)
- When the command is executed, a prompt to confirm execution of the command with the specified options is displayed. Enter "`y`" to execute the command or "`n`" to cancel the command.
- If "`-c disconnect`" is specified when either the domain power has been turned off or the XSB is already disconnected from the domain configuration, no operation is performed. If domain power-on or power-off is in progress, the command results in an error.
- If "`-c unassign`" is specified when either the domain power has been turned off or the XSB is already disconnected from the domain configuration, the XSB is switched from the assigned state to a system board pool. If the XSB is already in a system board pool, no operation is performed.
- If "`-c reserve`" is specified when either the domain power has been turned off or the XSB is already disconnected from the domain configuration, the XSB is immediately switched from the assigned state to a system board pool. If the XSB is already in a system board pool, no operation is performed. If domain power-on or power-off is in progress, the command results in an error.
- When the XSB is disconnected, the hardware resource on the XSB is disconnected from the operating system. For this reason, command execution may take time.
- The state in which an XSB has been assigned means that configuring the XSB in the specified domain has been reserved. The reserved XSB is configured when the domain is rebooted or the `addboard`(8) command is executed. An already assigned XSB cannot be specified for configuring or assignment from other domains.
- An XSB in the system board pool means that the XSB belongs to no domain and is therefore available for configuring or assignment.

EXAMPLES

EXAMPLE 1 Puts the system board XSB#00-0, #01-0, #02-0, and #03-0 in the system board pool

```
XSCF> deleteboard -c unassign 00-0 01-0 02-0 03-0
```

EXAMPLE 2 Reserves disconnection of XSB#00-0, #01-0, #02-0, and #03-0 .

```
XSCF> deleteboard -c reserve 00-0 01-0 02-0 03-0
```

EXIT STATUS

The following exit values are returned:

`0`	Successful completion.
`>0`	An error occurred.

SEE ALSO **addboard**(8), **moveboard**(8), **replacefru**(8), **setdcl**(8), **setupfru**(8), **showboards**(8), **showdcl**(8), **showdevices**(8), **showdomainstatus**(8), **showfru**(8)

NAME

deletecodactivation - remove a Capacity on Demand (COD) hardware activation key (COD key) from the COD database

SYNOPSIS

deletecodactivation [-f] *key-signature*

deletecodactivation -h

DESCRIPTION

The deletecodactivation(8) command removes the specified COD key from the COD database on the Service Processor.

This command is not available on the M3000 server.

Note – For details on COD keys, refer to the *SPARC Enterprise M4000/M5000/M8000/M9000 Servers Capacity on Demand (COD) User's Guide*.

The system checks the number of COD hardware activation permits (COD permits) against the number of COD CPUs in use. If the permit removal will result in an insufficient number of COD permits with respect to the CPUs in use, the system does not delete the COD key from the COD database. If you still want to delete the COD key, you must reduce the number of COD CPUs in use. Power off the appropriate number of domains or disconnect the appropriate number of the eXtended System Boards (XSBs).

Privileges

You must have platadm privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-f	Forces the specified key to be deleted from the COD database.
-h	Displays usage statement. When used with other options or operands, an error occurs.

OPERANDS

The following operands are supported:

key-signature	Specifies the key to be deleted from the COD database.

EXAMPLES

EXAMPLE 1 Deleting a key

```
XSCF> deletecodactivation \
01:84000000:104:0301010100:3:00000000:xxxxxxxxxxxxxxxxxxxxxx
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO *SPARC Enterprise M4000/M5000/M8000/M9000 Servers Capacity on Demand (COD) User's Guide*

NAME

deletecodlicense - remove a Capacity on Demand (COD) right-to-use (RTU) license key from the COD license database

SYNOPSIS

deletecodlicense [-f] *license-signature*

deletecodlicense -h

DESCRIPTION

The deletecodlicense(8) command removes the specified COD RTU license key from the COD license database on the Service Processor.

The deletecodlicense(8) command is not available on the M3000 server.

For further information about COD RTU license keys, refer to the *SPARC Enterprise M4000/M5000/M8000/M9000 Servers Capacity on Demand (COD) User's Guide*.

The system checks the number of COD RTU licenses against the number of COD CPUs in use. If the license removal will result in an insufficient number of COD RTU licenses with respect to the CPU in use, the system does not delete the license key from the COD RTU license database. If you still want to delete the COD RTU license key, you must reduce the number of COD CPUs in use. Power off the appropriate number of domains or disconnect the appropriate number of the eXtended System Boards (XSBs).

Privileges

You must have platadm privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-f Forces the specified COD RTU license key to be deleted from the COD license database.

-h Displays usage statement.

When used with other options or operands, an error occurs.

OPERANDS

The following operand is supported:

license-signature Specifies the COD RTU license key to be deleted from the COD license database.

EXAMPLES

EXAMPLE 1 Deleting a COD RTU license key

```
XSCF> deletecodlicense \
01:84000000:104:0301010100:3:00000000:xxxxxxxxxxxxxxxxxxxxxx
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

SPARC Enterprise M4000/M5000/M8000/M9000 Servers Capacity on Demand (COD) User's Guide

NAME

deletefru - delete a Field Replaceable Unit (FRU)

SYNOPSIS

deletefru

deletefru -h

DESCRIPTION

The deletefru(8) command deletes an FRU.

The deletefru(8) command is available only for the M8000/M9000 servers.

The deletefru(8) command allows the user to make the settings that are required for FRU deletion and related to selecting, confirming, and removing FRUs interactively using menus.

The following FRUs can be deleted:

- CPU/Memory Board unit (CMU)
- I/O unit (IOU)

Privileges

You must have fieldeng privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following option is supported:

-h	Displays usage statement.

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

addfru(8), **deleteboard**(8), **replacefru**(8), **setupfru**(8), **showdomainstatus**(8), **showfru**(8), **showhardconf**(8), **unlockmaintenance**(8)

NAME

deleteuser - delete an XSCF user account

SYNOPSIS

deleteuser *user*

deleteuser -h

DESCRIPTION

deleteuser(8) deletes a local XSCF user account. All local account data associated with the user account is deleted including password and Secure Shell (SSH) keys.

The local user's currently running XSCF shell and browser sessions are terminated at once. The user's account is removed from the system and they cannot log back in. You cannot delete your own account.

Privileges

You must have useradm privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following option is supported:

-h Displays usage statement.

When used with other options or operands, an error occurs.

OPERANDS

The following operands are supported:

user Specifies a valid user name. The name of the user account to be deleted.

EXAMPLES

EXAMPLE 1 Deleting a User

```
XSCF> deleteuser jsmith
```

EXIT STATUS

The following exit values are returned:

0 Successful completion.

>0 An error occurred.

SEE ALSO

adduser(8), **disableuser**(8), **enableuser**(8)

NAME

disableuser - disable an XSCF user account

SYNOPSIS

disableuser *user*

disableuser -h

DESCRIPTION

disableuser(8) disables a local XSCF user account for subsequent logins. Current sessions are not affected.

When an account is disabled, it cannot be used for login. This applies to console (serial) and telnet connections, as well as the Secure Shell (SSH). XSCF Web login is also disabled. All local XSCF account data associated with the user remains on the system. This includes password and SSH keys. You can reenable a disabled account using enableuser(8).

Privileges

You must have useradm privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following option is supported:

-h Displays usage statement.

When used with other options or operands, an error occurs.

OPERANDS

The following operands are supported:

user Specifies a valid user name of the user account to be disabled.

EXAMPLES

EXAMPLE 1 Disabling a User Account

```
XSCF> disableuser jsmith
```

EXIT STATUS

The following exit values are returned:

0 Successful completion.

>0 An error occurred.

SEE ALSO

adduser(8), **deleteuser**(8), **enableuser**(8), **showuser**(8)

NAME

dumpconfig - save system configuration information to a file

SYNOPSIS

dumpconfig [-v] [-V] [[-q] -{y|n}] [-e [-P *password*]] [-c *comment*] [-u *user*] [-p *proxy* [-t *proxty_type*]] *url*

dumpconfig -h

DESCRIPTION

The dumpconfig(8) command saves system configuration information, copying it from the XSCF to a file specified by the user. The information can later be downloaded from that file back to the XSCF using restoreconfig(8).

Privileges

You must have platadm, platop, or fieldeng privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-c *comment*

Accepts a user-provided comment in the file to distinguish between different backup copies. The comment is not read by the software. This comment must be 132 chars or less in length.

Special characters are not allowed in the comment. Allowed characters are [0-9 a-z A-Z] and " ". A space is also valid but if spaces are used the entire comment must be enclosed in double quotes.

Some examples:

```
-c "This is a valid comment"
```

```
-c This is an invalid comment
```

The above example is invalid because spaces are included without quotations.

```
-c "This! is @invalid"
```

The above example is invalid because it includes special characters, which are not allowed.

-e

Encrypt the file. "-P password" option can be used to specify the password. If a password is not specified the key will be prompted. Once encrypted the configuration file cannot be decrypted without the key. If the key is lost, there is no possibility of recovering the configuration data.

-h

Displays usage statement. When used with other options or operands, an error occurs.

-n

Automatically answers "n" (no) to all prompts.

-P *password*	With -e option, password can be provided on command line. The command will prompt for the password if a password is not provided on command line.
-p *proxy*	Specifies the proxy server to be used for transfers. The default transfer type is http, unless modified using the -t *proxy_type* option. The value for proxy must be in the format *servername*:*port*.
-q	Suppresses all messages to stdout, including prompts.
-t *proxy_type*	Used with the -p option to specify the type of proxy. Possible values for *proxy_type* are: http, socks4, and socks5. The default value is http.
-u *user*	Specifies the user name when logging in to a remote ftp or http server that requires authentication. You will be prompted for a password.
-v	Displays verbose output. This may be helpful when diagnosing server problems.
-V	Displays details of network activity. This may be helpful when diagnosing network or server problems.
-y	Automatically answers "y" (yes) to all prompts.

OPERANDS

The following operands are supported:

url Specifies the URL where the configuration will be dumped. Supported formats for this value include the following:

http://*server*[:*port*]/*path*/*file*

https://*server*[:*port*]/*path*/*file*

ftp://*server*[:*port*]/*path*/*file*

file:///media/usb_msd/*path*/*file*

EXAMPLES

EXAMPLE 1 Dumping the Configuration using FTP

```
XSCF> dumpconfig -V -p 129.145.155.156:8080 -u minilla \
ftp:/10.7.79.18/sollgell/proxytest-ftp.cfg
transfer from '/tmp/dumpconfig.EvY1Yf' to 'ftp://10.7.79.18/sollgell/
proxytest-ftp.cfg'
Password:
* About to connect() to 129.145.155.166 port 8080
*   Trying 129.145.155.166... * connected
* Connected to 129.145.155.166 (129.145.155.166) port 8080
* Proxy auth using (nil) with user ''
```

```
* Server auth using Basic with user 'minilla'
> PUT ftp://10.7.79.18/iktest/proxytest-ftp.cfg HTTP/1.1
Authorization: Basic bHdhbmc6bHdhbmc=
User-Agent: dumpconfig
Host: 10.7.79.18:21
Pragma: no-cache
Accept: */*
Content-Length: 24720
Expect: 100-continue
< HTTP/1.1 100 Continue
< HTTP/1.1 200 OK
< Server: Sun-Java-System-Web-Proxy-Server/4.0
< Date: Mon, 04 Aug 2008 16:46:11 GMT
< Transfer-encoding: chunked
* Connection #0 to host 129.145.155.166 left intact
* Closing connection #0
operation completed
XSCF>
```

EXAMPLE 2 Dumping the Configuration Using http

```
XSCF> dumpconfig -v -p 129.145.155.166:8080 \
http://10.7.79.18/sollgell/proxytest.cfg
reading database ... ..............*done
creating temporary file ... done
starting file transfer ...done
removing temporary file ... done
operation completed
XSCF>
```

EXAMPLE 3 Dumping the Configuration Using Https

```
XSCF> dumpconfig -V -p 129.145.155.166:8080 \
http://10.7.79.18/sollgell/proxytest-https.cfg
transfer from '/tmp/dumpconfig.ZMCI3d' to 'http://10.7.79.18/iktest/
proxytest-https.cfg'
* About to connect() to 129.145.155.166 port 8080
*   Trying 129.145.155.166... * connected
* Connected to 129.145.155.166 (129.145.155.166) port 8080
> > PUT http://10.7.79.18/iktest/proxytest-https.cfg HTTP/1.1
User-Agent: dumpconfig
Host: 10.7.79.18
Pragma: no-cache
Accept: */*
Content-Length: 24720
Expect: 100-continue
```

```
< HTTP/1.1 100 Continue
< HTTP/1.1 204 No Content
< Content-type: text/html
< Date: Mon, 04 Aug 2008 16:42:46 GMT
< Server: Apache/1.3.36 (Unix) mod_perl/1.29 mod_ssl/2.8.27 OpenSSL/
0.9.7d
< Via: 1.1 proxy-proxy
< Proxy-agent: Sun-Java-System-Web-Proxy-Server/4.0
* Connection #0 to host 129.145.155.166 left intact
* Closing connection #0
operation completed
XSCF>
```

EXAMPLE 4 Dumping the Configuration Using USB

```
XSCF> dumpconfig -v -V file:///media/usb_msd/proxytest.cfg
Making sure mount point is clear
Trying to mount USB device /dev/sda1 as /media/usb_msd
Mounted USB device
file '/media/usb_msd/proxytest.cfg' already exists
Do you want to overwrite this file? [y|n]: y
removing file 'file:///media/usb_msd/proxytest.cfg' ... done
reading database ... ..............*done
creating temporary file ... done
starting file transfer ...transfer from '/tmp/dumpconfig.HE1RZa' to
'file:///media/usb_msd/san-ff1-54.cfg'
done
removing temporary file ... done
operation completed
Unmounted USB device
XSCF>
```

EXAMPLE 5 Encrypting and Password Protecting the Configuration

```
XSCF> dumpconfig -v -e -P kamacuras -p 129.145.155.166:8080 \
http://10.7.79.18/sollgell/proxytest.cfg
reading database ... ..............*done
creating temporary file ... done
starting file transfer ...done
removing temporary file ... done
operation completed
XSCF>
```

EXIT STATUS

The following exit values are returned:

`0`	Successful completion.
`>0`	An error occurred.

SEE ALSO

restoreconfig`(8)`

NAME

enableuser - enable an XSCF user account

SYNOPSIS

enableuser *user*

enableuser -h

DESCRIPTION

enableuser(8) enables a local XSCF user account. An enabled account can be used for login at the console, using Secure Shell (SSH). Using this command, you can reenable accounts disabled by disableuser.

Privileges

You must have useradm privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following option is supported.

-h Displays usage statement.

When used with other options or operands, an error occurs.

OPERANDS

The following operands are supported:

user Specifies the valid user name of the account to be enabled.

EXAMPLES

EXAMPLE 1 Enable a User Account

```
XSCF> enableuser jsmith
```

EXIT STATUS

The following exit values are returned:

0 Successful completion.

>0 An error occurred.

SEE ALSO

adduser(8), **deleteuser**(8), **disableuser**(8), **showuser**(8)

NAME

flashupdate - update the firmware

SYNOPSIS

flashupdate -c check -m xcp -s *version*

flashupdate [[-q] -{y|n}] -c update -m xcp -s *version*

flashupdate -c sync

flashupdate -h

DESCRIPTION

The flashupdate(8) command updates the firmware.

The entire firmware shown below is updated. Whether update can be performed can be checked beforehand.

- Update of the entire firmware (XSCF, OpenBoot PROM including Power-On Self-Test (POST)) (xcp)

Privileges

You must have platadm or fieldeng privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:.

-c check	Checks whether the specified firmware can be updated.
-c update	Updates the specified firmware. In the M8000/M9000 servers, updates the firmware of both XSCF units.
-c sync	Synchronizes the firmware versions of the XSCF units in the M8000/M9000 servers. This option is used when replacing an XSCF unit.
-h	Displays usage statement. When used with other options or operands, an error occurs.
-m xcp	Specifies the entire firmware as a target.
-n	Automatically answers "n" (no) to all prompts.

`-q`	Suppresses all messages to stdout, including prompts.
`-s` *version*	Specifies an XCP comprehensive firmware version. For *version*, specify a major version, minor version and micro version continuously. The XCP version number appears as xyyz by four digits, where: *x* — Major firmware release number *yy* — Minor release number z — Micro release number
`-y`	Automatically answers "`y`" (yes) to all prompts.

EXTENDED DESCRIPTION

- When the command is executed, a prompt to confirm execution of the command with the specified options is displayed. Enter "**y**" to execute the command or "**n**" to cancel the command.
- When the firmware is updated, the XSCF unit is reset. Therefore, LAN connection to the XSCF is canceled if already established.
- When there's a faulty Field Replaceable Unit (FRU), can't update the firmware. Resolve the FRU fault then update.

EXAMPLES

EXAMPLE 1 Check whether the entire firmware can be updated to version 1082.

```
XSCF> flashupdate -c check -m xcp -s 1082
```

EXAMPLE 2 Updates the entire firmware to version from 1080 to 1082.

```
XSCF> flashupdate -c update -m xcp -s 1082
The XSCF will be reset. Continue? [y|n] :y
XCP update is started (XCP version=1082:last version=1080)
OpenBoot PROM update is started (OpenBoot PROM version=02090000)
OpenBoot PROM update has been completed (OpenBoot PROM version=02090000)
XSCF update is started (XSCFU=0,bank=1,XCP version=1082:last
version=1080)
XSCF download is started (XSCFU=0,bank=1,XCP version=1082:last
version=1080, Firmware Element ID=00:version=01080001:last
version=01080000)
XSCF download has been completed (XSCFU=0,bank=1,XCP version=1082:last
version=1080, Firmware Element ID=00:version=01080001:last
version=01080000)
     :
     :
XSCF download is started (XSCFU=0,bank=1,XCP version=1082:last
version=1080, Firmware Element ID=07:version=01080004:last
version=01080000)
```

```
XSCF download has been completed (XSCFU=0,bank=1,XCP version=1082:last
version=1080, Firmware Element ID=07:version=01080004:last
version=01080000)
XSCF update has been completed (XSCFU=0,bank=1,XCP version=1082:last
version=1080)
XCP update is started (XCP version=1082:last version=1080)
OpenBoot PROM update is started (OpenBoot PROM version=02090000)
OpenBoot PROM update has been completed (OpenBoot PROM version=02090000)
XSCF update is started (XSCFU=0,bank=0,XCP version=1082:last
version=1080)
XSCF download is started (XSCFU=0,bank=0,XCP version=1082:last
version=1080, Firmware Element ID=00:version=01080001:last
version=01080000)
XSCF download has been completed (XSCFU=0,bank=0,XCP version=1082:last
version=1080, Firmware Element ID=00:version=01080001:last
version=01080000)
     :
     :
XSCF download is started (XSCFU=0,bank=0,XCP version=1082:last
version=1080, Firmware Element ID=07:version=01080004:last
version=01080000)
XSCF download has been completed (XSCFU=0,bank=0,XCP version=1082:last
version=1080, Firmware Element ID=07:version=01080004:last
version=01080000)
XSCF update has been completed (XSCFU=0,bank=0,XCP version=1082:last
version=1080)
XSCF is rebooting to update the reserve bank
```

EXAMPLE 3 Synchronizes the firmware version of the replaced XSCF units in the M8000/M9000 servers.

```
XSCF> flashupdate -c sync
```

EXIT STATUS

The following exit values are returned:

0	Successful completion
>0	An error occurred.

SEE ALSO

version(8)

NAME

fmadm - fault management configuration tool

SYNOPSIS

fmadm [-q] config

fmadm -h

DESCRIPTION

fmadm (8) can be used to view system configuration parameters related to fault management.

fmadm can be used to:

- View the set of diagnosis engines and agents that are currently participating in fault management
- View the list of system components that have been diagnosed as faulty

The Fault Manager attempts to automate as many activities as possible, so use of fmadm is typically not required. When the Fault Manager needs help from a human administrator or service representative, it produces a message indicating its needs. It also refers you to a URL containing the relevant knowledge article. The web site might ask you to use fmadm or one of the other fault management utilities to gather more information or perform additional tasks. The documentation for fmdump(8) describes more about tools to observe fault management activities.

Privileges

You must have platop, platadm, or fieldeng privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported.

-h Displays usage statement.

When used with other options or operands, an error occurs.

-q Sets quiet mode. fmadm does not produce messages indicating the result of successful operations to standard output.

OPERANDS

The following operands are supported:

config Displays the configuration of the Fault Manager itself, including the module name, version, and description of each component module. Fault Manager modules provide services such as automated diagnosis, self-healing, and messaging for hardware and software present on the system.

EXAMPLES

EXAMPLE 1 Displaying the Fault Manager Configuration

```
XSCF> fmadm config
MODULE          VERSION STATUS  DESCRIPTION
case-close         1.0  active  Case-Close Agent
fmd-self-diagnosis 1.0  active  Fault Manager Self-Diagnosis
sysevent-transport 1.0  active  SysEvent Transport Agent
syslog-msgs        1.0  active  Syslog Messaging Agent
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

fmdump(8), **fmstat**(8)

NAME

fmdump - view fault management logs

SYNOPSIS

fmdump

fmdump [-e] [-f] [-M] [-v] [-V] [-c *class*] [-t *time*] [-T *time*] [-u *uuid*]

fmdump -m [-M] [-t *time*] [-T *time*]

fmdump -h

DESCRIPTION

The fmdump utility displays the contents of any of the logs associated with the Fault Manager (fault manager daemon). The Fault Manager runs in the background on each server. It records, in the error log, faults detected by the XSCF, and initiates proactive self-healing activities, such as disabling faulty components.

The Fault Manager maintains two sets of logs for use by system administrators and service personnel:

Error log	Records error telemetry, the symptoms of problems detected by the system
Fault log	Records fault diagnosis information; the problems believed to explain these symptoms. By default, fmdump displays the contents of the fault log, which records the result of each diagnosis made by the fault manager or one of its component modules.

Each problem recorded in the fault log is identified by:

- The time of its diagnosis
- A Universal Unique Identifier (UUID) that can be used to uniquely identify this particular problem across any set of systems
- A message identifier (MSG-ID) that can be used to access a corresponding knowledge article located at the specified website.

If a problem requires action by a system administrator or service personnel or affects system behavior, the Fault Manager also issues a human-readable message.

This message provides a summary of the problem and a reference to the knowledge article on the specified website.

You can use the -v and -V options to expand the display from a single-line summary to increased levels of detail for each event recorded in the log. You can also use the -M option to display only one screen at a time. The -c, -t, -T, and -u options can be used to filter the output by selecting only those events that match the specified *class*, range of times, or *uuid*. If more than one filter option is present on the command line, the options combine to display only those events that are selected by the logical AND of the options. If more than one instance of the same

filter option is present on the command-line, the like options combine to display any events selected by the logical OR of the options.

You can use the `-m` option to display the Fault Manager `syslog` contents.

Privileges

You must have `platop`, `platadm`, or `fieldeng` privileges to run this command.

Refer to `setprivileges`(8) for more information.

OPTIONS

The following options are supported.

`-c` *class*	Selects events that match the specified class. The class argument can use the global pattern matching syntax, which is similar to global pattern matching for files. For example `xyz.*` would match `xyz.sxc` and `xyz.pdf`. The class represents a hierarchical classification string indicating the type of telemetry event.
`-e`	Displays events from the fault management error log instead of the fault log. The error log contains private telemetry information used by XSCF's automated diagnosis software. This information is recorded to facilitate post-mortem analysis of problems and event replay, and should not be parsed or relied upon for the development of scripts and other tools.
`-f`	Displays only lines that have been appended to the dump file since the command was executed. Output continues until interrupted by `Ctrl-C`.
`-h`	Displays usage statement. When used with other options or operands, an error occurs.
`-m`	Displays the Fault Manager syslog message contents.
`-M`	Displays text by page. This option provides a function that is the same as that of the `more` command.
`-t` *time*	Selects events that occurred at or after the specified time. The time can be specified using the forms in the Time Formats following this section. Used with `-T` you can specify a range.
`-T` *time*	Selects events that occurred at or before the specified time. *time* can be specified using any of the time formats described for the `-t` option. Used with `-t` you can specify a range.

`-u` *uuid* Selects fault diagnosis events that exactly match the specified *uuid*. Each diagnosis is associated with a UUID for identification purposes. The `-u` option can be combined with other options such as `-v` to show all of the details associated with a particular diagnosis.

If the `-e` option and `-u` option are specified at the same time, `fmdump` displays the relevant error events.

`-v` Displays verbose event detail. The event display is enlarged to show additional common members of the selected events.

`-V` Displays very verbose event detail. The event display is enlarged to show every member of the name-value pair list associated with each event. In addition, for fault logs, the event display includes a list of cross-references to the corresponding errors that were associated with the diagnosis.

The following are the Time Formats:

Time Format	Description
mm/dd/yy hh:mm:ss	Month, day, year, hour in 24-hour format, minute, and second. Any amount of whitespace can separate the date and time. The argument should be quoted so that the shell interprets the two strings as a single argument.
mm/dd/yy hh:mm	Month, day, year, hour in 24-hour format, and minute. Any amount of whitespace can separate the date and time. The argument should be quoted so that the shell interprets the two strings as a single argument.
mm/dd/yy	12:00:00AM on the specified month, day, and year
ddMonyy hh:mm:ss	Day, month name, year, hour in 24-hour format, minute, and second. Any amount of whitespace can separate the date and time. The argument should be quoted so that the shell interprets the two strings as a single argument.
Mon dd hh:mm:ss	Month, day, hour in 24-hour format, minute, and second of the current year. Any amount of whitespace can separate the date and time. The argument should be quoted so that the shell interprets the two strings as a single argument.

Time Format	Description
yyyy-mm-dd[*T hh*:*mm*[:*ss*]]	Year, month, day, and optional hour in 24-hour format, minute, and second, where T is an integer value specified in base 10. The second, or hour, minute, and second, can be optionally omitted.
ddMonyy	12:00:00AM on the specified day, month name, and year.
hh:*mm*:*ss*	Hour in 24-hour format, minute, and second of the current day.
hh:*mm*	Hour in 24-hour format and minute of the current day.
Tns | *Tnsec*	T nanoseconds ago where T is an integer value specified in base 10.
Tus | *Tusec*	T microseconds ago where T is an integer value specified in base 10
Tms | *Tmsec*	T milliseconds ago where T is an integer value specified in base 10.
Ts | *Tsec*	T seconds ago where T is an integer value specified in base 10.
Tm | *Tmin*	T minutes ago where T is an integer value specified in base 10.
Th | *Thour*	T hours ago where T is an integer value specified in base 10.
Td | *Tday*	T days ago where T is an integer value specified in base 10.

You can append a decimal fraction of the form `.n` to any `-t` option argument to indicate a fractional number of seconds beyond the specified time.

EXAMPLES

EXAMPLE 1 Default `fmdump` Display

```
XSCF> fmdump
TIME                 UUID                                 MSG-ID
Aug 12 16:12:13.2811 7868c1cc-23d4-c575-8659-85cdbe61842e FMD-8000-77
Aug 12 16:12:13.2985 7868c1cc-23d4-c575-8659-85cdbe61842e FMD-8000-77
Sep 01 16:06:57.5839 3ceca439-b0b2-4db1-9123-c8ace3f2b371 FMD-8000-77
Sep 01 16:06:57.6278 3ceca439-b0b2-4db1-9123-c8ace3f2b371 FMD-8000-77
Sep 06 09:37:05.0983 6485b42b-6638-4c5d-b652-bec485290788 LINUX-8000-1N
Sep 06 09:38:10.8584 77435994-5b99-4db8-bdcd-985c7d3ae3e4 LINUX-8000-1N
Sep 06 09:57:44.6502 0087d58c-e5b9-415d-91bc-adf7c41dd316 LINUX-8000-1N
```

```
Sep 06 12:40:59.2801 97de2cef-8ea1-407a-8a53-c7a67e61987a LINUX-8000-1N
Sep 06 12:41:10.1076 fa7304f9-c9e8-4cd1-9ca5-e35f57d53b2c LINUX-8000-1N
Sep 06 13:01:49.1462 ce550611-4308-4336-8a9a-19676f828515 LINUX-8000-1N
Sep 06 15:42:56.6132 0f4b429f-c048-47cd-9d9f-a2f7b6d4c957 LINUX-8000-1N
Sep 06 16:07:14.4652 7d5fb282-e01b-476a-b7e1-1a0f8de80758 LINUX-8000-1N
Sep 06 16:08:16.3755 41379237-9750-4fd6-bce3-b5131d864d34 LINUX-8000-1N
Sep 29 14:49:27.8452 0455ceaa-e226-424a-9b34-27603ca603f1 FMD-8000-58
Sep 29 15:02:00.3039 fb550ebc-80e9-41c8-8afc-ac680b9eb613 FMD-8000-58
Sep 29 15:09:25.4335 8cec9a83-e2a3-4dc3-a7cd-de01caef5c63 FMD-8000-4M
Sep 29 15:10:09.6151 5f88d7d5-a107-4435-99c9-7c59479d22ed FMD-8000-58
```

EXAMPLE 2 Display in Verbose Mode

```
XSCF> fmdump -v
TIME                 UUID                                 MSG-ID
Nov 30 20:44:55.1283 9f773e33-e46f-466c-be86-fd3fcc449935 FMD-8000-0W
 100%  defect.sunos.fmd.nosub
:
```

EXAMPLE 3 Display Very Verbose Event Detail for the Last UUID

```
XSCF> fmdump -e -V -u 5f88d7d5-a107-4435-99c9-7c59479d22ed
TIME                           CLASS
Sep 29 2005 15:10:09.565220864 ereport.io.iox.cp.seeprom0.nresp
nvlist version: 0
        detector = (embedded nvlist)
        nvlist version: 0
                scheme = hc
                version = 0
                hc-root = /
                hc-list_sz = 0x1
                hc-list = (array of embedded nvlists)
                (start hc-list[0])
                nvlist version: 0
                        scheme = hc
                        hc-name = iox
                        hc-id = 0
                (end hc-list[0])
        (end detector)
        IOXserial_no = 123456
        class = ereport.io.iox.cp.seeprom0.nresp
        ena = 0x921b650000000001
```

EXAMPLE 4 Displaying the Full Fault Report for the Specified UUID

```
XSCF> fmdump  -V -u 5f88d7d5-a107-4435-99c9-7c59479d22ed
TIME                 UUID                                 MSG-ID
Sep 29 15:10:09.6151 5f88d7d5-a107-4435-99c9-7c59479d22ed FMD-8000-58
  TIME                 CLASS                                 ENA
  Sep 29 15:10:09.5652 ereport.io.iox.cp.seeprom0.nresp
0x921b650000000001
nvlist version: 0
        version = 0x0
        class = list.suspect
        uuid = 5f88d7d5-a107-4435-99c9-7c59479d22ed
        code = FMD-8000-58
        diag-time = 1128021009 615016
        de = (embedded nvlist)
        nvlist version: 0
                version = 0x0
                scheme = fmd
                authority = (embedded nvlist)
                nvlist version: 0
                        version = 0x0
                        product-id = SUNW,SPARC-Enterprise
                        chassis-id = BF0000001V
                        server-id = localhost
                (end authority)
                mod-name = sde
                mod-version = 1.13
        (end de)
        fault-list-sz = 0x1
        fault-list = (array of embedded nvlists)
        (start fault-list[0])
        nvlist version: 0
                version = 0x0
                class = fault.io.iox.cp.seeprom
                certainty = 0x64
                fru = (embedded nvlist)
                nvlist version: 0
                        scheme = hc
                        version = 0x0
                        hc-root =
                        hc-list-sz = 0x1
                        hc-list = (array of embedded nvlists)
                        (start hc-list[0])
                        nvlist version: 0
                                hc-name = iox
                                hc-id = 0
```

```
                        (end hc-list[0])
                 (end fru)
        (end fault-list[0])
```

EXAMPLE 5 Displaying Contents of the Fault Manager syslog Message

```
XSCF> fmdump  -m -M
MSG-ID: FMD-8000-11, TYPE: Defect, VER: 1, SEVERITY: Minor
EVENT-TIME: Tue Nov  7 07:01:44 PST 2006
PLATFORM: SUNW,SPARC-Enterprise, CSN: 7860000764, HOSTNAME: san-ff2-20-0
SOURCE: sde, REV: 1.5
EVENT-ID: 2daddee0-2f42-47ee-b5b2-57ae6a41bfc0
DESC: A Solaris Fault Manager component generated a diagnosis for which
no message summary exists. Refer to http://www.sun.com/msg/FMD-8000-11
for more information.
AUTO-RESPONSE: The diagnosis has been saved in the fault log for
examination by Sun.
IMPACT: The fault log will need to be manually examined using fmdump(1M)
in order to determine if any human response is required.

MSG-ID: FMD-8000-11, TYPE: Defect, VER: 1, SEVERITY: Minor
EVENT-TIME: Tue Nov  7 07:03:25 PST 2006
PLATFORM: SUNW,SPARC-Enterprise, CSN: 7860000764, HOSTNAME: san-ff2-20-0
SOURCE: sde, REV: 1.5
EVENT-ID: 2b03ab60-96db-439d-a13a-2f420a1b73c7
DESC: A Solaris Fault Manager component generated a diagnosis for which
no message summary exists. Refer to http://www.sun.com/msg/FMD-8000-11
for more information.
AUTO-RESPONSE: The diagnosis has been saved in the fault log for
examination by Sun.
IMPACT: The fault log will need to be manually examined using fmdump(1M)
in order to determine if any human response is required.
```

EXIT STATUS

The following exit values are returned:

0	Successful completion. All records in the log file were examined successfully.
>0	An error occurred.

SEE ALSO

fmadm(8), **fmstat**(8)

NAME

fmstat - report fault management module statistics

SYNOPSIS

fmstat [-a] [-s] [-z] [-m *module*] [*interval*] [*count*]

fmstat -h

DESCRIPTION

The fmstat utility can be used by system administrators and service personnel to report statistics associated with the Fault Manager (fault manager daemon), and its associated set of modules. The Fault Manager runs in the background on each system. It receives telemetry information relating to problems detected by the system software, diagnoses these problems, and initiates proactive self-healing activities such as disabling faulty components.

You can use fmstat to view statistics for diagnosis engines and agents that are currently participating in fault management. The fmadm(8), and fmdump(8) man pages describe more about tools to observe fault management activities.

If the -m option is present, fmstat reports any statistics kept by the specified fault management module. The module list can be obtained using fmadm config.

If the -m option is not present, fmstat reports the following statistics for each of its client modules:

module	The name of the fault management module as reported by fmadm config.
ev_recv	The number of telemetry events received by the module.
ev_acpt	The number of events accepted by the module as relevant to a diagnosis.
wait	The average number of telemetry events waiting to be examined by the module.
svc_t	The average service time for telemetry events received by the module, in milliseconds.
%w	The percentage of time that there were telemetry events waiting to be examined by the module.
%b	The percentage of time that the module was busy processing telemetry events.
open	The number of active cases (open problem investigations) owned by the module.

`solve`	The total number of cases solved by this module since it was loaded.
`memsz`	The amount of dynamic memory currently allocated by this module.
`bufsz`	The amount of persistent buffer space currently allocated by this module.

Privileges

You must have `platadm`, `platop`, or `fieldeng` privileges to run this command.

Refer to `setprivileges`(8) for more information.

OPTIONS

The following options are supported.

`-a` Prints the default global statistics for the Fault Manager or a module. If used without the `m module` option, the default global Fault Manager statistics are displayed. If used with the `m module` option, the global statistics for a module are displayed.

`-h` Displays usage statement.

When used with other options or operands, an error occurs.

`-m` *module* Prints a report on the statistics associated with the specified fault management module, instead of the default statistics report.

Modules can publish an arbitrary set of statistics to help service the fault management software itself.

If used without the `-a` option, displays only those statistics kept by the module. If used with the `-a` option, displays statistics kept by the module and the global statistics associated with the module.

`-s` Prints a report on Soft Error Rate Discrimination (SERD) engines associated with the module instead of the default module statistics report. A SERD engine is a construct used by fault management software to determine if a statistical threshold measured as *N* events in some time *T* has been exceeded. The `-s` option can only be used in combination with the `-m` option.

`-z` Omits statistics with a zero value from the report associated with the specified fault management module. The `-z` option can only be used in combination with the `-m` option.

OPERANDS

The following operands are supported:

count Print only *count* reports, and then exit.

interval Print a new report every *interval* seconds.

If neither *count* nor *interval* is specified, a single report is printed and `fmstat` exits.

If an *interval* is specified but no *count* is specified, `fmstat` prints reports every *interval* seconds indefinitely until the command is interrupted by Ctrl-C.

EXAMPLES

EXAMPLE 1 Displaying FM Statistics for the Syslog Module

```
XSCF> fmstat -a -m syslog-msgs
 NAME VALUE            DESCRIPTION
 bad_code 0            event code has no dictionary name
 bad_fmri 0            event fmri is missing or invalid
 bad_time 0            event time is not properly encoded
 bad_vers 0            event version is missing or invalid
 fmd.accepted 0        total events accepted by module
 fmd.buflimit 10M      limit on total buffer space
 fmd.buftotal 0        total buffer space used by module
 fmd.caseclosed 0      total cases closed by module
 fmd.caseopen 0        cases currently open by module
 fmd.casesolved 0      total cases solved by module
 fmd.ckptcnt 0         number of checkpoints taken
 fmd.ckptrestore true  restore checkpoints for module
 fmd.ckptsave true     save checkpoints for module
 fmd.ckpttime 0d       total checkpoint time
 fmd.ckptzero false    zeroed checkpoint at startup
 fmd.debugdrop 4       dropped debug messages
 fmd.dequeued 1        total events dequeued by module
 fmd.dispatched 1      total events dispatched to module
 fmd.dlastupdate 1144424838299131us hrtime of last event dequeue
completion
 fmd.dropped 0         total events dropped on queue overflow
 fmd.dtime 0d          total processing time after dequeue
 fmd.loadtime 1144424251692484us hrtime at which module was loaded
 fmd.memlimit 10M      limit on total memory allocated
 fmd.memtotal 97b      total memory allocated by module
 fmd.prdequeued 0      protocol events dequeued by module
 fmd.snaptime 1144424838299148us hrtime of last statistics snapshot
 fmd.thrlimit 8        limit on number of auxiliary threads
 fmd.thrtotal 0        total number of auxiliary threads
 fmd.wcnt 0            count of events waiting on queue
 fmd.wlastupdate 1144424838299131us hrtime of last wait queue update
```

```
 fmd.wlentime 30us     total wait length * time product
 fmd.wtime 30us        total wait time on queue
 fmd.xprtlimit 256     limit on number of open transports
 fmd.xprtopen 0        total number of open transports
 fmd.xprtqlimit 256    limit on transport event queue length
 log_err 0             failed to log message to log(7D)
 msg_err 0             failed to log message to sysmsg(7D)
 no_msg 0              message logging suppressed
```

```
XSCF> fmstat
module            ev_recv ev_acpt wait  svc_t  %w  %b  open solve  memsz
bufsz
case-close              0      0  0.0   0.0   0   0    0    0     0     0
fmd-self-diagnosis      1      1  0.0   0.2   0   0    1    0   27b     0
sysevent-transport      0      0  0.0 573.2   0   0    0    0     0     0
syslog-msgs             0      0  0.0   0.0   0   0    0    0   97b     0
```

EXAMPLE 2 Displaying FM Statistics for fmd Self-Diagnosis Module

```
XSCF> fmstat -z -m fmd-self-diagnosis
      NAME VALUE            DESCRIPTION
      module 1              error events received from fmd modules
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

fmadm(8), **fmdump**(8)

NAME

getflashimage - download a firmware image file

SYNOPSIS

getflashimage [-v] [[-q] -{y|n}] [-u *user*] [-p *proxy* [-t *proxy_type*]] *url*

getflashimage -l

getflashimage [[-q] -{y|n}] [-d]

getflashimage -h

DESCRIPTION

The getflashimage(8) command downloads a firmware image file for use by the flashupdate(8) command.

If any previous image files of the firmware are present on the XSCF unit, they are deleted prior to downloading the new version. After successful download, the image file is checked for integrity, and the MD5 checksum is displayed.

Privileges

You must have platadm or fieldeng privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-d	Deletes all previous firmware image files still on the XSCF unit, then exits.
-h	Displays usage statement. When used with other options or operands, an error occurs.
-l	Lists firmware image files that are still on the XSCF unit, then exits.
-n	Automatically answers "n" (no) to all prompts.
-p *proxy*	Specifies the proxy server to be used for transfers. The default transfer type is http, unless modified using the -t *proxy_type* option. The value for proxy must be in the format *servername*:*port*. (Refer to Example 3.)
-q	Suppresses all messages to stdout, including prompts.
-t *proxy_type*	Used with the -p option to specify the type of proxy. Possible values for *proxy_type* are: http, socks4, and socks5. The default value is http.

`-u` *user*	Specifies the user name when logging in to a remote ftp or http server that requires authentication. You will be prompted for a password.
`-v`	Displays verbose output. This may be helpful when diagnosing network or server problems.
`-y`	Automatically answers `"y"` (`yes`) to all prompts.

OPERANDS

The following operands are supported:

url Specifies the URL of the firmware image to download. Supported formats for this value include the following:

`http://`*server*`[:`*port*`]/`*path*`/`*file*

`https://`*server*`[:`*port*`]/`*path*`/`*file*

`ftp://`*server*`[:`*port*`]/`*path*`/`*file*

`file:///media/usb_msd/`*path*`/`*file*

where the value for *file* is in one of the following formats:

`XCP`*vvvv*`.tar.gz`

`IKXCP`*vvvv*`.tar.gz`

`FFXCP`*vvvv*`.tar.gz`

`DCXCP`*vvvv*`.tar.gz`

and *vvvv* is the four-character version number.

EXTENDED DESCRIPTION

When the command is executed, a prompt to confirm execution of the command with the specified options is displayed. Enter "**y**" to execute the command or "**n**" to cancel the command.

EXAMPLES

EXAMPLE 1 Downloading a Version from an http Server

```
XSCF> getflashimage http://imageserver/images/FFXCP1041.tar.gz
Existing versions:
        Version                Size  Date
        FFXCP1040.tar.gz   46827123  Wed Mar 14 19:11:40 2007
Warning: About to delete existing versions.
Continue? [y|n]: y
Removing FFXCP1040.tar.gz.
  0MB received
  1MB received
  2MB received
```

```
...
 43MB received
 44MB received
 45MB received
Download successful: 46827KB at 1016.857KB/s
Checking file...
MD5: e619e6dd367c888507427e58cdb8e0a0
```

EXAMPLE 2 Downloading a Version from an ftp Server

```
XSCF> getflashimage ftp://imageserver/images/FFXCP1041.tar.gz
Existing versions:
        Version                Size  Date
        FFXCP1040.tar.gz   46827123  Wed Mar 14 19:11:40 2007
Warning: About to delete existing versions.
Continue? [y|n]: y
Removing FFXCP1040.tar.gz.
  0MB received
  1MB received
  2MB received
...
  43MB received
  44MB received
  45MB received
Download successful: 46827KB at 1016.857KB/s
Checking file...
MD5: e619e6dd367c888507427e58cdb8e0a1
```

EXAMPLE 3 Downloading Using an http Proxy Server With Port 8080

```
XSCF> getflashimage -p webproxy.sun.com:8080 \
http://imageserver/images/FFXCP1041.tar.gz
Existing versions:
        Version                Size  Date
        FFXCP1040.tar.gz   46827123  Wed Mar 14 19:11:40 2007
Warning: About to delete existing versions.
Continue? [y|n]: y
Removing FFXCP1040.tar.gz.
  0MB received
  1MB received
  2MB received
...
  43MB received
  44MB received
  45MB received
```

```
Download successful: 46827KB at 1016.857KB/s
Checking file...
MD5: e619e6dd367c888507427e58cdb8e0a2
```

EXAMPLE 4 Downloading Using a User Name and Password

```
XSCF> getflashimage -u jsmith \
http://imageserver/images/FFXCP1041.tar.gz
Existing versions:
        Version                Size  Date
        FFXCP1040.tar.gz   46827123  Wed Mar 14 19:11:40 2007
Warning: About to delete existing versions.
Continue? [y|n]: y
Removing FFXCP1040.tar.gz.
Password: [not echoed]
  0MB received
  1MB received
  2MB received
...
  43MB received
  44MB received
  45MB received
Download successful: 46827KB at 1016.857KB/s
Checking file...
MD5: e619e6dd367c888507427e58cdb8e0a3
```

EXAMPLE 5 Downloading From a USB Memory Stick

```
XSCF> getflashimage file:///media/usb_msd/images/FFXCP1041.tar.gz
Existing versions:
        Version                Size  Date
        FFXCP1040.tar.gz    46827123  Wed Mar 14 19:11:40 2007
Warning: About to delete existing versions.
Continue? [y|n]: y
Removing FFXCP1040.tar.gz.
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
```

EXIT STATUS

The following exit values are returned:

`0`	Successful completion.
`>0`	An error occurred.

SEE ALSO

flashupdate`(8)`

NAME

ioxadm - manage External I/O Expansion Units and add-in cards that contain Energy Storage Modules and are attached to the host system

SYNOPSIS

ioxadm [-f] [-p] [-v] [-M] env [-e] [-l] [-t] [*target* [*sensors*]]

ioxadm [-f] [-p] [-v] [-M] lifetime [*target* | -z *target*]

ioxadm [-f] [-p] [-v] [-M] list [*target*]

ioxadm [-f] [-p] [-v] [-M] locator [on|off] [*target*]

ioxadm [-f] [-p] [-v] [-M] poweroff *target*

ioxadm [-f] [-p] [-v] [-M] poweron *target*

ioxadm [-f] [-p] [-v] [-M] reset *target*

ioxadm [-f] [-p] [-v] [-M] setled [on|off|slow|fast] *target led_type*

ioxadm -h

DESCRIPTION

ioxadm(8) manages External I/O Expansion Units, link cards, and cards that contain Energy Storage Modules (ESM) and are attached to the host system.

The M3000 server does not support External I/O Expansion Units.

When using this utility you must specify an operand, and any options that operand requires. The target device can be a card mounted in a built-in PCI slot in the host system; an External I/O Expansion Unit; or a field replaceable unit (FRU) in an External I/O Expansion Unit. The card in the host system is identified by a string that specifies the host path to the card. A linkcard installed in the host system is called a downlink. A linkcard installed in an I/O Expansion Unit boat is called an uplink.

For more information, see *target* in OPTIONS.

Privileges

You must have one of the following privileges to run these commands:

Required Privileges	Operands
platop	env, list
platadm	env, list, locator, poweroff, poweron
fieldeng	All operands

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

`-f` Forces command execution by ignoring warnings.

`-h` Displays usage statement.

When used with other options or operands, an error occurs.

`-M` Displays text by page.

`-p` Displays only parsable output, suppressing headers in that output. Fields are separated by single tabs.

`-v` Displays verbose output. Refer to specific operands for details.

target Specifies the target device, which can be a card mounted in a built-in PCI slot in the host system; an External I/O Expansion Unit; or a field replaceable unit (FRU) in an External I/O Expansion Unit.

The card in the host slot is identified by the *host_path* to the card.

host_path is platform dependent and indicates the path to the slot on the host system that contains the card. The *host_path* has the following format:

```
IOU#0-PCI#0 IO Board 0, PCI-E slot0
```

The External I/O Expansion Unit *(box_id)* is identified by serial number.

Use `iox@`*nnnn*, where *nnnn* represents the last four digits of the box serial number.

Some commands affect only a single component of an External I/O Expansion Unit system. For example, individual boats and power supplies can be turned on and turned off independently.

A FRU in an External I/O Expansion Unit *(fru)* is identified as:

`iox@nnnn/iob0` – I/O boat in the left tray (rear view)

`iox@nnnn/iob1` – I/O boat in the right tray (rear view)

`iox@nnnn/iob0/link` – Uplink card in boat 0

`iox@nnnn/iob1/link` – Uplink card in boat 1

`iox@nnnn/ps0` – Power supply in the left bay (front view)

`iox@nnnn/ps1` – Power supply in the right bay (front view)

OPERANDS

The following operands are supported:

`env` [`-elt`] [*target* [*sensors*]]

Displays a summary of an External I/O Expansion Unit or link card's environmental state.

`-e`	Displays electrical states: measured voltage, current, fan speed, switch settings.
`-l`	Displays LED states.
`-t`	Displays thermal readings.
target	See *target* in OPTIONS for a general description and the text below for information specific to `env`.
sensors	Specifies sensors about which data is to be displayed. If not specified, information about all sensors is shown. Cannot be used without *target*.

If you specify a FRU in an I/O Expansion Unit or a card in a host slot as the target, env only displays environmentals about that FRU.
If no `-e`, `-l`, or `-t` option is specified, the command displays all sensor information. If no sensors are specified, the command displays information about all sensors. If no target is specified, information about all External I/O Expansion Units is displayed.
If you specify a *box_id* as the target, `env` displays a list of sensor readings for all FRUs in the specified External I/O Expansion Unit and the attached cards in the host slot.
The options for `env` can be used in any combination.

The following information also applies to `env` and its display:

- Results are displayed in tabular format. Each FRU sensor is listed in the first column. The second column shows the sensor name, such as `T_AMBIENT` for ambient temperature, or `V_12V_0V` for the voltage reading of the 12V rail. The third, fourth, and fifth columns display the sensor reading (Value), sensor resolution (Res), and Units, respectively. See EXAMPLE 1.
- Each FRU can have a variety of different sensors. When specifying multiple values for *sensors,* use spaces to separate the values. Possible values for *sensors* can be seen in the `Sensor` column of EXAMPLE 1. Units are given in Celsius degrees, Volts, Amperes, SWITCH and RPM.
- The *sensors* names are FRU-dependent and may change from FRU type to FRU type and even among individual FRUs.

- If the `-v` option is set, verbose output is displayed. In addition to the regular output, the output also includes: the maximum and minimum values supported by the sensors (`Max` and `Min`), along with the low and high warning thresholds (`Min Alarm` and `Max Alarm`).
- LED indicators do not support these fields.
- Fields containing a "–" indicate an unsupported setting. For example, there may be no minimum temperature alarm threshold.

led_type

Used with the `setled` operand, specifies a software-controlled FRU LED. The following table indicates which LED states can be controlled using the `setled` operand with the `off`, `on`, `fast`, and `slow` LED state settings. Y (yes) indicates that the LED can be controlled, N (no) indicates that it cannot be controlled.

LED	Name	off	on	fast	slow
ACTIVE	Power/OK	Y	Y	Y	Y
LOCATE	Locate	Y	N	Y	N
SERVICE	Fault/Locate	Y	Y	Y	Y
RDY2RM	Ready to remove	Y	Y	Y	Y
OVERTEMP	Overtemp	*	*	*	*
DCOK	DC Power	N	N	N	N
POWER	AC Power	N	N	N	N
DATA	Data	N	N	N	N
MGMT	Management	N	N	N	N

* The `OVERTEMP` LED and chassis `ACTIVE` LED may be set to each state. However, the hardware frequently updates the LED state so changes to the LED state may not be visible.

Note - Other LEDs are not under software control. A list of LEDs present in the system can be displayed by using the `"env -l"` operand.

`lifetime` [*target* | `-z` *target*]

Clears or queries the runtime of cards that contain an energy storage module (ESM). Used without options, `lifetime` displays a list of cards with an ESM, one card per line, and shows, in minutes, each card's runtime and remaining lifespan. Runtime is updated at four-hour intervals.

If *target* is specified, the command lists only the specified ESM card.

If `-z` is specified, the command zeroes the runtime for the specified *target* and clears fault status for the the card. You must specify target with the `-z` option. See EXAMPLEs 6, 7, 8, and 9.

`list` [*target*]

Lists the External I/O Expansion Units under system management.

If no *target* is specified, `list` displays a list of External I/O Expansion Units, one per line. Each line contains the unique identifier for that box and the host-specific name(s) for its downlink card(s). See EXAMPLE 3.

If an External I/O Expansion Unit argument or downlink card path is specified, the command displays a single line with the indicated FRU. If a *host path* is specified, only the downlink card information is displayed. If the verbose option [`-v`] is set, the output includes detailed FRU information. See EXAMPLEs 4 and 5.

`locator [on |off] [target]`

Sets or queries the state of the locator indicator (LED).

Without options, `locator` reports the current state of the LED on the specified FRU.

A *target* argument is required when using the `on` or `off` field:

`on`	Turns the LED on.
`off`	Turns the LED off.

The chassis locator is a white LED. If a FRU is specified, the FRU yellow service LED is used along with the chassis (locator) LED.

Only one FRU can have a location indicator enabled at a time in an External I/O Expansion Unit chassis. Turning off the chassis (locator) LED will also turn off the blinking (service) FRU LED. See EXAMPLEs 10, 11, and 12.

`poweroff` *target*

Powers down the given FRU and lights appropriate LEDs to indicate the FRU is ready to remove. Must be used with the `-f` option. Be aware that using `-f` can crash the domain.

Do not remove both power supply units (PSUs) in the same External I/O Expansion Unit. If both PSUs are powered down in this way, then the External I/O Expansion Unit cannot be turned back on from the command line. It must be powered on physically.

Note - When a power supply is powered off, the LEDs and fan may still run since they receive power from both supplies.

`poweron` *target*

Restores full power to an I/O boat or reenables output from the power supply (PS) that has previously been marked ready-to-remove. When a PSU is newly installed and the power switch is in the on position, or a boat is connected to a powered link card, they automatically power themselves on. However, this command can be used to power a PSU or I/O boat back on that previously had been powered down for removal as long as the power switch is in the on position.

`reset` *target*

Reinitializes FRU components used to monitor External I/O Expansion Unit environmentals. If a boat or link card is specified, the bridge controllers in the link cards are reset and re-initialized. If a box is specified, the fan controller and demux in the box are reset and re-initialized along with all bridge controllers associated with the External I/O Expansion Unit.

`setled` [`on`|`off`|`slow`|`fast`] *target led_type*

Sets LED state:

`off`	Off.
`on`	On.
`fast`	Fast blink.
`slow`	Slow blink.

Refer to the entry for *led_type* in this section for detailed information about LED types.

EXAMPLES

EXAMPLE 1 Display temperature, voltage, current, and fan-speed sensor readings

```
XSCF> ioxadm env -te iox@A3B5
Location            Sensor            Value      Res     Units
IOX@A3B5/PS0        T_AMBIENT         28.000      1.000  C
IOX@A3B5/PS0        T_CHIP            28.000      1.000  C
IOX@A3B5/PS0        T_HOTSPOT         31.000      1.000  C
IOX@A3B5/PS0        SWITCH                On          -  SWITCH
IOX@A3B5/PS0        V_12V_ANODE       11.703      0.059  V
IOX@A3B5/PS0        V_12V_CATHODE     11.703      0.059  V
IOX@A3B5/PS0        V_ISHARE           0.632      0.040  V
IOX@A3B5/PS0        I_DC               2.316      0.289  A
IOX@A3B5/PS0        S_FAN_ACTUAL    3708.791     40.313  RPM
IOX@A3B5/PS0        S_FAN_SET       4500.000    300.000  RPM
IOX@A3B5/PS1        T_AMBIENT         28.000      1.000  C
IOX@A3B5/PS1        T_CHIP            29.000      1.000  C
IOX@A3B5/PS1        T_HOTSPOT         31.000      1.000  C
IOX@A3B5/PS1        SWITCH                On          -  SWITCH
IOX@A3B5/PS1        V_12V_ANODE       11.762      0.059  V
IOX@A3B5/PS1        V_12V_CATHODE     11.762      0.059  V
IOX@A3B5/PS1        V_ISHARE           0.672      0.040  V
IOX@A3B5/PS1        I_DC               5.211      0.289  A
IOX@A3B5/PS1        S_FAN_ACTUAL    4115.854     49.588  RPM
IOX@A3B5/PS1        S_FAN_SET       4500.000    300.000  RPM
IOX@A3B5/IOB0       T_CHIP            32.000      1.000  C
IOX@A3B5/IOB0       T_HOTSPOT         35.000      1.000  C
IOX@A3B5/IOB1       T_CHIP            33.000      1.000  C
IOX@A3B5/IOB1       T_HOTSPOT         36.000      1.000  C
IOX@A3B5/IOB1       V_12_0V           12.052      0.005  V
IOX@A3B5/IOB1       V_12V_MAIN        12.000      0.400  V
IOX@A3B5/IOB1       V_1_0V             1.030      0.001  V
IOX@A3B5/IOB1       V_1_5V             1.496      0.001  V
```

```
IOX@A3B5/IOB1       V_3_3V              3.291      0.002  V
IOX@A3B5/IOB1       V_3_3AUX            3.308      0.002  V
IOX@A3B5/IOB1       I_DC                8.600      0.200  A
```

EXAMPLE 2 Display all sensor readings on a link and suppress headers

```
XSCF> ioxadm -p env iou#1-pci#1
IOU#1-PCI#1  DATA      On      -      LED
IOU#1-PCI#1  MGMT      Flash   -      LED
```

EXAMPLE 3 Display all External I/O Expansion Units or downlink card paths

```
XSCF> ioxadm list
IOX           Link 0              Link 1
IOX@0033      IOU#1-PCI#4         IOU#1-PCI#1
IOX@12B4      -                   IOU#1-PCI#2
-             IOU#2-PCI#1
```

In this example the `list` command is used to display the connections between External I/O Expansion Units and downlink cards in the host. `IOX@0033` (which includes boats, uplink cards, and power supplies) is connected to the host through two downlink cards. The `Link 0` column shows which host downlink card is attached to `boat0`. The `Link 1` column shows which host downlink card is attached to `boat1`. `IOX@12B4` is connected to the host through one downlink card. This card is connected to `boat1`. A "–" shows that there is no host link connection to the box. It may have a boat and uplink card installed in the bay, or the bay could be empty. If the boat is installed, either it is not connected to the host, or the host downlink card slot is powered off.

EXAMPLE 4 Display a single External I/O Expansion Unit

```
XSCF> ioxadm list iox@12B4
IOX               Link 0           Link 1
IOX@12B4          -                IOU#1-PCI#2
```

EXAMPLE 5 Display a card using host_path in verbose mode with headers suppressed

```
XSCF> ioxadm -p -v list IOU#0-PCI#1
IOU#0-PCI#1     F20   -        000004      5111500-01     On
```

EXAMPLE 6 Show runtime of card with ESM

```
XSCF> ioxadm lifetime
NAC                 Total Time On  (% of life)
IOU#0-PCI#1       : 183520          17
IOU#0-PCI#3       : 36660           -
```

EXAMPLE 7 Show runtime of card with ESM using verbose output

```
XSCF> ioxadm -v lifetime
NAC            Total Time On   (% of life)   Warning Time   Fault Time
IOU#0-PCI#1    183520           17            1008000        1051200
IOU#0-PCI#3    36660            -             -              -
```

EXAMPLE 8 Clear runtime of card with ESM, show runtime is cleared

```
XSCF> ioxadm lifetime -z IOU#0-PCI#1
XSCF> ioxadm lifetime IOU#0-PCI#1
NAC            Total Time On   (% of life)
IOU#0-PCI#1    0                0
```

EXAMPLE 9 Show card with ESM after runtime has been cleared, using verbose output

```
XSCF> ioxadm -v lifetime IOU#0-PCI#1
NAC            Total Time On   (% of life)  Warning Time  Fault Time
IOU#0-PCI#1    0                0           1041120       1051200
```

EXAMPLE 10 Display locator LED status for the External I/O Expansion Unit

```
XSCF> ioxadm locator iox@12B4
Location            Sensor             Value     Resolution  Units
IOX@12B4            LOCATE              Fast     -           LED
IOX@12B4/PS0        SERVICE             Fast     -           LED
```

If the FRU service indicator is already on due to a detected fault condition, only the box locator LED will be set to fast.

EXAMPLE 11 Power-on the locator LED for power supply 0 in External I/O Expansion Unit 12B4

```
XSCF> ioxadm locator on iox@12B4/ps0
```

EXAMPLE 12 Enable the indicator for power supply 1 when power supply 1 has a fault indication

```
XSCF> ioxadm locator on iox@x031/ps1
XSCF> ioxadm locator
Location       Sensor     Value Resolution Units
IOX@X031       LOCATE      Fast          - LED
XSCF> ioxadm env -1 iox@x031/ps1 SERVICE
Location       Sensor     Value Resolution Units
IOX@X031/PS1   SERVICE       On          - LED
```

The External I/O Expansion Unit chassis white LED has an integrated push button. The button can be used to toggle the state of the chassis white locator LED between

off and fast. If the push button is used to turn off the locator LED, fast blink FRU service LEDs are cleared.

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

NAME

moveboard - move an eXtended System Board (XSB) from the current domain to another

SYNOPSIS

moveboard [[-q] -{y|n}] [-f] [-v] [-c configure] -d *domain_id xsb* [*xsb*...]

moveboard [[-q] -{y|n}] [-f] [-v] -c assign -d *domain_id xsb* [*xsb*...]

moveboard [[-q] -{y|n}] [-f] [-v] -c reserve -d *domain_id xsb* [*xsb*...]

moveboard -h

DESCRIPTION

The moveboard(8) command disconnects an XSB from the current domain and, based on the domain component list (DCL), assigns it to, or configures it in, the specified domain.

The moveboard(8) command is not available on the M3000 server.

One of the following movement methods can be specified:

configure — Disconnects a configured XSB from its domain configuration and configures it into the specified destination domain configuration. The incorporated XSB can be accessed from the Oracle Solaris OS.

assign — Disconnects a configured XSB from its domain configuration and assigns it to the specified destination domain configuration. The assigned XSB is reserved for the specified domain and cannot be configured in or assigned to other domains. The assigned system board is configured in the domain by reboot the domain or execution of the addboard(8) command with "-c configure".

reserve — Reserves disconnection of the specified XSB from the domain configuration of the move source, and reserves assignment of the XSB to the domain configuration of the move destination. The XSB is assigned to the domain configuration of the move destination when the domain power of the move source is turned off or rebooted. The XSB is subsequently incorporated when the domain power of the move destination is turned on or rebooted.

Privileges

You must have one of the following privileges to run this command:

platadm — Can run this command for all domains.

domainadm — Can run this command only for your managed domains.

Note - You must have the domainadm privileges for both of source domain and destination domain to run moveboard(8) command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

`-c assign`
: Disconnects a configured XSB from its domain configuration and assigns it to the domain configuration of the move destination. If the `-c` option is omitted, "`-c configure`" is used.

`-c configure`
: Disconnects a configured XSB from its domain configuration and configures it in the domain configuration of the move destination. If the `-c` option is omitted, "`-c configure`" is used.

`-c reserve`
: Reserves disconnection of an XSB from its current domain configuration, and reserves assignment of the XSB to the domain configuration of the move destination. If the `-c` option is omitted, "`-c configure`" is used.

`-d` *domain_id*
: Specifies the ID of the destination domain in which an XSB is to be moved. *domain_id* can be 0–23 depending on the system configuration.

`-f`
: Forcibly detaches the specified XSB.

Caution - If the `-f` option is used to forcibly remove the XSB from the source domain, a serious problem may occur in a process bound to CPU or process accessing a device. For this reason, use of the `-f` option is not recommended in normal operation. If the `-f` option must be specified, verify the statuses of the source domain and job processes.

Note - The XSB which failed or detected the failure will not be configured to the DCL forcibly.

`-h`
: Displays usage statement. When used with other options or operands, an error occurs.

`-n`
: Automatically answers "`n`" (no) to all prompts.

`-q`
: Suppresses all messages to stdout, including prompts.

`-v`
: Specifies verbose output. If this option is specified with the `-q` option, the `-v` option is ignored.

`-y`
: Automatically answers "`y`" (yes) to all prompts.

OPERANDS

The following operand is supported:

xsb Specifies the XSB number to be moved. Multiple *xsb* operands are permitted, separated by spaces. The following xsb form is accepted:

x–y

where:

x An integer from `00–15`.

y An integer from `0–3`.

EXTENDED DESCRIPTION

- You can execute the `moveboard`(8) command on a source domain or a destination domain that is not running. When the source domain is running, the `moveboard`(8) command with "`-c configure`" or "`-c assign`" will succeed only if the following Oracle Solaris Service Management Facility (SMF) services are active on that domain:
  - Domain SP Communication Protocol (dscp)
  - Domain Configuration Server (dcs)
  - Oracle Sun Cryptographic Key Management Daemon (sckmd)
- When the command is executed, a prompt to confirm execution of the command with the specified options is displayed. Enter "`y`" to execute the command or "`n`" to cancel the command.
- If "`-c configure`" is specified when either of the following conditions apply to the domains, the XSB is configured in the domain configuration:
  - The Oracle Solaris OS of both the source and destination domains are running.
  - The Oracle Solaris OS of the destination domain is running even though the source domain is powered off.
- If "`-c assign`" is specified when either of the following conditions apply to the domains, the XSB is assigned to the domain configuration:
  - The Oracle Solaris OS of the source domain is running.
  - The source domain is powered off
- If "`-c reserve`" is specified when either the domain power of the move source has been turned off or the Oracle Solaris OS is not running, the XSB is immediately disconnected from the domain of the move source and assigned to the domain of the move destination
- Moving the XSB involves the following internal operations and therefore command execution may take time.
  - Disconnecting the hardware resource of the XSB from the Oracle Solaris OS

- Running a hardware diagnosis on the XSB when connecting it
- See the `setdcl`(8) and `showdcl`(8) commands for DCL.

EXAMPLES

EXAMPLE 1 Disconnects XSB#00-0 from the current domain and attaches it to domain ID 1.

```
XSCF> moveboard -d 1 00-0
```

EXAMPLE 2 Reserves assignment of the XSB#00-0 to the domain ID 1.

```
XSCF> moveboard -d 1 -c reserve 00-0
```

EXIT STATUS

The following exit values are returned:

`0`	Successful completion.
`>0`	An error occurred.

SEE ALSO

addboard (8), **deleteboard** (8), **setdcl** (8), **setupfru** (8), **showboards** (8), **showdcl** (8), **showdevices** (8), **showdomainstatus** (8), **showfru** (8)

NAME

nslookup - refer to the DNS server for the host

SYNOPSIS

nslookup *hostname*

nslookup -h

DESCRIPTION

nslookup(8) refers to the DNS server for the host.

The following information is displayed:

Server	DNS server name
Address	IP address of DNS server
Name	Specified host name
Address	IP address of the host name

Privileges

You must have one of the following privileges to run this command:

useradm, platadm, platop, auditadm, auditop, domainadm, domainmgr, domainop, fieldeng

Refer to setprivileges(8) for more information.

OPTIONS

The following option is supported:

-h	Displays usage statement. When used with other options or operands, an error occurs.

OPERANDS

The following operand is supported:

hostname	Specifies the host name to be referred. A Fully Qualified Domain Name (FQDN) or a short form of the name can be specified.

EXAMPLES

EXAMPLE 1 Displays the host whose host name is scf0-hostname0.

```
XSCF> nslookup scf0-hostname0
Server:  server.example.com
Address: xx.xx.xx.xx

Name:    scf0-hostname0.example.com
Address: xx.xx.xx.xx
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

NAME

password - manage user passwords and expiration settings

SYNOPSIS

password [-e *days* | *date* | Never] [-i *inactive*] [-M *maxdays*] [-n *mindays*] [-w *warn*] [*user*]

password -h

DESCRIPTION

password (8) changes a user's password and password expiration settings.

The password is specified in up to 32 characters. The following characters are valid:

1. abcdefghijklmnopqrstuvwxyz

2. ABCDEFGHIJKLMNOPQRSTUVWXYZ

3. 0123456789

4. !@#$%^&*[]{}()_ - + ='~,></''?;:[SPACE]

When invoked with one or more options, password will make changes to the expiration settings of the account. See setpasswordpolicy(8) for a description of default values.

When invoked without options, password prompts you to change the account password.

When invoked without a *user* operand, password operates on the current user account.

Caution – When you change the password for another user by using the *user* operand, the system password policy is *not* enforced. The *user* operand is intended only for creating a new user's initial password or replacing a lost or forgotten password for a user account. When changing another user's password, be sure to choose a password that conforms with the system password policy. You can display the current password policy settings with the showpasswordpolicy(8) command.

Whether the user name is specified or not, the account must be local. password returns an error if it is not local.

Privileges

You must have one of the following privileges to run this command:

useradm	Can run this command with or without any options or operand. Can change the password for any account.

No privileges are required in the following cases:

- To change the password for the current user account
- To use the -h option

Refer to `setprivileges`(8) for more information.

OPTIONS

The following options are supported

`-e` *days*|*date*|`Never`

days sets the number of days, starting from today, during which the XSCF account is enabled. days is in the format of a number (0-10730). If the current date plus the number of days exceeds January 2038 the number is considered invalid and the command will fail.

date sets the date when the account expires, not exceeding January 2038. The date format can be:

mm/dd/yy (10/30/08)

yyyy-mm-dd (2008-10-30)

yy-mm-dd (08-10-30)

dd-Mmm-yy (30-Oct-08)

dd-Mmm-yyyy (30-Oct-2008)

dd Mmm yy ("30 Oct 08")

dd Mmm yyyy ("30 Oct 2008")

Mmm dd, yy ("Oct 30, 08")

Mmm dd, yyyy ("Oct 30, 2008")

Quotes must be used for formats with an embedded space. It is case insensitive.

Never means an account will not expire.

`-h`

Displays usage statement.

When used with other options or operands, an error occurs.

`-i` *inactive*

Sets the number of days after a password expires until the account is locked. This value is assigned to new user accounts when they are created. The initial value is `-1`. A value of `-1` means that the account will not be locked after the password expires. Valid values are integers with value of `-1` - 999999999.

`-M` *maxdays*	Sets the maximum number of days that a password is valid. This value is assigned to new user accounts when they are created. The initial value is `999999`. Valid values are integers with value of 0 - 999999999.
`-n` *mindays*	Sets the minimum number of days between password changes. An initial value of zero for this field indicates that you can change the password at any time. Valid values are integers with value of 0 - 999999999. This value is assigned to new user accounts when they are created.
`-w` *warn*	Sets the default number of days before password expiration at which to start warning the user. This value is assigned to new user accounts when they are created. The initial value is `7`. Valid values are integers with value of 0 - 999999999.

OPERANDS

The following operands are supported:

user	Specifies a valid user name.

EXAMPLES

EXAMPLE 1 Enabling Password Until February 2, 2008

```
XSCF> password -e 2008-02-02
```

EXAMPLE 2 Set Password Lock 10 Days After Password Expiration

```
XSCF> password -i 10
```

EXIT STATUS

The following exit values are returned:

`0`	Successful completion.
`>0`	An error occurred.

SEE ALSO

setpasswordpolicy`(8)`, **showpasswordpolicy**`(8)`

NAME

ping - send the ICMP ECHO_REQUEST packets to the network host or the network device

SYNOPSIS

ping [-c *count*] [-q] *host*

ping -h

DESCRIPTION

The ping(8) command utilizes the ICMP ECHO_REQUEST datagram to elicit an ICMP ECHO_RESPONSE from the specified host or network device.

When the ping(8) command normally executed, the network between XSCF and the specified host or network device can be judged as normal. And the network performance can be measured from the result.

Privileges

You must have one of the following privileges to run this command:

- To execute the command to DSCP address:

  platadm, fieldeng

- To execute the command to "localhost" or to the loopback address (127.0.0.0/8):

  fieldeng

- To execute the command to Inter SCF Network (ISN):

  fieldeng

- The case other than those above:

  No privileges are required.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-c *count*	Specifies the number of times to send the packet. After sent the packet for the number of specified times and received its response, the ping(8) command terminates. If omitted, the command continues sending the packet until the interrupt occurs.
-h	Displays usage statement. When used with other options or operands, an error occurs.
-q	Suppresses the output. Outputs the data at the start and at the end of the command.

OPERANDS

The following operand is supported:

host	Specifies the network host or the network device to send the packet. Can be specified with host name or IP address.

EXAMPLES

EXAMPLE 1 Sends the packet three times to a host named scf0-hostname0.

```
XSCF> ping -c 3 scf0-hostname0
PING scf0-hostname0 (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-hostname0 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.1/0.1 ms
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

NAME

poweroff - turn off the power to the specified domain

SYNOPSIS

poweroff [[-q] -{y|n}] [-f] [-M] -d *domain_id*

poweroff [[-q] -{y|n}] -a [-M]

poweroff -h

DESCRIPTION

The poweroff(8) command turns off the power to the specified domain.

The command can turn off the power to the specified domain or to all domains. After ordinary shutdown processing for the operating system is executed, the power is turned off.

Privileges

You must have one of the following privileges to run this command:

platadm, fieldeng	Can run this command for all domains.
domainadm, domainmgr	Can run this command only for your managed domains.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-a	Turns off the power to all domains. Only users who have the platadm and fieldeng privileges can specify this option. This option turns off the power to a system in process of warm-up or air-conditioning, or to a domain in process of power-on.
-d *domain_id*	Specifies the ID of the domain to be turned off. *domain_id* can be 0–23 depending on the system configuration. This option does not turn off the power to a system in process of warm-up or air-conditioning, or to a domain in process of power-on.
-f	Uses XSCF to forcibly turn off the power to the specified domain. This option is used together with the -d option.
-h	Displays usage statement. When used with other options or operands, an error occurs.
-M	Displays text by page. This option provides a function that is the same as that of the more command.
-n	Automatically answers "n" (no) to all prompts.
-q	Suppresses all messages to stdout, including prompts.
-y	Automatically answers "y" (yes) to all prompts.

EXTENDED DESCRIPTION

- When the command is executed, a prompt to confirm execution of the command with the specified options is displayed. Enter "**y**" to execute the command or "**n**" to cancel the command.
- If the Oracle Solaris OS of the target domain is running, the `poweroff`(8) command processing is equivalent to that of the `shutdown`(1M) command with the "`-i5`" option specified.
- A domain cannot be powered off while the Oracle Solaris OS of the domain is booting. Execute the `poweroff`(8) command again after the booting is completed.
- A domain cannot be powered off by the `poweroff`(8) command while the Oracle Solaris OS of the domain is running in single-user mode. Execute the `shutdown`(1M) command in the domain.
- When the `poweroff`(8) command is executed, power-off results for each of the specified domains are displayed in the following format:

`Powering off`	The power was turned off normally.
`Not Powering off`	An error occurred, and the power could not be turned off. An error message is displayed with "Not Powering off."

- The `showdomainstatus`(8) command can be used to check the power of each domain on the system is off.

EXAMPLES

EXAMPLE 1 Turns off power to all domains.

```
XSCF> poweroff -a
DomainIDs 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 "showlogs power".
```

EXAMPLE 2 Turns off power to domains with domain IDs 0.

```
XSCF> poweroff -d 0
DomainIDs 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 "showlogs power".
```

EXAMPLE 3 Forcibly turns off power to domains with domain IDs 0.

```
XSCF> poweroff -f -d 0
DomainIDs to power off:00
The -f option will cause domains to be immediately resets.
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 "showlogs power".
```

EXAMPLE 4 Turns off power to domains with domain IDs 2. Automatically replies with "y" to the prompt.

```
XSCF> poweroff -y -d 2
DomainIDs to power off:02
Continue? [y|n]:y
02:Powering off

*Note*
 This command only issues the instruction to power-off.
 The result of the instruction can be checked by the "showlogs power".
```

EXAMPLE 5 Turns off power to domains with domain IDs 2. Automatically replies with "y" without displaying the prompt.

```
XSCF> poweroff -q -y -d 2
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

poweron(8), **reset**(8), **showdomainstatus**(8)

NAME

poweron - turn on the power to the specified domain

SYNOPSIS

poweron [[-q] -{y|n}] [-M] -d *domain_id*

poweron [[-q] -{y|n}] [-M] -a

poweron -h

DESCRIPTION

The poweron(8) command turns on the power to the specified domain.

The command can turn on the power to the specified domain or to all domains.

Privileges

You must have one of the following privileges to run this command:

platadm, fieldeng	Can run this command for all domains.
domainadm, domainmgr	Can run this command only for your managed domains.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-a	Turns on the power to every domain that has been completely set up. Only users who have the platadm or fieldeng privileges can specify this option. The "domain that has been completely set up" means a domain that has been completely set up with the setupplatform(8) and setupfru(8) commands.
-d *domain_id*	Specifies the ID of the domain to be turned on. *domain_id* can be 0–23 depending on the system configuration.
-h	Displays usage statement. When used with other options or operands, an error occurs.
-M	Displays text by page. This option provides a function that is the same as that of the more command.
-n	Automatically answers "n" (no) to all prompts.
-q	Suppresses all messages to stdout, including prompts.
-y	Automatically answers "y" (yes) to all prompts.

EXTENDED DESCRIPTION

- When the command is executed, a prompt to confirm execution of the command with the specified options is displayed. Enter "y" to execute the command or "n" to cancel the command.

- When the `poweron`(8) command is executed, power-on results for each of the specified domains are displayed in the following format:

`Powering on`	The power was turned on normally.
`Not Powering on`	An error occurred, and the power could not be turned on. An error message is displayed with Not Powering on.

- The `showdomainstatus`(8) command can be used to check whether the power of each domain on the system is on.

EXAMPLES

EXAMPLE 1 Turns on power to all domains.

```
XSCF> poweron -a
DomainIDs 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 "showlogs power".
```

EXAMPLE 2 Turns on power to domains with domain IDs 0.

```
XSCF> poweron -d 0
DomainIDs 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 "showlogs power".
```

EXAMPLE 3 Turns on power to domains with domain IDs 0. Automatically replies with "y" to the prompt.

```
XSCF> poweron -y -d 0
DomainIDs 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 "showlogs power".
XSCF>
```

EXAMPLE 4 Turns on power to domains with domain IDs 1. Automatically replies with "y" without displaying the prompt.

```
XSCF> poweron -q -y -d 1
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

poweroff(8), **reset**(8), **showdomainstatus**(8)

NAME

prtfru - display FRUID data on the system and External I/O Expansion Unit

SYNOPSIS

prtfru [-c] [-l] [-M] [-x] [*container*]

prtfru -h

DESCRIPTION

prtfru is used to obtain Field Replaceable Unit Identifier (FRUID) data from the system and External I/O Expansion Unit. Its output is a tree structure, echoing the path in the FRU tree to each container. When a container is found, the data from that container is printed in a tree structure as well.

prtfru without any arguments prints the FRU hierarchy and all of the FRUID container data. prtfru prints to the screen. Output can be redirected to a file.

Note – FRU information from the domains is not available using this command.

Privileges

You must have fieldeng privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-c	Prints only the containers and their data. This option does not print the FRU tree hierarchy.
-h	Displays usage statement. When used with other options or operands, an error occurs.
-M	Displays text by page. This option provides a function that is the same as that of the more command.
-l	Prints only the FRU tree hierarchy. This option does not print the container data.
-x	Prints in XML format with a system identifier (SYSTEM) of prtfrureg.dtd.

OPERANDS

The following operands are supported:

container	The path and name of the particular hardware that holds data.

EXAMPLES

EXAMPLE 1 Displaying FRU Tree Hierarchy

```
XSCF> prtfru -l
/frutree
/frutree/chassis (fru)
/frutree/chassis/iou0
/frutree/chassis/iou0/IOU (fru)
/frutree/chassis/iou0/IOU/slot3
```

```
/frutree/chassis/iou0/IOU/slot3/LINK (container)
/frutree/chassis/iou0/IOU/slot3/LINK/iox983392.IOX.iob1.PCIX.LINK (fru)
/frutree/chassis/iox983392?Label=IOX@XCX031
/frutree/chassis/iox983392?Label=IOX@XCX031/IOX (container)
/frutree/chassis/iox983392?Label=IOX@XCX031/IOX/ps0
/frutree/chassis/iox983392?Label=IOX@XCX031/IOX/ps0/A195 (container)
/frutree/chassis/iox983392?Label=IOX@XCX031/IOX/ps1
/frutree/chassis/iox983392?Label=IOX@XCX031/IOX/ps1/A195 (container)
/frutree/chassis/iox983392?Label=IOX@XCX031/IOX/iob1
/frutree/chassis/iox983392?Label=IOX@XCX031/IOX/iob1/PCIX (container)
/frutree/chassis/iox983392?Label=IOX@XCX031/IOX/iob1/PCIX/LINK
(container)
/frutree/chassis/iox983392?Label=IOX@XCX031/IOX/iob1/PCIX/LINK/
iou0.IOU.slot3.LINK (fru)
/frutree/chassis/MBU_B (container)
/frutree/chassis/MBU_B/CPUM#0/CPUM (container)
/frutree/chassis/MBU_B/CPUM#1/CPUM (container)
/frutree/chassis/MBU_B/MEMB#0 (fru)
/frutree/chassis/MBU_B/CPUM#1/CPUM (container)
/frutree/chassis/MBU_B/MEMB#0 (fru)
/frutree/chassis/MBU_B/MEMB#0/MEMB (container)
/frutree/chassis/MBU_B/MEMB#0/MEMB/MEM#0/MEM (container)
/frutree/chassis/MBU_B/MEMB#0/MEMB/MEM#1/MEM (container)
/frutree/chassis/MBU_B/MEMB#0/MEMB/MEM#2/MEM (container)
/frutree/chassis/MBU_B/MEMB#0/MEMB/MEM#3/MEM (container)
/frutree/chassis/MBU_B/MEMB#0/MEMB/MEM#4/MEM (container)
/frutree/chassis/MBU_B/MEMB#0/MEMB/MEM#5/MEM (container)
/frutree/chassis/MBU_B/MEMB#0/MEMB/MEM#6/MEM (container)
/frutree/chassis/MBU_B/MEMB#0/MEMB/MEM#7/MEM (container)
/frutree/chassis/MBU_B/MEMB#1 (fru)
/frutree/chassis/MBU_B/MEMB#1/MEMB (container)
/frutree/chassis/MBU_B/MEMB#1/MEMB/MEM#8/MEM (container)
/frutree/chassis/MBU_B/MEMB#1/MEMB/MEM#9/MEM (container)
/frutree/chassis/MBU_B/MEMB#1/MEMB/MEM#10/MEM (container)
/frutree/chassis/MBU_B/MEMB#1/MEMB/MEM#11/MEM (container)
/frutree/chassis/MBU_B/MEMB#1/MEMB/MEM#12/MEM (container)
/frutree/chassis/MBU_B/MEMB#1/MEMB/MEM#13/MEM (container)
/frutree/chassis/MBU_B/MEMB#1/MEMB/MEM#14/MEM (container)
/frutree/chassis/MBU_B/MEMB#1/MEMB/MEM#15/MEM (container)
/frutree/chassis/XSCFU (container)
/frutree/chassis/OPNL (container)
/frutree/chassis/PSU#0 (fru)
/frutree/chassis/PSU#0/PSU (container)
/frutree/chassis/PSU#2 (fru)
/frutree/chassis/PSU#2/PSU (container)
```

```
/frutree/chassis/IOU#0 (fru)
/frutree/chassis/IOU#0/IOU (container)
/frutree/chassis/IOU#0/IOU/DDCR#0/DDCR (container)
/frutree/chassis/FANBP_C#0 (fru)
/frutree/chassis/FANBP_C#0/FANBP_C (container)
```

EXAMPLE 2 Displaying A list of Containers

```
XSCF> prtfru -lc
/frutree/chassis/iou0/IOU/slot3/LINK (container)
/frutree/chassis/iox983392?Label=IOX@XCX031/IOX (container)
/frutree/chassis/iox983392?Label=IOX@XCX031/IOX/ps0/A195 (container)
/frutree/chassis/iox983392?Label=IOX@XCX031/IOX/ps1/A195 (container)
/frutree/chassis/iox983392?Label=IOX@XCX031/IOX/iob1/PCIX (container)
/frutree/chassis/iox983392?Label=IOX@XCX031/IOX/iob1/PCIX/LINK
(container)
/frutree/chassis/MBU_B (container)
/frutree/chassis/MBU_B/CPUM#0/CPUM (container)
/frutree/chassis/MBU_B/CPUM#1/CPUM (container)
/frutree/chassis/MBU_B/MEMB#0/MEMB (container)
/frutree/chassis/MBU_B/MEMB#0/MEMB/MEM#0/MEM (container)
/frutree/chassis/MBU_B/MEMB#0/MEMB/MEM#1/MEM (container)
/frutree/chassis/MBU_B/MEMB#0/MEMB/MEM#2/MEM (container)
/frutree/chassis/MBU_B/MEMB#0/MEMB/MEM#3/MEM (container)
/frutree/chassis/MBU_B/MEMB#0/MEMB/MEM#4/MEM (container)
/frutree/chassis/MBU_B/MEMB#0/MEMB/MEM#5/MEM (container)
/frutree/chassis/MBU_B/MEMB#0/MEMB/MEM#6/MEM (container)
/frutree/chassis/MBU_B/MEMB#0/MEMB/MEM#7/MEM (container)
/frutree/chassis/MBU_B/MEMB#1/MEMB (container)
/frutree/chassis/MBU_B/MEMB#1/MEMB/MEM#8/MEM (container)
/frutree/chassis/MBU_B/MEMB#1/MEMB/MEM#9/MEM (container)
/frutree/chassis/MBU_B/MEMB#1/MEMB/MEM#10/MEM (container)
/frutree/chassis/MBU_B/MEMB#1/MEMB/MEM#11/MEM (container)
/frutree/chassis/MBU_B/MEMB#1/MEMB/MEM#12/MEM (container)
/frutree/chassis/MBU_B/MEMB#1/MEMB/MEM#13/MEM (container)
/frutree/chassis/MBU_B/MEMB#1/MEMB/MEM#14/MEM (container)
/frutree/chassis/MBU_B/MEMB#1/MEMB/MEM#15/MEM (container)
/frutree/chassis/XSCFU (container)
/frutree/chassis/OPNL (container)
/frutree/chassis/PSU#0/PSU (container)
/frutree/chassis/PSU#2/PSU (container)
/frutree/chassis/IOU#0/IOU (container)
/frutree/chassis/IOU#0/IOU/DDCR#0/DDCR (container)
/frutree/chassis/FANBP_C#0/FANBP_C (container)
```

EXIT STATUS

The following exit values are returned:

`0`	Successful completion.
`>0`	An error occurred.

SEE ALSO

ioxadm (8)

NAME

rebootxscf - reset the XSCF

SYNOPSIS

rebootxscf [[-q] -{y|n}]

rebootxscf -h

DESCRIPTION

The rebootxscf(8) command resets the XSCF.

The settings configured by using the following commands will be applied to XSCF after you reset XSCF by using the rebootxscf(8) command.

- applynetwork(8)
- setaltitude(8)
- setdualpowerfeed(8)
- sethttps(8)
- setntp(8)
- setssh(8)
- settelnet(8)

In the M8000/M9000 servers, both of the active XSCF and the standby XSCF will be reset.

Privileges

You must have platadm or fieldeng privilege to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-h	Displays usage statement. When used with other options or operands, an error occurs.
-n	Automatically answers "n" (no) to all prompts.
-q	Suppresses all messages to stdout, including prompts.
-y	Automatically answers "y" (yes) to all prompts.

EXTENDED DESCRIPTION

- When the command is executed, a prompt to confirm execution of the command is displayed. Enter "**y**" to execute the command or "**n**" to cancel the command.
- The rebootxscf(8) command terminates all connection to XSCF, such as telnet or ssh.
- When you cancel the XSCF reset using the setdate(8) which commands reset XSCF automatically, even if you perform this command, the information that is set is not applied in XSCF.

- By using the `rebootxscf`(8) command, you can reset XSCF while the domain is in operation. However, if you set up XSCF to serve as the upper NTP server of the domain, time lag may arise between XSCF and the domain. In such a case, adjust the domain time so that XSCF and the domain will be synchronized.

EXAMPLES

EXAMPLE 1 Resets the XSCF.

```
XSCF> rebootxscf
The XSCF will be reset. Continue? [y|n]:y
```

EXAMPLE 2 Resets the XSCF. Automatically replies with "`y`" to the prompt.

```
XSCF> rebootxscf -y
The XSCF will be reset. Continue? [y|n]:y
```

EXAMPLE 3 Resets the XSCF. Automatically replies with "`y`" without displaying the prompt.

```
XSCF> rebootxscf -q -y
```

EXAMPLE 4 Cancels the `rebootxscf`(8) command execution that is in progress.

```
XSCF> rebootxscf
The XSCF will be reset. Continue? [y|n]:n
XSCF>
```

EXIT STATUS

The following exit values are returned:

`0`	Successful completion.
`>0`	An error occurred.

SEE ALSO

applynetwork(8), **setaltitude**(8), **setdualpowerfeed**(8), **sethttps**(8), **setntp**(8), **setssh**(8), **settelnet**(8)

NAME

replacefru - replace a field replaceable unit (FRU)

SYNOPSIS

replacefru

replacefru -h

DESCRIPTION

The replacefru(8) command replaces an FRU. The command allows the user to select, confirm, and replace the FRU interactively using menus.

The following FRUs can be replaced using the replacefru(8) command.

- CPU/Memory Board unit (CMU)
- I/O unit (IOU)
- FAN unit (FANU)
- Power supply unit (PSU)
- XSCF unit (XSCFU)
- DC-DC converter (DDC_A)

Privileges

You must have fieldeng privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following option is supported.

-h Displays usage statement.

EXIT STATUS

The following exit values are returned:

0 Successful completion.

>0 An error occurred.

SEE ALSO

addboard(8), **addfru**(8), **deleteboard**(8), **deletefru**(8), **setupfru**(8), **showdcl**(8), **showdomainstatus**(8), **showfru**(8), **showhardconf**(8), **testsb**(8), **unlockmaintenance**(8)

NAME

reset - reset the specified domain

SYNOPSIS

reset [[-q] -{y|n}] -d *domain_id level*

reset -h

DESCRIPTION

Note – Since the reset(8) command forcibly resets the system, this command may cause a failure in a hard disk drive or other components. Use this command only for the purpose of recovery, such as if the Oracle Solaris OS hangs, and for other limited purposes.

The reset(8) command resets the specified domain.

The following three levels of resetting can be specified:

por	Resets the domain system.
panic	Instructs the Oracle Solaris OS of the domain to generate a panic. The command is ignored if it is issued during power-off or shutdown.
xir	Resets the domain CPU.

Privileges

You must have one of the following privileges to run this command:

platadm, fieldeng	Can run this command for all domains.
domainadm, domainmgr	Can run this command only for your managed domains.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-d *domain_id*	Specifies only one ID of the domain to be reset. *domain_id* can be 0–23 depending on the system configuration.
-h	Displays usage statement. When used with other options or operands, an error occurs.
-n	Automatically answers "n" (no) to all prompts.
-q	Suppresses all messages to stdout, including prompts.
-y	Automatically answers "y" (yes) to all prompts.

OPERANDS

The following operand is supported:

level Specifies the level of resetting. One of the following can be specified. This operand cannot be omitted.

`por`	Resets the domain system.
`panic`	Instructs the Oracle Solaris OS of the domain to generate a panic.
`xir`	Resets the domain CPU.

EXTENDED DESCRIPTION

- When the command is executed, a prompt to confirm execution of the command with the specified options is displayed. Enter "**y**" to execute the command or "**n**" to cancel the command.
- The `showdomainstatus`(8) command can be used to check whether the domain has been reset.
- If the `reset`(8) command is executed under either of the following conditions, processing is stopped before the Oracle Solaris OS is started:
  - The Mode switch on the operator panel is set to Service mode
  - The auto boot function has been disabled by the `setdomainmode` (8) command

EXAMPLES

EXAMPLE 1 Causes a panic in domain ID 0.

```
XSCF> reset -d 0 panic
DomainID to panic:00
Continue? [y|n]:y
00:Panicked

*Note*
 This command only issues the instruction to reset.
 The result of the instruction can be checked by the "showlogs power".
```

EXAMPLE 2 Resets the CPU in domain ID 0. Automatically answers "`y`" to all prompts.

```
XSCF> reset -y -d 0 xir
DomainID to reset:00
Continue? [y|n]:y
00:Reset

*Note*
 This command only issues the instruction to reset.
 The result of the instruction can be checked by the "showlogs power".
```

EXAMPLE 3 Resets domain ID 0. Suppresses prompts, and automatically answers "y" to all prompts.

```
XSCF> reset -q -y -d 0 por
```

EXAMPLE 4 Cancels the reset command execution that is in progress.

```
XSCF> reset -d 0 panic
DomainID to panic:00
Continue? [y|n]:n
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

poweroff(8), **poweron**(8), **setdomainmode**(8), **showdomainstatus**(8)

NAME

resetdateoffset - reset time of domains to match system time

SYNOPSIS

resetdateoffset

resetdateoffset -h

DESCRIPTION

The resetdateoffset(8) command resets the time settings on the domains, managed by each domain clock, to match the time setting of the system, which is managed by the XSCF clock.

If you change the time setting on a domain, for example by using the date(1M) command, the time of that domain differs from the time of the system. The difference between revised time of the domain and the time of the system is stored on the XSCF, and is retained after domain reboot and after XSCF reset.

Execute the resetdateoffset(8) command to realign the time on the domains with the time of the system. After this, the time of domain after rebooting will match the time of the system.

Privileges

You must have platadm or fieldeng privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following option is supported:

-h Displays usage statement.

EXTENDED DESCRIPTION

You can execute the resetdateoffset(8) command only when all domains are powered off. To verify that all domains are powered off, execute the showlogs power command and look for the value System Power Off.

EXAMPLES

EXAMPLE 1 Resets the time of the domains to match that of the system.

```
XSCF> resetdateoffset
```

EXIT STATUS

The following exit values are returned:

0 Successful completion.

>0 An error occurred.

SEE ALSO

showdateoffset(8)

NAME

restoreconfig - restore the system configuration information previously saved by dumpconfig

SYNOPSIS

restoreconfig [-v] [-V] [[-q] -{y|n}] [-P *password*] [-s network={yes|no}] [-u user] [-p proxy [-t *proxy_type*]] *url*

restoreconfig -h

DESCRIPTION

The restoreconfig(8) command restores to the XSCF the system configuration information previously saved using the dumpconfig(8) command.

The command verifies the integrity of the configuration file, looks for network information, and detects whether the configuration file version and system class are compatible.

Privileges

You must have platadm privileges to run this command. Reserved user accounts default and admin can also run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-h	Displays usage statement. When used with other options or operands, an error occurs.
-n	Automatically answers "n" (no) to all prompts.
-P *password*	The password to decode an encrypted file. The command prompts for the password if a password is not provided on the command line.
-p *proxy*	Specifies the proxy server to be used for transfers. The default transfer type is http, unless modified using the -t *proxy_type* option. The value for proxy must be in the format *servername*:*port*. (Refer to Example 3.)
-q	Suppresses all messages to stdout, including prompts.
-s network={yes|no}	force/prevent restoration of the network configuration. If network=yes, the network configuration data is restored. If network=no, the network configuration data is not restored. If this option is not specified, the serial number of the target system is compared with the serial number of the configuration file and if the numbers match, the configuration data is restored.

`-t` *proxy_type*	Used with the `-p` option to specify the type of proxy. Possible values for *proxy_type* are: `http`, `socks4`, and `socks5`. The default value is `http`.
`-u` *user*	Specifies the user name when logging in to a remote ftp or http server that requires authentication. You are prompted for a password.
`-v`	Displays verbose output. This may be helpful when diagnosing server problems.
`-V`	Displays details of network activity. This may be helpful when diagnosing network or server problems.
`-y`	Automatically answers `"y"` (`yes`) to all prompts.

OPERANDS

The following operand is supported:

url Specifies the URL of the firmware image to download. Supported formats for this value include the following:

`http://`*server*`[:`*port*`]/`*path*`/`*file*

`https://`*server*`[:`*port*`]/`*path*`/`*file*

`ftp://`*server*`[:`*port*`]/`*path*`/`*file*

`file:///media/usb_msd/`*path*`/`*file*

EXTENDED DESCRIPTION

Basic identification information is included in plain text at the top of the configuration file. You can use any text viewer to determine information such as:

- which system created the backup configuration
- when the backup was created
- if the backup is encrypted

All the domains must be turned off before this command can be used.

`restoreconfig`(8) downloads and validates the configuration file to the XSCF, then resets the XSCF with the configuration information restored. The system then halts the XSCF unit (both XSCF units on the M8000/M9000 server). At this point, verify that the XSCF unit(s) have been halted, cut power to the system, wait at least 30 seconds, then restore power.

Note that the configuration data file can be restored only to the same class of server; that is, a configuration file created by `dumpconfig`(8) on an M5000 server can be restored to another M5000 server, but it cannot be restored to an M3000 or M8000 server.

EXAMPLES

EXAMPLE 1 Restoring the Configuration using FTP

```
XSCF> restoreconfig -V -u manilla 129.145.155.156:8080 \
ftp:/10.7.79.18/sollgell/proxytest-ftp.cfg
transfer from '/tmp/dumpconfig.EvY1Yf' to 'ftp://10.7.79.18/sollgell/
proxytest-ftp.cfg'
Password:
* About to connect() to 129.145.155.166 port 8080
*   Trying 129.145.155.166... * connected
* Connected to 129.145.155.166 (129.145.155.166) port 8080
* Proxy auth using (nil) with user ''
* Server auth using Basic with user 'minilla'
> GET ftp://10.7.79.18/sollgell/proxytest-ftp.cfg HTTP/1.1
Authorization: Basic bHdhbmc6bHdhbmc=
User-Agent: restoreconfig
Host: 10.7.79.18:21
Pragma: no-cache
Accept: */*
< HTTP/1.1 200 OK
< Server: Sun-Java-System-Web-Proxy-Server/4.0
< Date: Thu, 07 Aug 2008 18:01:00 GMT
< Proxy-agent: Sun-Java-System-Web-Proxy-Server/4.0
< Via: 1.1 proxy-proxy
< Transfer-encoding: chunked
* Connection #0 to host 129.145.155.166 left intact
* Closing connection #0
Configuration backup created on Mon Aug  4 12:58:19 2008
 from system 'M3000' with serial number 'IKS08220xx', version '19830000'
*** 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]: y
requesting XSCF reboot to perform restore ... requested
Connection to ghidorah.com closed by foreign host.
```

EXAMPLE 2 Restoring the Configuration Using http

```
XSCF> restoreconfig -V -p 129.145.155.166:8080 \
http://10.7.79.18/sollgell/proxytest.cfg
transfer from '/scf/firmtmp/hcp/config/config_file.bin' to
'http://10.7.79.18/sollgell/proxytest.cfg'
* About to connect() to 129.145.155.166 port 8080
*   Trying 129.145.155.166... * connected
* Connected to 129.145.155.166 (129.145.155.166) port 8080
GET http://10.7.79.18/sollgell/proxytest.cfg HTTP/1.1
User-Agent: restoreconfig
Host: 10.7.79.18
Pragma: no-cache
```

```
Accept: */*
< HTTP/1.1 200 OK
< Content-length: 24603
< Content-type: text/plain
< Date: Thu, 07 Aug 2008 17:07:43 GMT
< Server: Apache/1.3.36 (Unix) mod_perl/1.29 mod_ssl/2.8.27 OpenSSL/
0.9.7d
< Last-modified: Mon, 04 Aug 2008 20:01:51 GMT
< Etag: "4fa2a-601b-4897602f"
< Accept-ranges: bytes
< Via: 1.1 proxy-proxy
< Proxy-agent: Sun-Java-System-Web-Proxy-Server/4.0
* Connection #0 to host 129.145.155.166 left intact
* Closing connection #0
Configuration backup created on Mon Aug  4 12:58:19 2008
 from system 'M3000' with serial number 'IKS08220xx', version '19830000'
*** 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]: y
requesting XSCF reboot to perform restore ... requested
Connection to ghidorah.com closed by foreign host.
```

EXAMPLE 3 Restoring the Configuration Using https

```
XSCF> restoreconfig -v -V \
https://10.7.79.18/sollgell/proxytest.cfg
obtaining lock ... done
initiating file transfer from 'https://10.7.79.18/sollgell/proxytest.cfg'
... transfer from
'/scf/firmtmp/hcp/config/config_file.bin' to 'https://10.7.79.18/
sollgell/proxytest.cfg'
* About to connect() to 10.7.79.18 port 443
*   Trying 10.7.79.18... * connected
* Connected to 10.7.79.18 (10.7.79.18) port 443
* error setting certificate verify locations, continuing anyway:
*  CAfile: /home/ares/cross/fje/pwrqcc3/target_root/usr/share/ssl/certs/
ca-bundle.crt
 CApath: none
* SSL connection using EDH-RSA-DES-CBC3-SHA
* Server certificate:
*        subject:
/C=US/ST=California/L=SanDiego/O=toho/OU=QT/CN=10.7.79.18/
emailAddress=minilla.zilla@toho.com
*        start date: 2008-07-22 18:32:49 GMT
*        expire date: 2009-07-22 18:32:49 GMT
*        common name: 10.7.79.18 (matched)
```

```
*        issuer:
/C=US/ST=California/L=SanDiego/O=toho/OU=QT/CN=Lwang/
emailAddress=minilla.zilla@toho.com
* SSL certificate verify result: error number 1 (20), continuing anyway.
> GET /sollgell/proxytest.cfg HTTP/1.1
User-Agent: restoreconfig
Host: 10.7.79.18
Pragma: no-cache
Accept: */*
< HTTP/1.1 200 OK
< Date: Tue, 12 Aug 2008 22:02:12 GMT
< Server: Apache/1.3.36 (Unix) mod_perl/1.29 mod_ssl/2.8.27 OpenSSL/
0.9.7d
< Last-Modified: Mon, 04 Aug 2008 20:01:51 GMT
< ETag: "4fa2a-601b-4897602f"
< Accept-Ranges: bytes
< Content-Length: 24603
< Content-Type: text/plain
* Connection #0 to host 10.7.79.18 left intact
* Closing connection #0
done
file decoding done.
Configuration backup created on Mon Aug  4 12:58:19 2008
 from system ‘M3000’ with serial number ‘IKS08220xx’, version ‘19830000’
validating backup configuration data
*** 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]: y
requesting XSCF reboot to perform restore ... requested
Connection to ghidorah.com closed by foreign host.
```

EXAMPLE 4 Restoring the Configuration Using USB

```
XSCF> restoreconfig -V -p 129.145.155.166:8080 \
file:///media/usb_msd/proxytest.cfg
transfer from ’/scf/firmtmp/hcp/config/config_file.bin’ to ’file:///
media/usb_msd/proxytest.cfg’
Configuration backup created on Mon Aug  4 14:38:27 2008
 from system ’M3000’ with serial number ’IKS08220xx’, version ’19830000’
*** 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]: y
requesting XSCF reboot to perform restore ... requested
Connection to ghidorah.com closed by foreign host.
```

EXAMPLE 5 Restoring An Encrypted Configuration

```
XSCF> restoreconfig -v -V -P encryption \
http://10.7.79.18/sollgell/proxytest.cfg
obtaining lock ... done
initiating file transfer from 'http://10.7.79.18/sollgell/proxytest.cfg'
... transfer from '/scf/firmtmp/hcp/config/config_file.bin' to
'http://10.7.79.18/sollgell/proxytest.cfg'
* About to connect() to 10.7.79.18 port 80
*   Trying 10.7.79.18... * connected
* Connected to 10.7.79.18 (10.7.79.18) port 80
GET /sollgell/proxytest.cfg HTTP/1.1
User-Agent: restoreconfig
Host: 10.7.79.18
Pragma: no-cache
Accept: */*
< HTTP/1.1 200 OK
< Date: Wed, 13 Aug 2008 23:29:42 GMT
< Server: Apache/1.3.36 (Unix) mod_perl/1.29 mod_ssl/2.8.27
OpenSSL/0.9.7d
< Last-Modified: Wed, 13 Aug 2008 23:25:16 GMT
< ETag: "4fa55-501b-48a36d5c"
< Accept-Ranges: bytes
< Content-Length: 20507
< Content-Type: text/plain
* Connection #0 to host 10.7.79.18 left intact
* Closing connection #0
done
file decoding done.
Configuration backup created on Wed Aug 13 16:21:01 2008
 from system 'M3000' with serial number 'IKS08220xx', version
'19830000'
validating backup configuration data
File decryption completed
*** 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]: y
requesting XSCF reboot to perform restore ... requested
Connection to ghidorah.com closed by foreign host.
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

NAME

restoredefaults - restore factory settings of the server or XSCF unit

SYNOPSIS

restoredefaults -c *range*

restoredefaults -h

DESCRIPTION

The restoredefaults(8) command restores factory settings and error information on either the server or the XSCF unit.

To execute this command, connect to the XSCF over a serial connection.

Used with the -c option, *range* is either factory, which restores settings and information to the server, or xscfu, which does so only to the specified XSCF unit.

Privileges

You must have platadm privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-c *range*

Specifies the target of restoration. In *range*, one of the following values can be specified:

factory

Restores the server (Operator panel and the XSCF unit) to factory settings. Clears information set by the user and error information of the Field Replaceable Unit (FRU).

Cannot be specified in the standby XSCF of the M8000/M9000 server.

xscfu

Restores the XSCF unit to factory settings. When the active XSCF of an M8000/M9000 server is specified, both the active and standby XSCF are restored. When the standby XSCF is specified, only the standby XSCF is restored. In both cases, user settings and error information of the Field Replaceable Unit (FRU) are cleared.

-h

Displays usage statement. When used with other options or operands, an error occurs.

EXTENDED DESCRIPTION

- After the restoredefaults(8) command has been executed, the restored XSCF unit will be stopped. To restart it, power the server off, then on.
- You can execute the restoredefaults(8) command only when the all domains are powered off. To verify that all domains are powered off, execute the showlogs power command and look for the value System Power Off.

- If you need to move the XSCF unit to another server, please specify "`-c xscfu`". The XSCF unit is restored to its factory state and the server is powered off. You can then move it to another server.
- If you specify "`-c xscfu`", information in the operator panel remains. Therefore, when the server is powered off then on, the information saved in the operator panel is read and the XSCF unit is restored to its previous state. At this point, the XSCF unit contains information about this server and must not be moved to another server.

EXAMPLES

EXAMPLE 1 Restores the XSCF unit.

```
XSCF> restoredefaults -c xscfu

WARNING:
 If this system does not have OPNL, this command will set all the user
 settable XSCF configuration parameters to their default value as they
 were set when the system was shipped out.
 Furthemore, this command will delete all logs on both XSCFUs.
 Check the man page of this command before you run it.

Continue?[yes/no](default no):yes
You must check the following points.

 1. Have the ability to powercycle the system.
 2. Have access to the serial console and hold the serial console of the
    XSCFU to confirm the completion of the command.

If you answer "yes" this command will HALT the XSCFU when it compltetes.
You will need to powercycle the system after the XSCF BOOT STOP.

Do you really want to continue?

Continue?[yes/no](default no):yes
The initialization of XSCFU will be started.
 XSCFU : all data clear
 OPNL  : not clear
XSCF will be automatically rebooted. Afterwards, XSCFU will be
initialized.
Continue?[yes/no](default no):yes
The NVRAM setting of XSCFU#0 was completed.
XSCF shutdown request was completed.

             <snip>....XSCF reboot..<snip>

***** WARNING *****
```

```
XSCF initialization terminate for XSCF data clear.
execute "setdefaults xscf" (AUTO)

setdefaults : XSCF clear : start
setdefaults : XSCF clear : DBS start
setdefaults : XSCF clear : wait 20s for DBS initialization
setdefaults : XSCF clear : common database clear complete
setdefaults : XSCF clear : /bin/rm /var/log/lastlog >/dev/null 2>&1
setdefaults : XSCF clear : /bin/rm /var/log/boot.log >/dev/null 2>&1
...
setdefaults : XSCF clear : /bin/rm /hcpcommon/tmp/panel_up_to_date_fail
>/dev/null 2>&1
setdefaults : XSCF clear : log data clear complete
setdefaults : XSCF clear : NVRAM(PAGE#0) clear complete
...
setdefaults : XSCF clear : NVRAM(PAGE#7) clear complete
setdefaults : XSCF clear : NVRAM reset complete
...
setdefaults : XSCF clear : unmount filesystem start
dbs[282]: NOTICE: received signal: 15
setdefaults : XSCF clear : unmount /hcp0/linux
...
setdefaults : XSCF clear : unmount /hcpcommon/firmtmp  --  complete
setdefaults : XSCF clear : unmount filesystem complete
setdefaults : XSCF clear : end
setdefaults : complete

Please turn off the breaker after XSCF halt.

The system is going down NOW !!
Please stand by while rebooting the system.
Restarting system.
XSCF uboot  01950000  (Apr  15 2007 - 11:08:18)


XSCF uboot  01950000  (Apr  15 2007 - 11:08:18)

SCF board boot factor = a040
 DDR Real size: 512 MB
 DDR: 480 MB


XSCF BOOT STOP (recover by NFB-OFF/ON)
```

EXAMPLE 2 Restores the server.

```
XSCF> restoredefaults -c factory

WARNING:
 If this system does not have OPNL, this command will set all the user
 settable XSCF configuration parameters to their default value as they
 were set when the system was shipped out.
 Furthemore, this command will delete all logs on both XSCFUs.
 Check the man page of this command before you run it.

Continue?[yes/no](default no):yes
You must check the following points.

 1. Have the ability to powercycle the system.
 2. Have access to the serial console and hold the serial console of the
    XSCFU to confirm the completion of the command.

If you answer "yes" this command will HALT the XSCFU when it compltetes.
You will need to powercycle the system after the XSCF BOOT STOP.

Do you really want to continue?

Continue?[yes/no](default no):yes
The initialization of XSCFU will be started.
 XSCFU : all data clear
 OPNL  : all data clear (exclude SYSTEM ID data)
XSCF will be automatically rebooted. Afterwards, XSCFU will be
initialized.
Continue?[yes/no](default no):yes
The NVRAM setting of XSCFU#0 was completed.
XSCF shutdown request was completed.

             <snip>....XSCF reboot..<snip>

***** WARNING *****
XSCF initialization terminate for XSCF/OPNL data clear.
execute "setdefaults factory" (AUTO)

setdefaults : FACTORY mode clear : start
setdefaults : FACTORY mode clear : DBS start
setdefaults : FACTORY mode clear : wait 20s for DBS initialization
initialize OPNL SEEPROM 1/6  --  complete
...
initialize OPNL SEEPROM 6/6  --  complete
setdefaults : FACTORY mode clear : OPNL reset complete
```

```
setdefaults : FACTORY mode clear : restore SYSTEM-ID data complete
setdefaults : FACTORY mode clear : /bin/rm /var/log/lastlog >/dev/null
2>&1
setdefaults : FACTORY mode clear : /bin/rm /var/log/boot.log >/dev/null
2>&1
...
setdefaults : FACTORY mode clear : /bin/rm /hcpcommon/tmp/
panel_up_to_date_fail >/dev...
setdefaults : FACTORY mode clear : log data clear complete
setdefaults : FACTORY mode clear : NVRAM(PAGE#0) clear complete
...
setdefaults : FACTORY mode clear : NVRAM(PAGE#7) clear complete
setdefaults : FACTORY mode clear : NVRAM reset complete
...
setdefaults : FACTORY mode clear : unmount filesystem start
dbs[283]: NOTICE: received signal: 15
setdefaults : FACTORY mode clear : unmount /hcp0/linux
...
setdefaults : FACTORY mode clear : unmount /hcpcommon/firmtmp  --
complete
setdefaults : FACTORY mode clear : unmount filesystem complete
Please stand by while rebooting the system.
Restarting system.
XSCF uboot  01950000  (Apr  15 2007 - 11:08:18)


XSCF uboot  01950000  (Apr  15 2007 - 11:08:18)

SCF board boot factor = 4040
 DDR Real size: 512 MB
 DDR: 480 MB


XSCF BOOT STOP (recover by NFB-OFF/ON)
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

NAME

sendbreak - send a break signal to the specified domain

SYNOPSIS

sendbreak -d *domain_id*

sendbreak [[-q] -{y|n}] -d *domain_id*

sendbreak -h

DESCRIPTION

The sendbreak(8) command sends a break signal to the specified domain.

When a break signal is sent from the domain console to the Oracle Solaris OS of the domain, control is transferred from the Oracle Solaris OS to OpenBoot PROM and the OpenBoot PROM prompt "ok" is displayed.

Note – sendbreak(8) command will not work when the secure mode is set to 'on' while the mode switch on the operator panel is set to "Locked". Refer to the setdomainmode(8) for more information.

Privileges

You must have one of the following privileges to run this command:

platadm	Can run this command for all domains.
domainadm	Can run this command only for your managed domains.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-d *domain_id*	Specifies only one ID of the domain to which to send the break signal. *domain_id* can be 0–23 depending on the system configuration.
-h	Displays usage statement. When used with other options or operands, an error occurs.
-n	Automatically answers "n" (no) to all prompts.
-q	Suppresses all messages to stdout, including prompts.
-y	Automatically answers "y" (yes) to all prompts.

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

console(8), **showconsolepath**(8)

NAME

setad - configure Active Directory

SYNOPSIS

setad enable | disable

setad loadcert [[-q] -{y|n}] [-i *n*] [-u *username*] [-p *proxy* [-t *proxy_type*]] *URI*

setad loadcert [[-q] -{y|n}] [-i *n*] console

setad rmcert [[-q] -{y|n}] [-i *n*]

setad group administrator -i *n* name [*groupname*]

setad group operator -i *n* name [*groupname*]

setad group custom -i *n* name [*groupname*]

setad group custom -i *n* roles [*privileges*]

setad userdomain -i *n* [*domainname*]

setad defaultrole [*privileges*]

setad timeout *seconds*

setad server [-i *n*] [*ipaddr* [:*port*]]

setad logdetail none | high | medium | low | trace

setad log [[-q] -{y|n}] clear

setad dnslocatormode | expsearchmode | strictcertmode enable | disable

setad dnslocatorquery -i *n* [*service*]

setad default [[-q] -{y|n}]

setad -h

DESCRIPTION

setad(8) configures Active Directory. To simply enable or disable Active Directory, execute the command with only those operands. To enable or disable an Active Directory mode, such as dnslocatormode, specify the mode along with enable or disable.

To clear or unset a property, issue a setad command with no value for the operand. For example, setad group custom -i 1 name clears the name property from custom group 1. If a property is not set, it is displayed with no value.

Note – If you are an Active Directory or LDAP/SSL user, do not upload a public key. If one has already been uploaded, use the following command to delete it:
XSCF> **setssh -c delpubkey -a -u proxyuser**

Privileges

You must have useradm privileges to run this command.

Refer to `setprivileges`(8) for more information.

OPTIONS

The following options are supported:

`-h`	Displays usage statement. When used with other options or operands, an error occurs.
`-i` *n*	Sets an index marker, value 1 - 5.
`-n`	Automatically answers "`n`" (no) to all prompts.
`-p`	Specifies the proxy server to be used for transfers. The default transfer type is `http`, unless modified using the `-t` *proxy_type* option. The value for proxy must be in the format *servername*:*port*. See EXAMPLE 8.
`-q`	Suppresses all messages to stdout, including prompts.
`-t`	Use with the `-p` option to specify proxy type as `http`, `socks4`, or `socks5`. The default is `http`.
`-u`	Specifies the user name when logging in to a remote ftp or http server that requires authentication. Prompts for a password. See EXAMPLE 9.
`-y`	Automatically answers "`y`" (yes) to all prompts.

OPERANDS

The following operands are supported:

enable|disable	When used with no other operands, enable or disable the Active Directory feature.
loadcert	`loadcert console` prompts for certificate information to be entered at the console. Use this command to paste certificate information copied from a file. Terminate input with `CTRL-D`. `loadcert` *URI* loads a certificate file for the Active Directory server. Supported formats for *URI* are: `http://server[:port]/path/file` `https://`*server*`[:`*port*`]/`*path*`/`*file* `ftp://`*server*`[:`*port*`]/`*path*`/`*file* `file:///media/usb_msd/`*path*`/`*file*
rmcert	Delete certificate file for the Active Directory server. strictcertmode must be in the disabled state for a certificate to be removed.

group administrator	Assign group name for up to five specified administrator groups. The administrator group has platadm, useradm, and auditadm privileges and you cannot change that.
group operator	Assign group name for up to five specified operator groups. The operator group has platop and auditop privileges and you cannot change that.
group custom	Assign group name and privileges for up to five groups.
userdomain	Configure the specified user domain. A user domain can be configured explicitly through the **setad userdomain** command on XSCF, or entered at the login prompt using the form, *user@domain*. • If a user domain is specified at the login prompt – for example, `login`: **ima.admin@dc01.example.com** – that user domain is used for this login attempt. Any pre-configured user domains (as displayed by **showad userdomain**) are ignored. • If a user domain is not specified at the login prompt – for example, `login`: **ima.admin** – XSCF checks each of the pre-configured user domains, in turn, to authenticate the user. See EXAMPLE 6, below, for important information.
defaultrole	Configure default privileges. If defaultrole is configured, users have privileges as specified by defaultrole after authentication; user group membership is not checked. If defaultrole is not configured, users' privileges will be learned from Active Directory based on group membership.
timeout	Configure transaction timeout, in seconds. *seconds* can be 1 to 20. The default is 4. If the specified timeout is too brief for the configuration, the login process or retrieval of user privilege settings could fail.
server	Configure the primary and up to five alternate Active Directory servers. To use a host name, DNS must be enabled. An IP address can be specified with port number; otherwise, the default port is used.

logdetail

Enable logging of Active Directory authentication and authorization diagnostic messages at the specified detail level. This log is for use in troubleshooting and is cleared on SP reboot. Level can be one of the following:

none	Do not log diagnostic messages. Use this setting during normal system operation
high	Log only high-severity diagnostic messages
medium	Log only high-severity and medium-severity diagnostic messages
low	Log high-severity, medium-severity, and informational diagnostic messages
trace	Log high-severity, medium-severity, informational, and trace-level diagnostic messages

log [*options*] clear

Clear the log file of Active Directory authentication and authorization diagnostic messages.

dnslocatormode

Enable or disable DNS locator mode. This mode is disabled by default. If enabled, XSCF queries a DNS server to learn the Active Directory server to use for user authentication.

expsearchmode

Enable or disable expanded search mode. The default Active Directory functionality is intentionally restrictive to ensure proper security. Search criteria can be expanded to accommodate specific customer environments. The expanded search mode is disabled by default, which means the UserPrincipalName (UPN) is expected to have a fully qualified domain name suffix. When expanded search mode is enabled, more searches are attempted if the more specific UPN search does not immediately succeed.

strictcertmode	Enable or disable strictcertmode mode. This mode is disabled by default; the channel is secure, but limited validation of the certificate is performed. If strictcertmode is enabled, the server's certificate must have already been uploaded to the server so that the certificate signatures can be validated when the server certificate is presented. Data is always protected, even if strictcertmode is disabled. Strictcertmode applies to primary and alternate servers alike.
dnslocatorquery	Configure the DNS locator query. DNS and DNS Locator Mode must be enabled for DNS Locator Queries to work. The DNS Locator service query identifies the named DNS service. See EXAMPLES, below, for important information.
default	Reset Active Directory settings to factory default.

EXAMPLES

EXAMPLE 1 Configures the Active Directory primary server, specifying a port other than the default.

```
XSCF> setad server 10.1.12.250:4040
```

EXAMPLE 2 Sets name for administrator group 3.

```
XSCF> setad group administrator -i 3 name CN=spSuperAdmin, \
OU=Groups,DC=Sales,DC=aCompany,DC=com
```

EXAMPLE 3 Sets name for custom group 2.

```
XSCF> setad group custom -i 2 name CN=spLimitedAdmin, \
OU=Groups,DC=Sales,DC=aCompany,DC=com
```

EXAMPLE 4 Sets roles for custom group 2.

```
XSCF> setad group custom -i 2 roles auditadm,platop
```

EXAMPLE 5 Loads certificate information for Alternate Server 4 from the console.

```
XSCF> setad loadcert -i 4 console
Warning: About to load certificate for Alternate Server 4:
Continue? [y|n]: y
Please enter the certificate:

-----BEGIN CERTIFICATE-----
MIIETjCCAzagAwIBAgIBADANBgkqhkiG9w0BAQQFADB8MQswCQYDVQQGEwJVUzET
MBEGA1UECBMKQ2FsaWZvcm5pYTESMBAGA1UEBxMJU2FuIERpZWdvMRkwFwYDVQQK
ExBTdW4gTWljcm9zeXN0ZW1zMRUwEwYDVQQLEwxTeXN0ZW0gR3JvdXAxEjAQBgNV
...
```

```
-----END CERTIFICATE-----
CTRL-D
XSCF>
```

EXAMPLE 6 Configures user domain 2. <USERNAME> is a template that must be entered exactly as shown. During authentication the user's login name replaces <USERNAME>. `userdomain` can take the form of UPN or Distinguished Name (DN).

```
XSCF> setad userdomain -i 2 '<USERNAME>@yoshi.example.aCompany.com'
```

EXAMPLE 7 Loads a server certificate for Active Directory using the specified URI.

```
XSCF> setad loadcert http://domain_2/UID_2333/testcert
```

EXAMPLE 8 Loads a server certificate for Active Directory using an http Proxy Server with port 8080 .

```
XSCF> setad loadcert -p webproxy.aCompany.com:8080 \
http://domain_2/UID_2333/testcert
```

EXAMPLE 9 Loads a server certificate for Active Directory using a username and password.

```
XSCF> setad loadcert -u yoshi \
http://domain_2/UID_2333/testcert
```

EXAMPLE 10 Removes the certificate for alternate server 3.

```
XSCF> setad rmcert -i 3
```

EXAMPLE 11 Sets logging of high-severity diagnostic messages.

```
XSCF> setad logdetail high
```

EXAMPLE 12 Clears diagnostic messages from the log file, answering Yes to all prompts.

```
XSCF> setad log -y clear
```

EXAMPLE 13 Enables strictcertmode.

```
XSCF> setad strictcertmode enable
```

EXAMPLE 14 Configures the dnslocatorquery configuration. *service* represents the DNS query to be performed. The port ID is generally part of the record, but you can override it by using the format <PORT:*portnumber*>. Also, named services specific for the domain being authenticated can be specified by using the <DOMAIN> substitution marker.

```
XSCF> setad dnslocatorquery -i 2 \
'_ldap._tcp.gc._msdcs.<DOMAIN>.<PORT:3269>'
```

EXAMPLE 15 Configures the default privileges, where *privileges* are the same as those used in the `setad group custom roles` command.

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

EXIT STATUS

The following exit values are returned:

`0`	Successful completion.
`>0`	An error occurred.

SEE ALSO

showad `(8)`

NAME

setaltitude - set the altitude of the system or whether or not the air filter installed

SYNOPSIS

setaltitude -s *key=value*

setaltitude -h

DESCRIPTION

The setaltitude(8) command sets the altitude of the system or whether or not the air filter installed.

Whether or not the air filter installed can be specified on the M4000/M5000 servers only.

Privileges

You must have platadm or fieldeng privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-h — Displays usage statement. When used with other options or operands, an error occurs.

-s *key=value* — The item to be set is specified by *key*. The following value can be specified:

- altitude — Sets the altitude of the system.
- filter — Sets whether or not to install the air filter. You can specify this on the M4000/M5000 servers only.

When you specified altitude as *key*, specify the altitude of the system in *value* in units of meters (m). An integer equal to or greater than 0 can be specified, and the specified value is rounded up to the nearest hundred meters. The default value is 0 meters.

When you specified filter as *key*, either of the following can be specified for value:

- installed — Air filter is installed.
- uninstalled — Air filter is not installed.

EXTENDED DESCRIPTION

- If the altitude of the system is set, any abnormality in the intake air temperature can be detected quickly. If the altitude of the system is unknown, set a high value. However, even if no altitude is set for the system, any abnormality in temperatures such as the CPU temperature can still be detected, so the system would not be damaged by a fatal error.

- To apply the specified configuration, execute the `rebootxscf`(8) command and reset XSCF.
- The command does not accept negative numbers. If the system is below sea-level use `altitude=0`.
- When you specified either of the altitude of the system or whether or not the air filter installed, the current settings are listed. The setting of the air filter is displayed only when it is set to `installed`.
- When the `showaltitude`(8) command is executed, the current settings are displayed.

EXAMPLES

EXAMPLE 1 Sets the altitude of the system to 1000 m.

```
XSCF> setaltitude -s altitude=1000
1000m
```

EXAMPLE 2 Sets the altitude of the system to 200 m. The specified value is rounded up to the nearest hundred meters.

```
XSCF> setaltitude -s altitude=157
200m
```

EXAMPLE 3 Sets the altitude of the system to 1000 m, on the M4000/M5000 servers with the air filter installed.

```
XSCF> setaltitude -s altitude=1000
1000m
Filter is installed.
```

EXAMPLE 4 Sets the air filter uninstalled, on the M4000/M5000 servers.

```
XSCF> setaltitude -s filter=uninstalled
1000m
```

EXIT STATUS

The following exit values are returned:

`0`	Successful completion.
`>0`	An error occurred.

SEE ALSO

rebootxscf`(8)`, **showaltitude**`(8)`

NAME

setarchiving - configure the log archiving functionality

SYNOPSIS

setarchiving [-k *host-key*] [-l *audit-limit,non-audit-limit*] [-p *password*|-r] [-t *user@host:directory*] [-v] [-y|-n]

setarchiving enable|disable

setarchiving -h

DESCRIPTION

setarchiving(8) manages the log archiving configuration. Persistent storage space on the Service Processor is limited. Some logs may grow to the point where old log entries must be overwritten or deleted. Log archiving allows the user to set up the Service Processor to automatically archive its log data on a remote host.

Note – Logs archived on the archive host should be rotated at regular intervals to avoid loss of log information. Use logadm(1M) to configure log rotation on a system that runs the Oracle Solaris OS.

Note – You must set up the archive host correctly prior to enabling the log archiving feature. (See EXAMPLE 1.) If you attempt to enable archiving while the configuration is invalid (for example, if the specified archive host does not exist), setarchiving exits with an error message. setarchiving exits with an error message if you request invalid configuration changes while archiving is enabled.

Note – setarchiving(8) requires at least one option or operand.

Privileges

You must have platadm privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS The following options are supported:

`-h`

Displays usage statement.

When used with other options or operands, an error occurs.

`-k` *host-key*

Sets the public key that XSCF uses to verify the identity of the host. Possible values for the *host-key* are shown here:

`none`

This literal value specifies that a public key should not be used to authenticate the archive host. If an archive host public key was previously configured, it is deleted.

`download`

This literal value specifies that `setarchiving` should download the public host key from the archive host using the `SSH` protocol. If the `t` option is used, `setarchiving` downloads the key from the host specified in the argument to `-t`. Otherwise, `setarchiving` downloads the key from the current archive host. Next, `setarchiving` displays the key's `md5` fingerprint and prompts you for confirmation of the identity of the host to continue. If you accept the key, it is saved and used for server authentication. If you reject the key, `setarchiving` exits without changing the configuration.

public-key

The specified public key is stored and used for server authentication. The *host-key* argument should be the complete *public-key* for the archive host, beginning with the key type.

Note – The *public-key* should be enclosed in quotes to ensure that the shell treats it as a single word.

`-l` *audit-limit,non-audit-limit* Sets the space limits for log archives in megabytes. The option argument must consist of two values separated by a comma.

The *audit-limit* value specifies the archive space limit for audit logs. It must be either `0` (zero), `unlimited` or an integer in the range of 500–50000. If you do not use the `-l` option to modify the value of *audit-limit*, the initial archive space limit for audit logs is unlimited.

The *non-audit-limit* value specifies the archive space limit for all other logs, in megabytes. It must be an integer in the range of 500–50000. If unset, the initial value for *non-audit-limit* depends on the type of server. Use the `showarchiving`(8) command to determine the value for your server.

If either of the specified values is invalid, the command displays an error and exits without making any changes.

`-n` Automatically answers "`n`" (no) to all prompts. Prompts are displayed.

`-p` *password* Sets the password used for `ssh` login. This option is provided to facilitate scripting. To change the password interactively, use the `-r` option.

`-r` Reads the password used for `ssh` login. The `setarchiving` command displays a prompt and reads the new password without echoing it to the screen.

`-t` *user@host:directory* Sets the archive target. The *host* field specifies the host name or IP address of the archive host. The *user* field specifies the user name for the `ssh` login to the archive host. The *directory* field specifies the archive directory on the archive host where the archives should be stored. The directory field must not begin with a "`~`".

`-v` Specifies verbose output. When this option is used in conjunction with `-k download`, `setarchiving` displays the downloaded public key in addition to its `md5` fingerprint.

`-y` Automatically answers "`y`" (yes) to all prompts. Prompts are displayed.

OPERANDS

The following operands are supported:

`enable` Activates the log archiving feature. Cannot be used with any options.

`disable` De-activates the log archiving feature. Cannot be used with any options.

EXAMPLES

EXAMPLE 1 Setting the Archiving Target and Password

```
XSCF> setarchiving -t jsmith@somehost.company.com:/home/jsmith/logs -r
Enter ssh password for jsmith@somehost.company.com:[]
```

EXAMPLE 2 Setting the Public Host Key

```
XSCF> setarchiving -k download
Downloading public host key from somehost.company.com....
Fingerprint: c3:75:f9:97:7d:dc:1e:1e:62:06:c1:6f:87:bc:e8:0d
Accept this public key (yes|no): yes
```

EXAMPLE 3 Setting the Space Limits for Archives

```
XSCF> setarchiving -l 10000,10000
```

EXAMPLE 4 Enabling Archiving

```
XSCF> setarchiving enable
Testing the archiving configuration...
Logs will be archived to somehost.company.com.
```

EXIT STATUS

The following exit values are returned:

`0` Successful completion. Configuration updated.

`>0` An error occurred.

SEE ALSO

showarchiving(8)

NAME

setaudit - manage the system auditing functionality

SYNOPSIS

setaudit enable | disable | archive | delete

setaudit [-p count | suspend] [-m *mailaddr*] [-a *users*=enable | disable | default] [-c *classes*={enable | disable}]... [-e *events*=enable | disable]... [-g {enable | disable}] [-t *percents*]

setaudit -h

DESCRIPTION

setaudit(8) manages the collection of data on the use of system resources. Audit data provides a record of security-related system events. This data can be used to assign responsibility for actions that have taken place on the system. Auditing generates records when specified events occur. Events that generate audit records include:

- System startup and shutdown
- Login and logout
- Authentication actions
- Administrative actions

Privileges

You must have auditadm privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-a *users*=enable|disable|default

Sets the audit record generation policy for the specified users. *users* is a comma-separated list of valid user names.

When set to enable or disable, audit record generation for the users is turned on or off respectively. This setting overrides the global policy for each specified user. To set the global policy for users, use the -g option.

When set to default, the policy for the users is set to follow the global policy. Use showaudit -g to display the global user audit record generation policy.

`-c` *classes*`=enable|disable`

Changes the audit record generation policy for the specified audit classes. *classes* is a comma-separated list of audit classes. A class may be specified by its numeric value or its name. The `ACS_` prefix may be omitted. For example, the class of audit-related events can be expressed as `ACS_AUDIT`, `AUDIT` or `16`.

The following are valid classes:

`all`	Denotes all classes.
`ACS_SYSTEM(1)`	System-related events
`ACS_WRITE(2)`	Commands that can modify a state
`ACS_READ(4)`	Commands that read a current state
`ACS_LOGIN(8)`	Login-related events
`ACS_AUDIT(16)`	Audit-related events
`ACS_DOMAIN(32)`	Domain management–related events
`ACS_USER(64)`	User management–related events
`ACS_PLATFORM(128)`	Platform management–related events
`ACS_MODES(256)`	Mode-related events

This option may be specified multiple times. Multiple specifications are processed together with `-e` options in the order listed. See EXAMPLE 1.

When set to `enable` or `disable`, audit record generation for the specified classes is turned on or off respectively. You can use the `-e` option to override these settings for an individual event.

The class and event audit record generation policy applies to all users. Unique class and event policies cannot be specified for individual users.

`-e` *events*`=enable|disable`

Changes the audit record generation policy for the specified audit events. *events* is a comma-separated list of audit events. An event may be specified by its numeric value or its name. The `AEV_` prefix may be omitted. For example, the event for SSH login can be expressed as `AEV_LOGIN_SSH`, `LOGIN_SSH` or `0`.

See `showaudit -e all` for a list of valid events.

This option may be specified multiple times. Multiple specifications are processed together with `-c` options in the order listed. See EXAMPLE 3.

When set to `enable` or `disable`, audit record generation for the specified events is turned on or off respectively. These settings override the class settings for the event. Class settings are set by the `-c` option.

The class and event audit record generation policy applies to all users. Unique class and event policies cannot be specified for individual users.

`-g enable|disable`

Sets the global user audit record generation policy.

When set to `disable`, no audit record which can be attributed to any user account is generated. These settings can be overridden on an individual user basis using the `-a` option.

`-h`

Displays usage statement.

When used with other options or operands, an error occurs.

`-m` *mailaddr*

Sets the mail address to which email is sent when the local audit storage space usage reaches a threshold (see option `-t`). Email addresses must be a valid email address of the form *user@company.com*. Specifying `none` for *mailaddr* turns off email notification.

`-p suspend|count`

Sets the policy to follow when the audit trail becomes full. The following are valid values:

`suspend`	All processes which try to write to audit records will be suspended until either space becomes available and records can be written, or the policy is changed to `count`.
`count`	New audit records are dropped and a count is kept of how many records are dropped.

`-t` *percents*

Sets thresholds at which to issue a warning about local audit storage usage. *percents* is a comma-separated list of percentages of available space used. At most four values may be set. For example, values of `50, 75, 80, 90` would cause warnings to be issued when 50%, 75%, 80% and 90% respectively, of the available storage for audit records is consumed. The default value is 80%.

Warnings are issued as a message to the console and optionally to an administrator using email. See `-m` *mailaddr*.

OPERANDS

The following operands are supported:

`archive`	Notifies the log archiving facility to archive the current audit trail.
`delete`	Deletes audit trail data from the older audit log partition and makes it the current partition. `delete` can be used to free space for new audit records if the local audit trail becomes full. Space in the partitions is automatically cleared as needed when logs are archived. The operation is only necessary if audit policy or network problems prevent archiving of audit logs. **Note -** Executing `setaudit delete` a second time deletes data from the newer audit log partition, leaving no audit trail data. For more information on managing audit logs see the *SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers Administration Guide*.
`disable`	Turns off the writing of audit records to the audit trail and notifies the log archiving facility to archive the current audit trail.
`enable`	Turns on the writing of audit records to the audit trail.

EXAMPLES

EXAMPLE 1 Changing Classes Using Names

```
XSCF> setaudit -c LOGIN,AUDIT=disable -c ACS_READ=enable
```

Auditing for LOGIN and AUDIT classes has been disabled. Auditing for READ class is enabled.

EXAMPLE 2 Changing Classes Using Numbers

```
XSCF> setaudit -c 8,16=disable -c 1=enable
```

Auditing for classes 8 (LOGIN) and 16 (AUDIT) has been disabled. Auditing for class 1 (SYSTEM) is enabled.

EXAMPLE 3 Changing Classes and Enabling an Event

```
XSCF> setaudit -c 1=enable -e 64=disable
```

Auditing is enabled for all of Class 1 (SYSTEM) except for event 64 (USER) is disabled.

EXAMPLE 4 Enabling Auditing

```
XSCF> setaudit enable
```

Turns on writing of the audit records for the audit trail.

EXAMPLE 5 Enabling Warnings

```
XSCF> setaudit -t 50,75
```

Warnings will be sent at 50% capacity and 75% capacity.

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

showaudit(8)

NAME

setautologout - set the session timeout time of the XSCF shell

SYNOPSIS

setautologout -s *timeout*

setautologout -h

DESCRIPTION

The setautologout(8) command sets the session timeout time of the XSCF shell.

The default of the session timeout time is 10 minutes.

Privileges

You must have platadm or fieldeng privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-h	Displays usage statement. When used with other options or operands, an error occurs.
-s *timeout*	Specifies the session timeout time of the XSCF shell. Specify a timeout time value in units of minutes for *timeout*. An integer ranging from 1 to 255 can be specified.

EXTENDED DESCRIPTION

The specified session timeout time becomes effective after the subsequent login.

EXAMPLES

EXAMPLE 1 Sets the session timeout time of the XSCF shell to 30 minutes.

```
XSCF> setautologout -s 30
30min
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

showautologout(8)

NAME

setcod - set up the Capacity on Demand (COD) resources used for domains

SYNOPSIS

setcod

setcod [-v]

setcod [[-q] -{y|n}] [-v] *headroom*

setcod [-v] -d *domain_id* [*proc-permits*]

setcod -h

DESCRIPTION

setcod(8) sets up the COD resources to be used for domains. COD hardware activation keys (COD keys) must be installed before COD boards in a domain can be utilized. You can also enable headroom and reserve COD hardware activation permits (COD permits) for some domains with setcod(8).

The setcod(8) command is not available on the M3000 server.

When no *domain_id* is specified, current values are displayed in the square brackets ([]) at the command prompt. If no value is specified for an operand, it retains its current value.

Privileges

You must have platadm privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-d *domain_id*	Domain identifier. *domain_id* can be 0–23 depending on the system configuration.
-h	Displays usage statement.
	When used with other options or operands, an error occurs.
-n	Automatically answers "n" (no) to all prompts.
-q	Suppresses all messages to stdout, including prompts.
-v	Specifies verbose output.
-y	Automatically answers "y" (yes) to all prompts.

OPERANDS

The following operands are supported:

headroom Amount of headroom (processors to be used on demand) to be enabled. Maximum value is `4`.

proc-permits The number of COD permits reserved for a domain. One COD permit is required for each CPU.

EXTENDED DESCRIPTION

If you run the `setcod` command without specifying any options, the command prompts you for COD information.

You are asked to specify the amount of COD headroom to be used, and the number of COD permits to be reserved for your domains. When you are prompted for COD information, the maximum values allowed are displayed within parentheses and default values are displayed within brackets `([])`.

`setcod` enables COD headroom. Use the `-d` *domain_id* to specify the number of domain COD permits to be reserved.

EXAMPLES

EXAMPLE 1 Setting COD CPU Headroom Quantity and Reserve Domain COD Permits

```
XSCF> setcod

PROC Permits installed: 0
PROC Headroom Quantity (0 to disable, 4 MAX) [0]: 1
WARNING:Using headroom requires you to install hardware activation key(s)
within 30 days.  Do you agree? [y|n]: y
PROC Permits reserved for domain 0 (1 MAX) [0]:
PROC Permits reserved for domain 1 (0 MAX) [0]:
PROC Permits reserved for domain 2 (0 MAX) [0]:
PROC Permits reserved for domain 3 (0 MAX) [0]:
PROC Permits reserved for domain 4 (0 MAX) [0]:
PROC Permits reserved for domain 5 (0 MAX) [0]:
PROC Permits reserved for domain 6 (0 MAX) [0]:
PROC Permits reserved for domain 7 (0 MAX) [0]:
PROC Permits reserved for domain 8 (0 MAX) [0]:
PROC Permits reserved for domain 9 (0 MAX) [0]:
PROC Permits reserved for domain 10 (0 MAX) [0]:
PROC Permits reserved for domain 11 (0 MAX) [0]:
PROC Permits reserved for domain 12 (0 MAX) [0]:
PROC Permits reserved for domain 13 (0 MAX) [0]:
PROC Permits reserved for domain 14 (0 MAX) [0]:
PROC Permits reserved for domain 15 (0 MAX) [0]:
```

After this command completes, you will see a message similar to this one in the XSCF console:

```
Aug 28 17:28:30 FF1-1-0 codd[PID]: COD PROC Headroom changed to 1
```

EXAMPLE 2 Set the COD Headroom CPUs to 0

```
XSCF> setcod 0
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

SPARC Enterprise M4000/M5000/M8000/M9000 Servers Capacity on Demand (COD) User's Guide

NAME

setdate - set the date and time of XSCF

SYNOPSIS

setdate [[-q] -{y|n}] [-u] -s *date*

setdate -h

DESCRIPTION

The setdate(8) command sets the date and time of XSCF.

If the local date and time are specified, they are set following conversion to coordinated universal time (UTC).

After the command executed, XSCF will be reset automatically.

Privileges

You must have platadm or fieldeng privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-h	Displays usage statement. When used with other options or operands, an error occurs.
-n	Automatically answers "n" (no) to all prompts.
-q	Suppresses all messages to stdout, including prompts.
-s *date*	Sets date and time. *date* can be specified in either of the following formats:
	yyyy.MM.DD-hh:mm:ss — Specifies date in the format of "*year.month.day-hour:minute:second*."
	MMDDhhmmyyyy.ss — Specifies data in the format "*MonthDayHourMinuteYear.second*."
-u	Specifies time in UTC. When omitted, the local time is specified.
-y	Automatically answers "y" (yes) to all prompts.

EXTENDED DESCRIPTION

- When the command is executed, a prompt to confirm execution of the command with the specified options is displayed. Enter "**y**" to execute the command or "**n**" to cancel the command.
- In the M8000/M9000 servers, the setting automatically reflected to the standby XSCF. When there is a defect on the standby XSCF, it leads to an error and the setting will be reflected to the active XSCF only.

- When you use the `setdate`(8) command to set the time, it may affect the time difference to the domain, and a gap of time may arise at the domain start. After you set the time, use the `showdateoffset`(8) command to confirm the time difference between XSCF and the domain. In case the difference has become enlarged, use the `resetdateoffset`(8) command to reset the time difference.
- When an NTP server has been set to XSCF, you cannot set the the time. To check whether an NTP server is set to XSCF, use the `showntp`(8) command.
- You can execute the `setdate`(8) command only when all domains are powered off. To verify that all domains are powered off, execute the `showlogs power` command and look for the value `System Power Off`.
- To check the currently set XSCF date and time, execute the `showdate`(8) command.

EXAMPLES

EXAMPLE 1 Sets "January 27 16:59:00 2006" of the local time (JST) as the current time.

```
XSCF> setdate -s 012716592006.00
Fri Jan 27 16:59:00 JST 2006
The XSCF will be reset. Continue? [y|n] :y
Fri Jan 27 07:59:00 UTC 2006
XSCF>
The reset continues after this point.
```

EXAMPLE 2 Sets "January 27 07:59:00 2006" of UTC as the current time.

```
XSCF> setdate -u -s 012707592006.00
Fri Jan 27 07:59:00 UTC 2006
The XSCF will be reset. Continue? [y|n] :y
Fri Jan 27 07:59:00 UTC 2006
XSCF>
The reset continues after this point.
```

EXAMPLE 3 Sets "January 27 16:59:00 2006" of the local time (JST) as the current time. Automatically replies with "y" to the prompt.

```
XSCF> setdate -y -s 012716592006.00
Fri Jan 27 16:59:00 JST 2006
The XSCF will be reset. Continue? [y|n] :y
Fri Jan 27 07:59:00 UTC 2006
XSCF>
The reset continues after this point.
```

EXAMPLE 4 Sets "January 27 16:59:00 2006" of the local time (JST) as the current time. Automatically replies with "y" without displaying the prompt.

```
XSCF> setdate -q -y -s 012716592006.00
XSCF>
The reset continues after this point.
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

setntp(8), **settimezone**(8), **showdate**(8), **showntp**(8), **showtimezone**(8)

NAME

setdcl - set a domain component list (DCL)

SYNOPSIS

setdcl -d *domain_id* -s *policy=value*

setdcl -d *domain_id* -s *option=value lsb* [*lsb*...]

setdcl -d *domain_id* -a *lsb=xsb* [*lsb=xsb*...]

setdcl -d *domain_id* -r *lsb* [*lsb*...]

setdcl -h

DESCRIPTION

The setdcl(8) command sets a DCL.

A DCL is hardware resource information that can be set for a domain or the logical system boards (LSBs) that are components of a domain.

An LSB is a board unit recognized by the Oracle Solaris OS in a domain. Up to 16 boards can be registered in each domain, and they are represented by integer numbers ranging from 0 to 15.

An extended system board (XSB) is a board unit that can be used in the system and is one partition of a partitioned physical system board (PSB). An XSB is represented by *x-y*, a combination of a PSB number and the number of one partition of the partitioned PSB (*x* is an integer ranging from 00 to 15, and *y* is an integer ranging from 0 to 3).

The setdcl(8) command associates an XSB with an LSB that can be recognized by the Oracle Solaris OS in the domain, and its settings enable the Oracle Solaris OS in the domain to use hardware resources on the associated XSB.

The setdcl(8) command can set the following types of DCL information:

For the domain:

- Degradation range applicable for an error detected during an initial diagnosis of hardware (policy)

On the M3000 server, the setdcl(8) command can set policy only.

For the LSB:

- XSB number of the XSB to be associated with an LSB (lsb, xsb)

  The XSB with the specified XSB number is associated with an LSB.

- Using memory mounted on an LSB (no-mem)

  The user can specify whether an operating system in the domain can use memory mounted on an LSB.

- Using I/O devices mounted on an LSB (no-io)

The user can specify whether an operating system in the domain can use I/O devices, such as a PCI card, mounted on an LSB.

- Whether to set a priority for the specified LSB as a floating board, relative to other boards (`float`)

  The user can specify whether to set a priority for the specified LSB as a floating board, relative to other boards. A floating board is used for dynamic reconfiguration (DR) for purposes such as changing the domain configuration, while minimizing effect of DR on the operating system.

Privileges

You must have `platadm` privileges to run this command.

Refer to `setprivileges`(8) for more information.

OPTIONS

The following options are supported:

`-a` *lsb=xsb*

Specifies an XSB number to be associated with an LSB number in the domain. The following form can be accepted. On the M3000 server, you cannot specify this option.

lsb=xsb

lsb — Specifies an LSB number. An integer ranging from 0 to 15 can be specified.

xsb — Specifies an XSB number. The following *xsb* form is accepted:

x-y — *x*: An integer from 00–15.
y: An integer from 0–3.

lsb and *xsb* can be specified with an equal sign (=) as a delimiter. The space character must not be inserted immediately before and after "=". *lsb=xsb* can be repeated multiple times by using a space character as a delimiter.

If the same pair of an LSB number and XSB number is duplicated, an error occurs. Also, if an XSB number has already been set for the specified *lsb*, an error occurs.

If the specified *xsb* has already been set for another LSB, the existing setting is canceled and the specified xsb is set for the specified *lsb*.

`-d` *domain_id*

Specifies the domain ID to be set. An integer ranging from 0 to 23 can be specified for *domain_id*, depending on the system configuration.

`-h`

Displays usage statement. When used with other options or operands, an error occurs.

`-r` Clears the XSB number associated with an LSB number in the specified domain. On the M3000 server, you cannot specify this option.

`-s` *option=value* Makes settings regarding hardware resources of the XSB associated with an LSB. An item to be set is specified for *option*, and a value corresponding to *option* is specified for *value*. *option* and *value* are specified only once in a format using an equal sign (=) to delimit the specified values. The space character must not be inserted immediately before and after "=".

One of the following can be specified for *option*. On the M3000 server, only `policy` can be specified.

`policy`	Degradation range applicable for a detected error during an initial diagnosis of hardware.
`no-mem`	Whether to omit the use of memory on a domain
`no-io`	Whether to omit the use of I/O devices on a domain
`float`	Whether to set a priority for the board as a floating board, relative to other boards

If `policy` is specified for *option*, either of the following can be specified for *value*:

`fru`	Degrades the target Field Replaceble Unit (FRU) for an error detected by a diagnosis.
`xsb`	Degrades the target XSB for an error detected by a diagnosis.
`system`	Stops the target domain for an error detected by a diagnosis.

If `no-mem` is specified for *option*, either of the following can be specified for *value*:

`true`	Omits the use of memory on a domain.
`false`	Does not omit the use of memory on a domain (default).

If `no-io` is specified for *option*, either of the following can be specified for *value*:

`true`	Omits the use of I/O devices on a domain.
`false`	Does not omit the use of I/O devices on a domain (default).

If `float` is specified for *option*, either of the following can be specified for *value*:

`true`	Gives a higher priority regarding floating boards.
`false`	Does not give a higher priority regarding floating boards (default).

OPERANDS

The following operands are supported:

lsb Specifies the number of the LSB whose information is to be set. Specify by using an integer ranging from 0 to 15. Multiple lsbs can be specified by delimiting with spaces. Specifies unique *lsb* within the domain. If the same *lsb* number is specified, an error occurs. On the M3000 server, you cannot specify this option.

EXTENDED DESCRIPTION

- If the XSB associated with the specified LSB has been configured in the domain configuration, the information that is set for the LSB cannot be changed. Before making such a change, unassign the XSB from the domain configuration by executing the `deleteboard`(8) command, or re-configure it in another domain configuration by executing the `moveboard`(8) command.
- If the specified domain is running, the value of `policy` cannot be changed. To change the value, first turn off power to the domain.
- The currently set DCL information can be checked by using the `showdcl`(8) command.

EXAMPLES

EXAMPLE 1 Sets XSB#00-0 for LSB#00 and XSB#00-1 for LSB#01 of domain ID 0.

```
XSCF> setdcl -d 0 -a 00=00-0 01=00-1
```

EXAMPLE 2 Sets `no-mem=true` for LSB#00 and #01 of domain ID 0.

```
XSCF> setdcl -d 0 -s no-mem=true 00 01
```

EXAMPLE 3 Sets `policy=system` for domain ID 0.

```
XSCF> setdcl -d 0 -s policy=system
```

EXAMPLE 4 Clear the XSBs associated with LSB#00 and #01 of domain ID 0.

```
XSCF> setdcl -d 0 -r 00 01
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

addboard(8), **deleteboard**(8), **moveboard**(8), **setupfru**(8), **showboards**(8), **showdcl**(8), **showdevices**(8), **showfru**(8)

NAME

setdomainmode - set the modes of operation for the specified domain

SYNOPSIS

setdomainmode [[-q] -{y|n}] -d *domain_id* -m *function=mode*

setdomainmode -h

DESCRIPTION

setdomainmode(8) sets the modes of operation for the specified domain.

The modes of operation for the specified domain include the following types:

Diagnostics Level — OpenBoot PROM diagnostic levels. The default is standard.

Secure Mode — Whether to enable or disable the host watchdog and suppress break signal reception. The default of the host watchdog is enable and suppress break signal reception is enable.

Autoboot — Whether to enable or disable the auto boot function used at domain startup. The default is enable.

CPU Mode — Way of determining the CPU operational mode mounted on the domain. The CPU operational mode can be automatically determined at domain startup (auto), or manually set to the compatible mode (compatible). The default is to let it automatically determined at domain startup. On the M3000 server, you cannot specify CPU Mode.

The CPU operational mode includes the following two types:

SPARC64 VII enhanced mode

Operates using the enhanced functions of SPARC64 VII+ or SPARC64 VII processors. This mode is set to the domain that has only SPARC64 VII+ or SPARC64 VII processors and when the CPU operational mode is determined automatically.

SPARC64 VI compatible mode

All the mounted CPUs operate with the functions equivalent to the SPARC64 VI processor. This mode can be set to a domain of any CPU configuration.

If any of the modes of operation for the specified domain is set, the current settings are listed.

Privileges

You must have one of the following privileges to run this command:

- OpenBoot PROM diagnostic levels:

fieldeng — Can run this command for all domains.

- Host watchdog and suppress break signal reception, auto boot function, and operational mode of CPU:

`platadm`	Can run this command for all domains.
`domainadm`	Can run this command only for your managed domains.

Refer to `setprivileges`(8) for more information.

OPTIONS

The following options are supported:

`-d` *domain_id*	Specifies the domain ID to be set. *domain_id* can be 0–23 depending on the system configuration.
`-h`	Displays usage statement. When used with other options or operands, an error occurs.

`-m` *function=mode* Sets the modes of operation and specifies its values. Use *function* to set the modes of operation. One of the following can be specified:

`diag`	Specifies the OpenBoot PROM diagnostic level.
`secure`	Specifies whether to enable or disable the host watchdog and suppress break signal reception.
`autoboot`	Specifies whether to enable or disable the Auto boot function.
`cpumode`	Sets the operational mode of CPU. When you specified `cpumode` on the M3000 server, it results in an error.

When `diag` is specified for *function*, any of the following can be specified for *mode*:

Note - When the domain is in any status other than `powered off`, it results in an error.

`none`	No diagnosis is performed.
`min`	Sets standard for the diagnostic level.
`max`	Sets maximum for the diagnostic level.

When `secure` is specified for *function*, one of the following can be specified for *mode*. The setting will be reflected after domain power on or restart.

`on`	Enables the host watchdog and suppress break signal reception.
`off`	Disables the host watchdog and suppress break signal reception.

When `autoboot` is specified for *function*, one of the following can be specified for *mode*. The setting will be reflected after domain power on or restart.

`on`	Enables the Auto boot function.
`off`	Disables the Auto boot function.

(*continued*) When `cpumode` is specified for *function*, one of the following can be specified for *mode*:

Note - When the domain is in any status other than `powered off`, it results in an error.

`auto`

Automatically determines the operational mode of CPU at domain startup. Depending on the CPU configuration on the domain, any of the following CPU operational mode is set:

o Consists only of SPARC64 VII+ or SPARC64 VII processors: SPARC64 VII enhanced mode

o SPARC64 VII+ or SPARC64 VII processors, and VI processors mixed: SPARC64 VI compatible mode

o Consists only of SPARC64 VI processors: SPARC64 VI compatible mode

`compatible`

Regardless of the CPUs mounted, sets the operational mode of CPU to the SPARC64 VI compatible mode.

`-n` Automatically answers "`n`" (no) to all prompts.

`-q` Suppresses all messages to stdout, including prompts.

`-y` Automatically answers "`y`" (yes) to all prompts.

EXTENDED DESCRIPTION

- When the command is executed, a prompt to confirm execution of the command with the specified options is displayed. Enter "**`y`**" to execute the command or "**`n`**" to cancel the command.
- The system board (XSB) which can be added by Dynamic Reconfiguration (DR) is decided by the CPU operational mode currently set to the domain, which is as follows:

Domain CPU configuration	Value of CPU Mode	Current CPU operational mode	CPU configuration of a system board which can be added by DR operation
SPARC64 VII+/VII	`auto`	SPARC64 VII enhanced mode	SPARC64 VII+/VII

Domain CPU configuration	Value of CPU Mode	Current CPU operational mode	CPU configuration of a system board which can be added by DR operation
SPARC64 VII+/VII	`compatible`	SPARC64 VI compatible mode	Any CPU configuration
SPARC64 VII+/VII and SPARC64 VI	`auto` or `compatible`	SPARC64 VI compatible mode	Any CPU configuration
SPARC64 VI	`auto` or `compatible`	SPARC64 VI compatible mode	Any CPU configuration

For details of the CPU operational mode and the DR operation, see the *DR User's Guide*.

- To add the XSB other than those above, you need to perform the domain reconfiguration accompanied by the domain power off/on or reboot.
- When the operational mode of CPU has been automatically determined, if a situation as described below occurred, the CPU operational mode changes at the domain restart, from the SPARC64 VI compatible mode to the SPARC64 VII enhanced mode. In the SPARC64 VII enhanced mode, an XSB mounted with the SPARC64 VI processors cannot be added by DR operation.
  - When the SPARC64 VII+ or SPARC64 VII processors and VI processors are mixed, after the restart due to the SPARC64 VI processor failure, there is no SPARC64 VI processor on a domain.

  When the SPARC64 VI processors mounted, or planned to be mounted on the domain, set the operational mode of CPU to the SPARC64 VI compatible mode.
- To check the mode of CPUs which currently set to the domain, execute the `prtdiag`(1M) command on Oracle Solaris OS. For the `prtdiag`(1M) command, see the manual page of Oracle Solaris OS.
- If the Mode switch of the operator panel is set to `Service`, the settings of the modes of operation for the specified domain have the following values, regardless of the settings of the `setdomainmode`(8) command:
  - OpenBoot PROM diagnostic level (`Diagnostic Level`), operational mode of CPU (`CPU Mode`): operates as the `setdomainmode`(8) command setting
  - Host watchdog and suppress break signal reception (`Secure Mode`), auto boot function (`Autoboot`): `off`
- When the OpenBoot PROM environmental variable `'auto-boot?'` has been set to `false`, the auto boot function is disabled.
- The diagnostics level of OpenBoot PROM is applied to the `diag level` of the `addboard`(8) command and `moveboard`(8) command.

- The settings of the current modes of operation for the specified domain can be checked by using the showdomainmode(8) command. When you use the showdomainmode(8) command after the setdomainmode(8) command, it will display the pending modifications performed by the setdomainmode(8), which might not yet be effective.

EXAMPLES

EXAMPLE 1 Sets the OpenBoot PROM diagnostic level for domain ID 0 to none.

```
XSCF> setdomainmode -d 0 -m diag=none
Diagnostic Level    :min      -> none
Secure Mode         :on       -> -
Autoboot            :on       -> -
CPU Mode            :auto     -> -
The specified modes will be changed.
Continue? [y|n]:y
configured.
Diagnostic Level    :none
Secure Mode         :on (host watchdog: available  Break-signal:non-
receive)
Autoboot            :on (autoboot:on)
CPU Mode            :auto
```

EXAMPLE 2 Enables the auto boot function for domain ID 0. Automatically answers "y" to all prompts.

```
XSCF> setdomainmode -y -d 0 -m autoboot=on
Diagnostic Level    :none     -> -
Secure Mode         :on       -> -
Autoboot            :off      -> on
CPU Mode            :auto     -> -
The specified modes will be changed.
Continue? [y|n]:y
configured.
Diagnostic Level    :none
Secure Mode         :on (host watchdog: available  Break-signal:non-
receive)
Autoboot            :on (autoboot:on)
CPU Mode            :auto
```

EXAMPLE 3 Cancels the setdomainmode(8) command execution that is in progress.

```
XSCF> setdomainmode -d 0 -m diag=none
Diagnostic Level    :min      -> none
Secure Mode         :on       -> -
Autoboot            :on       -> -
```

```
CPU Mode            :auto     -> -
The specified modes will be changed.
Continue? [y|n]:n
```

EXAMPLE 4 Enables the auto boot function for domain ID 0. Suppresses prompts, and automatically answers "y" to all prompts

```
XSCF> setdomainmode -q -y -d 0 -m autoboot=on
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

showdomainmode(8), **showdomainstatus**(8)

NAME

setdomparam - forcibly rewrite OpenBoot PROM environment variables

SYNOPSIS

setdomparam [[-q] -{y|n}] -d *domain_id* use-nvramrc

setdomparam [[-q] -{y|n}] -d *domain_id* security-mode

setdomparam [[-q] -{y|n}] -d *domain_id* set-defaults

setdomparam -h

DESCRIPTION

The setdomparam(8) command rewrites OpenBoot PROM environment variables of a specified domain.

The following OpenBoot PROM environment variables can be specified.

use-nvramrc?	Whether to execute the contents of the NVRAM at the boot or reboot of a domain.
security-mode?	Firmware security level setting
set-defaults	Whether to restore OpenBoot PROM environment variables to the settings at the time of shipment from the factory

Privileges

You must have one of the following privileges to run this command:

platadm	Can run this command for all domains.
domainadm	Can run this command only for your managed domain.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:.

-d *domain_id*	Specifies the ID of the domain which OpenBoot PROM environment variables are rewritten. *domain_id* can be 0–23 depending on the system configuration. **Note -** The domain which is powered on cannot specify.
-h	Displays usage statement. When used with other options or operands, an error occurs.
-n	Automatically answers "n" (no) to all prompts.
-q	Suppresses all messages to stdout, including prompts.
-y	Automatically answers "y" (yes) to all prompts.

OPERANDS

The following operands are supported:

`use-nvramrc`	Sets `false` for the `use-nvramrc?` environment variable.
`security-mode`	Sets `none` to the `security-mode?` environment variable.
`set-defaults`	Restores the OpenBoot PROM environment variables to the settings at the time of shipment from the factory

EXTENDED DESCRIPTION

When the command is executed, a prompt to confirm execution of the command with the specified options is displayed. Enter "**y**" to execute the command or "**n**" to cancel the command.

EXAMPLES

EXAMPLE 1 Sets `false` for the `use-nvramrc?` OpenBoot PROM environment variable of domain ID 0.

```
XSCF> setdomparam -d 0 use-nvramrc
DomainIDs of domains that will be affected:00
OpenBoot PROM variable use-nvram will be set to false.
Continue? [y|n]:y
```

EXAMPLE 2 Sets `none` for the `security-mode` OpenBoot PROM environment variable of domain ID 0.

```
XSCF> setdomparam -d 0 security-mode
DomainIDs of domains that will be affected:00
OpenBoot PROM variable security-mode will be set to none.
Continue? [y|n]:y
```

EXAMPLE 3 Initializes the OpenBoot PROM environment variables of the domain ID 0 to the settings at the time of shipment from the factory.

```
XSCF> setdomparam -d 0 set-defaults
DomainIDs of domains that will be affected:00
All OpenBoot PROM variable will be reset to original default values.
Continue? [y|n]:y
```

EXAMPLE 4 Initializes the OpenBoot PROM environment variables of the domain ID 1 to the settings at the time of shipment from the factory. Automatically replies with "y" without displaying the prompt.

```
XSCF> setdomparam -q -y -d 1 set-defaults
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

NAME

setdscp - set the IP address assignments for the Domain to Service Processor Communications Protocol (DSCP)

SYNOPSIS

setdscp -v

setdscp [-f] [-v] [[-q] -{y|n}] -i *address* -m *netmask*

setdscp [-f] [-v] [[-q] -{y|n}] -s -i *address*

setdscp [-f] [-v] [[-q] -{y|n}] -d *domain_id* -i *address*

setdscp -h

DESCRIPTION

setdscp(8) assigns IP addresses to the DSCP links.

setdscp is intended for initial configuration only. Domains should not be powered on when running this command.

Note – You are required to reboot the Service Processor after modifying the DSCP IP address assignment using this command, and before the IP addresses you specified are used.

You can specify a network address for use by all of the DSCP links using the -i *address* and -m *netmask* arguments. In this mode of operation, the IP addresses used by the Service Processor and each domain-specific DSCP link are automatically selected from within the range of addresses indicated by the network address. The specified netmask must be a subset of the default netmask based on network class.

You can set the IP address of an individual, domain-specific DSCP link independently of all other DSCP address settings using the -d *domain_id* and -i *address* arguments.

You can set the IP address of the Service Processor independently of all other DSCP address settings using the -s and -i *address* arguments.

If DSCP has been previously configured, the current settings are displayed. If they are correct, they can be accepted by pressing the Enter key.

An error occurs if you set the address of the Service Processor or a domain to a value that either is out of range for a previously configured network address, or conflicts with an address already assigned to another domain or the Service Processor. You can override such errors by using the -f option.

Using the -f option with a conflicting IP address may cause misconfiguration. You must resolve such conflicts for DSCP to operate properly.

With no arguments, setdscp enters an interactive mode that prompts you to enter all of the DSCP IP address information sequentially. (The noninteractive method, setting up the IP addresses of all domains using the -i and -m options, is preferred.) After inputting all the requested settings, you can review the settings and decide whether to commit them to the DSCP configuration database.

Note – The `-y` and `-n` options can be used (with or without the `-q` option) when running `setdscp` in interactive mode.

Privileges

You must have `platadm` or `fieldeng` privileges to run this command.

Refer to `setprivileges`(8) for more information.

OPTIONS

The following options are supported:

`-d` *domain_id*	Domain identifier. Must be used with `-i` *address* option. *domain_id* can be 0–23 depending on the system configuration.
`-f`	Forces `setdscp` to ignore out of range and address conflict errors and commits the new settings.
`-h`	Displays usage statement. When used with other options or operands, an error occurs.
`-i` *address*	Specifies an IP address in the IPv4 dotted decimal format. When used with `-m` *netmask* it specifies a network address for all DSCP links in the system. When used with `-d` *domain_id* it specifies an individual, domain-specific IP address for use by DSCP. When used with `-s`, it specifies the IP address used for the Service Processor end of all DSCP links in the system.
`-m` *netmask*	Specifies a netmask address for all DSCP links in the system. Must be used with `-i` *address*.
`-n`	Automatically answers "`n`" (no) to all prompts.
`-q`	Suppresses all messages to stdout, including prompts.
`-s`	Must be used with the `-i` *address* option. Specifies the Service Processor end of all DSCP links in the system.
`-v`	Displays a detailed message. If this option is specified with the `-q` option, the `-v` option is ignored.
`-y`	Automatically answers "`y`" (yes) to all prompts.

EXAMPLES

Caution – The IP addresses shown in the following examples are examples only. When choosing DSCP IP addresses avoid choosing addresses that are used elsewhere in your local area network (LAN). For information about DSCP IP addresses refer to the System Configuration chapter of the Administration Guide.

EXAMPLE 1 Assigning All DSCP Addresses

```
XSCF> setdscp -y -i 10.1.1.0 -m 255.255.255.0
Commit these changes to the database? [y|n] : y
```

EXAMPLE 2 Assigning an Alternative IP address to Domain 1

```
XSCF> setdscp -d 1 -i 10.1.1.26
Commit these changes to the database? [y|n] : y
```

EXAMPLE 3 Specifying a Netmask Address With `-q` and `-y` Options

```
XSCF> setdscp -q -y -i 10.1.1.0 -m 255.255.255.0
```

EXAMPLE 4 Setting DSCP Addresses Using Interactive Mode

The default value displayed by each prompt in interactive mode matches the previous configuration. This makes it possible to interactively review and modify DSCP configuration. In this example you only input the network address portion and then press the `Enter` key to accept all subsequent settings.

```
XSCF>  setdscp
DSCP network  [0.0.0.0        ] > 10.1.1.0

DSCP netmask  [255.0.0.0      ] > 255.255.255.0

XSCF address  [10.1.1.1       ] > [Enter]
Domain #00 address  [10.1.1.2       ] > [Enter]
Domain #01 address  [10.1.1.3       ] > [Enter]
Domain #02 address  [10.1.1.4       ] > [Enter]
Domain #03 address  [10.1.1.5       ] > [Enter]
Domain #04 address  [10.1.1.6       ] > [Enter]
Domain #05 address  [10.1.1.7       ] > [Enter]
Domain #06 address  [10.1.1.8       ] > [Enter]
Domain #07 address  [10.1.1.9       ] > [Enter]
Domain #08 address  [10.1.1.10      ] > [Enter]
Domain #09 address  [10.1.1.11      ] > [Enter]
Domain #10 address  [10.1.1.12      ] > [Enter]
Domain #11 address  [10.1.1.13      ] > [Enter]
Domain #12 address  [10.1.1.14      ] > [Enter]
Domain #13 address  [10.1.1.15      ] > [Enter]
Domain #14 address  [10.1.1.16      ] > [Enter]
Domain #15 address  [10.1.1.17      ] > [Enter]
Domain #16 address  [10.1.1.18      ] > [Enter]
Domain #17 address  [10.1.1.19      ] > [Enter]
Domain #18 address  [10.1.1.20      ] > [Enter]
Domain #19 address  [10.1.1.21      ] > [Enter]
Domain #20 address  [10.1.1.22      ] > [Enter]
```

```
Domain #21 address  [10.1.1.23      ] > [Enter]
Domain #22 address  [10.1.1.24      ] > [Enter]
Domain #23 address  [10.1.1.25      ] > [Enter]
Commit these changes to the database [y|n]? y
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

showdscp(8)

NAME

setdualpowerfeed - set dual power feed mode

SYNOPSIS

setdualpowerfeed -s *key*

setdualpowerfeed -h

DESCRIPTION

The setdualpowerfeed(8) command specifies dual power feed mode in the system.

Note – The ability to enable and disable dual power feed is available on M3000/M4000/M5000 servers only. However, dual power feed mode cannot be used with 100V power on M4000/M5000 servers. When the optional power cabinet for dual power feed is connected on M8000/M9000 servers, it automatically configures dual power feed mode. For details about the setting of dual power feed, see the *Installation Guide* for your server.

To enable the dual power feed mode, you need to execute the rebootxscf(8) command or turn off and on the input power.

To disable the dual power feed mode, you need to turn off and on the input power.

Privileges

You must have platadm or fieldeng privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-h	Displays usage statement. When used with other options or operands, an error occurs.
-s *key*	Sets dual power feed mode in the system. Either of the following can be specified for *key*:
	enable — Enables the dual power feed mode.
	disable — Disables dual power feed mode.

EXTENDED DESCRIPTION

The state of the current dual power feed mode can be checked by using the showdualpowerfeed(8) command.

EXAMPLES

EXAMPLE 1 Disables dual power feed mode in the system. Before rebooting the system, a message is displayed.

```
XSCF> setdualpowerfeed -s disable
enable -> disable
NOTE: Dual power feed will be disabled the next time the platform is
powered on.
```

EXAMPLE 2 Enables dual power feed mode in the system. Before rebooting the system, a message is displayed.

```
XSCF> setdualpowerfeed -s enable
disable -> enable
NOTE: Dual power feed will be enabled the next time the platform is powered
on.
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

rebootxscf(8), **showdualpowerfeed**(8)

NAME

setemailreport - set up the email report configuration data

SYNOPSIS

setemailreport [-v] [-t]

setemailreport [-s *variable=value*]...

setemailreport -h

DESCRIPTION

setemailreport(8) sets up email reporting configuration data for remote maintenance. Once the configuration data is set up, it is used by the fault management daemon to send email reports as required.

If you run the setemailreport command without specifying any options, you will be prompted to answer whether email reporting is to be enabled. If enabled, you will be prompted to provided a list of email addresses.

Where:

-a	Add recipient
-d	Delete recipient
-r	Replace recipient (Default)

You can set up email reporting noninteractively by using the -s option.

After the email server and port have been set up using setsmtp(8), you can use setemailreport -t to send a test email message.

Privileges

You must have platadm privileges to run this command.

Refer to setprivileges(8) and for more information.

OPTIONS

The following options are supported:

`-h`	Displays usage statement. When used with other options or operands, an error occurs.

`-s` *variable=value*	Configures email reporting.
	
	Valid entries for *variable* are:
	`enable`
	`recipient`
	
	Valid *value* entries for enable are:
	`yes`
	`no`
	
	Valid *value* entries for `recipient` are:
	Any valid company email account

`-t`	Sends test email.
`-v`	Specifies verbose output.

EXAMPLES

EXAMPLE 1 Enable Email Reporting Interactively

```
XSCF> setemailreport
Enable Email Reporting? [no]:yes
Email Recipient Address [useradm@company.com]: adm2@company.com
Do you want to send a test mail now (Yes/No): no
```

EXAMPLE 2 Adding an Email Report Recipient Using `-a`

```
XSCF> setemailreport
Enable Email Reporting? [yes]:[RETURN]
Email Recipient Address[useradmin@company.com]: -a adm2@company.com
```

EXAMPLE 3 Deleting an Email Report Recipient Using `-d`

```
XSCF> setemailreport
Enable Email Reporting? [yes]:[RETURN]
Email Recipient Address[adm2@company.com]: -d adm2@company.com
```

EXAMPLE 4 Enable Email Reporting Noninteractively

```
XSCF> setemailreport -s enable=yes -s \
recipient="useradm@company.com, adm2@company.com"
```

EXAMPLE 5 Sending Test Email

```
XSCF> setemailreport -t
....Sending test email to useradm@company.com
[Email contents shown below]
Host Name: jupiter
Send Timestamp: 04-20-2006 16:31:45 PST
Mail Server: 10.4.1.1
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

setsmtp(8), **showemailreport**(8)

NAME

sethostname - set a host name and a DNS domain name for an XSCF unit

SYNOPSIS

sethostname *xscfu hostname*

sethostname -d *domainname*

sethostname -h

DESCRIPTION

sethostname(8) command sets a host name and a DNS domain name for an XSCF unit.

In M8000/M9000 servers, the DNS domain name becomes common to XSCF units. The host name can be specified for each XSCF unit.

Privileges

You must have platadm privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-d *domainname* Specifies a DNS domain name to be set for the XSCF unit. The *domainname* is specified in up to 254 characters with the *hostname* included, with label elements delimited by a "." (period). If a domain name exceeding 254 characters is specified, an error occurs. A label element can contain alphanumeric characters and "-". Each label element must always begin with an alphabetic character and end with an alphanumeric character. If "localdomain" specified, an error occurs.

-h Displays usage statement. When used with other options or operands, an error occurs.

OPERANDS

The following operands are supported:

hostname Specifies a host name to be set for the XSCF unit. The *hostname* is specified in up to 64 characters, not in Fully Qualified Domain Name (FQDN) but in an abbreviated form. If a host name exceeding 64 characters is specified, an error occurs. Alphanumeric character and "-" can be used. However, a host name must always begin with an alphabetic character and end with an alphanumeric character. If "`localhost`" specified, an error occurs.

xscfu Specifies the name of the XSCF unit to be set. The following values can be specified, depending on the system configuration. If no value is specified, an error occurs.

`xscf#0`	XSCF unit 0
`xscf#1`	XSCF unit 1 (In M8000/M9000 servers)

EXTENDED DESCRIPTION

- The following situations result in an error by the `applynetwork`(8) command:
  - Both host name and domain name are not set.
  - On M8000/M9000 servers, the host name is not set to both xscf#0 and xscf#1.
  - The total number of characters of the DNS domain name that you set by using the `sethostname`(8) command and the search path that you set by using the `setnameserver`(8) command exceeds 256.
- To apply the host name and the DNS domain name to XSCF, execute the `applynetwork`(8) command. Then, use the `rebootxscf`(8) command to reset XSCF to make the changes to the XSCF permanent.
- The currently set host name and DNS domain name of the XSCF unit can be checked by using the `shownetwork`(8) command.

EXAMPLES

EXAMPLE 1 Sets the host name scf0-hostname for XSCF unit 0.

```
XSCF> sethostname xscf#0 scf0-hostname
```

EXAMPLE 2 Sets the DNS domain name example.com for XSCF unit.

```
XSCF> sethostname -d example.com
```

EXIT STATUS

The following exit values are returned:

`0`	Successful completion.
`>0`	An error occurred.

SEE ALSO

applynetwork`(8)`, **setnameserver**`(8)`, **showhostname**`(8)`

NAME

sethttps - start or stop the HTTPS service, which is used in the XSCF network. This command also performs authentication-related settings

SYNOPSIS

sethttps [[-q] -{y|n}] -c enable

sethttps -c disable

sethttps -c gencsr *country state|province locality organization organizationalunit common e-mail*

sethttps [[-q] -{y|n}] -c genserverkey

sethttps -c *importca*

sethttps [[-q] -{y|n}] -c selfsign *country state | province locality organization organizationalunit common e-mail*

sethttps -h

DESCRIPTION

The sethttps(8) command starts or stops the HTTPS service, which is used in the XSCF network. Also, this command performs authentication-related settings for authentication used in the HTTPS service.

The following authentication-related items can be set:

- Configuring the self-certification authority
- Creating a self-signed web server certificate
- Creating the private key of the web server
- Creating a web server certificate signing request (CSR) to an external certification authority
- Importing a web server certificate signed by an external certification authority

XSCF does not support HTTP service. Only HTTPS service is supported.

Privileges

You must have platadm privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

`-c {enable|disable}`	Specify whether to enable the HTTPS service. One of the following values can be specified. If none of them is specified, an error occurs. `enable` Starts the HTTPS service. `disable` Stops the HTTPS service.
`-c gencsr`	Creates a CSR.
`-c genserverkey`	Creates the private key of the web server.
`-c importca`	Imports a web server certificate signed by the certification authority to the XSCF.
`-c selfsign`	Configures the self-certification authority. Also, this operand creates a self-signing web server certificate.
`-h`	Displays usage statement. When used with other options or operands, an error occurs.
`-n`	Automatically answers "`n`" (no) to all prompts.
`-q`	Suppresses all messages to stdout, including prompts.
`-y`	Automatically answers "`y`" (yes) to all prompts.

OPERANDS

The following operands are supported:

common	Specifies common names, such as the creator name and the host name of a server, using up to 64 characters. If "`-c selfsign`" is specified, the value cannot be omitted.
country	Specifies a country name with a two-letter code such as JP or US. If "`-c selfsign`" is specified, the value cannot be omitted.
e-mail	Specifies an E-mail address using up to 64 characters. If "`-c selfsign`" is specified, do not specify the value with only spaces.
locality	Specifies a city name and so on using up to 64 characters.
organization	Specifies a company name and so on using up to 64 characters. If "`-c selfsign`" is specified, the value cannot be omitted.
organizationalunit	Specifies an organization such as a section or department using up to 64 characters.
state|province	Specifies the name of a state, province, and so on using up to 64 characters. If "`-c selfsign`" is specified, the value cannot be omitted.

Operand formatting rules:

- The order for specifying the operands with "`-c selfsign`" or "`-c gencsr`" is fixed. Please see the SYNOPSIS section.
- If you specify only spaces in a value, enclose the value in single or double quotation marks; for example, " ". However, some operands are not allowed to specify the value with only spaces. For detail, see the descriiption of each operand.
- To omit a value, use a pair of single or double quotation marks; for example, "". When no value is specified, the previously set value is used.
- If you include symbols or blanks in a value, enclose the value in single or double quotation marks; for example, "Kawasaki city".
- If you include a backslash or dollar mark in a value, put a backslash before the symbol; for example, "`\\`" or "`\$`".

EXTENDED DESCRIPTION

- When the HTTPS server is enabled or there is a private certificate authority, web server certificate, or web server secret key, a prompt to confirm execution of the command with the specified options is displayed. Enter "**y**" to execute the command or "**n**" to cancel the command.
- The CSR is overwritten.
- In case the XSCF unit is duplicated configuration, the setting automatically reflected to the standby XSCF. When there's a defect on the standby XSCF, it leads to an error.
- When using an external certification authority, it leads to an error in the following cases.
  - When the "`-c gencsr`" option or the "`-c enable`" option is executed, without executing the "`-c genserverkey`" option.

    Create the private key of the web server using the "`-c genserverkey`" option.
  - When the "`-c enable`" option is executed, without executing the "`-c importca`" option.

    Import a web server certificate using the "`-c importca`" option.
  - When the web server certificate which imported by executing the "`-c importca`" option does not correspond to the private key of the web server which has been created by executing the "`-c genserverkey`" option.

    Confirm the validity of the web server certificate.
- The size of the file to be generated by `sethttps`(8) grows with total character count typed in the operands of configuring the self-certification authority and creating a self-signed web server certificate, and creating a CSR. If the file to be

generated is too large for XSCF, the command fails with an error. If you see this error, reduce the number of characters in the operands and execute the sethttps(8) command again.

- When you use sethttps(8) command to disable the HTTPS service (sethttps -c disable), the HTTPS service is disabled immediately. At this time, any opened HTTPS sessions are terminated.

  For all other settings using the sethttps(8) command, you must reboot the XSCF using the rebootxscf(8) command for the changes to take effect.

- Using the showhttps(8) command you can check the current settings in relation to the HTTPS service.

EXAMPLES

EXAMPLE 1 Starts the HTTPS service.

```
XSCF> sethttps -c enable
Continue? [y|n] :y
Please reset the XSCF by rebootxscf to apply the https settings.
```

EXAMPLE 2 Stops the HTTPS service.

```
XSCF> sethttps -c disable
```

EXAMPLE 3 Creates a CSR with the following settings: *country*: JP, *state | province*: Kanagawa, *locality*: Kawasaki, *organization*: Example, *organizationalunit*: development, *common*: scf-host, *e-mail*: abc@example.com

```
XSCF> sethttps -c gencsr JP Kanagawa Kawasaki Example \
development scf-host abc@example.com
```

EXAMPLE 4 Creates the self-certification authority with the following settings, and creates a self-signed web server certificate:*country*: JP, *state | province*: Kanagawa, *locality*: Kawasaki, *organization*: Example, *organizationalunit*: development, *common*: scf-host, *e-mail*: abc@example.com

```
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:
Verifying - Enter passphrase:
```

EXAMPLE 5 Creates the private key of the web server.

```
XSCF> sethttps -c genserverkey
Server key already exists. Do you still wish to update? [y|n] :y
Enter passphrase:
Verifying - Enter passphrase:
```

EXAMPLE 6 Creates the private key of the web server. Automatically replies with "y" to the prompt.

```
XSCF> sethttps -c genserverkey -y
Server key already exists. Do you still wish to update? [y|n] :y
Enter passphrase:
Verifying - Enter passphrase:
```

EXAMPLE 7 Creates the private key of the web server. Automatically replies with "y" without displaying the prompt.

```
XSCF> sethttps -c genserverkey -q -y
Enter passphrase:
Verifying - Enter passphrase:
```

EXAMPLE 8 Imports the web server certificate. To exit, press the Enter key and then press "Ctrl" and "D".

```
XSCF> sethttps -c importca
Please import a certificate:
-----BEGIN CERTIFICATE-----
MIIDdTCCAt6gAwIBAgIBATANBgkqhkiG9w0BAQQFADCBgTELMAkGA1UEBhMCamox
DjAMBgNVBAgTBXN0YXRlMREwDwYDVQQHEwhsb2NhbGl0eTEVMBMGA1UEChMMb3Jn
YW5pemF0aW9uMQ8wDQYDVQQLEwZvcmdhbmkxDzANBgNVBAMTBmNvbW1vbjEWMBQG
CSqGSIb3DQEJARYHZWUubWFpbDAeFw0wNjA1MzAwNTI5MTVaFw0xNjA1MjcwNTI5
MTVaMG4xCzAJBgNVBAYTAmpqMQ4wDAYDVQQIEwVzdGF0ZTEVMBMGA1UEChMMb3Jn
YW5pemF0aW9uMQ8wDQYDVQQLEwZvcmdhbmkxDzANBgNVBAMTBmNvbW1vbjEWMBQG
CSqGSIb3DQEJARYHZWUubWFpbDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
nkPntf+TjYtyKlNYFbO/YavFpUzkYTLHdt0Fbz/tZmGd3e6Jn34A2W9EC7D9hjLs
j+kAP41Al6wFwGO7KP3H4iImX0Uysjl9Hyk4jLBU51sw8JqvT2utTjltV5mFPKL6
5A51Yuhf8OGrR+bYGli6H1a6RPmlMSD7Z0AGDxR0eY0CAwEAAaOCAQ0wggEJMAkG
A1UdEwQCMAAwLAYJYIZIAYb4QgENBB8WHU9wZW5TU0wgR2VuZXJhdGVkIENlcnRp
ZmljYXRlMB0GA1UdDgQWBBQHIlCmI7QyZa8zpt1Hl6EfLR+EwDCBrgYDVR0jBIGm
MIGjgBTnQYs6jzD7wdDhk7wsFeJGVaUTtaGBh6SBhDCBgTELMAkGA1UEBhMCamox
DjAMBgNVBAgTBXN0YXRlMREwDwYDVQQHEwhsb2NhbGl0eTEVMBMGA1UEChMMb3Jn
YW5pemF0aW9uMQ8wDQYDVQQLEwZvcmdhbmkxDzANBgNVBAMTBmNvbW1vbjEWMBQG
CSqGSIb3DQEJARYHZWUubWFpbIIBADANBgkqhkiG9w0BAQQFAAOBgQCqBFbo88Hi
yvOUyW8E8ll1AbuA04IrnjHI4cjHq9NuSX1w8mJsXKTVMx3WZCJpJDC+f/WoRMKw
R+OpXAVQvb2tjIn3kO99dq+begECo4mwknW1t7QI7A1BkcW2/MkOolIRa6iP1Zwg
JoPmwAbrGyAvGUtdzUoyIH0jl7dRQrVIRA==
-----END CERTIFICATE-----
[Enter]
[Ctrl]and[D]
```

EXAMPLE 9 Specifies "\development" to organizationunit to create a CSR.

```
XSCF> sethttps -c gencsr JP Kanagawa Kawasaki Example \
"\\development" scf-host abc@example.com
```

EXIT STATUS

The following exit values are returned:

`0`	Successful completion.
`>0`	An error occurred.

SEE ALSO

rebootxscf`(8)`, **showhttps**`(8)`

NAME

setldap - configure the Service Processor as a Lightweight Directory Access Protocol (LDAP) client

SYNOPSIS

setldap [-b *bind*] [-B *baseDN*] [-c *certchain*] [-p] [-s *servers*] [-t *user*] -T *timeout*

setldap -h

DESCRIPTION

setldap(8) allows you to configure the Service Processor as an LDAP client.

Note – The LDAP client supports passwords only in CRYPT format, either UNIX Crypt or MD5. Therefore passwords on LDAP server must support it, as well. Refer to the *Administration Guide* for more information. Also note that an XSCF user account user name cannot match an LDAP user name, and an XSCF user account (UID) number cannot match an LDAP UID number.

Privileges

You must have useradm privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-B baseDN	Specifies distinguished name for the search base. Maximum character length is 128 characters.
-b bind	Sets the identity to use when binding to the LDAP server. Maximum character length is 128 characters
-c certchain	Imports an LDAP server certificate chain from the remote file specified in *certchain*. The certificate chain must be in PEM format. Remote files are specified using the standard scp syntax, that is, [user@]host:file., and imported using scp. If the copy requires a user password you will be prompted for it. Use of this option implicitly enables the use of Transport Layer Security (TLS) when connecting to LDAP. This may be disabled by specifying *certchain* as none. The certificate chain must be 64 Kbytes in size or less, and it must be valid or it will be rejected.
-h	Displays usage statement. When used with other options or operands, an error occurs.
-p	Sets a password to use when binding to the LDAP server. You will be prompted for the password.

`-s servers`	Sets the primary and secondary LDAP servers and ports. *servers* is a comma-separated list of *server:port*. Ports are specified numerically and servers can be specified either by name or IP address in the dotted decimal format. For example, `10.8.31.14.636,company:636`. The first server in the list is the primary. Server names must be resolvable. Maximum name length is 128 characters.
`-t user`	Tests connections to all configured LDAP servers. Attempts to retrieve the password data for the specified user from each configured server and reports success or failure in each case.
`-T timeout`	Sets the maximum time allowed for an LDAP search before it returns search results.

EXAMPLES

EXAMPLE 1 Configuring Bind Name

```
XSCF> setldap -b user -p
Password: <Enter password>
XSCF> showldap
Bind Name:                user
Base Distinguished Name:  Not set
LDAP Search Timeout:      0
Bind Password:            Set
LDAP Servers:             None
CERTS:                    None
```

EXAMPLE 2 Configuring Base Distinguished Name

```
XSCF> setldap -B  ou=people,dc=company,dc=com
XSCF> showldap
Bind Name:                user
Base Distinguished Name:  ou=people,dc=company,dc=com
LDAP Search Timeout:      0
Bind Password:            Set
LDAP Servers:             None
CERTS:                    None
```

EXAMPLE 3 Setting the LDAP Timeout

```
XSCF> setldap -T 60
XSCF> showldap
Bind Name:                user
Base Distinguished Name:  ou=people,dc=company,dc=com
LDAP Search Timeout:      60
```

```
Bind Password:           Set
LDAP Servers:            None
CERTS:                   None
```

EXAMPLE 4 Setting the LDAP Server

```
XSCF> setldap -s ldap://company.com,ldaps://company2.com
XSCF> showldap
Bind Name:               user
Base Distinguished Name: ou=people,dc=company,dc=com
LDAP Search Timeout:     60
Bind Password:           Set
LDAP Servers:            ldap://company.com:389 ldaps://company2.com:636
CERTS:                   None
```

EXAMPLE 5 Importing a Certificate

```
XSCF> setldap -c user@remote.machine:/path/to/cacert.pem
XSCF> showldap
Bind Name:               user
Base Distinguished Name: ou=people,dc=company,dc=com
LDAP Search Timeout:     60
Bind Password:           Set
LDAP Servers:            ldap://company.com:389 ldaps://company2.com:636
CERTS:                   cacert.pem
```

EXAMPLE 6 Testing the LDAP connection

```
XSCF> setldap -t jsmith
company.com:389 PASSED
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

setlookup(8), **showldap**(8)

NAME

setldapssl - configure LDAP/SSL

SYNOPSIS

setldapssl enable | disable

setldapssl `loadcert` [[`-q`] `-{y|n}`] [`-i` *n*] [`-u` *username*] [`-p` *proxy* [`-t` *proxy_type*]] *URI*

setldapssl `loadcert` [[`-q`] `-{y|n}`] [`-i` *n*] console

setldapssl `rmcert` [[`-q`] `-{y|n}`] [`-i` *n*]

setldapssl group administrator `-i` *n* name [*groupname*]

setldapssl group operator `-i` *n* name [*groupname*]

setldapssl group custom `-i` *n* name [*groupname*]

setldapssl group custom `-i` *n* roles [*privileges*]

setldapssl userdomain `-i` *n* [*domainname*]

setldapssl defaultrole [*privileges*]

setldapssl timeout *seconds*

setldapssl server [`-i` *n*] [*ipaddr* [:*port*]]

setldapssl logdetail none | high | medium | low | trace

setldapssl log [[`-q`] `-{y|n}`] clear

setldapssl strictcertmode | usermapmode enable | disable

setldapssl usermap attributeInfo | binddn | bindpw | searchbase [*value*]

setldapssl default [[`-q`] `-{y|n}`]

setldapssl `-h`

DESCRIPTION

`setldapssl`(8) configures LDAP/SSL. To enable or disable LDAP/SSL, execute only the command and one of those operands. To enable or disable LDAP/SSL strictcertrmode or usermapmode, specify the mode along with enable or disable.

To clear or unset a property, issue a `setldapssl` command with no value for the operand. For example, `setldapssl group custom -i 1 name` clears the name property from custom group 1, and `setldapssl usermap searchbase` clears the searchbase property from the optional user mapping settings. If a property is not set, it is displayed with no value.

Note – If you are an Active Directory or LDAP/SSL user, do not upload a public key. If one has already been uploaded, use the following command to delete it:
`XSCF>` **`setssh -c delpubkey -a -u proxyuser`**

Privileges

You must have `useradm` privileges to run this command.

Refer to `setprivileges`(8) for more information.

OPTIONS

The following options are supported:

`-h`	Displays usage statement. When used with other options or operands, an error occurs.
`-i` *n*	Sets an index marker, value 1 - 5.
`-n`	Automatically answers "`n`" (no) to all prompts.
`-p`	Specifies the proxy server to be used for transfers. The default transfer type is `http`, unless modified using the `-t` *proxy_type* option. The value for proxy must be in the format *servername*:*port*. See EXAMPLE 12.
`-q`	Suppresses all messages to stdout, including prompts.
`-t`	Use with the `-p` option to specify proxy type as `http`, `socks4`, or `socks5`. The default is `http`.
`-u`	Specifies the user name when logging in to a remote ftp or http server that requires authentication. Prompts for a password. See EXAMPLE 13.
`-y`	Automatically answers "`y`" (yes) to all prompts.

OPERANDS The following operands are supported:

enable | disable — When used with no other operands, enable or disable LDAP/SSL.

loadcert — `loadcert console` prompts for certificate information to be entered at the console. Use this command to paste certificate information copied from a file. Terminate input with `CTRL-D`.

`loadcert` *URI* loads a certificate file for the LDAP/SSL server. Supported formats for *URI* are:

`http://server[:port]/path/file`

`https://`*server*`[:`*port*`]/`*path*`/`*file*

`ftp://`*server*`[:`*port*`]/`*path*`/`*file*

`file:///media/usb_msd/`*path*`/`*file*

rmcert — Delete certificate for an LDAP/SSL server. strictcertmode must be in the disabled state for a certificate to be removed.

group administrator — Assign group name for up to five specified administrator groups. The administrator group has platadm, useradm, and auditadm privileges and you cannot change that.

group operator — Assign group name for up to five specified operator groups. The operator group has platop and auditop privileges and you cannot change that.

group custom — Assign group name and privileges for up to five groups.

userdomain — Configure the user domain. See EXAMPLE 6, below, for important information.

defaultrole — Configure default privileges. If defaultrole is configured, users have privileges as specified by defaultrole after authentication; user group membership is not checked. If defaultrole is not configured, users' privileges will be learned from the LDAP/SSL server based on group membership.

timeout — Configure transaction timeout, in seconds. *seconds* can be 1 to 20. The default is 4. If the specified timeout is too brief for the configuration, the login process or retrieval of user privilege settings could fail.

server

Configure the primary and up to five alternate LDAP/SSL servers. To use a host name, DNS must be enabled. An IP address can be specified with port number; otherwise, the default port is used.

logdetail

Enable logging of LDAP/SSL authentication and authorization diagnostic messages at the specified detail level. This log is for use in troubleshooting and is cleared on SP reboot. Level can be one of the following:

none	Do not log diagnostic messages. Use this setting during normal system operation
high	Log only high-severity diagnostic messages
medium	Log only high-severity and medium-severity diagnostic messages
low	Log high-severity, medium-severity, and informational diagnostic messages
trace	Log high-severity, medium-severity, informational, and trace-level diagnostic messages

log *options* clear

Clear the log file of LDAP/SSL authentication and authorization diagnostic messages.

strictcertmode

Enable or disable strictcertmode mode. This mode is disabled by default; the channel is secure, but limited validation of the certificate is performed. If strictcertmode is enabled, the server's certificate must have already been uploaded to the server so that the certificate signatures can be validated when the server certificate is presented. Data is always protected, even if strictcertmode is disabled. Strictcertmode applies to primary and alternate servers alike.

usermapmode — Enable or disable use of the usermap. When enabled, user attributes specified with the usermap operand, rather than userdomain, are used for user authentication.

usermap — Only if `usermapmode` is enabled, configure the specified usermap parameter:

attributeInfo

Use the specified attribute information for user validation

binddn

Use the specified Distinguished Name for binding with the LDAP/SSL server

bindpw

Use the specified password for binding with the LDAP/SSL server

searchbase

Configure the specified search base

For more information, see EXAMPLES.

default — Reset LDAP/SSL settings to factory default.

EXAMPLES

EXAMPLE 1 Configures the LDAP/SSL primary server, specifying a port other than the default.

```
XSCF> setldapssl server 10.1.12.250:4040
```

EXAMPLE 2 Sets name for administrator group 3.

```
XSCF> setldapssl group administrator -i 3 name CN=spSuperAdmin, \
OU=Groups,DC=Sales,DC=aCompany,DC=com
```

EXAMPLE 3 Sets name for custom group 2.

```
XSCF> setldapssl group custom -i 2 name CN=spLimitedAdmin, \
OU=Groups,DC=Sales,DC=aCompany,DC=com
```

EXAMPLE 4 Sets roles for custom group 2.

```
XSCF> setldapssl group custom -i 2 role auditadm,platop
```

EXAMPLE 5 Loads certificate information for Alternate Server 4 from the console.

```
XSCF> setldapssl loadcert -i 4 console
Warning: About to load certificate for Alternate Server 4:
. Continue? [y|n]: y
Please enter the certificate:

-----BEGIN CERTIFICATE-----
MIIETjCCAzagAwIBAgIBADANBgkqhkiG9w0BAQQFADB8MQswCQYDVQQGEwJVUzET
MBEGA1UECBMKQ2FsaWZvcm5pYTESMBAGA1UEBxMJU2FuIERpZWdvMRkwFwYDVQQK
ExBTdW4gTWljcm9zeXN0ZW1zMRUwEwYDVQQLEwxTeXN0ZW0gR3JvdXAxEjAQBgNV
...
-----END CERTIFICATE-----
CTRL-D
XSCF>
```

EXAMPLE 6 Configures user domain 2. <USERNAME> is a template that must be entered exactly as shown. During authentication the user's login name replaces <USERNAME>. `userdomain` can only take the form of Distinguished Name (DN).

```
XSCF> setldapssl userdomain -i 2 \
'UID=<USERNAME>,OU=people,DC=aCompany,DC=com'
```

EXAMPLE 7 Configures the optional user mapping attribute info setting.

```
XSCF> setldapssl usermap attributeInfo \
'(&(objectclass=person)(uid=<USERNAME>))'
```

EXAMPLE 8 Configures the optional user mapping bind distinguished name setting.

```
XSCF> setldapssl usermap binddn CN=SuperAdmin,DC=aCompany,DC=com
```

EXAMPLE 9 Configures the optional user mapping bind password setting.

```
XSCF> setldapssl usermap bindpw b.e9s#n
```

EXAMPLE 10 Configures the optional user mapping search base setting.

```
XSCF> setldapssl usermap searchbase OU=yoshi,DC=aCompany,DC=com
```

EXAMPLE 11 Loads a server certificate for LDAP/SSL using the specified URI.

```
XSCF> setldapssl loadcert http://domain_2/UID_2333/testcert
```

EXAMPLE 12 Loads a server certificate for LDAP/SSL using an http Proxy Server with port 8080 .

```
XSCF> setldapssl loadcert -p webproxy.aCompany.com:8080 \
http://domain_2/UID_2333/testcert
```

EXAMPLE 13 Loads a server certificate for LDAP/SSL using a username and password.

```
XSCF> setldapssl loadcert -u yoshi \
http://domain_2/UID_2333/testcert
```

EXAMPLE 14 Sets logging of high-severity diagnostic messages.

```
XSCF> setldapssl logdetail high
```

EXAMPLE 15 Clears diagnostic messages from the log file, answering Yes to all prompts.

```
XSCF> setldapssl log -y clear
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

showldapssl(8)

NAME

setlocale - set the default locale of the XSCF

SYNOPSIS

setlocale -s *locale*

setlocale -h

DESCRIPTION

The setlocale(8) command sets the default locale of the XSCF.

The locale that can be set is English or Japanese.

Privileges

You must have platadm privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-h — Displays usage statement. When used with other options or operands, an error occurs.

-s *locale* — Specifies the default locale of the XSCF. Either of the following can be specified for *locale*:

- C — Sets the locale for English.
- ja_JP.UTF-8 — Sets the locale for Japanese.

EXTENDED DESCRIPTION

- The specified locale becomes effective after the subsequent login.
- The currently set locale can be checked by using the showlocale(8) command.

EXAMPLES

EXAMPLE 1 Sets the XSCF default locale for English.

```
XSCF> setlocale -s C
C
```

EXAMPLE 2 Sets the XSCF default locale for Japanese.

```
XSCF> setlocale -s ja_JP.UTF-8
ja_JP.UTF-8
```

EXIT STATUS

The following exit values are returned:

0 — Successful completion.

>0 — An error occurred.

SEE ALSO

showlocale(8)

NAME

setlocator - control the blinking of the CHECK LED on the operator panel

SYNOPSIS

setlocator *value*

setlocator -h

DESCRIPTION

setlocator(8) command controls the blink state of the CHECK LED on the operator panel.

The following states can be set:

Start blinking	Makes the CHECK LED blink.
Stop blinking	Stops the blinking of the CHECK LED.

Privileges

You must have platadm or fieldeng privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following option is supported:

-h	Displays usage statement. When used with other options or operands, an error occurs.

OPERANDS

The following operand is supported:

value	Specifies the CHECK LED state. One of the following can be specified:
	blink — Starts the CHECK LED blinking.
	reset — Stops the CHECK LED blinking.

EXTENDED DESCRIPTION

The showlocator(8) command can be used to check the CHECK LED state.

EXAMPLES

EXAMPLE 1 Starts the CHECK LED blinking.

```
XSCF> setlocator blink
```

EXAMPLE 2 Stops the CHECK LED blinking.

```
XSCF> setlocator reset
```

EXIT STATUS

The following exit values are returned:

`0`	Successful completion.
`>0`	An error occurred.

SEE ALSO

showlocator`(8)`

NAME

setloginlockout - enable or disable login lockout feature

SYNOPSIS

setloginlockout -s *time*

setloginlockout -h

DESCRIPTION

The setloginlockout(8) command sets the amount of time, in minutes, that users are prevented from logging into their accounts after the third unsuccessful login attempt.

Privileges

You must have useradm privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-h	Displays usage statement. When used with other options or operands, an error occurs.
-s *time*	Specifies the account lockout time, in minutes, using a number ranging from 0 to 1440 (24 hours). The default value, which disables the lockout, is 0 minutes.

EXTENDED DESCRIPTION

When login lockout is set, a user is allowed three consecutive attempts to log in. An attempt to log in is defined as typing the user name at the login prompt and pressing the Return key, even if no password is entered or the login attempt times out. After the third consecutive failed attempt, the system prevents further tries for the set amount of time. During lockout, the system allows entry of the login name and asks for a password. But it rejects every further attempt, even if the password entered is valid. Failed attempts during lockout do not extend the lockout time.

setloginlockout -s 0 disables the account lockout. When the account lockout is disabled, a user can attempt to log in and fail an unlimited number of times.

If account lockout is disabled then re-enabled, locked-out users are able to try again between those two events. But locked-out users who do not retry until after the feature is re-enabled see no change, and remain locked out as if the disabling and renabling did not occur. The lockout time for such users is not changed.

EXAMPLES

EXAMPLE 1 Sets the lockout timeout time to 90 minutes.

```
XSCF> setloginlockout -s 90
90 minutes
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO | **showloginlockout** (8)

NAME

setlookup - enable or disable the use of the Lightweight Directory Access Protocol (LDAP) server for authentication and privilege lookup

SYNOPSIS

setlookup -a {local|ldap}

setlookup -p {local|ldap}

setlookup -h

DESCRIPTION

setlookup(8) sets whether authentication and privileges data are looked up in LDAP or not.

Privileges

You must have useradm privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-a	Sets the authentication lookup. Used with one of the required operands ldap or local.
-h	Displays usage statement. When used with other options or operands, an error occurs.
-p	Sets privileges lookup. Used with one of the required operands ldap or local.

OPERANDS

The following operands are supported:

ldap	Used with the -a and -p options. When set to ldap, authentication or privileges are first looked up locally and then in LDAP if not found locally. Verify that LDAP servers have been correctly configured before executing **setlookup -a ldap** or **setlookup -p ldap**.
local	Used with the -a and -p options. When set to local, authentication or privileges are looked up only locally.

EXAMPLES

EXAMPLE 1 Enabling LDAP Lookup of Privilege Data

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

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO | **setldap**(8), **showlookup**(8)

NAME

setnameserver - set the domain name system (DNS) servers and the DNS search paths used in the XSCF network

SYNOPSIS

setnameserver [-c add] *address...*

setnameserver -c del *address...*

setnameserver -c del -a

setnameserver -c addsearch *domainname...*

setnameserver -c delsearch *domainname...*

setnameserver -c delsearch -a

setnameserver -h

DESCRIPTION

The setnameserver(8) command specifies the DNS servers and DNS search paths used in the XSCF network.

Up to three DNS servers can be registered for XSCF. Up to five DNS search paths can be registered.

Privileges

You must have platadm privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-a	Deletes all the DNS servers and the DNS search paths that are currently registered. When deleting all DNS servers, this option is used together with "-c del." When deleting all DNS search paths, this option is used together with "-c delsearch."
-c add	Adds the host with the specified IP address as a DNS server. This option is used together with *address*. If the -c option is omitted, "-c add" is assumed specified. When a DNS server is registered, the existing setting is deleted and the specified address is added.
-c addsearch	Registers the specified domain name to the DNS search path. This option is used together with *domainname*. If the -c option is omitted, "-c add" is assumed specified. When a DNS search path is registered, the existing setting is deleted and the specified domain name is added.

`-c del` Deletes specified DNS servers. If the `-c` option is omitted, "`-c add`" is assumed specified. When deleting multiple DNS servers, the servers are deleted in the order they are specified. See EXAMPLE 3.

`-c delsearch` Deletes specified DNS search path. If the `-c` option is omitted, "`-c add`" is assumed specified. When deleting multiple DNS search paths, the search paths are deleted in the order they are specified.

`-h` Displays usage statement. When used with other options or operands, an error occurs.

OPERANDS

The following operand is supported:

address Specifies the IP address of a DNS server to be added or deleted using four sets of integers. Up to three addresses delimited by the space can be specified. The following *address* form is accepted:

xxx.xxx.xxx.xxx

xxx An integer from 0–255. Zero suppression can be used to specify the integer.

You cannot specify the loopback address (127.0.0.0/8), the network address, or a broadcast address.

domainname Specifies the domain name of the DNS search path to be registered or deleted. You can use a RFC 1034-compliant format. The label element can contain letters (a to z, A to Z), numbers (0 to 9), and the special characters "-" (hyphens) and "." (period). The domain name must begin with a letter and end with either a letter or number. A "." (period) can be used as delimiter. You can specify up to five domain names, each separated by a space, but the total number of characters cannot exceed 256.

EXTENDED DESCRIPTION

- If multiple DNS servers are specified, the servers are used in the order specified.
- The registered DNS search path is used, as in the case where you use the `nslookup`(8) command and refer to the DNS server for the host name. The host name that you specified in the `nslookup`(8) command will be appended with the domain name which registered in the DNS search path, and be referred to the DNS server in the FQDN format.
- If multiple search paths are registered, domain names are assigned in order of registration and referred to the DNS server.
- If you set the DNS search path, you must also specify the DNS server.

- The DNS domain name (set by the `sethostname`(8) command) and search path (set by the `setnameserver`(8) command) together can contain up to 256 characters.
- To change the DNS servers and the DNS search paths in XSCF, execute the `applynetwork`(8) command. Then, use the `rebootxscf`(8) command to reset XSCF, completing the change.
- The currently set DNS server can be checked by using the `shownameserver`(8) command.

EXAMPLES

EXAMPLE 1 Adds the hosts with the IP addresses 192.168.1.2, 10.18.108.10, and 10.24.1.2 as DNS server. Names are solved in the order specified.

```
XSCF> setnameserver 192.168.1.2 10.18.108.10 10.24.1.2
```

EXAMPLE 2 Deletes the host with the IP address 10.18.108.10 from the DNS server.

```
XSCF> setnameserver -c del 10.18.108.10
```

EXAMPLE 3 Deletes the first two DNS servers whose IP addresses are 10.24.1.2. This case is when a DNS server is listed multiple times.

```
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
```

EXAMPLE 4 Deletes all the DNS servers.

```
XSCF> setnameserver -c del -a
```

EXAMPLE 5 Registers the domain names search1.com, search2.com, search3.com, search4.com, and search5.com to the search path.

```
XSCF> setnameserver -c addsearch search1.com search2.com search3.com \
search4.com search5.com
```

EXAMPLE 6 Deletes the domain name search5.com from the DNS search path.

```
XSCF> setnameserver -c delsearch search5.com
```

EXAMPLE 7 Deletes all the registered domain names from the DNS search path.

```
XSCF> setnameserver -c delsearch -a
```

EXIT STATUS

The following exit values are returned:

`0`	Successful completion.
`>0`	An error occurred.

SEE ALSO

applynetwork`(8)`, **sethostname**`(8)`, **shownameserver**`(8)`

NAME

setnetwork - set or remove an XSCF network interface

SYNOPSIS

setnetwork [-m *addr*] *interface address*

setnetwork -c {up|down}*interface*

setnetwork [[-q] -{y|n}] -r *interface*

setnetwork -h

DESCRIPTION

setnetwork(8) command sets or removes an XSCF network interface.

The following settings can be made for the specified network interface:

- Whether to enable or disable the network interface.
- IP address
- Netmask

When you set an IP address or netmask, the specified network interface will be enabled at the same time as the setting.

When you removed the netmask interface, the specified network interface will be disabled at the same time as the removal. And when the routing information is set to the target network interface, it will be removed together.

Privileges

You must have platadm privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

`-c {up|down}` Specifies whether to enable the specified network interface. One of the following values can be specified. If none of them is specified, an error occurs.

- `up` Enables the network interface.
- `down` Disables the network interface.

`-h` Displays usage statement. When used with other options or operands, an error occurs.

`-m` *addr* Specifies a netmask. To specify *addr*, use the standard form of four integer values delimited by "`.`" (periods). For example, use *xxx.xxx.xxx.xxx*, where *xxx* is an integer from 0-255. Zero suppression can be used to specify the integer.

If the `-m` option omitted, one of the following netmask values is set depending on the address specified in the *address* operand:

- If the address specified is class A (e.g. 20.1.1.1), the netmask value 255.0.0.0 is set.
- If the address specified is class B (e.g. 136.18.1.1), the netmask value `255.255.0.0` is set.
- If the address specified is class C (e.g. 200.18.108.1), the netmask value `255.255.255.0` is set.

`-n` Automatically answers "`n`" (no) to all prompts.

`-q` Suppresses all messages to stdout, including prompts.

`-r` Removes the IP address and netmask of the network interface.

`-y` Automatically answers "`y`" (yes) to all prompts.

OPERANDS

The following operands are supported:

address

Specifies an IP address. To specify *address*, use the standard form of four integer values delimited by "`.`" (periods). For example, use *xxx.xxx.xxx.xxx*, where *xxx* is an integer from 0-255. Zero suppression can be used to specify the integer.

You cannot specify the loopback address (127.0.0.0/8), the network address, a broadcast address, or class D or E (224.0.0.0 - 255.255.255.255) address.

interface

Specifies the network interface to be configured. One of the following values can be specified:

- In M3000/M4000/M5000 servers:

For XSCF unit 0:

`xscf#0-lan#0`	XSCF-LAN#0
`xscf#0-lan#1`	XSCF-LAN#1

For abbreviation:

`lan#0`	an abbreviation of XSCF-LAN#0
`lan#1`	an abbreviation of XSCF-LAN#1

- In M8000/M9000 servers:

Specifying the `-c` or `-r` option and Inter SCF Network (ISN) together, it results in errors.

For XSCF unit 0:

`xscf#0-lan#0`	XSCF-LAN#0
`xscf#0-lan#1`	XSCF-LAN#1
`xscf#0-if`	ISN

For XSCF unit 1 :

`xscf#1-lan#0`	XSCF-LAN#0
`xscf#1-lan#1`	XSCF-LAN#1
`xscf#1-if`	ISN

For takeover IP address:

`lan#0`	takeover IP address for XSCF-LAN#0
`lan#1`	takeover IP address for XSCF-LAN#1

EXTENDED DESCRIPTION

- In M8000/M9000 servers, a takeover IP address can be used without a need to determine whether XSCF has been switched. By setting the LAN ports of the active XSCF unit as `lan#0 and lan#1`, they can be accessed with the names `lan#0 and lan#1`.
- In M3000/M4000/M5000 servers, the value of the `lan#0` is fixed with `xscf#0-lan#0`, and the `lan#1` is fixed with `xscf#0-lan#1`.
- After you set the network interface, if you disable that network interface and execute the `applynetwork`(8) command, the setting data of IP address and netmask will be stored in XSCF. When you enable the network interface, the setting of IP address and netmask will be used.
- In the following cases, the `setnetwork`(8) command results in an error:
  - When specified the same IP address as an existing IP address
  - When specified a subnet which is the same with DSCP
  - When specified the same subnets in ISN and in other network interface
  - When specified the `-c` or `-r` option and ISN together
  - When the netmask that specified by using the `-m` *addr* option does not correspond to either of the cases below:

    Only the most significant bit is 1

    Repeated 1 from the most significant bit
- If M3000/M4000/M5000 servers corresponds to the cases below, the `applynetwork`(8) command results in an error.
  - If xscf#0-lan#0 and xscf#0-lan#1 are in the down status
  - If xscf#0-lan#0 and xscf#0-lan#1 are in the up status and the same subnets have been set
- On M8000/M9000 servers, if xscf#0-lan#0, xscf#1-lan#0, xscf#0-lan#1, and xscf#1-lan#1 are all in the down status, the `applynetwork`(8) command results in an error.
- On M8000/M9000 servers, if the network interface which is in the up status has the following settings, the `applynetwork`(8) command results in an error.
  - If the subnet of xscf#0-lan#0, xscf#1-lan#0, and the takeover IP address lan#0 are different
  - If the subnet of xscf#0-lan#1, xscf#1-lan#1, and the takeover IP address lan#1 are different
  - If the subnet of ISN is different
  - If the subnet of xscf#0-lan#0 and xscf#0-lan#1 are the same
  - If the subnet of xscf#1-lan#0 and xscf#1-lan#1 are the same
- In case you specified the IP address and the netmask to the interfaces other than ISN and when the ISN is not configured, the following default value will be set:

- `xscf#0-if`:

  IP address: `192.168.1.1` Netmask: `255.255.255.0`
- `xscf#1-if`:

  IP address: `192.168.1.2` Netmask: `255.255.255.0`

- The `shownetwork`(8) command can display current information on a network interface configured for XSCF.
- To reflect information on the specified network interface, execute the `applynetwork`(8) command and reset XSCF.

EXAMPLES

EXAMPLE 1 Sets the IP address 192.168.10.10 and netmask 255.255.255.0 for XSCF-LAN#0 on XSCF unit 0.

```
XSCF> setnetwork xscf#0-lan#0 -m 255.255.255.0 192.168.10.10
```

EXAMPLE 2 Sets the IP address 192.168.10.10 and netmask 255.255.255.0 for XSCF-LAN#0 on XSCF unit 0 in an M3000/M4000/M5000 server.

```
XSCF> setnetwork lan#0 -m 255.255.255.0 192.168.10.10
```

EXAMPLE 3 Disables XSCF-LAN#1 on XSCF unit 0.

```
XSCF> setnetwork xscf#0-lan#1 -c down
```

EXAMPLE 4 Sets the IP address 192.168.10.128 on ISN on the XSCF unit 0. By default, 255.255.255.0 is set for the netmask.

```
XSCF> setnetwork xscf#0-if 192.168.10.128
```

EXAMPLE 5 Sets the IP address 192.168.11.10 and netmask 255.255.255.0 for XSCF-LAN#0 on XSCF unit 1.

```
XSCF> setnetwork xscf#1-lan#0 -m 255.255.255.0 192.168.11.10
```

EXAMPLE 6 Sets the IP address 192.168.1.10 and netmask 255.255.255.0 for the takeover IP address of XSCF-LAN#0.

```
XSCF> setnetwork lan#0 -m 255.255.255.0 192.168.1.10
```

EXAMPLE 7 Removes the IP address and netmask that set in XSCF-LAN#0 on XSCF unit 0

```
XSCF> setnetwork -r xscf#0-lan#0
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.
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

applynetwork(8), **rebootxscf**(8), **shownetwork**(8)

NAME

setntp - set the NTP servers used on the XSCF network, the stratum value, the preferred server and the clock address of the local clock of XSCF

SYNOPSIS

setntp [-c add]*address...*

setntp -c del *address...*

setntp -c del -a

setntp -c stratum -i *stratum_no*

setntp -m *type=value*

setntp -h

DESCRIPTION

setntp(8) command sets the NTP information for XSCF.

The setntp(8) command can specify the following information:

- The NTP servers which are used on the XSCF network. Up to three NTP servers can be registered for the XSCF network. Any attempt to register four or more servers causes an error.
- The stratum value which has been set to XSCF.
- Whether to specify the preferred server.
- The clock address of the local clock of XSCF.

Privileges

You must have platadm privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-a	Deletes all the NTP servers that are currently registered. This option is used with the "-c del".
-c add	Adds the host with the specified address or the host as an NTP server. This option is used together with *address*. If the -c option is omitted, "-c add" is used. When an NTP server is registered, the existing setting is deleted and overwriting is performed with the specified *address*.
-c del	Deletes the host with the specified address or the host from the NTP servers. If the -c option is omitted, "-c add" is assumed specified. When deleting multiple NTP servers, the servers are deleted in the order they are specified. See EXAMPLE 4.
-c stratum	Sets the stratum value in case you regard XSCF as an NTP server.

`-h` Displays usage statement. When used with other options or operands, an error occurs.

`-i` *stratum_no* Specifies the stratum value. This option is used together with the "`-c stratum`". An integer from 1 to 15 can be specified. If the stratum value not specified, it is 5.

`-m` *type=value* Sets the preferred server or the local clock of XSCF. You can specify either of the following for *type*:

`prefer` Specifies whether priority should be given to the NTP server at the top of the registered list at the time of synchronization.

`localaddr` Sets the local clock of XSCF.

When `prefer` is specified for *type*, either of the following can be specified for *value*:

`on` That server is the first choice and alternatives servers are given preference in order of increasing stratum value, from lowest to the highest. The default value is `on`.

`off` The same preferences are given with no priority for the server at the top of the list.

When `localaddr` is specified for *type*, specify the least significant byte of the clock address of the local clock 127.127.1.*x* for value. A numeric from 0 to 3 can be specified. The default is 0, and the clock address of the local clock at this time is 127.127.1.0.

OPERANDS

The following operands are supported:

address

Specifies the IP address or host name of an NTP server to be added or deleted. You can specify up to three IP addresses or host names using a space as a delimiter. The host name can be specified in the format that complies with RFC 1034. Host name, if specified, must be resolvable.

A specified IP address is a set of four integer values delimited by the "." (period). The following address form is accepted:

xxx.xxx.xxx.xxx

xxx

An integer from 0–255. Zero suppression can be used to specify the integer.

You cannot specify the loopback address (127.0.0.0/8), the network address, or a broadcast address.

If "`-c add`" is specified and *address* is omitted, an error occurs.

EXTENDED DESCRIPTION

- In M8000/M9000 servers the setting is automatically passed to the standby XSCF. If the standby XSCF is unable to accept that setting, an error occurs.
- To apply the specified configuration, execute the `rebootxscf`(8) command and reset XSCF.
- After the XSCF is reset, its time is synchronized with the time of the selected NTP server.
- If you set the NTP server to XSCF, the domain time may be changed due to the time difference retained in XSCF. Execute the `resetdateoffset`(8) command to reset the time difference.
- The current NTP server settings set by the `setntp`(8) command can be checked by using the `showntp`(8) command.

EXAMPLES

EXAMPLE 1 Adds the three NTP servers with the addresses 192.168.1.2, 10.18.108.10, and 10.24.1.2.

```
XSCF> setntp 192.168.1.2 10.18.108.10 10.24.1.2
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

EXAMPLE 2 Deletes the NTP server 10.18.108.10.

```
XSCF> setntp -c del 10.18.108.10
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

EXAMPLE 3 Adds the two NTP servers ntp1.examples.com and ntp2.example.com.

```
XSCF> setntp ntp1.example.com ntp2.example.com
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

EXAMPLE 4 Deletes the first NTP server whose IP address is 192.168.1.2. This case is when a NTP server is listed multiple times.

```
XSCF> setntp -a
server 192.168.1.2
server 10.18.108.10
server 192.168.1.2
XSCF> setntp -c del 192.168.1.2
XSCF> setntp -a
server 10.18.108.10
server 192.168.1.2
```

EXAMPLE 5 Sets the stratum value to 7.

```
XSCF> setntp -c stratum -i 7
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

EXAMPLE 6 Cancels the designation of preferred server of the NTP server.

```
XSCF> setntp -m prefer=off
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

EXAMPLE 7 Sets the clock address of the local clock of XSCF.

```
XSCF> setntp -m localaddr=3
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

rebootxscf(8), **setnameserver**(8), **showntp**(8)

NAME

setpacketfilters - set the IP packet filtering rules to be used in the XSCF network

SYNOPSIS

setpacketfilters [[-q] -{y|n}] -c {add|del} [-i *interface*] [-s *address* [/ *mask*]] -j *target*

setpacketfilters [[-q] -{y|n}] -c clear

setpacketfilters -h

DESCRIPTION

The setpacketfilters(8) command sets the IP packet filtering rules to be used in the XSCF network.

IP packet filtering rules can be used to prevent illegal access to the XSCF network. Settings specified with setpacketfilters(8) are applied immediately after the command is executed.

Privileges

You must have platadm or fieldeng privilege to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

`-c {add|del|clear}`

Specifies the operation to define the IP packet filtering rule. Any of the following can be specified. This option cannot be omitted.

`add`	Adds an IP packet filtering rule.
`del`	Deletes specified IP packet filtering rule.
`clear`	Clears all IP packet filtering rules which have been set.

`-h`

Displays usage statement. When used with other options or operands, an error occurs.

`-i` *interface*

Specifies the XSCF network interface to which you set the IP packet filtering rules. Any of the following can be set.

- In M3000/M4000/M5000 servers:

For XSCF unit 0:

`xscf#0-lan#0`	XSCF-LAN#0
`xscf#0-lan#1`	XSCF-LAN#1

For abbreviation:

`lan#0`	XSCF-LAN#0
`lan#1`	XSCF-LAN#1

- In M8000/M9000 servers:

For XSCF unit 0:

`xscf#0-lan#0`	XSCF-LAN#0
`xscf#0-lan#1`	XSCF-LAN#1

For XSCF unit 1:

`xscf#1-lan#0`	XSCF-LAN#0
`xscf#1-lan#1`	XSCF-LAN#1

If the `-i` option is omitted, the default settings are:

- In M4000/M5000 servers:
  `xscf#0-lan#0, xscf#0-lan#1`
- In M8000/M9000 servers:
  `xscf#0-lan#0, xscf#0-lan#1, xscf#1-lan#0, xscf#1-lan#1`

`-j` *target*	Specifies action to be taken when the received IP packet matches the filtering rule, where *target* is one of the following: `ACCEPT` Permits the IP packet to go through `DROP` Drops the IP packet
`-n`	Automatically answers "`n`" (no) to all prompts.
`-q`	Suppresses all messages to stdout, including prompts.
`-s` *address*[/*mask*]	Specifies the sender of the IP packet. Either an IP address or a network IP address with a netmask (/mask) added can be specified. To specify an IP address or a network IP address, use the standard form of four integer values delimited by "`.`" (periods). For example, use *xxx.xxx.xxx.xxx*, where *xxx* is an integer from 0-255. Zero suppression can be used to specify the integer. If the `-s` option is omitted, the filtering rule is applied to all IP packets received via the specified network interface.
`-y`	Automatically answers "`y`" (no) to all prompts.

EXTENDED DESCRIPTION

- When the command is executed, a prompt to confirm execution of the command with the specified options is displayed. Enter "`y`" to execute the command or "`n`" to cancel the command.
- The IP packet filtering rules are applied in the order in which they are defined.
- Rules for permitted senders must be defined before filter restrictions. First, configure permitted senders; then, configure the setting for dropped packets. If specified in reverse order, all IP packets will be dropped.
- Improper filtering rules can prevent normal network functions for the interface.
- If both the `-i` *interface* and the `-s` *address* [/*mask*] options are omitted, the rule is applied to all IP packets received through XSCF-LAN.
- If the netmask value specified by the `-s` *address* [/*mask*] option does not correspond to any of the following, an error results.
  - Only the most significant bit is 1
  - Repeated 1 from the most significant bit
- A rule which overlaps with an already-defined IP packet filtering rule cannot be set.
- Up to 16 IP packet filtering rules can be set.

- If a message indicates that the XSCF must be reset, do so using the `rebootxscf`(8) command. .
- Use the `showpacketfilters`(8) command to display the current IP packet filtering rules.

EXAMPLES

EXAMPLE 1 Drops the IP packet sent from the IP address 10.10.10.10.

```
XSCF> setpacketfilters -c add -s 10.10.10.10 -j DROP
-s 10.10.10.10/255.255.255.255 -j DROP
NOTE: applied IP packet filtering rules.
Continue? [y|n] :y
XSCF>
```

EXAMPLE 2 On M3000/M4000/M5000 servers, communication to xscf#0-lan#0 exclusively accepts those IP packets sent from the 192.168.100.0/255.255.255.0 network.

```
XSCF> setpacketfilters -c add -s 192.168.100.0/255.255.255.0 -i \
xscf#0-lan#0 -j ACCEPT
-s 192.168.100.0/255.255.255.0 -i xscf#0-lan#0 -j ACCEPT
NOTE: applied IP packet filtering rules.
Continue? [y|n] :y
XSCF> setpacketfilters -c add -i xscf#0-lan#0 -j DROP
-s 192.168.100.0/255.255.255.0 -i xscf#0-lan#0 -j ACCEPT
-i xscf#0-lan#0 -j DROP
NOTE: applied IP packet filtering rules.
Continue? [y|n] :y
XSCF>
```

EXAMPLE 3 Deletes the IP packet drop setting which has been set in the IP address 10.10.10.10..

```
XSCF> showpacketfilters -a
-s 172.16.0.0/255.255.0.0 -i xscf#0-lan#0 -j DROP
-s 10.10.10.10/255.255.255.255 -j DROP
XSCF>
XSCF> setpacketfilters -c del -s 10.10.10.10 -j DROP
-s 172.16.0.0/255.255.0.0 -i xscf#0-lan#0 -j DROP
NOTE: applied IP packet filtering rules.
Continue? [y|n] :y
XSCF>
```

EXAMPLE 4 Clears all IP packet filtering rules which have been set.

```
XSCF> setpacketfilters -c clear
(none)
```

```
NOTE: applied IP packet filtering rules.
Continue? [y|n] :y
XSCF>
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

showpacketfilters(8)

NAME

setpasswordpolicy - manage the system password policy

SYNOPSIS

setpasswordpolicy [-d *dcredit*] [-e *expiry*] [-i *inactive*] [-k *diflk*] [-l *lcredit*] [-M *maxdays*] [-m *minlen*] [-n *mindays*] [-o *ocredit*] [-r *remember*] [-u *ucredit*] [-w *warn*] [-y *retry*]

setpasswordpolicy -h

DESCRIPTION

setpasswordpolicy(8) allows an administrator to change the system password policy. These policies are enforced by XSCF on the Service Processor. The new password policy applies only to users added after the setpasswordpolicy(8) command is executed.

When a user is created, the adduser(8) command uses the *expiry*, *inactive*, *maxdays*, *mindays*, and *warn* paramaters as the password settings for the new account. The password(8) command can be used to change the password expiration settings for an existing account.

Privileges

You must have useradm privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-d *dcredit* — Sets the maximum credit for digits in a password. The minimum acceptable password length is decreased by one for each digit in the password, up to *dcredit* value. Valid values are integers with value of 0 - 999999999. The initial setting is 1. See EXAMPLE 2.

-e *expiry* — Sets the number of days a new account will be valid before expiring and becoming disabled. This value is assigned to new user accounts when they are created. The initial value is 0. A zero means that the account will not expire. Valid values are integers with value of 0 - 999999999.

-h — Displays usage statement.

When used with other options or operands, an error occurs.

-i *inactive* — Sets the number of days after a password expires until the account is locked. This value is assigned to new user accounts when they are created. The initial value is -1. A value of -1 means that the account will not be locked after the password expires. Valid values are integers with value of -1 - 999999999.

-k *difok* — Sets the minimum number of new characters (characters which were not present in the old password) that a new password must contain. The initial setting is 3.

Valid values are integers with value of 0 - 999999999.

`-l` *lcredit*
: Sets the maximum credit for lowercase letters in a password. The minimum acceptable password length is decreased by one for each lowercase letter in the password, up to *lcredit* value. Valid values are integers with value of 0 - 999999999. The initial setting is `1`. See EXAMPLE 2.

`-M` *maxdays*
: Sets the maximum number of days that a password is valid. This value is assigned to new user accounts when they are created. The initial value is `999999`.

  Valid values are integers with value of 0 - 999999999.

`-m` *minlen*
: Sets the minimum acceptable password length if no password credits are applied. If credits are specified by options `-d`, `-u`, `-l`, and `-o`, the required password length is reduced when the specified character types are used.

  Note - Passwords cannot contain fewer than 6 characters regardless of credits.

  Valid values are integers with value of 6 - 99999999. See EXAMPLE 2.

`-n` *mindays*
: Sets the minimum number of days between password changes. An initial value of zero for this field indicates that you can change the password at any time. This value is assigned to new user accounts when they are created.

  Valid values are integers with value of 0 - 999999999.

`-o` *ocredit*
: Sets the maximum credit for nonalphanumeric characters in a password. The minimum acceptable password length is decreased by one for each nonalphanumeric character in the password, up to *ocredit* value. Valid values are integers with value of 0 - 999999999. The initial setting is `1`. See EXAMPLE 2.

`-r` *remember*
: Sets the number of passwords remembered in password history. Valid values are integers 1 - 10. The initial setting is 3. A zero value is not supported and will prevent further password modification by the user.

`-u` *ucredit* Sets the maximum credit for uppercase letters in a password. The minimum acceptable password length is decreased by one for each uppercase letter in the password, up to *ucredit* value. Valid values are integers with value of 0 - 999999999. The initial setting is `1`. See EXAMPLE 2.

`-w` *warn* Sets the default number of days before password expiration at which to start warning the user. This value is assigned to new user accounts when they are created. The initial value is `7`.

Valid values are integers with value of 0 - 999999999.

`-y` *retry* Sets the number of retries permitted when using the password command to change the password for a user account. The initial value is `3`.

Valid values are integers with value of 0 - 999999999.

EXAMPLES

EXAMPLE 1 Setting the Minimum Size and Number of Passwords Remembered

```
XSCF> setpasswordpolicy -m 12 -r 5
```

EXAMPLE 2 Setting Minimum Password Length and Maximum Credits

```
XSCF> setpasswordpolicy -m 10 -d 1 -u 0 -l 0 -o 1
```

After running this command, the minimum password length for new passwords is 10 characters. A password of 9 characters is accepted if it contains at least one digit or nonalphanumeric character. A password of 8 characters is accepted if it contains a digit and a nonalphanumeric character.

EXIT STATUS

The following exit values are returned:

`0` Successful completion.

`>0` An error occurred.

SEE ALSO

adduser`(8)`, **password**`(8)`, **showpasswordpolicy**`(8)`

NAME

setpowerupdelay - set the warm-up time of the system and wait time before system startup

SYNOPSIS

setpowerupdelay -c warmup -s *time*

setpowerupdelay -c wait -s *time*

setpowerupdelay -h

DESCRIPTION

The setpowerupdelay(8) command sets the warm-up time of the system and wait time before system startup.

The wait time before system startup can be used to control the system startup time so that the system is started only after air-conditioning makes the temperature of the computer room suitable. If the system power has already been turned on and the system is operating, the setting takes effect at the next startup.

Privileges

You must have platadm or fieldeng privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-c warmup	Specifies the warm-up time.
-c wait	Specifies the wait time before system startup.
-h	Displays usage statement. When used with other options or operands, an error occurs.
-s *time*	Specifies the warm-up time or wait time before system startup in minutes. An integer ranging from 0 to 255 can be specified for time.

EXTENDED DESCRIPTION

- You can use the showpowerupdelay(8) command to check the warm-up time and the wait time before system startup, previously set by the setpowerupdelay(8) command, regardless of whether the system is in operation.
- When the power is turned on from the operator panel, the wait time and warm-up time that you set are ignored. If you have set these times and wish to observe them at startup, perform the poweron(8) command.

EXAMPLES

EXAMPLE 1 Sets the warm-up time to 10 minutes.

```
XSCF> setpowerupdelay -c warmup -s 10
```

EXAMPLE 2 Sets the wait time before system startup to 20 minutes.

```
XSCF> setpowerupdelay -c wait -s 20
```

EXIT STATUS

The following exit values are returned:

`0`	Successful completion.
`>0`	An error occurred.

SEE ALSO

showpowerupdelay`(8)`

NAME

setprivileges - assign user privileges

SYNOPSIS

setprivileges *user* [privileges] [*domainprivilege@domains*]

setprivileges -h

DESCRIPTION

setprivileges(8) assigns privileges to an XSCF user. setprivileges modifies only local privileges data. Multiple privileges are separated by one or more spaces. There is a maximum of 100 unique users to whom privileges can be assigned. Each of the 100 unique user can be assigned more than one privilege. A list of privileges can be found in the OPERANDS section.

The privileges domainop, domainmgr, and domainadm must be assigned to a specific domain. Other privileges do not have this ability. Refer to the OPERANDS section and EXAMPLE 1 for details.

If no privileges are specified, setprivileges deletes any local privilege data for the specified user. Subsequently, the user's privilege data is looked up in Lightweight Directory Access Protocol (LDAP), if LDAP privilege lookup is enabled.

If the none privilege is specified, the specified user does not have any privileges, regardless of privilege data in LDAP.

Privileges

You must have useradm privileges to run this command.

OPTIONS

The following option is supported:

-h Displays usage statement.

When used with other options or operands, an error occurs.

OPERANDS

The following operands are supported:

domainprivilege@domains

Specifies `domainadm`, `domainmgr`, or `domainop` privileges for a specific domain or domains.

The following are valid values for *domainprivilege*, each of which must be used with `@`*domains*:

`domainadm`	Can perform all operations and view status on the hardware assigned to the domains on which this privilege is held (assign, unassign, power, and so on). Can perform all operations on domains on which this privilege is held. Can view all states of domains on which this privilege is held.
`domainmgr`	Can reboot and power on and off all domains on which this privilege is held. Can view all states of all hardware assigned to the domains on which this privilege is held. Can view all states of domains on which this privilege is held.
`domainop`	Can view all states of all the hardware assigned to the domains on which this privilege is held. Can view all states of all domains on which this privilege is held.
domains	Specifies a domain or domains, using the appropriate value for *domainprivilege* with the `@` symbol and the *domains* descriptor: To specify a single domain, use the `@` symbol followed by a single domain number. Example: `domainadm@3`. To specify a range of domains, use a "–" to indicate to start and end of the domains in the range, inclusive. Example: `domainadm@3-4`. To specify multiple single domains and multiple domain ranges, separate the domains or domain ranges with commas. Do not repeat domains or cause them to overlap or an error will result. Example: `domainadm@1-2,4`.

privileges

The following are valid values for *privileges*:

`auditadm`	Can configure auditing. Can delete audit trail.
`auditop`	Can view all audit state and audit trail.
`fieldeng`	Can perform all operations reserved for field engineers and authorized service personnel.
`none`	Cannot perform any operations on the Service Processor that require privilege, even if privileges are set for the user in LDAP. This privilege allows the administrator to restrict access to such operations on the Service Processor and domains.
`platadm`	Can perform all Service Processor configuration other than the `useradm` and `auditadm` tasks. Can assign and unassign hardware from domains, perform domain and XSCF power operations and all operations on domain hardware (assign, unassign, power, and so on). Can perform Service Processor failover operations and view all platform states.
`platop`	Can view all platform states but not perform any modifications.
`useradm`	Can create, delete, disable, or enable user accounts. Can change a user's password and password properties (for example, *expiry*). Can modify a user's privileges.

user

Specifies a valid user name.

EXAMPLES

EXAMPLE 1 Setting Privileges for JSmith

```
XSCF> setprivileges jsmith platadm domainadm@1-4,6,9
```

EXAMPLE 2 Removing All Privileges for JSmith

```
XSCF> setprivileges jsmith none
```

EXIT STATUS

The following exit values are returned:

`0`	Successful completion.
`>0`	An error occurred.

SEE ALSO

setpasswordpolicy`(8)`, **showuser**`(8)`

NAME

setroute - set routing information for an XSCF network interface

SYNOPSIS

setroute -c{add|del} -n *address* [-m *address*] [-g *address*] *interface*

setroute -h

DESCRIPTION

setroute(8) command sets routing information for an XSCF network interface.

Up to eight routing information items can be registered for each network interface. Any attempt to register more than eight items causes an error.

Privileges

You must have platadm privilege to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-c {add|del}

Specifies a function for routing information. One of the following values can be specified. If none of them is specified, an error occurs.

add — Adds routing information.

del — Deletes routing information.

-g *address*

Specifies a gateway address used for routing. To specify *address*, use the standard form of four integer values delimited by "." (periods). For example, use *xxx.xxx.xxx.xxx*, where *xxx* is an integer from 0-255. Zero suppression can be used to specify the integer.

You cannot specify the loopback address (127.0.0.0/8), the network address, or a broadcast address.

When you specify a default route for a certain interface, the specified gateway must be part of the same network for that interface. For example, if xscf#0-lan#0 has IP address 192.168.10.154 with netmask 255.255.255.0, the specified gateway must also be in network 192.168.10.0/24.

`-h`

Displays usage statement. When used with other options or operands, an error occurs.

`-m` *address*

Specifies the netmask to which routing information is forwarded. To specify *address*, use the standard form of four integer values delimited by "`.`" (periods). For example, use *xxx.xxx.xxx.xxx*, where *xxx* is an integer from 0-255. Zero suppression can be used to specify the integer.

If you omitted the `-m` option, or if the destination IP address is other than 0.0.0.0 and you specified 0.0.0.0 to the netmask, any of the netmask will be set according to the address specified by using the `-n` option.

- In case of a "class A" address:

  If the host portion of the address (lower 24 bits) is "0" (e.g. 20.0.0.0), then the netmask value 255.0.0.0 will be set.

  If the host portion of the address (lower 24 bits) is other than "0" (e.g. 20.18.108.10), then the netmask value 255.255.255.255 will be set.
- In case of a "class B" address:

  If the host portion of the address (lower 16 bits) is "0" (e.g. 136.18.0.0), then the netmask value 255.255.0.0 will be set.

  If the host portion of the address (lower 16 bits) is other than "0" (e.g. 136.18.108.10), then the netmask value 255.255.255.255 will be set.
- In case of a "class C" address:

  If the host portion of the address (lower 8 bits) is "0" (e.g. 200.18.108.0), then the netmask value 255.255.255.0 will be set.

  If the host portion of the address (lower 8 bits) is other than "0" (e.g. 200.18.108.10), then the netmask value 255.255.255.255 will be set.

If you specified 0.0.0.0 in the `-n` option, you must specify 0.0.0.0 in the `-m` option or you must omit the `-m` option.

`-n` *address*

Specifies an IP address to which routing information is forwarded. To specify *address*, use the standard form of four integer values delimited by "`.`" (periods). For example, use *xxx.xxx.xxx.xxx*, where *xxx* is an integer from 0-255. Zero suppression can be used to specify the integer.

If 0.0.0.0 is specified for *address*, the default routing information is set.

OPERANDS

The following operand is supported:

interface

Specifies the network interface to be set with routing information. One of the following values can be specified:

- In M3000/M4000/M5000 servers:

For XSCF unit 0:

`xscf#0-lan#0`	XSCF-LAN#0
`xscf#0-lan#1`	XSCF-LAN#1

For abbreviation:

`lan#0`	XSCF-LAN#0
`lan#1`	XSCF-LAN#1

- In M8000/M9000 servers:

For XSCF unit 0:

`xscf#0-lan#0`	XSCF-LAN#0
`xscf#0-lan#1`	XSCF-LAN#1

For XSCF unit 1:

`xscf#1-lan#0`	XSCF-LAN#0
`xscf#1-lan#1`	XSCF-LAN#1

EXTENDED DESCRIPTION

- In the following cases, the `setroute`(8) command results in an error.
  - When you tried to set more than eight routing information
  - When the netmask that specified by using the `-m` *addr* option does not correspond to any of the cases below:

    - Only the most significant bit is 1

    - Repeated 1 from the most significant bit

    - All bits are zero
  - When you set the routing to ISN
  - When you set a subnet which is the same with ISN
  - When you set a subnet which is the same with DSCP
  - On M8000/M9000 servers, when you set the routing to the takeover IP address
- Only the routing information that has been added by using the `setroute`(8) command can be deleted.

- To reflect the routing information to XSCF, execute the `applynetwork`(8) command. After reflected the information, use the `rebootxscf`(8) command to reset XSCF to complete the setting.
- The `showroute`(8) command can display the current routing information that is set for the XSCF network.

EXAMPLES

EXAMPLE 1 Adds the routing of destination 192.168.1.0 and netmask 255.255.255.0 for XSCF-LAN#0 on XSCF unit 0.

```
XSCF> setroute -c add -n 192.168.1.0 -m 255.255.255.0 xscf#0-lan#0
```

EXAMPLE 2 Adds the routing of destination 192.168.1.0 and gateway 192.168.1.1 for XSCF-LAN#1 on XSCF unit 0.

```
XSCF> setroute -c add -n 192.168.1.0 -g 192.168.1.1 xscf#0-lan#1
```

EXAMPLE 3 Adds the routing of destination 192.168.1.0 and default netmask (255.255.255.0) for XSCF-LAN#1 on XSCF unit 0.

```
XSCF> setroute -c add -n 192.168.1.0 xscf#0-lan#1
```

EXAMPLE 4 Deletes the routing of destination 192.168.1.0 and default netmask (255.255.255.0) from XSCF-LAN#1 on XSCF unit 0.

```
XSCF> setroute -c del -n 192.168.1.0 -m 255.255.255.0 xscf#0-lan#1
```

EXAMPLE 5 Adds the routing of destination 192.168.1. 4 for XSCF-LAN#1 on XSCF unit 0.

```
XSCF> setroute -c add -n 192.168.1.4 xscf#0-lan#1
```

EXAMPLE 6 Deletes the routing of destination 192.168.1. 4 from XSCF-LAN#1 on XSCF unit 0.

```
XSCF> setroute -c del -n 192.168.1.4 xscf#0-lan#1
```

EXAMPLE 7 Adds routing information for the default gateway 192.168.10.1 for XSCF-LAN#1 on XSCF unit 0.

```
XSCF> setroute -c add -n 0.0.0.0 -g 192.168.10.1 xscf#0-lan#1
```

EXIT STATUS

The following exit values are returned:

`0`	Successful completion.
`>0`	An error occurred.

SEE ALSO

applynetwork (8), **showroute** (8)

NAME

setshutdowndelay - set the shutdown wait time at power interruption of the uninterruptible power supply (UPS)

SYNOPSIS

setshutdowndelay -s *time*

setshutdowndelay -h

DESCRIPTION

The setshutdowndelay(8) command sets the wait time before the start of system shutdown for when power interruption occurs in a system connected to the UPS.

The start of system shutdown can be delayed until the specified time. When power recovery is reported from the UPS within the specified time, shutdown will not occur.

Privileges

You must have platadm or fieldeng privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-h	Displays usage statement. When used with other options or operands, an error occurs.
-s *time*	Specifies the wait time before the start of shutdown in units of seconds. Specify an integer number ranging from 0 to 9999 for *time*. The default value is 10 seconds.

EXTENDED DESCRIPTION

The currently set wait time can be displayed by using the showshutdowndelay(8) command.

EXAMPLES

EXAMPLE 1 Sets 600 seconds as the wait time before the start of shutdown.

```
XSCF> setshutdowndelay -s 600
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

showshutdowndelay(8)

NAME

setsmtp - set up the Simple Mail Transfer Protocol (SMTP) settings

SYNOPSIS

setsmtp [-v]

setsmtp [-s *variable*=*value*] ...

setsmtp -h

DESCRIPTION

setsmtp(8) sets up the SMTP configuration values.

When used without options, this command prompts for the name of the SMTP email server to be used, and for the port and the Reply-To address to be used on outgoing email. Make sure that a valid email address is specified here. The -s option lets you specify SMTP settings noninteractively.

After you have set up the email server and port have been set up using setsmtp(8), you can use setemailreport(8) to set up email report configuration data and send a test email message.

Privileges

You must have platadm privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

`-h` Displays usage statement.

When used with other options or operands, an error occurs.

`-s` *variable=value* Sets SMTP.

Valid entries for *variable* are:

`mailserver`
`port`
`auth`
`user`
`password`
`replyaddress`

Where:

`mailserver` is specified by IP address or server name. Server name, if specified, must be resolvable.

`port` is the port address for replies.

`auth` is the authentication mechanism. Valid values are: `none`, `pop`, and `smtp-auth`.

`user` and `password` are for smtp mail service authentication.

`replyaddress` is the address to which replies are sent. This value can be specified in the format that complies with Section 3.4.1 of RFC 5322.

`-v` Specifies verbose output.

EXAMPLES

EXAMPLE 1 Setting Up Mailserver and No Authentication in Noninteractive Mode

```
XSCF> setsmtp -s mailserver=10.4.1.1 -s auth=none
```

EXAMPLE 2 Setting Up Authentication in Noninteractive Mode

```
XSCF> setsmtp -s auth=pop -s user=jsmith -s password=******
```

EXAMPLE 3 Setting Up SMTP Authentication in Interactive Mode

```
XSCF> setsmtp
Mail Server [10.4.1.1]:
Port [25]:
Authentication Mechanism [none]: smtp-auth
 User Name []: jsmith
 Password []: ******
Reply Address [useradm@company.com]:
```

EXAMPLE 4 Setting Up Mailserver With Invalid Authentication Mechanism

```
XSCF> setsmtp
Mail Server [10.4.1.1]:
Port [25]:
Authentication Mechanism [none]: ?
Invalid value '?'. Valid authentication mechanism are: none pop smtp-auth
Authentication Mechanism [none]:
Reply Address [useradm@company.com]:
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

setemailreport(8), **setnameserver**(8), **showsmtp**(8)

NAME

setsnmp - manage the SNMP agent

SYNOPSIS

setsnmp `enable` [*mib_name*]

setsnmp `disable` [*mib_name*]

setsnmp `addtraphost -t` *type* `-s` *community-string* [`-p` *trap-port*] *traphost*

setsnmp `remtraphost -t` *type traphost*

setsnmp `addv3traphost -u` *username* `-r` *authentication-protocol* {`-n` *engine_id* | `-i`} [`-a` *authentication-password*] [`-e` *encryption-password*] [`-p` *trap-port*] *traphost*

setsnmp `remv3traphost -u` *username traphost*

setsnmp `enablev1v2c` *read-only-community-string*

setsnmp `disablev1v2c`

setsnmp [`-l` *system-location*] [`-c` *system-contact*] [`-d` *system-description*] [`-p` *agent-port*]

setsnmp `default`

setsnmp `-h`

DESCRIPTION

`setsnmp`(8) enables or disables the SNMP agent, as well as configures the SNMP agent settings.

Privileges

You must have `platadm` privileges to run this command.

Refer to `setprivileges`(8) for more information.

OPTIONS

The following options are supported:

`-c` *system-contact*	Specifies the system contact information for the agent.
`-d` *system-description*	Specifies the system description for the agent.
`-h`	Displays usage statement. When used with other options or operands, an error occurs.
`-l` *system-location*	Specifies the system location for the agent.
`-p` *agent-port*	Specifies the listening port for the agent. The default is `161`.
`-s` *community-string*	Acts like a password to control access to the SNMP v1 and v2 agents. It is a clear text string which can be intercepted. For password encryption and no visibility, use `addv3traphost` instead.

OPERANDS

The following operands are supported:

`addtraphost` Enables the SNMP agent to send the chosen type of trap to the desired host. If no *trap-port* is provided, the default is `162`. A community string is mandatory.

`addtraphost` takes the following options and operand:

`-p` *trap-port*	ID of the trap port. Default value is 162.
`-s` *community-string*	Acts like a password to control access to the SNMP v1 and v2 agents. It is a clear text string which can be intercepted. For password encryption and no visibility, use `addv3traphost` instead.
`-t` *type*	Type of trap. Valid trap types are: `v1` = The agent sends SNMPv1 traps `v2` = The agent sends SNMPv2 traps `inform` = The agent sends inform notifications
traphost	Host name or IP address of the trap host.

`addv3traphost` Enables the SNMP agent to send SNMPv3 traps or informs to the desired host. An authentication protocol must be chosen. Valid protocols are:

`MD5` = Uses the MD5 algorithm for authentication

`SHA` = Uses SHA (Secure Hash Algorithm) for authentication

The encryption protocol used in all communication is DES (Data Encryption Standard). If the password option is not used, you will be prompted for a password. Passwords will be read but not echoed to the screen. `addv3traphost` takes the following options:

`-a` *authentication-password*

Sets the authentication password. Must be equal to or greater than 8 characters.

`-e` *encryption-password*

Sets the encryption password.

`-i`

Asks for an acknowledgment from the receiving host.

`-n` *engine_id*

Sets identifier of the local agent sending the trap. It can be the engine ID of the local SNMP agent or not but it must match the engine ID expected by the receiving host. Must start with "`0x`" and should consist of even hexadecimal characters or you will get an error.

`-p` *trap-port*

ID of the trap port. Default value is 162.

`-r` *authentication-protocol*

Sets the authentication protocol.

traphost

Host name or IP address of the trap host.

`-u` *username*

Specifies a valid user name.

`default` Stops the SNMP agent and changes the SNMP configuration to the factory default settings. After using this option, SNMP must be configured again before the SNMP agent is restarted.

When used with `default`, the command also stops the SNMP agent for Sun MC in servers running Sun MC. The Sun MC configuration is not affected, but to enable SNMP for Sun MC again, execute the `setsunmc`(8) command with its -s option – **`setsunmc -s`** *sunmc-server*, where *sunmc-server* is the server hostname previously set – then, execute **`setsnmp enable`**. And then execute **`setsunmc enable`**. For more information, see `setsunmc`(8).

`disable` When used alone or with the value `ALL` for the optional *mib_name*, stops the SNMP agent.

When used with a value other than `ALL` for the optional *mib_name*, removes support for the targeted MIB module. If support remains for another MIB module, the SNMP agent remains enabled. If support for both MIB modules is removed, the SNMP agent is disabled and, therefore, stops. You can specify only one value at a time for *mib_name*.

mib_name

Name of the MIB module to be disabled.

Valid MIB modules are:

`SP_MIB` = XSCF extension MIB

`FM_MIB` = Fault Management MIB

`ALL` = All the MIB modules in this list.

`disablev1v2c` Disables the SNMP agent from communicating using SNMPv1/v2c. These versions provide insecure SNMP communication.

`enable`

When used alone, activates the SNMP agent with support for all MIB modules.

When used with the value `ALL` for the optional *mib_name*, activates the SNMP agent with support for all MIB modules.

When used with a value other than `ALL` for the optional *mib_name*, adds support for the targeted MIB module and, if necessary, activates the SNMP agent. You can specify only one value at a time for *mib_name*.

mib_name

Name of the MIB module to be enabled.

Valid MIB modules are:

`SP_MIB` = XSCF extension MIB

`FM_MIB` = Fault Management MIB

`ALL` = All the MIB modules in this list.

`enablev1v2c`

Enables the SNMP agent to communicate using SNMPv1/v2c. These versions provide insecure SNMP communication, which is why the agent runs SNMPv3 by default. This agent is read-only. The only community string asked for is read-only.

`remtraphost`

Disables the SNMP agent from sending the chosen type of trap to the desired host.

`-t` *type*

Type of trap. Valid trap types are:

`v1` = The agent will send SNMPv1 traps

`v2` = The agent will send SNMPv2 traps

`inform` = The agent will send inform notifications

traphost

Host name or IP address of the trap host.

`remv3traphost`

Disables the SNMP agent from sending SNMPv3 traps to the desired host.

traphost

Host name or IP address of the trap host.

`-u` *username*

Specifies a valid user name.

EXAMPLES

EXAMPLE 1 Setting Up System Information

```
XSCF> setsnmp -l sandiego -c username@company.com -d ff1
```

EXAMPLE 2 Setting Up and SNMPv3 Trap Host With Password Options

```
XSCF> setsnmp addv3traphost -u jsmith -n 0x### -r SHA -a xxxxxxxx \
-e yyyyyyyy fiche
```

EXAMPLE 3 Setting Up and SNMPv3 Trap Host without Password Options

```
XSCF> setsnmp addv3traphost -u bob -i -r SHA fiche
Authentication Password:
Encryption Password:
```

EXAMPLE 4 Starting the Agent

```
XSCF> setsnmp enable SP_MIB
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

setsunmc(8), **showsnmp**(8)

NAME

setsnmpusm - specify the SNMPv3 agent's User-based Security Model (USM) configuration

SYNOPSIS

setsnmpusm `create -a` *authentication_protocol* [`-p` *authentication_password*] [`-e` *encyrption_password*] *user*

setsnmpusm `delete` *user*

setsnmpusm `clone -u` *clone_user user*

setsnmpusm `passwd` [`-c` {`auth` | `encrypt`}] [`-o` *old_password*] [`-n` *new_password*] *user*

setsnmpusm `-h`

DESCRIPTION

`setsnmpusm`(8) modifies the SNMP Agent's USM configuration.

Privileges

You must have `platadm` privileges to run this command.

Refer to `setprivileges`(8) for more information.

OPTIONS

The following options are supported:

`-h` Displays usage statement.

When used with other options or operands, an error occurs.

OPERANDS

The following operands are supported:

`clone`

Makes the supplied user known to the agent for subsequent SNMP communication with the identical settings as the specified *clone_user*.

`-u` *clone_user*

Specifies a valid user name of the user settings to be cloned.

user

Specifies a different user name for the clone of *clone_user*.

`create`

Makes the supplied user known to the agent for subsequent SNMP communication. When used without the `-a` or `-p` options, `create` displays a prompt for passwords and reads them without echoing them to the screen. The encryption protocol used in all SNMP communication is Data Encryption Standard (DES). An authentication protocol must be chosen for SNMP communication. Possible values are MD5 Algorithm and Secure Hash Algorithm (SHA).

user

Specifies a valid user name.

`-a` *authentication_protocol*

Specifies the authentication protocol.

`-e` *encryption_password*

Specifies the encryption password. Must be equal to or greater than 8 characters.

`-p` *authentication_password*

Specifies the authentication password. Must be equal to or greater than 8 characters.

`delete`

Removes the supplied user making the user unknown to the agent for subsequent SNMP communication.

user Specifies a valid user name.

`passwd`

Changes the appropriate password for the specified user. The changed password is either the authentication password or the encrypted password, or both, if `-c` is not used. If `-c` is not used then both passwords must be the same or an error is generated. With no options, `password` displays a prompt for the passwords and reads them without echoing them to the screen.

`-c auth|encrypt`	Specifies whether to change the authentication password or the encrypted password.
`-n` *new_password*	Specifies the new password. The password must be equal to or greater than 8 characters.
`-o` *old_password*	Specifies the old password.
user	Specifies a valid user name.

EXAMPLES

EXAMPLE 1 Adding a User With Password Options

```
XSCF> setsnmpusm create -a SHA -p xxxxxxxx -e yyyyyyyy jsmith
```

EXAMPLE 2 Adding a User Without Specifying Password Options

```
XSCF> setsnmpusm create -a SHA bob
Authetication Password:
Encryption Password:
```

EXAMPLE 3 Cloning a User

```
XSCF> setsnmpusm clone -u sue joe
Authentication Password:
Encryption Password:
```

EXAMPLE 4 Deleting a User

```
XSCF> setsnmpusm delete joe
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

showsnmpusm(8)

NAME

setsnmpvacm - modify the SNMPv3 agent's View-based Access Control Model (VACM) configuration

SYNOPSIS

setsnmpvacm `creategroup -u` *username groupname*

setsnmpvacm `deletegroup -u` *username groupname*

setsnmpvacm `createview -s` *OID_subtree* [`-e`] [`-m` *OID_Mask*] *viewname*

setsnmpvacm `deleteview -s` *OID_subtree viewname*

setsnmpvacm `createaccess -r` *read_viewname groupname*

setsnmpvacm `deleteaccess` *groupname*

setsnmpvacm `-h`

DESCRIPTION

`setsnmpvacm`(8) modifies the SNMP Agent's VACM configuration. Using this command requires a basic knowledge of SNMP.

Privileges

You must have `platadm` privileges to run this command.

Refer to `setprivileges`(8) for more information.

OPTIONS

The following options are supported:

`-h` Displays usage statement.

When used with other options or operands, an error occurs.

OPERANDS

The following operands are supported:

`createaccess` Sets access to a MIB view for the specified group.

- `-r` *read_viewname* — Specifies an SNMP Agent view.
- *groupname* — Specifies a valid group name.

`creategroup` Sets up a group for the specified user for view access.

- `-u` *username* — Specifies a valid user name.
- *groupname* — Specifies a valid group name.

`createview` Sets up a view of the SNMP Agent exported MIB information. View access is limited to read-only for this Agent. The view is identified through a MIB OID subtree and can be limited to specific portions of that subtree using the OID Mask.

- `-e` — Specifies an excluded view. The default is an included view.
- `-m` *OID_Mask* — Specifies a valid OID subtree mask. By default, the mask is `ff` (entire subtree).
- `-s` *OID_subtree* — Specifies a MIB OID subtree. Values start at `.1` for the entire MIB tree.
- *viewname* — Specifies a valid view name.

`deleteaccess` Removes access entry.

- *groupname* — Specifies a valid group name.

`deletegroup` Removes a group from use.

- `-u` *username* — Specifies a valid user name.
- *groupname* — Specifies a valid group name.

`deleteview` Removes this view from use.

- `-s` *OID_subtree* — Specifies a MIB OID subtree. Values start at `.1` for the entire MIB tree.
- *viewname* — Specifies a valid view name.

EXAMPLES

EXAMPLE 1 Create a Group

```
XSCF> setsnmpvacm creategroup -u jsmith admin
```

EXAMPLE 2 Create a View of the Entire MIB

```
XSCF> setsnmpvacm createview -s .1 all_view
```

EXAMPLE 3 Create a View Where the Subtree Is Excluded

```
XSCF> setsnmpvacm createview -e -s .1.3.6.1.2.1.1 -m fe excl_view
```

EXAMPLE 4 Create Access

```
XSCF> setsnmpvacm createaccess -r all admin
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

showsnmpvacm (8)

NAME

setssh - configure the settings for the Secure Shell (SSH) service used in the XSCF network

SYNOPSIS

setssh [[-q] -{y | n}] -c enable

setssh -c disable

setssh [[-q] {-y | -n}] -m dscp=*mode*

setssh -c addpubkey [-u *user_name*]

setssh -c delpubkey {-a | -s *line*} [-u *user_name*]

setssh [[-q] -{y | n}] -c genhostkey

setssh -h

DESCRIPTION

The setssh(8) command configures the settings for the SSH service used in the XSCF network.

Only SSH2 is supported for XSCF. You can configure the following:

- Starts or stops the SSH service used in the XSCF network
- Accesses control from domain to the SSH service

  Sets whether or not to permit access from domain to the SSH service via the Domain to Service Processor Communications Protocol (DSCP).
- Generates the host public key
- Registers or deletes the user public key

  The user public key can be registered on each user account. Per user account, multiple user public keys can be registered. Per user account, the user public keys can be registered up to 1,023 characters including the linefeed.

Privileges

You must have one of the following privileges to run this command:

- To start or stop the SSH service, to control access from domain to the SSH service, and to generate the host public key:

  platadm
- To register or delete the user public key of other user account:

  useradm
- To register or delete the user public key of the current login user account:

  useradm, platadm, platop, auditadm, auditop, domainadm, domainmgr, domainop, fieldeng

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

`-a`	Deletes all registered user public keys. Should be specified with "`-c delpubkey`."
`-c addpubkey`	Registers the user public key.
`-c delpubkey`	Deletes the user public key.
`-c {enable|disable}`	Specifies whether to enable the SSH service. One of the following values can be specified: `enable` Starts the SSH service. `disable` Stops the SSH service.
`c genhostkey`	Generates a host public key for SSH2.
`-h`	Displays usage statement. When used with other options or operands, an error occurs.
`-m dscp=`*mode*	Specifies whether or not to permit access from domain to the SSH service via DSCP. One of the following values can be specified. It is set to `accept` by default. `accept` Permits access to the SSH service. `deny` Restricts access to the SSH service.
`-n`	Automatically answers "`n`" (no) to all prompts.
`-q`	Suppresses all messages to stdout, including prompts.
`-s` *line*	Specifies the user public key number to delete. For line, specify the number which displayed after the `showssh -c pubkey` command executed. Should be specified with "`-c delpubkey`."
`-u` *user_name*	Specifies the user account name to register or delete the user public key. Should be specified with "`-c addpubkey`" or "`-c delpubkey`." When the `-u` option omitted, the user public key of the current login user account becomes the target.
`-y`	Automatically answers "`y`" (yes) to all prompts.

EXTENDED DESCRIPTION

- If you are an Active Directory or LDAP/SSL user, you cannot register the user piblic key. Log in to the XSCF network through the SSH service by the authentication not with the user public key but with the password.
- When a host public key is created, a prompt to confirm execution of the command with the specified options is displayed. Enter "`y`" to execute the command or "`n`" to cancel the command.

- When a host public key already exists, if you generate a host public key, a prompt to confirm the update is displayed. Enter "y" to update or "n" to cancel the command.
- The setssh(8) command can register one user public key at a time.
- In time of setssh(8) command execution, finish the input of user public key by pressing Enter and then pressing "Ctrl" and "D" (EOF).
- In case the XSCF unit is duplicated configuration, the setting automatically reflected to the standby XSCF. When there is a defect on the standby XSCF, it leads to an error and the setting will be reflected to the active XSCF only.
- When you use the setssh(8) command to generate a host public key or to disable the SSH service (setssh -c disable), the command takes effect immediately. In case of disabling the SSH service, any open SSH sessions are terminated.

  For all other settings using the setssh(8) command, you must reboot the XSCF using rebootxscf(8) command for the changes to take effect.
- Using the showssh(8) command, you can check the current settings of the SSH service.

EXAMPLES

EXAMPLE 1 Starts the SSH service.

```
XSCF> setssh -c enable
Continue? [y|n] :y
Please reset the XSCF by rebootxscf to apply the ssh settings.
```

EXAMPLE 2 Starts the SSH service. Automatically replies with "y" to the prompt.

```
XSCF> setssh -y -c enable
Continue? [y|n] :y
Please reset the XSCF by rebootxscf to apply the ssh settings.
```

EXAMPLE 3 Starts the SSH service. Automatically replies with "y" without displaying the prompt.

```
XSCF> setssh -q -y -c enable
```

EXAMPLE 4 Stops the SSH service.

```
XSCF> setssh -c disable
```

EXAMPLE 5 Generates a host public key for SSH2.

```
XSCF> setssh -c genhostkey
Host key create. Continue? [y|n] :y
```

EXAMPLE 6 Generates a SSH2 host public key, even if one already exists. Automatically replies with "y" to the prompt.

```
XSCF> setssh -c genhostkey -y
Host key already exists. The key will be updated. Continue? [y|n] :y
```

EXAMPLE 7 Generates a host public key for SSH2. Automatically replies with "y" without displaying the prompt.

```
XSCF> setssh -c genhostkey -q -y
```

EXAMPLE 8 Registers the user public key. Finish the input of public key by pressing Enter and then pressing "Ctrl" and "D"

```
XSCF> setssh -c addpubkey
Please input a public key:
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAzFh95SohrDgpnN7zFCJCVNy+jaZPTjNDxcid
QGbihYDCBttI4151Y0Sv85FJwDpSNHNKoVLMYLjtBmUMPbGgGVB61qskSv/
FeV44hefNCZMiXGItIIpK
P0nBK4XJpCFoFbPXNUHDw1rTD9icD5U/wRFGSRRxFI+Ub5oLRxN8+A8=abcd@example.com
[Enter]
[Ctrl]and[D]
```

EXAMPLE 9 Registers the user public key by specifying the user name. Finish the input of public key by pressing Enter and then pressing "Ctrl" and "D".

```
XSCF> setssh -c addpubkey -u efgh
Please input a public key:
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAzFh95SohrDgpnN7zFCJCVNy+jaZPTjNDxcid
QGbihYDCBttI4151Y0Sv85FJwDpSNHNKoVLMYLjtBmUMPbGgGVB61qskSv/
FeV44hefNCZMiXGItIIpK
P0nBK4XJpCFoFbPXNUHDw1rTD9icD5U/wRFGSRRxFI+Ub5oLRxN8+A8=abcd@example.com
[Enter]
[Ctrl]and[D]
```

EXAMPLE 10 Specifies the public key number to delete the user public key.

```
XSCF> setssh -c delpubkey -s 1
 1  ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAzFh95SohrDgpnN7zFCJCVNy+jaZPTjNDxcid
QGbihYDCBttI4151Y0Sv85FJwDpSNHNKoVLMYLjtBmUMPbGgGVB61qskSv/
FeV44hefNCZMiXGItIIpK
P0nBK4XJpCFoFbPXNUHDw1rTD9icD5U/wRFGSRRxFI+Ub5oLRxN8+A8=abcd@example.com
```

EXAMPLE 11 Deletes all user public keys.

```
XSCF> setssh -c delpubkey -a
```

EXAMPLE 12 Restricts access from domain to the SSH service via DSCP.

```
XSCF> setssh -m dscp=deny
Continue? [y|n] :y
Please reset the XSCF by rebootxscf to apply the ssh settings.
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

rebootxscf(8), **showssh**(8)

NAME

setsunmc - start or stop the Sun Management Center agent and make changes to its configuration

SYNOPSIS

setsunmc [enable | disable]

setsunmc [-s *server*] [-z *seed*] [-p *agent_port*] [-c *community_string*] [-t *trap_port*] [-e *event_port*] [-a *SNMP_agent_port*] [-d *dmn_agent_port*]

setsunmc [-h]

DESCRIPTION

When invoked with one or more options, setsunmc makes changes to the Sun Management Center agent configuration, as described in the Options section.

When invoked with the operand enable, setsunmc activates the Sun Management Center agent. This activation includes starting the Sun Management Center agent and notifying the startup daemon to start the agent on subsequent reboots. When invoked with the operand disable, the agent is stopped and the startup daemon will be notified to disable starting the agent on subsequent reboots.

The operands cannot be used together with the options.

Privileges

You must have platadm or fieldeng privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported. The options cannot be used together with the operands.

-a *SNMP_agent_port* Specifies the listening port on the SNMP agent. The default value is 161. Change this value only if you change the port on the SNMP agent.

-c *community_string* Specifies the community string used for SNMPv1 trap host snmp setup. The default value is public.

-d *dmn_agent_port* Specifies the port for the Sun Management Center agents running on the domains. The default value is 1161. This domain agent port is used during creation of a composite object. Sun Management Center domain agents generally use the same port to ensure proper creation of composite object domains.

-e *event_port* Specifies the port on the Sun Management Center server to which events are sent. The default value is 163.

-h Displays usage statement.

When used with other options or operands, an error occurs.

-p *agent_port* Specifies the port number that the Sun Management Center agent listens on. The default value is 1161.

`-s` *server*	Specifies the Sun Management Center server with which the agent will be communicating. The server can be specified using either a host name or an IP address. It must be set prior to enabling the agent.
`-t` *trap_port*	Specifies the port on the Sun Management Center server to which traps are sent. The default value is `162`.
`-z` *seed*	Specifies the seed to generate a security key for communication between Sun Management Center server and agent. This value must be the same as the seed used on the server setup. It must be set prior to enabling the agent.

OPERANDS

The following operands are supported. The operands cannot be used together with the options.

enable	When invoked with the operand `enable`, `setsunmc` activates the Sun Management Center agent. This means the Sun Management Center agent is started, and the startup daemon is notified to start the agent on subsequent reboots.
disable	When invoked with the operand `disable`, `setsunmc` stops the agent, and the startup daemon is notified to disable starting of the agent on subsequent reboots.

EXAMPLES

EXAMPLE 1 Basic Setup Command With Arguments

```
XSCF> setsunmc -s balon -z maplesyr -c double_secret
```

EXAMPLE 2 Starting the Agent

```
XSCF> setsunmc enable
```

EXIT STATUS

No exit values are returned.

SEE ALSO

showsunmc(8)

NAME

settelnet - start or stop the Telnet service used in the XSCF network

SYNOPSIS

settelnet -c {enable | disable}

settelnet -h

DESCRIPTION

settelnet(8) command starts or stops the Telnet service used in the XSCF network.

Privileges

You must have platadm privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-c {enable|disable} Specify whether to start the Telnet service. One of the following values can be specified. If none of them is specified, an error occurs.

enable	Starts the Telnet service.
disable	Stops the Telnet service.

-h Displays usage statement. When used with other options or operands, an error occurs.

EXTENDED DESCRIPTION

Caution – To stop the Telnet service, you must execute the rebootxscf(8) command to reset XSCF. If you fail to reset XSCF, problems might occur when you start the Telnet service next time.

- In the M8000/M9000 servers, the setting automatically reflected to the standby XSCF. When there's a defect on the standby XSCF, it leads to an error and the setting will be reflected to the active XSCF only.
- Stop of the Telnet service is reflected immediately after the settelnet(8) command executed. Any open Telnet sessions are terminated.
- Using the showtelnet(8) command, you can check the current settings of the Telnet service.

EXAMPLES

EXAMPLE 1 Starts the Telnet service.

```
XSCF> settelnet -c enable
```

EXAMPLE 2 Stops the Telnet service.

```
XSCF> settelnet -c disable
Please reset the XSCF by rebootxscf to apply the telnet settings.
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

rebootxscf(8), **showtelnet**(8)

NAME

settimezone - set the time zone and Daylight Saving Time of XSCF

SYNOPSIS

settimezone -c settz -s *timezone*

settimezone -c settz -a [-M]

settimezone -c adddst -b *std* -o *offset* -d *dst* [-p *offset*] -f *date* [/*time*] -t *date* [/*time*]

settimezone -c deldst -b *std* -o *offset*

settimezone -h

DESCRIPTION

The settimezone(8) command sets the time zone and Daylight Saving Time of XSCF.

The time zone provided by default is pursuant to POSIX standard.

Privileges

You must have platadm or fieldeng privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-a — Lists the time zones that can be set.

-c settz — Sets the time zone which complies with POSIX standards. The time zone is applied immediately after the settimezone(8) command executed.

-c adddst — Manually sets the time zone and Daylight Saving Time. Daylight Saving Time complies with the data of time zone which has been specified by using the -b, -o, -d, -p, -f and -t options. In case you set the time zone manually, the time zone data which set by using the "-c settz" option will be ignored. When you execute the settimezone(8) command and then execute the login procedures to XSCF, the configuration will be applied.

-c deldst — Deletes the time zone and Daylight Saving Time which set manually. After the deletion of Daylight Saving Time which set manually, XSCF starts operating with the time zone set by using the "-c settz" option. When you execute the settimezone(8) command and then execute the login procedures to XSCF, the configuration will be applied.

-b *std* — Specifies the abbreviations of time zone. For *std*, specify an abbreviation of 3 letters or more. You can specify it in the format which complies with RFC2822. Specify this option in combination with "-c adddst" or "-c deldst."

`-d` *dst*

Specifies the zone name of Daylight Saving Time. For *dst*, specify the alphabets of 3 letters or more. You can specify it in the format which complies with RFC2822. Specify this option in combination with "`-c adddst`."

`-f` *date* [/*time*]

Specifies the starting time of Daylight Saving Time. It should be specified in the same format as *date* in the `-t` option. You can specify *date* in any of the following formats.

`Mm.w.d`

`M`*m*: Specifies the month to start Daylight Saving Time. For *m*, you can specify any integer from `1` to `12`.

w: Specifies the week to start Daylight Saving Time. You can specify the integer from `1` to `5`, "`1`" for the first week and "`5`" for the last week in the month.

d: Specifies the day of the week to start Daylight Saving Time. You can specify the integer from `0` to `6`, "`0`" for Sunday and "`6`" for Saturday.

`J`*n*

`J`*n*: Specifies the sequential day in the year to start Daylight Saving Time. You can specify the integer from `1` to `365`, "`1`" for January 1st. It does not count the leap-year day. If you specified `365`, it corresponds to December 31st even in a leap year.

n

n: Specifies the sequential day in the year to start Daylight Saving Time. You can specify the integer from `1` to `365`, "`1`" for January 2nd. It counts the leap-year day.

In *time*, you specify the time. You can specify it in the following format.

hh:mm:ss

Specifies the time in "*hh*:*mm*:*ss*" format. *hh* is `00`–`23`, *mm* is `00`–`59`, *ss* is `00`–`60`. In case omitted, "`02:00:00`."

`-h`

Displays usage statement. When used with other options or operands, an error occurs.

`-M`

Displays text by page. This option provides a function that is the same as that of the `more` command.

`-o` *offset*

Specifies the offset of time zone and Greenwich mean time (GMT). Specify this option in combination with "`-c adddst`" or "`-c deldst`." You can specify *offset* in the following format.

`GMT`{+ | −}*hh*[:*mm*[:*ss*]]

`GMT`	Greenwich mean time
{+ | −}	Specifies "−" to set the standard time to the time which is ahead of GMT. (To adjust to the local time east to Greenwich, the offset is a negative value.) Specifies "+" to set the standard time to the time which is behind the GMT. (To adjust to the local tome west to Greenwich, the offset is a positive value.)
hh[:*mm*[:*ss*]]	Specifies the offset time. *hh* is `00–23`, *mm* is `00–59`, *ss* is `00–59`.

`-p` *offset*

Specifies the offset of Daylight Saving Time and Greenwich mean time (GMT). Specify this option in combination with "`-c adddst`." In case omitted, it is 1 hour ahead of the offset time that specified using the `-o` option. You can specify *offset* in the following format.

`GMT`{`+`|`-`}*hh*[:*mm*[:*ss*]]

`GMT`	Greenwich mean time
{`+`|`-`}	Specifies "–" to set the standard time to the time which is ahead of GMT. (To adjust to the local time east to Greenwich, the offset is a negative value.)Specifies "+" to set the standard time to the time which is behind the GMT. (To adjust to the local tome west to Greenwich, the offset is a positive value.)
hh[:*mm*[:*ss*]]	Specifies the offset time. *hh* is `00`–`23`, *mm* is `00`–`59`, *ss* is `00`–`59`.

`-s` *timezone*

Specifies the time zone. Specify this option in combination with "`-c settz`." One of the time zone displayed by the `-a` option can be specified for *timezone*.

`-t` *date* [/*time*] Specifies the termination time of Daylight Saving Time. It should be specified in the same format as *date* in the `-f` option. You can specify *date* in any of the following formats.

`Mm.w.d`

Mm: Specifies the month to terminate Daylight Saving Time. For *m*, you can specify any integer from `1` to `12`.

w: Specifies the week to terminate Daylight Saving Time. You can specify the integer from `1` to `5`, "`1`" for the first week and "`5`" for the last week in the month.

d: Specifies the day of the week to terminate Daylight Saving Time. You can specify the integer from `0` to `6`, "`0`" for Sunday and "`6`" for Saturday.

`J`*n*

`J`*n*: Specifies the sequential day in the year to terminate Daylight Saving Time. You can specify the integer from `1` to `365`, "`1`" for January 1st. It does not count the leap-year day. If you specified `365`, it corresponds to December 31st even in a leap year.

n

n: Specifies the sequential day in the year to terminate Daylight Saving Time. You can specify the integer from `1` to `365`, "`1`" for January 2nd. It counts the leap-year day.

In *time*, you specify the time. You can specify it in the following format.

hh:mm:ss Specifies the time in "*hh*:*mm*:*ss*" format. *hh* is `00`–`23`, *mm* is `00`–`59`, *ss* is `00`–`60`. In case omitted, "`02:00:00`."

EXTENDED DESCRIPTION

- You cannot specify the years of validity for time zone and Daylight Saving Time. In case the Daylight Saving Time is changed each year, you need to set anew by using the `settimezone`(8) command.
- When Daylight Saving Time has been set, XSCF is not affected by the time zone.
- The setting of Daylight Saving Time using `-c adddst` results in an error in any of the following cases:
  - The J*n* or *n* format is used and the period between start and termination is less than 14 days.
  - The M*m.w.d* format is used, start and termination are in the same month, and the period between them is less than two weeks.
  - The value specified for `-o` *offset* is smaller than the value of `-p` *offset*.
  - The difference between `-o` *offset* and `-p` *offset* is larger than 24 hours.

- The addition of the offset time to the standard time which has been set by the `settimezone`(8) command comes to GMT.
- The current time zone settings can be checked by using the `showtimezone`(8) command.
- To apply the Daylight Saving Time information modified by the "`-c adddst`" or the "`-c adddst`" option, log out of XSCF and then log in again.

EXAMPLES

EXAMPLE 1 Sets "`Asia/Tokyo`" as the time zone.

```
XSCF> settimezone -c settz -s Asia/Tokyo
Asia/Tokyo
```

EXAMPLE 2 Lists the time zones that can be set.

```
XSCF> settimezone -c settz -a
Africa/Abidjan
Africa/Accra
Africa/Addis_Ababa
Africa/Algiers
Africa/Asmara
Africa/Asmera
Africa/Bamako
Africa/Bangui
  .
  .
```

EXAMPLE 3 Sets the Daylight Saving Time information as follows: abbreviation of time zone is JST, offset from GMT is +9, zone name of Daylight Saving Time is JDT, Daylight Saving Time is 1 hour ahead, and time period is from the last Sunday of March 2:00(JST) to the last Sunday of October 2:00(JDT).

```
XSCF> settimezone -c adddst -b JST -o GMT-9 -d JDT -f M3.5.0 -t M10.5.0
JST-9JDT,M3.5.0,M10.5.0
```

EXAMPLE 4 Sets the Daylight Saving Time information as follows: abbreviation of time zone is JST, offset from GMT is +9, zone name of Daylight Saving Time is JDT, the offset of Daylight Saving Time from GMT is +10, and time period is from the first Sunday of April 0:00(JST) to the first Sunday of September 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
```

EXAMPLE 5 Deletes the Daylight Saving Time information of current settings.

```
XSCF> settimezone -c deldst -b JST -o GMT-9
```

EXIT STATUS

The following exit values are returned:

`0`	Successful completion.
`>0`	An error occurred.

SEE ALSO

setdate`(8)`, **showdate**`(8)`, **showtimezone**`(8)`

NAME

setupfru - set up device hardware

SYNOPSIS

setupfru [-m {y|n }] [-x {1|4}] *device location*

setupfru -h

DESCRIPTION

The setupfru(8) command makes hardware settings for the specified device.

The setupfru(8) command is not supported on the M3000 server.

Only a physical system board (PSB) can be specified as a device. After a PSB is added, the following settings can be specified for PSB:

XSB type	To use an added PSB in the system, hardware resources on the PSB must be logically divided and reconfigured as eXtended System Boards (XSBs). Two types of XSB are used: Uni-XSB and Quad-XSB. The Uni-XSB is configured with undivided PSB, and the Quad-XSB is configured with one of divided PSB into four parts. Specify either the Uni-XSB configuration or Quad-XSB configuration for the PSB.
Memory mirror mode	In mirror mode, data is mirrored by dividing the memory mounted on a PSB into two parts. Since the memory is divided into two parts, the memory capacity is halved, but data reliability increases. Specify whether to operate the memory in mirror mode.

Privileges

You must have platadm or fieldeng privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-h	Displays usage statement. When used with other options or operands, an error occurs.
-m {y|n}	Specifies whether to use the memory mounted on the XSB in mirror mode. Specify this option when sb is specified for *device*. Specify y to enable mirror mode; otherwise, specify n. If the -m option is omitted, the previous setting is inherited.
-x {1|4}	Specifies whether to configure PSB as a Uni-XSB or Quad-XSB. Specify this option when sb is specified for *device*. Specify 1 for Uni-XSB or specify 4 for Quad-XSB. If the -x option is omitted, the previous setting is inherited.

OPERANDS

The following operands are supported:

device Specifies the device to be set up. Only the following device can be specified:

`sb` Physical system board (PSB)

location Specifies the location of the device.

`sb` Integer from 0–15. Specify only one *location*.

EXTENDED DESCRIPTION

- In the M8000/M9000 server, the Quad-XSB configuration cannot be set in memory mirror mode.
- To set up an already mounted PSB again, all XSBs comprising the target PSB must have been disconnected from the domain configuration and placed under the system board pool. See the `deleteboard`(8) command for information on how to disconnect XSBs from the domain configuration.
- The configuration of the PSB varies according to the system as shown below.
  - In the M8000/M9000 servers, the PSB consists of one CPU/memory board unit and one I/O unit in combination.
  - In the M4000/M5000 servers, the PSB consists of one CPU module and one memory module logically divided into two on the motherboard unit, and one I/O module.
- Although a CMU with two CPUs can be configured into Quad-XSB mode on an M8000/M9000 server, the server generates a "configuration error" message for those XSBs that do not have a CPU and memory.
- The current PSB settings can be checked by using the `showfru`(8) command.

EXAMPLES

EXAMPLE 1 Configures PSB#00 as a Quad-XSB (with memory in non-mirror mode because the memory mirror mode setting is omitted).

```
XSCF> setupfru -x 4 sb 0
```

EXIT STATUS

The following exit values are returned:

`0` Successful completion.

`>0` An error occurred.

SEE ALSO

addboard`(8)`, **deleteboard**`(8)`, **moveboard**`(8)`, **setdcl**`(8)`, **showboards**`(8)`, **showdcl**`(8)`, **showdevices**`(8)`, **showfru**`(8)`

NAME

setupplatform - set up platform specific settings

SYNOPSIS

setupplatform [-v]

setupplatform [-v] -p *part* [-p *part*]

setupplatform -h

DESCRIPTION

The setupplatform(8) command sets up platform specific settings. The command leads an administrator through Service Processor installation tasks.

By default, setupplatform command walks through each of the available settings. Individual settings may be selected using the -p option.

Privileges

You must have one of the following privileges to run this command:

- To use the -p user option: usradm
- To use the -p network, -p altitude, -p timezone options: platadm

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-h — Displays usage statement. When used with other options or operands, an error occurs.

-p *part* — Specifies the setting you want to do. One of the following can be specified for part:

- altitude — Configures the chassis altitude.
- network — Configures the XSCF network, DSCP, DNS, NTP, SSH, https, and SMTP.
- timezone — Sets the time zone for the XSCF. The time zone is chosen from a list of time zones.
- user — Creates a new local XSCF user account with platadm, platop, and useradm privileges. Note that an XSCF user account user name cannot match an LDAP user name, and an XSCF user account (UID) number cannot match an LDAP UID number.

-v — Specifies verbose output.

EXTENDED DESCRIPTION

The available interfaces on the M3000/M4000/M5000 servers are xscf#0-lan#0, xscf#0-lan#1, lan#0, lan#1. The available interfaces on the M8000/M9000 servers are the same but they also include the xscf#0-if, xscf#1-lan#0, xscf#1-lan#1, and xscf#1-if.

In user setup, a new local user account can be created with a user supplied password.

In network setup, the following items can be optionally configured:

- XSCF Network Settings
- Internal DSCP Network
- DNS
- NTP
- SSH
- HTTPS Server
- Email reports

EXAMPLES

EXAMPLE 1 Creating a New User.

```
XSCF> setupplatform -p user
Do you want to set up an account? [y|n]: y
Username: myadminuser
User id in range 100 to 65533 or leave blank to let the system
choose one:
              Username: myadminuser
              User id:
Are these settings correct? [y|n]: y
XSCF> adduser myadminuser
XSCF> setprivileges myadminuser useradm platadm platop
XSCF> password myadminuser
New XSCF password: [not echoed]
Retype new XSCF password: [not echoed]
```

EXAMPLE 2 Configuring the XSCF Network.

```
XSCF> setupplatform
Do you want to set up an account? [y|n]: n
Do you want to set up the XSCF network interfaces? [y|n]: y
Do you want to configure xscf#0-lan#0? [y|n]: y
xscf#0-lan#0 ip address? []: 192.168.1.4
xscf#0-lan#0 netmask? [255.255.255.0]: 255.255.254.0
xscf#0-lan#0 default gateway? []: 192.168.1.1
              xscf#0-lan#0 ip address: 192.168.1.4
              xscf#0-lan#0 netmask: 255.255.254.0
              xscf#0-lan#0 default gateway: 192.168.1.1
Are these settings correct? [y|n]: y
XSCF> setnetwork xscf#0-lan#0 -m 255.255.254.0 192.168.1.4
. . .
```

EXAMPLE 3 Enabling ssh.

```
XSCF> setupplatform -p network
Do you want to set up the XSCF network interfaces? [y|n]: n
Do you want to set up the DSCP network? [y|n]: n
Do you want to set up the domain name service? [y|n]: n
Do you want to set up the network time protocol? [y|n]:n
Do you want to set up ssh? [y|n]: y
Enable ssh service? [y|n]: y
XSCF> setssh -q -y -c enable
Do you want to set up https? [y|n]: n
. . .
```

EXAMPLE 4 Configuring the Altitude.

```
XSCF> setupplatform -p altitude
Do you want to set up the chassis altitude? [y|n]: y
Chassis altitude is already configured:
               Chassis altitude in meters: 200
Continue setting up the chassis altitude? [y|n]: y
Chassis altitude in meters: 400
               Chassis altitude in meters: 400
Is this setting correct? [y|n]: y
XSCF> setaltitude -s altitude=400
400m

The specified altitude becomes valid when the circuit breakers of the
system
are switched on again.
Do you want to reboot the XSCF now? [y|n]: n
XSCF>
```

EXAMPLE 5 Setting the Time Zone.

```
XSCF> setupplatform -p timezone
Do you want to set up the XSCF time zone? [y|n]: y
Chassis time zone is already configured:
               XSCF time zone: US/Pacific
Continue setting up the XSCF time zone? [y|n]: y
0       Africa/Abidjan
1       Africa/Accra
2       Africa/Addis_Ababa
3       Africa/Algiers
4       Africa/Asmera
5       Africa/Bamako
6       Africa/Bangui
7       Africa/Banjul
```

```
8       Africa/Bissau
9       Africa/Blantyre
10      Africa/Brazzaville
11      Africa/Bujumbura
12      Africa/Cairo
13      Africa/Casablanca
14      Africa/Ceuta
15      Africa/Conakry
16      Africa/Dakar
17      Africa/Dar_es_Salaam
18      Africa/Djibouti
19      Africa/Douala
20      Africa/El_Aaiun
21      Africa/Freetown
22      Africa/Gaborone
Enter number to choose time zone or return for next set of time zones: 21
    XSCF time zone: Africa/Freetown
Is this setting correct? [y|n]: y
XSCF> settimezone -c settz -s Africa/Freetown
Africa/Freetown
XSCF>
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

adduser(8), **applynetwork**(8), **password**(8), **setaltitude**(8), **setdscp**(8), **setemailreport**(8), **sethostname**(8), **sethttps**(8), **setnameserver**(8), **setnetwork**(8), **setntp**(8), **setprivileges**(8), **setsmtp**(8), **setssh**(8), **setroute**(8), **settimezone**(8)

NAME

showad - show Active Directory configuration and messages

SYNOPSIS

showad

showad `cert` [`-v`] [`-i` *n*]

showad `log` [`-M`] [`-C`] [`-S` *start_record_number*] [`-E` *end_record_number*]

showad `log -f`

showad `group administrator` [`-i` *n*]

showad `group operator` [`-i` *n*]

showad `group custom` [`-i` *n*]

showad `userdomain` [`-i` *n*]

showad `dnslocatorquery` [`-i` *n*]

showad `defaultrole`

showad `server` [`-i` *n*]

showad `-h`

DESCRIPTION

`showad`(8) displays Active Directory configuration and diagnostic messages.

Privileges

You must have `useradm` privileges to run this command.

Refer to `setprivileges`(8) for more information.

OPTIONS

The following options are supported:

`-f`	Displays diagnostic messages in real time. When this option is used, the command does not terminate. Each diagnostic message is displayed when it is registered. To stop the real-time display, press `Ctrl-C`.
`-h`	Displays usage statement. When used with other options or operands, an error occurs.
`-i` *n*	Sets an index marker, value 1 - 5. When executed without `-i`, or with `-i` and no value, `showad` walks sequentially through items 1 through 5. Exceptions: When used without `-i`, the command `showad cert` displays the certificate information for the Primary server, and `showad server` displays the Primary server configuration.
`-v`	Specifies verbose output. Used only with the cert operand to display the full certificate.

`-C`	Appends to end of output the number of records in the log.
`-E`	Specifies the last record number to display, where *end_record_number* can be any record number in the log. Use `-C` to obtain the number of records in the log.
`-M`	Displays text by page, like the `more`(1) command does.
`-S`	Specifies the first record to display, where *start_record_number* can be any record number in the log. Use `-C` to obtain the number of records in the log.

OPERANDS

The following operands are supported:

cert	Display current server certificates.
log	Display diagnostic messages.
group administrator	Display current group configurations.
group operator	Display current group configurations.
group custom	Display current group configurations.
userdomain	Display current userdomain settings.
dnslocatorquery	Display current DNS locator query configuration.
defaultrole	Display current defaultrole setting.
server	Display current Active Directory server settings.

EXAMPLES

EXAMPLE 1 Displays the current state of the active directory.

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

EXAMPLE 2 Displays certificate information for the Primary server.

```
XSCF> showad cert
Primary Server:
certstatus = certificate present
issuer = C=US, ST=California, L=San Diego, O=aCompany,
OU=System Group, CN=John User serial number = 0 (00000000)
subject = C=US, ST=California, L=San Diego, O=aCompany,
OU=System Group, CN=John User serial number = 0 (00000000)
```

```
valid from = Apr 18 05:38:36 2009 GMT
valid until = Apr 16 05:38:36 2019 GMT
version = 3 (0x02)
```

EXAMPLE 3 Displays specified diagnostic messages.

```
XSCF> showad log -S 5 -E 10
Thu Sep 2 01:43 2009 (ActDir): -error- authentication status: auth-ERROR
Thu Sep 2 01:44 2009 (ActDir): -error- authentication status: auth-ERROR
Thu Sep 2 01:47 2009 (ActDir): -error- authentication status: auth-ERROR
Thu Sep 2 01:51 2009 (ActDir): -error- authentication status: auth-ERROR
Thu Sep 2 01:52 2009 (ActDir): -error- authentication status: auth-ERROR
Thu Sep 2 01:55 2009 (ActDir): -error- authentication status: auth-ERROR
```

EXAMPLE 4 Displays configuration for administrator group 3.

```
XSCF> showad group administrator -i 3
Administrator Group 3
name: CN=pSuperAdmin,OU=Groups,DC=sales,DC=company,DC=com
```

EXAMPLE 5 Displays alternate server 1 setting. A port number of 0 indicates that the default port for Active Directory is used.

```
XSCF> showad server -i 1
Alternate Server  1
address: (none)
port: 0
```

EXAMPLE 6 Displays the dnslocatorquery 1 configuration.

```
XSCF> showad dnslocatorquery -i 1
service 1: \ _ldap._tcp.gc._msdcs.<DOMAIN>.<PORT:3269>
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

setad (8)

NAME

showaltitude - display the altitude of the system and whether the air filter installed

SYNOPSIS

showaltitude

showaltitude -h

DESCRIPTION

The showaltitude(8) command displays the current settings for the altitude of the system and whether the air filter installed.

Whether the air filter installed is displayed on the M4000/M5000 servers only.

The displayed altitude value is a multiple of 100 meters.

Privileges

You must have platadm or fieldeng privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following option is supported:

-h Displays usage statement.

EXTENDED DESCRIPTION

- The air filter is displayed only when it is installed. If the filter is not installed nothing is displayed.
- The setaltitude(8) command sets the altitude of the system and whether or not the air filter installed.

EXAMPLES

EXAMPLE 1 Displays the altitude of the system.

```
XSCF> showaltitude
1000m
```

EXAMPLE 2 Displays the altitude of the M4000/M5000 servers with the air filter installed.

```
XSCF> showaltitude
1000m
Filter is installed.
```

EXIT STATUS

The following exit values are returned:

0 Successful completion.

>0 An error occurred.

SEE ALSO

setaltitude(8)

NAME

showarchiving - display log archiving configuration and status

SYNOPSIS

showarchiving

showarchiving [-e] [-v]

showarchiving -h

DESCRIPTION

showarchiving(8) displays the status and configuration information for log archiving on the Service Processor.

Privileges

You must have platadm, platop or fieldeng privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-e	Displays information about the last ten archiving errors.
-h	Displays usage statement. When used with other options or operands, an error occurs.
-v	Specifies verbose output.

EXTENDED DESCRIPTION

If the -e option is not specified, showarchiving displays the following information:

1. A list of archiving configuration data:

Archiving state	Log archiving is enabled or disabled.
Archive host	The host on which the logs are archived. Initial value is Not configured. Possible values are a host name or IPv4 address.
Archive directory	The directory on the archive host where the archives are stored. Initial value is Not configured.

`Username for ssh login`	User name which the Service Processor uses to login to the archive host. Initial value is `Not configured`.
`Archive host public key`	The public key which the Service Processor uses to verify the identity of the archive host. This field is not displayed unless the `-v` option is specified.
`Archive host fingerprint`	The `md5` fingerprint of the public key which the Service Processor uses to verify the identity of the archive host.

2. Time of the most recent attempt to connect to the archive host, and the outcome of that attempt (success or failure):

`Latest communication`	The completion time of the latest attempt to communicate with the archive host.
`Connection status`	The outcome of the latest attempt to connect to the archive host; successful (`OK`) or unsuccessful (`FAILED`).

3. Table of the status information for audit logs and non-audit logs:

`Archive space limit`	The amount of space allocated for the archives.
`Archive space used`	The amount of space currently consumed by the archives.
`Total archiving failures`	A counter of failed archiving operations.
`Unresolved failures`	A counter of failed archiving operations which the Service Processor will continue to retry.

If the `-e` option is specified `showarchiving` displays the details of the last ten archiving errors that occurred.

EXAMPLES

EXAMPLE 1 Viewing Status and Configuration Data

```
XSCF>  showarchiving
*** Archiving Configuration ***
Archiving state ---------- Disabled
Archive host ------------- Not configured
Archive directory -------- Not configured
User name for ssh login -- Not configured
Archive host fingerprint - Server authentication disabled
```

```
*** Connection to Archive Host ***
Latest communication ----- None
Connection status -------- None

                              AUDIT LOGS     OTHER LOGS
                              ----------     ----------
Archive space limit            Unlimited        2000 MB
Archive space used         Not monitored  Not monitored
Total archiving failures               0              0
Unresolved failures                    0              0
```

EXAMPLE 2 Displaying Archiving Error Information

```
XSCF>  showarchiving -e
No archiving errors have occurred.
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

setarchiving (8)

NAME

showaudit - display the current auditing system state

SYNOPSIS

showaudit

showaudit `all`

showaudit [`-a` *users*] [`-c` *classes*] [`-e` *events*] [`-g`] [`-m`] [`-p`] [`-s`] [`-t`]

showaudit `-h`

DESCRIPTION

`showaudit`(8) displays the current state of system auditing. When invoked without options `showaudit` displays whether the writing of audit records is enabled or disabled.

Privileges

You must have `auditadm` or `auditop` privileges to run this command.

Refer to `setprivileges`(8) for more information.

OPTIONS

The following options are supported:

`-a` *users*

Displays the audit record generation policy for the specified users. *users* is a comma-separated list of valid user names.

`-c` *classes*

Displays the audit record generation policy for the specified audit classes. *classes* is a comma-separated list of audit classes. A class may be specified by its numeric value or its name. The `ACS_` prefix may be omitted. For example, the class of audit related events can be expressed as `ACS_AUDIT`, `AUDIT` or 16.

The following are valid classes:

`all`	Denotes all classes.
`ACS_SYSTEM(1)`	System-related events
`ACS_WRITE(2)`	Commands that can modify a state
`ACS_READ(4)`	Commands that read a current state
`ACS_LOGIN(8)`	Login-related events
`ACS_AUDIT(16)`	Audit-related events
`ACS_DOMAIN(32)`	Domain management–related events
`ACS_USER(64)`	User management–related events
`ACS_PLATFORM(128)`	Platform management–related events
`ACS_MODES(256)`	Mode-related events

`-e` *events*

Displays the audit record generation policy for the specified audit events. *events* is a comma-separated list of audit events. An event may be specified by its numeric value or its name. The `AEV_` prefix may be omitted. For example, the event for `SSH` login can be expressed as `AEV_LOGIN_SSH`, `LOGIN_SSH`, or `0`.

See `showaudit -e all` for a list of all valid events.

`-g`

Displays the global user audit record generation policy.

`-h`

Displays usage statement.

When used with other options or operands, an error occurs.

`-m`

Displays the address to which email is sent when the local audit storage space usages reaches a threshold.

`-p` Displays the policy to follow when the audit trail reaches full capacity.

`-s` Displays the following auditing states:

- Space consumed by local audit records
- Free space remaining for local audit records
- Number of audit records dropped (since the last boot) since the audit trail reached full capacity.

`-t` Displays the thresholds at which to issue warning(s) about local storage usage.

OPERANDS

The following operands are supported:

`all` Displays the following information:

- Whether the writing of audit trails is set to `enable` or `disable`. This is the same display that is shown for `showaudit` when invoked without any options.
- All the information that would be displayed by invoking `showaudit` with the options: `-a`, `-c all`, `-e all`, `-g`, `-m`, `-p`, `-s`, `-t`.

EXAMPLES

EXAMPLE 1 Displaying Auditing Status

```
XSCF> showaudit
Auditing: enabled
```

EXAMPLE 2 Displaying All Class Information For Login Auditing

```
XSCF> showaudit -c LOGIN
Events:
AEV_LOGIN_BUI                    enabled
AEV_LOGIN_CONSOLE                enabled
AEV_LOGIN_SSH                    enabled
AEV_LOGIN_TELNET                 enabled
AEV_LOGOUT                       enabled
AEV_AUTHENTICATE                 enabled
```

EXAMPLE 3 Displaying All Event Information

```
XSCF> showaudit -e all
Events:
AEV_AUDIT_START                  enabled
AEV_AUDIT_STOP                   enabled
AEV_ENTER_MODE                   enabled
AEV_EXIT_MODE                    enabled
AEV_LOGIN_BUI                    enabled
AEV_LOGIN_CONSOLE                enabled
```

```
AEV_LOGIN_SSH                    enabled
AEV_LOGIN_TELNET                 enabled
AEV_LOGOUT                       enabled
AEV_AUTHENTICATE                 enabled
AEV_addboard                     enabled
AEV_addfru                       enabled
[...]
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

setaudit(8)**, viewaudit**(8)

NAME

showautologout - display the session timeout time of the XSCF shell

SYNOPSIS

showautologout

showautologout -h

DESCRIPTION

The showautologout(8) command displays the session timeout time of the XSCF shell.

The session timeout time is displayed in units of minutes. If the session timeout time has not been specified with the setautologout(8) command, a time of 10 minutes is set by default.

Privileges

You must have one of the following privileges to run this command:

useradm, platadm, platop, auditadm, auditop, domainadm, domainmgr, domainop, fieldeng

Refer to setprivileges(8) for more information.

OPTIONS

The following option is supported:

-h	Displays usage statement.

EXAMPLES

EXAMPLE 1 Displays the session timeout time of the XSCF shell.

```
XSCF> showautologout
30min
```

EXAMPLE 2 Displays the session timeout time of the XSCF shell (the time is default).

```
XSCF> showautologout
10min
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

setautologout(8)

NAME

showboards - display information on an eXtended System Board (XSB)

SYNOPSIS

showboards [-v] -a [-c sp]

showboards [-v] -d *domain_id* [-c sp]

showboards [-v] *xsb*

showboards -h

DESCRIPTION

The showboards(8) command displays information on XSBs.

This command displays information on XSBs currently configured in or assigned to a domain and information on all mounted XSBs. If a domain is specified, the command displays only information defined with the corresponding domain component list (DCL).

The following types of information are displayed:

XSB — XSB number. The format of the displayed number is as follows:

x–y

x — An integer from 00–15.

y — An integer from 0–3.

DID — Domain ID. One of the following is displayed:

00–23 — Domain ID to which the XSB is assigned

SP — This is displayed if the XSB does not belong to any domain but is located in the system board pool.

Other — This is displayed if the XSB belongs to a domain to which no user privilege has been granted.

LSB — Logical system board (LSB) number defined for the domain. The displayed number is an integer ranging from 0 to 15.

`Assignment` Domain assignment state of the XSB. One of the following is displayed:

- `Unavailable` The XSB is in the system board pool (not assigned to a domain) and its status is one of the following: not-yet diagnosed, under diagnosis, or diagnosis error. All XSBs that are not mounted are also shown as `Unavailable`.
- `Available` The XSB is in the system board pool and its diagnosis has completed normally.
- `Assigned` The XSB is reserved for or assigned to the domain.

`Pwr` Power status of the XSB

- `n` Power is off.
- `y` Power is on.

`Conn` Status of the XSB connection to the domain configuration

- `n` The XSB is not connected to the domain, or it is located in the system board pool.
- `y` The XSB is connected to the domain.

`Conf` Incorporation state of XSB hardware resources into the Oracle Solaris OS

- `n` The resources are not connected to the Oracle Solaris OS.
- `y` The resources are incorporated in the Oracle Solaris OS.

`Test` Status of an initial diagnosis on an XSB

- `Unmount` The XSB cannot be recognized because it is not mounted or because it has an error.
- `Unknown` Not performed.
- `Testing` The initial diagnosis is in progress.
- `Passed` The initial diagnosis ended normally.
- `Failed` Error (test=fail) detected by an initial diagnosis. The XSB cannot be used or is in a degraded state.

`Fault` XSB degradation status

- `Normal` Normal
- `Degraded` Component in a degraded state. The XSB can operate.
- `Faulted` An error occurred and the XSB cannot operate.

When the `-v` option is specified, the following types of information are displayed as XSB detail status information:

`R` Dynamic reconfiguration(DR) involving the reservation state of the XSB in the domain

- `*` DR processing is reserved. When the domain is rebooted, the XSB is incorporated into or disconnected from the domain, and the domain configuration is changed.

`Cod` Whether the XSB is a COD board

- `n` The XSB is not a COD board.
- `y` The XSB is a COD board.

Privileges

You must have one of the following privileges to run this command:

`platadm`, `platop`, `fieldeng`

Can execute the command for all domains.

`domainadm`, `domainmgr`, `domainop`

Can execute the command only for accessible domains.

Refer to `setprivileges`(8) for more information.

OPTIONS

The following options are supported:

`-a`	Displays the state of XSBs configured in or assigned to a domain and the state of all mounted XSBs.
`-c sp`	Displays the system boards located in the system board pool. System boards in the system board pool do not belong to any domain.
`-d` *domain_id*	Specifies the ID of the domain whose status of XSB is displayed. Only information that is defined with the DCL of the specified domain is displayed. An integer ranging from `0` to `23` can be specified for *domain_id*, depending on the system configuration.
`-h`	Displays usage statement. When used with other options or operands, an error occurs.
`-v`	Displays detailed information on XSB.

OPERANDS

The following operand is supported:

xsb Specifies the XSB number to be displayed. The following xsb form is accepted:

x–y

where:

x	An integer from `00–15`.
y	An integer from `0–3`.

EXAMPLES

EXAMPLE 1 Displays information on all mounted system boards.

```
XSCF> showboards -a
XSB  DID(LSB) Assignment  Pwr  Conn Conf Test    Fault
---- -------- ---------- ---  ---- ---- ----    -----
00-0 00(00)   Assigned    y    y    y    Passed  Normal
00-1 00(01)   Assigned    y    y    y    Passed  Normal
00-2 SP       Available   y    n    n    Passed  Normal
00-3 02(00)   Unavailable y    n    n    Unknown Normal
```

EXAMPLE 2 Displays detailed information on all mounted system boards.

```
XSCF> showboards -v -a
XSB  R DID(LSB) Assignment  Pwr  Conn Conf Test    Fault    COD
---- - -------- ----------  ---  ---- ---- ----    -----    ---
00-0   00(00)   Assigned    y    y    y    Passed  Normal   n
00-1 * 00(01)   Assigned    y    y    y    Passed  Normal   n
00-2   SP       Available   y    n    n    Passed  Normal   n
00-3   02(00)   Unavailable y    n    n    Unknown Normal   n
```

EXAMPLE 3 Displays information on XSB#00-0.

```
XSCF> showboards 00-0
XSB  DID(LSB) Assignment  Pwr  Conn Conf Test    Fault
---- -------- ----------  ---  ---- ---- ----    -----
00-0 15(00)   Assigned    y    y    y    Passed  Normal
```

EXAMPLE 4 Displays detailed information on XSB#00-0.

```
XSCF> showboards -v 00-0
XSB  R DID(LSB) Assignment  Pwr  Conn Conf Test    Fault    COD
---- - -------- ----------  ---  ---- ---- ----    -----    ---
00-0 * 15(00)   Assigned    y    n    n    Passed  Normal   y
```

EXAMPLE 5 Displays system boards located in the system board pool.

```
XSCF> showboards -a -c sp
XSB  DID(LSB) Assignment  Pwr  Conn Conf Test    Fault
---- -------- ----------  ---  ---- ---- ----    -----
00-0 SP       Available   y    n    n    Passed  Normal
00-2 SP       Available   y    n    n    Passed  Normal
00-3 SP       Available   y    n    n    Passed  Normal
```

EXAMPLE 6 Displays the system boards that are defined for domain ID 0 and located in the system board pool.

```
XSCF> showboards -d 0 -c sp
XSB  DID(LSB) Assignment  Pwr  Conn Conf Test    Fault
---- -------- ----------  ---  ---- ---- ----    -----
00-2 SP       Available   y    n    n    Passed  Normal
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

addboard(8), **deleteboard**(8), **moveboard**(8), **setdcl**(8), **setupfru**(8), **showcodusage**(8), **showdcl**(8), **showdevices**(8), **showfru**(8)

NAME

showcod - display Capacity on Demand (COD) information

SYNOPSIS

showcod [-v] [-d *domain_id*]

showcod -h

DESCRIPTION

showcod(8) displays COD information which includes the headroom amount, number of installed COD hardware activation permits (COD permits), the number of COD permits reserved for domains, and the Chassis Hostid.

The showcod(8) command is not supported on the M3000 server.

When used without arguments this command displays the current COD information.

Privileges

You must have one of the following privileges to run this command:

platadm, platop

Can execute the command for all domains.

domainadm, domainmgr, domainop

Can execute the command only for accessible domains.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-d *domain_id*	Domain identifier. *domain_id* can be 0–23 depending on system configuration.
-h	Displays usage statement. When used with other options or operands, an error occurs.
-v	Specifies verbose output.

EXAMPLES

EXAMPLE 1 Displaying All COD Information

The output shown is what you might see if you had domainadm, domainop, or domainmgr privileges for Domain 1.

```
XSCF>  showcod
PROC Permits reserved for domain 1 : 0
```

EXAMPLE 2 Displaying All COD Information

The output shown is what you might see if you had platform privileges.

```
XSCF>  showcod
Chassis HostID : 81000001
PROC Permits installed : 8
PROC Headroom Quantity : 0
PROC Permits reserved for domain 0 : 4
PROC Permits reserved for domain 1 : 0
PROC Permits reserved for domain 2 : 0
PROC Permits reserved for domain 3 : 0
PROC Permits reserved for domain 4 : 0
PROC Permits reserved for domain 5 : 0
PROC Permits reserved for domain 6 : 0
PROC Permits reserved for domain 7 : 0
PROC Permits reserved for domain 8 : 0
PROC Permits reserved for domain 9 : 0
PROC Permits reserved for domain 10 : 0
PROC Permits reserved for domain 11 : 0
PROC Permits reserved for domain 12 : 0
PROC Permits reserved for domain 13 : 0
PROC Permits reserved for domain 14 : 0
PROC Permits reserved for domain 15 : 0
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

SPARC Enterprise M4000/M5000/M8000/M9000 Servers Capacity on Demand (COD) User's Guide

NAME

showcodactivation - display the current Capacity on Demand (COD) hardware activation permits (COD permits) stored in the COD database

SYNOPSIS

showcodactivation [-r] [-v]

showcodactivation -h

DESCRIPTION

showcodactivation(8) displays information stored in the COD database.

This command is not available on the M3000 server.

When used without options this command displays the current COD hardware activation keys (COD keys).

Note – For details on COD keys, refer to the *SPARC Enterprise M4000/M5000/M8000/M9000 Servers Capacity on Demand (COD) User's Guide*.

Privileges

You must have platadm or platop privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-h	Displays usage statement. When used with other options or operands, an error occurs.
-r	Displays COD permit information in the raw *permit-signature* format, as stored in the COD database.
-v	Specifies verbose output. Displays both the formatted COD permit information and raw *permit-signature* data.

EXTENDED DESCRIPTION

The showcodactivation(8) command displays the following information:

Description	Type of resource (processor).
Ver	Version number of the COD permit, which is always set to 01.
Expiration	Expiration of the COD permit.
Count	Number of COD permits granted for the given resource.
Status	GOOD, which indicates that the given resource is valid, or EXPIRED, which indicates that the COD permit is no longer valid.

EXAMPLES

EXAMPLE 1 Displaying Verbose Permit Data

```
XSCF> showcodactivation -v
Description  Ver   Expiration  Count   Status
-----------  ---  -----------  -----  -------
PROC          01         NONE     16     GOOD
01:84000000:000000001:0301010100:16:00000000:xxxxxxxxxxxxxxxxxxxxxx
```

EXAMPLE 2 Displaying Raw Permit Data

```
XSCF> showcodactivation -r
01:84000000:104:0301010100:3:00000000:xxxxxxxxxxxxxxxx
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

SPARC Enterprise M4000/M5000/M8000/M9000 Servers Capacity on Demand (COD) User's Guide

NAME

showcodactivationhistory - show Capacity on Demand (COD) activation log

SYNOPSIS

showcodactivationhistory [-v | -V] [-m *mail_address*]

showcodactivationhistory [-v | -V] [-u *username*] [-p *proxy* [-t *proxy_type*]] *target_url*

showcodactivationhistory -h

DESCRIPTION

showcodactivationhistory(8) shows information in the COD activation log, a record of additions and deletions of COD hardware activation permits.

This command is not available on the M3000 server.

Privileges

You must have one of the following privileges to run this command: platadm, platop, fieldeng.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-h	Displays usage statement. When used with other options or operands, an error occurs.
-m *mail_address*	Specifies the email address to which the information is to be sent.
-p *proxy*	Specifies the proxy server to be used for transfers. The default transfer type is http, unless modified using the -t *proxy_type* option. The value for proxy must be in the format *servername*:*port*.
-t *proxy_type*	Used with the -p option, specifies the type of proxy. Possible values for *proxy_type* are: http, socks4, and socks5. The default value is http.
-u *username*	Specifies the user name when logging in to a remote ftp or http server that requires authentication. You will be prompted for a password.
-v	Displays verbose output.
-V	Displays details of network activity, which might be helpful in diagnosing network or server problems.

OPERANDS

The following operand is supported:

target_url Specifies the URL to which the activation log content is to be transferred. Supported formats for this value include the following:

`http://`*server*`[:`*port*`]/`*path*`/`*file*

`https://`*server*`[:`*port*`]/`*path*`/`*file*

`ftp://`*server*`[:`*port*`]/`*path*`/`*file*

`file:///media/usb_msd/`*path*`/`*file*

EXAMPLES

EXAMPLE 1 Displays COD activation log

```
XSCF> showcodactivationhistory
11/30/2010 01:42:41PM PST: Report Generated M5000 SN: 843a996d
10/02/2010 02:08:49PM PST: Activation history initialized: PROC 0 cpus
10/15/2010 01:36:13PM PST: Capacity added: (legacy) PROC 3 cpus
11/07/2010 01:36:23PM PST: Capacity deleted: (legacy) PROC 3 cpus
11/28/2010 01:37:12PM PST: Capacity added: (unlocked) PROC 1 cpus
11/30/2010 01:37:19PM PST: Capacity added: (unlocked) PROC 4 cpus
11/30/2010 01:42:41PM PST: Summary: PROC 5 cpus
Signature: 9138HVZQ0zFJh8EoRy7i1A
```

EXAMPLE 2 Sends results to the specified user via email

```
XSCF> showcodactivationhistory -m sysadmin@comany.com
XSCF>
```

EXAMPLE 3 Sends results to the specified user via FTP

```
XSCF> showcodactivationhistory -u admin ftp://somehost/tmp/history.txt
Password:
file transfer complete
XSCF>
```

EXIT STATUS

The following exit values are returned:

0 Successful completion.

>0 An error occurred.

SEE ALSO

SPARC Enterprise M4000/M5000/M8000/M9000 Servers Capacity on Demand (COD) User's Guide

NAME

showcodlicense - display the current Capacity on Demand (COD) right-to-use (RTU) licenses stored in the COD license database

SYNOPSIS

showcodlicense [-r] [-v]

showcodlicense -h

DESCRIPTION

showcodlicense(8) displays COD license information stored in the COD license database.

The showcodlicense(8) command is not available on the M3000 server.

When used without options it displays the current licenses.

Privileges

You must have platadm or platop privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-h	Displays usage statement. When used with other options or operands, an error occurs.
-r	Displays the license information in the raw *license-signature* format, as stored in the COD license database.
-v	Specifies verbose output. Displays both the formatted license information and raw *license-signature* data.

EXTENDED DESCRIPTION

The showcodlicense command displays the following COD information:

Description	Type of resource (processor).
Ver	Version number of the license, which is always set to 01.
Expiration	Expiration of the license.
Count	Number of right-to-use licenses granted for the given resource.
Status	GOOD, which indicates that the given resource is valid, or EXPIRED, which indicates that the resource license is no longer valid.

EXAMPLES

EXAMPLE 1 Displaying Verbose License Data

```
XSCF> showcodlicense -v
Description  Ver   Expiration  Count   Status
```

```
-----------  ---  -----------  -----  -------
PROC          01         NONE     16     GOOD
01:84000000:000000001:0301010100:16:00000000:xxxxxxxxxxxxxxxxxxxxxx
```

EXAMPLE 2 Displaying Raw License Data

```
XSCF> showcodlicense -r
01:84000000:104:0301010100:3:00000000:xxxxxxxxxxxxxxx
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

SPARC Enterprise M4000/M5000/M8000/M9000 Servers Capacity on Demand (COD) User's Guide

NAME

showcodusage - display the current usage statistics for Capacity on Demand (COD) resources

SYNOPSIS

showcodusage [-v] [-M] [-p resource | domain | all]

showcodusage -h

DESCRIPTION

showcodusage(8) shows current information about COD hardware activation permits (COD permits) in use.

The showcodusage(8) command is not available on the M3000 server.

By default, this command displays a summary of COD permits used and installed, along with the current state of each resource. When used without options, it displays the current usage.

Privileges

You must have one of the following privileges to run this command:

platadm, platop, fieldeng

Can run this command for all resources and domains.

domainadm, domainmgr, domainop

Can run this command for available resources only for those domains that you can access.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-h	Displays usage statement. When used with other options or operands, an error occurs.
-M	Displays text by page.
-p domain	Displays COD permit usage for each domain. The statistics reported include the number of COD permits used by the domain, resources assigned to the domain, and COD permits reserved for the domain.
-p resource	Displays COD permit usage by resource type.
-p all	Displays all COD usage information.
-v	Specifies verbose output. Displays all available COD usage information, including COD permit use for both the system and its domains.

EXTENDED DESCRIPTION

The `showcodusage -p resource` command displays the following COD usage information for the system:

`Resource` Identifies the type of COD resources available (processors).

`In Use` Specifies the number of COD CPUs currently used in the system.

`Installed` Specifies the number of COD CPUs installed in the system.

`COD Permitted` Specifies the number of COD permits installed.

`Status` Specifies one of the following COD attributes:

- `OK` Indicates that there are sufficient permits for the COD CPUs in use, and displays the number of COD CPUs that are available, and the number that can be used to provide headroom.
- `HEADROOM` The number of COD CPUs in use providing headroom.
- `Violation` Indicates a COD permit violation exists. Displays the number of COD CPUs in use that exceeds the number of COD permits available. This situation can occur when you force the deletion of a COD hardware activation key (COD key) from the COD database, but the COD CPU associated with the COD key is still in use.

The `showcodusage -p domain` command displays the following COD usage information for each domain:

`Domain/Resource` Identifies COD resources (processors) for each domain. An Unused processor is a COD CPU that has not yet been assigned to a domain.

`In Use` Specifies the number of COD CPUs currently used in the domain.

`Installed`	Specifies the number of COD CPU resources installed in the domain.
`Reserved`	Specifies the number of COD permits allocated to the domain.
`Status`	Contains one of the following when the `-v` option is specified:
	`COD Permitted` — The domain's COD CPU has a COD permit and it is in use.
	`Not COD Permitted` — A COD permit for the domain's COD CPU could not be obtained; the COD CPU is not in use.
	`Unused` — The COD CPU is not in use.

EXAMPLES

Users with platform-related privileges can view both resource and domain usage summaries. Users with domain-related privileges can view only the domain usage summaries for which they have privileges, and a report of unused COD permits.

EXAMPLE 1 Displaying COD Usage by Resource

```
XSCF> showcodusage -p resource
Resource  In Use  Installed  COD Permitted  Status
--------  ------  ---------  -------------  ------
PROC           4          4             16  OK: 12 available
```

EXAMPLE 2 Displaying COD Usage by Domain

```
XSCF> showcodusage -p domains
Domain/Resource  In Use  Installed  Reserved
---------------  ------  ---------  --------
0 - PROC              4          4         0
1 - PROC              4          4         0
2 - PROC              4          4         0
3 - PROC              4          4         0
4 - PROC              0          0         0
Unused - PROC         0          0        12
```

EXAMPLE 3 Displaying COD Usage by Resource and Domain: M8000 Server With CMU00 Quad-XSB, CMU02 Uni-XSB

```
XSCF> showcodusage -v
Resource  In Use  Installed  COD Permitted  Status
--------  ------  ---------  -------------  ------
PROC           0          8              0  OK: 0 available Headroom: 2
```

```
Domain/Resource  In Use  Installed  Reserved  Status
---------------  ------  ---------  --------  ------
0  - PROC             0          8         0
     00-0 - PROC      0          1
     CMU00-CPU0                               Unused
     00-1 - PROC      0          1
     CMU00-CPU1                               Unused
     00-2 - PROC      0          1
     CMU00-CPU2                               Unused
     00-3 - PROC      0          1
     CMU00-CPU3                               Unused
     02-0 - PROC      0          4
     CMU02-CPU0                               Unused
     CMU02-CPU1                               Unused
     CMU02-CPU2                               Unused
     CMU02-CPU3                               Unused
1  - PROC             0          0         0
2  - PROC             0          0         0
3  - PROC             0          0         0
4  - PROC             0          0         0
5  - PROC             0          0         0
6  - PROC             0          0         0
7  - PROC             0          0         0
8  - PROC             0          0         0
9  - PROC             0          0         0
10 - PROC             0          0         0
11 - PROC             0          0         0
12 - PROC             0          0         0
13 - PROC             0          0         0
14 - PROC             0          0         0
15 - PROC             0          0         0
Unused - PROC         0          0         2
```

EXAMPLE 4 Displaying COD Usage by Resource and Domain: M5000 Server

```
XSCF> showcodusage -v
Resource  In Use  Installed  COD Permitted  Status
--------  ------  ---------  -------------  ------
PROC           0          4              0  OK: 0 available
Domain/Resource  In Use  Installed  Reserved  Status
---------------  ------  ---------  --------  ------
0  - PROC             0          0         0
1  - PROC             0          0         0
2  - PROC             0          0         0
3  - PROC             0          0         0
```

```
Unused - PROC         0          4          0
        00-0 - PROC   0          4
        CPUM00-CPU0                            Unused
        CPUM00-CPU1                            Unused
        CPUM01-CPU0                            Unused
        CPUM01-CPU1                            Unused
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

SPARC Enterprise M4000/M5000/M8000/M9000 Servers Capacity on Demand (COD) User's Guide

NAME

showconsolepath - displays information on the domain console that is currently connected

SYNOPSIS

showconsolepath -a

showconsolepath -d *domain_id*

showconsolepath -h

DESCRIPTION

The showconsolepath(8) command displays information on the domain console that is currently connected.

The following information can be displayed:

User	User account of the XSCF connected to the domain console	
DID	Domain ID	
ro/rw	Domain console type	
	ro	Read-only console
	rw	Writable console
escape	Escape mark specified for the console	
Date	Date connected to the domain console	

Privileges

You must have one of the following privileges to run this command:

useradm, platadm, platop

Can run this command for all domains.

domainadm, domainmgr, domainop

Can run this command only for your accessible domains.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported.

-a	Displays console information on all domains that can be accessed.
-d *domain_id*	Specifies only one ID of the domain for which information is to be displayed. *domain_id* can be 0–23 depending on the system configuration.
-h	Displays usage statement. When used with other options or operands, an error occurs.

EXTENDED DESCRIPTION

Only one writable console and one or more read-only consoles can be connected to one domain.

EXAMPLES

EXAMPLE 1 Displays console information on all domains that can be accessed.

```
XSCF> showconsolepath -a
User            DID  ro/rw  escape   Date
nakagawa        00   rw     @        Fri Jul 29 21:23:34
hana            00   ro     #        Fri Jul 29 09:49:12
k-okano         00   ro     #        Fri Jul 29 18:21:50
yuuki           01   rw     |        Fri Jul 29 10:19:18
uchida          01   ro     *        Fri Jul 29 13:30:41
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

console(8), **sendbreak**(8)

NAME

showdate - display the date and time of XSCF

SYNOPSIS

showdate [-u]

showdate -h

DESCRIPTION

The showdate(8) command displays the date and time of XSCF.

Privileges

You must have one of the following privileges to run this command:

useradm, platadm, platop, auditadm, auditop, domainadm, domainmgr, domainop, fieldeng

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-h	Displays usage statement. When used with other options or operands, an error occurs.
-u	Specifies time in coordinated universal time (UTC). When the -u option is omitted, the local time is specified.

EXTENDED DESCRIPTION

The setdate(8) command sets the XSCF date and time.

EXAMPLES

EXAMPLE 1 Displays the current time as the local time (JST).

```
XSCF> showdate
Mon Jan 23 14:53:00 JST 2006
```

EXAMPLE 2 Displays the current time in UTC.

```
XSCF> showdate -u
Mon Jan 23 05:56:15 UTC 2006
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

setdate(8), **settimezone**(8), **showtimezone**(8)

NAME

showdateoffset - display the time differences between the time of the system and the time of the domains

SYNOPSIS

showdateoffset -d *domain_id*

showdateoffset -a

showdateoffset -h

DESCRIPTION

The showdateoffset(8) command displays the time differences between the time of the system, managed by the XSCF clock, and the time of the domains, which is managed by each domain clock in second.

If you change the time setting on a domain, for example by using the date(1M) command, the time of that domain differs from the time of the system. The difference between revised time of the domain and the time of the system is stored on the XSCF, and is retained after domain reboot and after XSCF reset.

Execute the showdateoffset(8) command to display the time differences between the time of the system and the time of all domains. The outputs of the command will be displayed in second.

Privileges

You must have one of the following privileges to run this command:

useradm, platadm, platop, fieldeng

Can run this command for all domains.

domainadm, domainmgr, domainop

Can run this command only for your accessible domains.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-a	Displays the time differences between the time of the system and the time of all accessible domains.
-d *domain_id*	Specifies only one ID of the domain on which the time differences is displayed. *domain_id* can be 0–23 depending on the system configuration.
-h	Displays usage statement.

EXAMPLES

EXAMPLE 1 On the M3000 server, displays the time differences between the time of the system and the time of the domains with specifying the ID of the domain.

```
XSCF> showdateoffset
DID             Domain Date Offset
00              128 sec
```

EXAMPLE 2 On the M5000 server, displays the time differences between the time of the system and the time of the domains.

```
XSCF> showdateoffset
DID             Domain Date Offset
00              128 sec
01              0 sec
02              -1024 sec
03              -9999999 sec
```

EXAMPLE 3 On the M8000 server, displays the time differences between the time of the system and the time of the domains.

```
XSCF> showdateoffset
DID             Domain Date Offset
00              128 sec
01              0 sec
02              -1024 sec
03              1 sec
04              199 sec
05              -82 sec
06              0 sec
07              0 sec
08              9999 sec
09              -14 sec
10              -123 sec
11              -6 sec
12              54 sec
13              0 sec
14              300 sec
15              901 sec
16              0 sec
17              0 sec
18              -111 sec
19              0 sec
20              3 sec
21              21 sec
22              -621 sec
23              -9999999 sec
```

EXIT STATUS

The following exit values are returned:

`0`	Successful completion.
`>0`	An error occurred.

SEE ALSO

resetdateoffset`(8)`

NAME

showdcl - display the current domain component list (DCL)

SYNOPSIS

showdcl [-v] -a

showdcl [-v] -d *domain_id* [-l *lsb* [-l *lsb*]]...

showdcl -h

DESCRIPTION

The showdcl(8) command displays the DCL that has been set by the setdcl(8) command.

The DCL is hardware resource information that can be set for a domain or the logical system boards (LSBs) that are components of a domain.

An LSB is a board unit recognized by the Oracle Solaris OS in a domain. Up to 16 LSBs can be registered for each domain, and they are represented by integer numbers ranging from 0 to 15.

An XSB is a board unit that can be used in the system and is one division of a divided physical system board (PSB). An XSB is represented by *x*–*y*, a combination of a PSB number and the number of one division of the divided PSB (*x* is an integer ranging from 00 to 15, and *y* is an integer ranging from 0 to 3).

The showdcl(8) command can display the following information that is part of a DCL:

DID	Domain ID

`LSB`
: LSB number. The displayed number is an integer ranging from 00 to 15.

`XSB`
: XSB number corresponding to the LSB. The displayed number has the following format:

  x–y

  where:

  x — An integer from `00–15`.

  y — An integer from `0–3`.

`Status`
: Domain status. One of the following status is displayed. Additional information may be displayed.

  `Powered Off`
  : Power is off.

  `Panic State`
  : A panic occurred, and the domain is in the reboot state.

  `Shutdown Started`
  : The power-off process is starting.

  `Initialization Phase`
  : OpenBoot PROM initialization is in progress.

  `OpenBoot Executing Completed`
  : The system is in the OpenBoot PROM (ok prompt) state.

  `Booting/OpenBoot PROM prompt`
  : The Oracle Solaris OS is booting. Or due to the domain shutdown or reboot, the system is in the OpenBoot PROM running state or is suspended in the OpenBoot PROM (`ok` prompt) state.

  `Running`
  : The Oracle Solaris OS is running.

If the `-v` option is specified, the following information is added:

`Cfg-policy` Degradation range applicable for an error detected during an initial diagnosis of hardware. Any of the following is displayed:

- `FRU` Degradation of a component (default)
- `XSB` Degradation of an XSB.
- System Degradation of a domain

`No-Mem` Whether to omit the use of memory on a domain. Either of the following is displayed:

- `True` Omits the use of memory on a domain.
- `False` Does not omits the use of memory on a domain (default).

`No-IO` Whether to omit the use of I/O devices on a domain. Either of the following is displayed:

- `True` Omits the use of I/O devices on a domain.
- `False` Does not omit the use of I/O devices on a domain (default).

`Float` Whether to set a priority for the specified LSB as a floating board, relative to other boards. Either of the following is displayed:

- `True` Gives a higher priority to the LSB to become a floating board.
- `False` Does not give a higher priority regarding floating boards (default).

Privileges

You must have one of the following privileges to run this command:

`platadm`, `platop`, `fieldeng`

Can execute the command for all domains.

`domainadm`, `domainmgr`, `domainop`

Can execute the command only for accessible domain.

Refer to `setprivileges`(8) for more information.

OPTIONS

The following options are supported:.

`-a`	Displays information that is set for all domains.
`-d` *domain_id*	Specifies the ID of the domain for which information is to be displayed. The *domain_id* can be 0–23 depending on the system configuration.
`-h`	Displays usage statement. When used with other options or operands, an error occurs.
`-l` *lsb*	Specifies the LSB number whose information is to be displayed. Multiple `-l` options can be specified by delimiting them with spaces. Specify an *lsb* value by using an integer ranging from 0 to 15. If *lsb* is omitted, all the LSBs in the domain are targets.
`-v`	Also displays information on `Cfg-policy`, `No-Mem`, `No-IO`, and `Float` in the DCL.

EXTENDED DESCRIPTION

- An XSB for which the floating board priority is set to a low value is difficult to use as a floating board. Accordingly, it is difficult for the system board to affect the domain Oracle Solaris OS.
- The `setdcl`(8) command sets the DCL.

EXAMPLES

EXAMPLE 1 Displays detailed information on the DCL that is set for domain ID 0

```
XSCF> showdcl -d 0
DID   LSB   XSB   Status
00                Running
      00    00-0
      04    01-0
      08    02-0
      12    03-0
```

EXAMPLE 2 Displays details in the DCL that is set for domain ID 0.

```
XSCF> showdcl -v -d 0
DID   LSB   XSB   Status   No-Mem   No-IO    Float    Cfg-policy
00                Running                             FRU
      00    00-0           False    False    False
      01    -
      02    -
      03    -
      04    01-0           False    True     False
      05    -
      06    -
      07    -
      08    02-0           True     True     True
```

```
      09    -
      10    -
      11    -
      12    03-0           True     True     False
      13    -
      14    -
      15    -
```

EXAMPLE 3 Displays details in the DCL that are set for all domains.

```
XSCF> showdcl -v -a
DID   LSB   XSB   Status   No-Mem   No-IO    Float    Cfg-policy
00                Running                             FRU
      00    00-0           False    False    False
      01    -
      02    -
      03    -
      04    01-0           False    True     False
      05    -
      06    -
      07    -
      08    02-0           True     True     True
      09    -
      10    -
      11    -
      12    03-0           True     True     False
      13    -
      14    -
      15    -
-------------------------------------------------------------
01                Running (Waiting for OS Shutdown)   FRU
      00    01-2           True     True     False
      01    04-0           False    False    False
      02    -
      03    -
      04    -
      05    -
      06    -
      07    05-0           True     False    False
      08    -
      09    -
      10    -
      11    -
      12    -
      13    -
```

```
        14    06-0           True     True     True
        15    -
 ------------------------------------------------------------
    :
    :
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

addboard(8), **deleteboard**(8), **moveboard**(8), **setdcl**(8), **setupfru**(8), **showboards**(8), **showdevices**(8), **showfru**(8)

NAME

showdevices - display current information on an eXtended System Board (XSB)

SYNOPSIS

showdevices [-v] [-p bydevice | byboard | query | force] *xsb*

showdevices [-v] [-p bydevice | byboard] -d *domain_id*

showdevices -h

DESCRIPTION

The showdevices(8) command displays the information of the physical devices configured on XSB and their available resources of these devices.

The information of available resources can be obtained for the devices managed by the operating system. The command can also display in advance whether the XSB can be disconnected from the domain using the dynamic reconfiguration (DR) function.

The following types of information are displayed:

Common:

DID	Domain ID
XSB	XSB number

CPU:

id	processor ID
state	status of processor
speed	CPU frequency (MHz)
ecache	CPU external cache size (MB)

MEMORY:

board mem	Size of memory mounted on the XSB (MB)
perm mem	Size of memory that mounted and cannot be relocated on the XSB (MB)
base address	Physical address of memory mounted on the XSB
domain mem	Size of memory on the domain (MB)

When memory is being disconnected, the following items are displayed:

`target XSB`	XSB number at the move destination
`deleted mem`	Size of memory which was already deleted (MB)
`remaining mem`	Size of remaining memory to be deleted (MB)

I/O devices:

`device`	Instance name of I/O device
`resource`	Managed resource name
`usage`	Description of the instance using resources
`query`	Results of an off-line inquiry about resources

Privileges

You must have one of the following privileges to run this command:

`platadm`, `platop`, `fieldeng`

Can run this command for all domains.

`domainadm`, `domainmgr`, `domainop`

Can run this command only for your accessible domains.

Refer to `setprivileges`(8) for more information.

OPTIONS

The following options are supported.

`-d` *domain_id*	Specifies the ID of the domain for which information is to be displayed. *domain_id* can be 0–23 depending on the system configuration.
`-h`	Displays usage statement. When used with other options or operands, an error occurs.
`-p byboard`	Displays results organized by XSB. The results can be further summarized by device and displayed. If the `-p` option is omitted, "`-p bydevice`" is used.
`-p bydevice`	Displays results organized by device type (CPU, memory, I/O, etc.). If the `-p` option is omitted, "`-p bydevice`" is used.

`-p force` Predicts system resources deleted from the Oracle Solaris OS when an XSB is forcibly disconnected by "`deleteboard -f`" command. If the `-p` option is omitted, "`-p bydevice`" is used.

`-p query` Predicts system resources deleted from the Oracle Solaris OS when an XSB is disconnected by `deleteboard` command. If the `-p` option is omitted, "`-p bydevice`" is used.

`-v` Displays information on all I/O devices, including those that are not management targets. As information on the I/O devices that are not management targets, however, only physical configurations are displayed, and resources and use states are not displayed.

OPERANDS

The following operand is supported:

xsb Specifies the XSB number for which information is to be displayed. The following xsb form is accepted:

x–y

where:

x An integer from 00–15.

y An integer from 0–3.

EXTENDED DESCRIPTION

- The `showdevices`(8) command will succeed only if the following Oracle Solaris Service Management Facility (SMF) services are active on that domain:
  - Domain SP Communication Protocol (dscp)
  - Domain Configuration Server (dcs)
  - Oracle Sun Cryptographic Key Management Daemon (sckmd)
- The `showdevices`(8) command displays a complete list of devices when executed right after an Oracle Solaris OS boot or a DR operation. However, when executed at other times, `showdevices` does not display a complete list if the Oracle Solaris OS has unloaded drivers for any unused devices. To be certain the displayed list is complete, run the `devfsadm` command with `-v` option on the domain before running showdevices. For more information about the `devfsadm` command, see the Oracle Solaris `devfsadm`(1M) man page.

EXAMPLES

EXAMPLE 1 Displays the information of the physical devices configured on the XSB#00-0 and their available resources.

```
XSCF> showdevices 00-0

CPU:
```

```
----
DID XSB  id  state    speed  ecache
00  00-0 0   on-line   2530     5.5
00  00-0 1   on-line   2530     5.5
00  00-0 2   on-line   2530     5.5
00  00-0 3   on-line   2530     5.5
00  00-0 4   on-line   2530     5.5
00  00-0 5   on-line   2530     5.5
00  00-0 6   on-line   2530     5.5
00  00-0 7   on-line   2530     5.5

Memory:
-------
        board   perm   base             domain  target  deleted  remaining
DID XSB   mem MB  mem MB  address           mem MB  XSB     mem MB   mem MB
00  00-0   2048   1290  0x000003c000000000   4096  03-0      250      1500

IO Devices:
----------
DID XSB       device  resource                usage
00  00-0      sd3     /dev/dsk/c0t3d0s0       mounted filesystem "/"
00  00-0      sd3     /dev/dsk/c0t3s0s1       dump device (swap)
00  00-0      sd3     /dev/dsk/c0t3s0s1       swap area
00  00-0      sd3     /dev/dsk/c0t3d0s3       mounted filesystem "/var"
00  00-0      sd3     /var/run               mounted filesystem "/var/run"
```

EXAMPLE 2 Displays detail information of the physical devices and their available resources in domain ID 0.

```
XSCF> showdevices -v -d 0

CPU:
----
DID XSB  id  state    speed  ecache
00  00-0 0   on-line   2530     5.5
00  00-0 1   on-line   2530     5.5
00  00-0 2   on-line   2530     5.5
00  00-0 3   on-line   2530     5.5
00  00-0 4   on-line   2530     5.5
00  00-0 5   on-line   2530     5.5
00  00-0 6   on-line   2530     5.5
00  00-0 7   on-line   2530     5.5
00  01-0 50  on-line   2048       4
00  01-0 51  on-line   2048       4
00  01-0 52  on-line   2048       4
```

```
00  01-0 53  on-line   2048       4

Memory:
-------
        board   perm   base             domain  target  deleted  remaining
DID XSB   mem MB  mem MB  address            mem MB  XSB     mem MB   mem MB
00  00-0   2048   1290  0x000003c000000000   4096  00-1       250     1500
00  01-0    2048      0  0x000002c000000000    4096

IO Devices:
----------
DID XSB       device  resource                usage
00  00-0      sd0
00  00-0      sd1
00  00-0      sd2
00  00-0      sd3     /dev/dsk/c0t3d0s0       mounted filesystem "/"
00  00-0      sd3     /dev/dsk/c0t3s0s1       dump device (swap)
00  00-0      sd3     /dev/dsk/c0t3s0s1       swap area
00  00-0      sd3     /dev/dsk/c0t3d0s3       mounted filesystem "/var"
00  00-0     sd3     /var/run               mounted filesystem "/var/run"
00  00-0      sd4
00  00-0      sd5
00  00-0      sd6
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

addboard(8), **deleteboard**(8), **moveboard**(8), **setdcl**(8), **setdscp**(8), **setupfru**(8), **showboards**(8), **showdcl**(8), **showfru**(8)

NAME

showdomainmode - display the modes of operation for the specified domain

SYNOPSIS

showdomainmode -d *domain_id* [-v]

showdomainmode -h

DESCRIPTION

showdomainmode(8) command displays the modes of operation that are set for the specified domain.

The following states are displayed:

HOST-ID	Displays the host ID.
Diagnostic Level	Displays the OpenBoot PROM diagnostic level. One of the following is displayed:
	none — None
	min — Standard
	max — Maximum
Secure Mode	Displays the states of the host watchdog function and function that suppresses break signal reception. One of the following is displayed:
	on — Enabled
	off — Disabled

`Autoboot` Displays the state of the auto boot function. One of the following is displayed:

- `on` Enabled
- `off` Disabled

`CPU Mode` Way of determining the CPU operational mode mounted on the domain. One of the following is displayed.

- `auto`
  Automatically determines at domain startup
- `compatible`
  Sets to the SPARC64 VI compatible mode regardless of the CPUs mounted

`Ethernet Address` XSCF-supplied domain ethernet (mac) address. This is the address that OpenBoot PROM/Oracle Solaris will use when its configuration parameter `local-mac-address?` is set to `false`. This information will be displayed only if the `-v` option is specified.

Privileges

You must have one of the following privileges to run this command:

`platadm`, `fieldeng`	Can run this command for all domains.
`domainadm`	Can run this command only for your managed domains.

Refer to `setprivileges`(8) for more information.

OPTIONS

The following operands are supported:

`-d` *domain_id*	Specifies the domain ID of the domain to be displayed. *domain_id* can be `0–23` depending on the system configuration.
`-h`	Displays usage statement. When used with other options or operands, an error occurs.
`-v`	Displays detailed information. When this option is specified, the XSCF-supplied domain ethernet (mac) address will also be displayed.

EXTENDED DESCRIPTION

- If the Mode switch of the operator panel is set to `Service`, the settings of the modes of operation for the specified domain have the following values, regardless of the domain mode displayed by the `showdomainmode`(8) command:

- OpenBoot PROM diagnostic level (`Diagnostic Level`), CPU operational mode (`CPU Mode`): operates as the `showdomainmode`(8) command display
- Host watchdog and suppress break signal reception (`Secure Mode`), auto boot function (`Autoboot`): `off`

- When the OpenBoot PROM environmental variable `'auto-boot?'` has been set to `false`, the auto boot function is disabled.
- The `setdomainmode`(8) command sets the modes of operation specified for a domain.

EXAMPLES

EXAMPLE 1 Displays the modes of operation that are set for domain ID 0.

```
XSCF> showdomainmode -d 0
Host-ID             :0f010f10
Diagnostic Level    :min
Secure Mode         :on
Autoboot            :on
CPU Mode            :auto
```

EXAMPLE 2 Displays the modes of operation that are set for domain ID 0 with `-v` option specified.

```
XSCF> showdomainmode -d 0 -v
Host-ID             :8099010c
Diagnostic Level    :min
Secure Mode         :off
Autoboot            :on
CPU Mode            :auto
Ethernet Address    :00:0b:5d:e2:01:0c
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

setdomainmode(8)

NAME

showdomainstatus - display the current domain component list (DCL)

SYNOPSIS

showdomainstatus -d *domain_id*

showdomainstatus -a

showdomainstatus -h

DESCRIPTION

The showdomainstatus(8) command displays the current status of the specified domain.

One of the following states is displayed for each domain. Additional information may be displayed.

Powered Off

Power is off.

Panic State

A panic occurred, and the domain is in the reboot state.

Shutdown Started

The power-off process is starting.

Initialization Phase

OpenBoot PROM initialization is in progress.

OpenBoot Execution Completed

The system is in the OpenBoot PROM (ok prompt) state.

Booting/OpenBoot PROM prompt

The Oracle Solaris OS is booting. Or due to the domain shutdown or reboot, the system is in the OpenBoot PROM running state or is suspended in the OpenBoot PROM (ok prompt) state.

Running

The Oracle Solaris OS is running.

-

Domain is not defined.

Privileges

You must have one of the following privileges to run this command:

useradm, platadm, platop, fieldeng

Can run this command for all domains.

`domainadm`, `domainmgr`, `domainop`

Can run this command only for your accessible domains.

Refer to `setprivileges`(8) for more information.

OPTIONS

The following options are supported.

`-a`	Displays status information on all domains that can be accessed.
`-d` *domain_id*	Specifies only one ID of the domain to be displayed. *domain_id* can be 0–23 depending on the system configuration.
`-h`	Displays usage statement. When used with other options or operands, an error occurs.

EXAMPLES

EXAMPLE 1 Displays status information on all domains.

```
XSCF> showdomainstatus -a
DID             Domain Status
00              Running
01              Running (Waiting for OS Shutdown)
02              Powered Off
03              Panic State
04              Shutdown Started
05              Booting/OpenBoot PROM prompt
06              Initialization Phase
07              OpenBoot Execution Completed
```

EXIT STATUS

The following exit values are returned:

`0`	Successful completion.
`>0`	An error occurred.

SEE ALSO

poweroff`(8)`, **poweron**`(8)`, **reset**`(8)`, **showdcl**`(8)`

NAME

showdscp - display the IP addresses assigned to the Domain to Service Processor Communications Protocol (DSCP)

SYNOPSIS

showdscp

showdscp [-v] [-p]

showdscp [-v] [-p] -d *domain_id*

showdscp [-v] [-p] -s

showdscp -h

DESCRIPTION

showdscp(8) displays the IP addresses assigned for DSCP usage, the IP addresses for an individual domain, the Service Processor, or for the entire system. When used without options, it displays current IP data.

When displaying IP addresses for all DSCP links in the system, the output is a table. The table is sorted by numerical domain IDs.

When displaying IP addresses for a particular domain or just the Service Processor, then the output is not a table but simply the IP address of the specified domain or Service Processor.

The -p option can be used to generate parsable output that would then be suitable for use in a script. Parsable displays of individual IP addresses exclude any additional labels, and only an IPv4 address in dotted-decimal form is output. The parsable version of tabular output includes only the values (no table headings are included), and each column is separated by a single tab character.

Privileges

You must have one of the following privileges to run this command:

fieldeng, platadm, platop:

Can display any DSCP IP information.

domainadm, domainmgr, domainop:

Can display individual IP addresses for domains for which you have privileges only.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

`-d` *domain_id*	Displays an individual domain's IP address.
`-h`	Displays usage statement. When used with other options or operands, an error occurs.
`-p`	Generates parsable output.
`-s`	Displays the Service Processor's IP address.
`-v`	Specifies verbose output. Prints additional information about internal progress of the program's operations to the screen.

EXAMPLES

Caution – The IP addresses shown in the following examples are examples only.

EXAMPLE 1 Displaying a Table of All DSCP IP Addresses

```
XSCF>  showdscp

DSCP Configuration

Network: 10.1.1.0
Netmask: 255.255.255.0

 Location     Address
----------   ---------
XSCF         10.1.1.1
Domain #00   10.1.1.2
Domain #01   10.1.1.3
Domain #02   10.1.1.4
Domain #03   10.1.1.5
Domain #04   10.1.1.6
Domain #05   10.1.1.7
Domain #06   10.1.1.8
Domain #07   10.1.1.9
Domain #08   10.1.1.10
Domain #09   10.1.1.11
Domain #10   10.1.1.12
Domain #11   10.1.1.13
Domain #12   10.1.1.14
Domain #13   10.1.1.15
Domain #14   10.1.1.16
Domain #15   10.1.1.17
```

```
Domain #16   10.1.1.18
Domain #17   10.1.1.19
Domain #18   10.1.1.20
Domain #19   10.1.1.21
Domain #20   10.1.1.22
Domain #21   10.1.1.23
Domain #22   10.1.1.24
Domain #23   10.1.1.25
```

EXAMPLE 2 Displaying a Specific Domain's IP Address

```
XSCF>  showdscp -d 1
Domain #01 Address: 10.1.1.3
```

EXAMPLE 3 Displaying a Specific Domain's IP Address in a Parsable Form

```
XSCF>  showdscp -p -d 1
Domain[1] 10.1.1.3
```

EXAMPLE 4 Displaying All DSCP Address Information In a Parsable Form

```
XSCF>  showdscp -p
Network 10.1.1.0
Netmask 255.255.255.0
XSCF    10.1.1.1
Domain[0]       10.1.1.2
Domain[1]       10.1.1.3
Domain[2]       10.1.1.4
Domain[3]       10.1.1.5
Domain[4]       10.1.1.6
Domain[5]       10.1.1.7
Domain[6]       10.1.1.8
Domain[7]       10.1.1.9
Domain[8]       10.1.1.10
Domain[9]       10.1.1.11
...
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

setdscp(8)

NAME

showdualpowerfeed - display the current setting of dual power feed mode

SYNOPSIS

showdualpowerfeed

showdualpowerfeed -h

DESCRIPTION

The showdualpowerfeed(8) command displays the current setting of dual power feed mode in the system.

Note – The ability to display the current status of the dual power feed is available on M3000/M4000/M5000 servers only. However, the dual power feed mode cannot be used with 100V power on M4000/M5000 servers. When the optional power cabinet for dual power feed is connected on M8000/M9000 servers, it automatically configures the dual power feed mode. For details about the setting the dual power feed, see the *Installation Guide* for your server.

The dual power feed mode can be set by the setdualpowerfeed(8) command. Also, before the dual power feed mode is changed by the setdualpowerfeed(8) command, the values of changed settings are displayed.

Privileges

You must have platadm or fieldeng privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-h	Displays usage statement.

EXAMPLES

EXAMPLE 1 Displays the current setting of dual power feed mode in the system.

```
XSCF> showdualpowerfeed
Dual power feed is enabled.
```

EXAMPLE 2 Changes the dual power feed mode with the setdualpowerfeed(8) command and then displays the current state.

```
XSCF> showdualpowerfeed
enable -> disable
NOTE: Dual power feed will be disabled the next time the platform is
powered on.
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

setdualpowerfeed(8)

NAME

showemailreport - display the email report configuration data

SYNOPSIS

showemailreport [-v]

showemailreport -h

DESCRIPTION

showemailreport(8) displays the email reporting configuration data. When used without options, it displays current email report configuration data.

Privileges

You must have platadm, platop or fieldeng privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-h Displays usage statement.

When used with other options or operands, an error occurs.

-v Specifies verbose output.

EXTENDED DESCRIPTION

Emailreport information includes whether Emailreporting is enabled. If enabled, it also includes the list of addresses.

EXAMPLES

EXAMPLE 1 Displaying Emailreport configuration

```
XSCF>  showemailreport
EMail Reporting: enabled
Email Recipient Address: admin@company.com, adm2@company.com
```

EXIT STATUS

The following exit values are returned:

0 Successful completion.

>0 An error occurred.

SEE ALSO

setemailreport(8)

NAME

showenvironment - display the airflow volume, intake air temperature and humidity, temperature sensor, voltage sensor, fan speed, and power consumption information in the server

SYNOPSIS

showenvironment [-M] [*type*]

showenvironment -h

DESCRIPTION

showenvironment(8) command displays the information listed below.

The following types of the information are displayed:

Exhaust air information	Amount of exhaust air from the server.	
Environment information	Intake temperature and humidity of the system Humidity is supported only on the M8000/M9000 servers.	
Temperature information	Intake temperature of the system and exhaust temperature of each component You can check the exhaust temperature of the following components.	
	M3000 server	motherboard unit(MBU_A), CPU
	M4000/M5000 servers	CPU module(CPUM), I/O unit(IOU)
	M8000/M9000 servers	CPU/memory board unit(CMU), CPU module(CPUM), crossbar unit(XBU_B)
Voltage information	Voltage sensor value	
Fan speed information	Fan rotational state and revolutions per unit of time	
Power consumption information	Maximum rated power consumption value The power consumption information is supported only on the M3000 server.	

Privileges

You must have one of the following privileges to run this command:

useradm, platadm, platop, fieldeng

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

`-h` Displays usage statement. When used with other options or operands, an error occurs.

`-M` Displays text by page. This option provides a function that is the same as that of the `more` command.

OPERANDS

The following operand is supported:

type Specifies the one of the type of information to be displayed. The following types can be specified. If this type setting is omitted, intake temperature and humidity information about the system is displayed:

- `temp` Displays temperature information.
- `volt` Displays voltage information.
- `Fan` Displays fan speed information.
- `power` Displays power consumption information.
- `air` Displays the volume of air exhausted from the server.

EXTENDED DESCRIPTION

The result displayed by using the `power` and `air` operands does not include the information of external I/O expansion unit and the peripheral I/O devices.

EXAMPLES

EXAMPLE 1 Displays the intake temperature and humidity of the system on the M8000/M9000 servers.

```
XSCF> showenvironment
Temperature:30.71C
Humidity:90.05%
```

EXAMPLE 2 Displays temperature information about the system and each component on the M8000 server.

```
XSCF> showenvironment temp
Temperature:30.71C
CMU#0:30.71C
 CPUM#0-CHIP#0:30.71C
 CPUM#1-CHIP#0:30.71C
 CPUM#2-CHIP#0:30.71C
 CPUM#3-CHIP#0:30.71C
CMU#1:30.71C
 CPUM#0-CHIP#0:30.71C
```

```
 CPUM#1-CHIP#0:30.71C
 CPUM#2-CHIP#0:30.71C
 CPUM#3-CHIP#0:30.71C
CMU#2:30.71C
 CPUM#0-CHIP#0:30.71C
 CPUM#1-CHIP#0:30.71C
 CPUM#2-CHIP#0:30.71C
 CPUM#3-CHIP#0:30.71C
CMU#3:30.71C
 CPUM#0-CHIP#0:30.71C
 CPUM#1-CHIP#0:30.71C
 CPUM#2-CHIP#0:30.71C
 CPUM#3-CHIP#0:30.71C
```

EXAMPLE 3 Displays voltage information about each component on the M4000 server.

```
XSCF> showenvironment volt
MBU_A
 1.0V Power Supply Group:1.010V
 1.8V Power Supply Group:1.700V
 CPUM#0-CHIP#0
   1.0V Power Supply Group:1.000V
 CPUM#1-CHIP#0
   1.0V Power Supply Group:1.000V
MEMB#0
 1.2V Power Supply Group:1.200V
 1.8V Power Supply Group:1.700V
 2.5V Power Supply Group:2.500V
MEMB#1
 1.2V Power Supply Group:1.200V
 1.8V Power Supply Group:1.700V
 2.5V Power Supply Group:2.500V
MEMB#2
 1.2V Power Supply Group:1.200V
 1.8V Power Supply Group:1.700V
 2.5V Power Supply Group:2.500V
MEMB#3
 1.2V Power Supply Group:1.200V
 1.8V Power Supply Group:1.700V
 2.5V Power Supply Group:2.500V
IOU#0
 1.0V Power Supply Group:1.020V
 1.2V Power Supply Group:1.180V
 1.5V Power Supply Group:1.500V
 1.8V Power Supply Group:1.850V
```

```
 2.5V Power Supply Group:2.510V
 3.3V Power Supply Group:3.300V
 5.0V Power Supply Group:5.000V
  12V Power Supply Group:12.000V
 -12V Power Supply Group:-12.000V
FANBP
 3.3V Power Supply Group:3.300V
 5.0V Power Supply Group:5.010V
  12V Power Supply Group:12.020V
 -12V Power Supply Group:-12.030V
```

EXAMPLE 4 Displays the fan speed information on the M5000 server.

```
XSCF> showenvironment Fan
FAN_A#0:Low speed
        FAN_A#0:  4101rpm
FAN_A#1:Low speed
        FAN_A#1:  4101rpm
FAN_A#2:Low speed
        FAN_A#2:  4177rpm
FAN_A#3:Low speed
        FAN_A#3:  4101rpm
PSU#0
    PSU#0:Low speed
        PSU#0:  3879rpm
        PSU#0:  3835rpm
PSU#1
    PSU#1:Low speed
        PSU#1:  3924rpm
        PSU#1:  3970rpm
PSU#2
    PSU#2:Low speed
        PSU#2:  4218rpm
        PSU#2:  4066rpm
PSU#3
    PSU#3:Low speed
        PSU#3:  3835rpm
        PSU#3:  3970rpm
```

EXAMPLE 5 Displays the fan speed information on the M3000 server.

```
XSCF> showenvironment Fan
FAN_A#0:Low speed (level-4)
        FAN_A#0:  4134rpm
FAN_A#1:Low speed (level-4)
        FAN_A#1:  4212rpm
```

```
PSU#0
    PSU#0:Low speed (level-4)
        PSU#0:  6436rpm
PSU#1
    PSU#1:Low speed (level-4)
        PSU#1:  6352rpm
```

EXAMPLE 6 Displays power consumption information on the M3000 server (in case of AC power supply).

```
XSCF> showenvironment power
Permitted AC power consumption:470W
Actual AC power consumption:450W
```

EXAMPLE 7 Displays power consumption information on the M3000 server (in case of DC power supply).

```
XSCF> showenvironment power
Permitted DC power consumption:470W
Actual DC power consumption:450W
```

EXAMPLE 8 Displays the volume of air exhausted from the M3000 server.

```
XSCF> showenvironment air
Air Flow:63CMH
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

NAME

showfru - display the hardware settings of specified device

SYNOPSIS

showfru *device location*

showfru -a *device*

showfru -h

DESCRIPTION

The showfru(8) command displays the hardware settings of specified device by the setupfru(8) command.

The command can display the settings of the specified device or of all devices. Only the physical system board (PSB) can be specified as a device.

The following settings are displayed:

Device	Specified device name. Only sb is displayed.	
Location	Device location. If the *device* is "sb", the indicated location is an integer ranging from 00 to 15.	
XSB Mode	XSB mode set for the PSB. One of the following values is displayed:	
	Uni	Uni-XSB
	Quad	Quad-XSB
Memory Mirror Mode	Memory mirror mode set for the PSB. One of the following values is displayed:	
	yes	Memory mirror mode
	no	Memory no-mirror mode

Privileges

You must have platadm or fieldeng privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported.

-a	Displays the settings of all devices.
-h	Displays usage statement. When used with other options or operands, an error occurs.

OPERANDS

The following operands are supported:

device Specifies the device to display. Currently, only the following device can be specified:

`sb` Physical system board (PSB)

location Specifies the location of *device*. If the *device* is `"sb"`, an integer ranging from `00` to `15` can be specified.

EXTENDED DESCRIPTION

The `setupfru`(8) command makes hardware settings for a device.

EXAMPLES

EXAMPLE 1 Displays the settings of all PSBs.

```
XSCF> showfru -a sb
Device    Location     XSB Mode    Memory Mirror Mode
sb        00           Quad        no
sb        01           Uni         yes
sb        02           Quad        no
sb        03           Uni         no
```

EXIT STATUS

The following exit values are returned:

`0` Successful completion.

`>0` An error occurred.

SEE ALSO

addboard`(8)`, **deleteboard**`(8)`, **moveboard**`(8)`, **setdcl**`(8)`, **setupfru**`(8)`, **showboards**`(8)`, **showdcl**`(8)`, **showdevices**`(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.

The following information is displayed:

- Current configuration and status
- Number of installed FRUs
- Domain information
- External I/O Expansion Unit information
- PCI card information

Privileges

You must have one of the following privileges to run this command:

useradm, platadm, platop, fieldeng

Can run this command for all domains.

domainadm, domainmgr, domainop

Can run this command only for your accessible domains.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:.

-h Displays usage statement. When used with other options or operands, an error occurs.

-M Displays text by page.

-u Displays the number of FRUs installed in each unit. In addition, for CPU modules, the operating frequencies are displayed. For memory, the DIMM type and size are displayed. If this option is omitted, the current configuration and status information regarding FRUs and domain information are displayed.

EXTENDED DESCRIPTION

- When the configuration and status information regarding FRUs and domain information are displayed, for any failed or degraded unit, an asterisk (*) indicating an abnormal unit is displayed along with any of the following states:

Status	Description
Faulted	The component is faulty and is not operating
Degraded	The component is operating. However, either an error has been detected or the component is faulty. As a result, the component might be operating with reduced functionality or performance.
Deconfigured	As a result of another component's faulted or degraded status, the component is not operating. (The component itself is not faulted or degraded.)
Maintenance	The component is under maintenance. A deletefru(8), replacefru(8), or addfru(8) operation is currently underway
Normal	It is operating normally.

- On the Type field of the memories, the number indicates the DIMM size and the alphabet, A or B, indicates the DIMM rank.

Example	Description
Type: 1A	1 GB, rank 1
Type: 2A	2 GB, rank 1
Type: 2B	2 GB, rank 2

EXAMPLES

EXAMPLE 1 Displays the information of the FRUs in the M5000 server.

```
XSCF> showhardconf
SPARC Enterprise M5000;
    + Serial:BCF07500B6; Operator_Panel_Switch:Locked;
    + Power_Supply_System:Dual; SCF-ID:XSCF#0;
    + System_Power:On; System_Phase:Cabinet Power On;
    Domain#0 Domain_Status:Initialization Phase;
    Domain#1 Domain_Status:Initialization Phase;

    MBU_B Status:Normal; Ver:4401h; Serial:BC07490823  ;
        + FRU-Part-Number:CF00541-4360 01   /541-4360-01         ;
        + Memory_Size:64 GB;
        + Type:2;
        CPUM#0-CHIP#0 Status:Normal; Ver:0601h; Serial:PP0723016Q ;
            + FRU-Part-Number:CA06761-D205 A0   /371-4932-01          ;
            + Freq:2.660 GHz; Type:48;
            + Core:4; Strand:2;
```

```
                    :
        CPUM#3-CHIP#1 Status:Normal; Ver:0601h; Serial:PP074804E9  ;
            + FRU-Part-Number:CA06761-D205 A0   /371-4932-01          ;
            + Freq:2.660 GHz; Type:48;
            + Core:4; Strand:2;
        MEMB#0 Status:Normal; Ver:0101h; Serial:BF09061G0E  ;
            + FRU-Part-Number:CF00541-0545 06   /541-0545-06          ;
            MEM#0A Status:Normal;
                + Code:c100000000000000005372T128000HR3.7A  356d-0d016912;
                + Type:1A; Size:1 GB;
                    :
            MEM#3B Status:Normal;
                + Code:c100000000000000004572T128000HR3.7A  252b-04123424;
                + Type:1A; Size:1 GB;
                    :
        MEMB#7 Status:Normal; Ver:0101h; Serial:BF09061GBA  ;
            + FRU-Part-Number:CF00541-0545 06   /541-0545-06          ;
            MEM#0A Status:Normal;
                + Code:2cffffffffffffff0818HTF12872Y-53EB3 0300-
d504600c;
                + Type:1A; Size:1 GB;
                    :
            MEM#3B Status:Normal;
                + Code:7f7ffe00000000004aEBE10RD4AGFA-5C-E 3020-
2229c19c;
                + Type:1A; Size:1 GB;
        DDC_A#0 Status:Normal;
        DDC_A#1 Status:Normal;
        DDC_A#2 Status:Normal;
        DDC_A#3 Status:Normal;
        DDC_B#0 Status:Normal;
        DDC_B#1 Status:Normal;
        IOU#0 Status:Normal; Ver:0201h; Serial:BF07486TEU  ;
            + FRU-Part-Number:CF00541-4361 01   /541-4361-01          ;
            + Type:1;
            DDC_A#0 Status:Normal;
            DDCR Status:Normal;
                DDC_B#0 Status:Normal;
        IOU#1 Status:Normal; Ver:0201h; Serial:BF073226HP  ;
            + FRU-Part-Number:CF00541-4361 01   /541-4361-01          ;
            + Type:1;
            DDC_A#0 Status:Normal;
            DDCR Status:Normal;
                DDC_B#0 Status:Normal;
        XSCFU Status:Normal,Active; Ver:0101h; Serial:BF07435D98  ;
```

```
            + FRU-Part-Number:CF00541-0481 04   /541-0481-04          ;
        OPNL Status:Normal; Ver:0101h; Serial:BF0747690D  ;
            + FRU-Part-Number:CF00541-0850 06   /541-0850-06          ;
        PSU#0 Status:Normal; Serial:0017527-0738063762;
            + FRU-Part-Number:CF00300-1898 0350 /300-1898-03-50;
            + Power_Status:Off; AC:200 V;
                  :
        PSU#3 Status:Normal; Serial:0017527-0738063767;
            + FRU-Part-Number:CF00300-1898 0350 /300-1898-03-50;
            + Power_Status:Input fail; AC: - ;
        FANBP_C Status:Normal; Ver:0501h; Serial:FF2#24      ;
            + FRU-Part-Number:CF00541-3099 01   /541-3099-01          ;
            FAN_A#0 Status:Normal;
            FAN_A#1 Status:Normal;
            FAN_A#2 Status:Normal;
            FAN_A#3 Status:Normal;
```

EXAMPLE 2 Displays the number of installed FRUs in the M5000 server.

```
XSCF> showhardconf -u
SPARC Enterprise M5000; Memory_Size:64 GB;
 +-----------------------------------+------------+
 |              FRU                  |  Quantity  |
 +-----------------------------------+------------+
 | MBU_B                             |       1    |
 |     Type:2;                       |   (   1)   |
 |     CPUM                          |       4    |
 |         Freq:2.660 GHz;           |   (   8)   |
 |     MEMB                          |       8    |
 |         MEM                       |      64    |
 |             Type:1A; Size:1 GB;   |   (  64)   |
 |     DDC_A                         |       4    |
 |     DDC_B                         |       2    |
 | IOU                               |       2    |
 |     Type:1;                       |   (   2)   |
 |     DDC_A                         |       2    |
 |     DDCR                          |       2    |
 |         DDC_B                     |       2    |
 | IOBOX                             |       1    |
 |     IOB                           |       2    |
 |     PSU                           |       2    |
 | XSCFU                             |       1    |
 | OPNL                              |       1    |
 | PSU                               |       4    |
```

```
| FANBP_C                          |       1    |
|     FAN_A                        |       4    |
+----------------------------------+------------+
```

EXAMPLE 3 Displays the information of the FRUs in the M9000 server.

```
XSCF> showhardconf
SPARC Enterprise M9000;
    + Serial:PA30601004; Operator_Panel_Switch:Locked;
    + Power_Supply_System:Single-1Phase; Ex:Single-1Phase; SCF-ID:XSCF#0;
    + System_Power:On; System_Phase:Cabinet Power On;
    Domain#0 Domain_Status:Running;

    CMU#0 Status:Normal; Ver:0101h; Serial:PP0616B579  ;
        + FRU-Part-Number:CA06629-D001 A4                        ;
        + Memory_Size:128 GB;
        + Type:A
        CPUM#0-CHIP#0 Status:Normal; Ver:0101h; Serial:PP091505ZY  ;
            + FRU-Part-Number:CA06620-D021 A3                        ;
            + Freq:2.280 GHz; Type:16;
            + Core:2; Strand:2;
        CPUM#1-CHIP#0 Status:Normal; Ver:0101h; Serial:PP091505ZW  ;
            + FRU-Part-Number:CA06620-D021 A3                        ;
            + Freq:2.280 GHz; Type:16;
            + Core:2; Strand:2;
        CPUM#2-CHIP#0 Status:Normal; Ver:0101h; Serial:PP0915060H  ;
            + FRU-Part-Number:CA06620-D021 A3                        ;
            + Freq:2.280 GHz; Type:16;
            + Core:2; Strand:2;
        CPUM#3-CHIP#0 Status:Normal; Ver:0101h; Serial:PP09150603  ;
            + FRU-Part-Number:CA06620-D021 A3                        ;
            + Freq:2.280 GHz; Type:16;
            + Core:2; Strand:2;
        MEM#00A Status:Normal;
            + Code:7f7ffe00000000004aEBE41RE4ABHA-5C-E 3020-22211d88;
            + Type:4B; Size:4 GB;
        MEM#00B Status:Normal;
            + Code:7f7ffe00000000004aEBE41RE4ABHA-5C-E 3020-2a002a55;
            + Type:4B; Size:4 GB;
                :
        MEM#33A Status:Normal;
            + Code:ce0000000000000001M3 93T5168AZ0-CD5 3041-741a8ea1;
            + Type:4B; Size:4 GB;
        MEM#33B Status:Normal;
            + Code:ce0000000000000001M3 93T5168AZ0-CD5 3041-741a8ed3;
```

```
            + Type:4B; Size:4 GB;
                :
CMU#2 Status:Normal; Ver:4201h; Serial:PP0618K472  ;
    + FRU-Part-Number:CA06620-D003 A0   /371-4617-01          ;
    + Memory_Size:32 GB;
    + Type:B
    CPUM#0-CHIP#0 Status:Normal; Ver:0901h; Serial:PP0608J517  ;
        + FRU-Part-Number:CA06620-D051 A0   /371-4616-01          ;
        + Freq:2.880 GHz; Type:32;
        + Core:4; Strand:2;
    CPUM#1-CHIP#0 Status:Normal; Ver:0901h; Serial:PP0620P552  ;
        + FRU-Part-Number:CA06620-D051 A0   /371-4616-01          ;
        + Freq:2.880 GHz; Type:32;
        + Core:4; Strand:2;
    CPUM#2-CHIP#0 Status:Normal; Ver:0901h; Serial:PP0631Q396  ;
        + FRU-Part-Number:CA06620-D051 A0   /371-4616-01          ;
        + Freq:2.880 GHz; Type:32;
        + Core:4; Strand:2;
    CPUM#3-CHIP#0 Status:Normal; Ver:0901h; Serial:PP0629H443  ;
        + FRU-Part-Number:CA06620-D051 A0   /371-4616-01          ;
        + Freq:2.880 GHz; Type:32;
        + Core:4; Strand:2;
    MEM#00A Status:Normal;
        + Code:7f7ffe00000000004aEBE10RD4AGFA-5C-E 3020-221d6855;
        + Type:1A; Size:1 GB;
    MEM#00B Status:Normal;
        + Code:7f7ffe00000000004aEBE10RD4AGFA-5C-E 3020-221fcdb7;
        + Type:1A; Size:1 GB;
            :
    MEM#33A Status:Normal;
        + Code:7f7ffe00000000004aEBE10RD4AGFA-5C-E 3020-221d678b;
        + Type:1A; Size:1 GB;
    MEM#33B Status:Normal;
        + Code:2cffffffffffffff0818HTF12872Y-53EB3 0300-69aedd7a;
        + Type:1A; Size:1 GB;
CMU#3 Status:Normal; Ver:8301h; Serial:PP0638F192  ;
    + FRU-Part-Number:CA06620-D004 A0   /371-4930-01          ;
    + Memory_Size:64 GB;
    + Type:C
    CPUM#0-CHIP#0 Status:Normal; Ver:a01h; Serial:PP0631P606  ;
        + FRU-Part-Number:CA06620-D061 A1   /371-4929-01          ;
        + Freq:3.000 GHz; Type:48;
        + Core:4; Strand:2;
    CPUM#1-CHIP#0 Status:Normal; Ver:a01h; Serial:PP0630M355  ;
        + FRU-Part-Number:CA06620-D061 A1   /371-4929-01          ;
```

```
            + Freq:3.000 GHz; Type:48;
            + Core:4; Strand:2;
        CPUM#2-CHIP#0 Status:Normal; Ver:0a01h; Serial:PP0628D036  ;
            + FRU-Part-Number:CA06620-D061 A1   /371-4929-01          ;
            + Freq:3.000 GHz; Type:48;
            + Core:4; Strand:2;
        CPUM#3-CHIP#0 Status:Normal; Ver:0a01h; Serial:PP0630M365  ;
            + FRU-Part-Number:CA06620-D061 A1   /371-4929-01          ;
            + Freq:3.000 GHz; Type:48;
            + Core:4; Strand:2;
        MEM#00A Status:Normal;
            + Code:7f7ffe00000000004aEBE10RD4AGFA-5C-E 3020-221d6855;
            + Type:1A; Size:1 GB;
        MEM#00B Status:Normal;
            + Code:7f7ffe00000000004aEBE10RD4AGFA-5C-E 3020-221fcdb7;
            + Type:1A; Size:1 GB;
                :
        MEM#33A Status:Normal;
            + Code:7f7ffe00000000004aEBE10RD4AGFA-5C-E 3020-221d678b;
            + Type:1A; Size:1 GB;
        MEM#33B Status:Normal;
            + Code:2cffffffffffffff0818HTF12872Y-53EB3 0300-69aedd7a;
            + Type:1A; Size:1 GB;
                :
    IOU#0 Status:Normal; Ver:0101h; Serial:PP072102UN  ;
        + FRU-Part-Number:CA06620-D102 B1   /371-2217-02          ;
        + Type:A;
        PCI#0 Name_Property:pci; Card_Type:IOUA;
            + Serial:PP0611T826  ;
            + FRU-Part-Number:CA21126-B20X 002AB
        PCI#1 Status:Normal; Name_Property:LSILogic,sas; Card_Type:Other;
            + Serial:0000004; Type:F20;
            + FRU-Part-Number:5111500-01;
    IOU#1 Status:Normal; Ver:0101h; Serial:PP072102UM  ;
        + FRU-Part-Number:CA06620-D102 B1   /371-2217-02          ;
        + Type:A;
        PCI#0 Name_Property:pci; Card_Type:IOUA;
            + Serial:PP0611T825  ;
            + FRU-Part-Number:CA21126-B20X 002AB
    IOU#2 Status:Normal; Ver:4201h; Serial:PP0727053S  ;
        + FRU-Part-Number:CA06620-D103 A0   /371-4931-01          ;
        + Type:B;
        PCI#4 Name_Property:pci; Card_Type:IOUA;
            + Serial:PP0611T823  ;
            + FRU-Part-Number:CA21126-B20X 002AB                      ;
```

```
                :
    XSCFU_B#0 Status:Normal,Active; Ver:0201h; Serial:PP080600DW  ;
        + FRU-Part-Number:CA06620-D342 C0   /371-2228-02          ;
                :
    XBU_B#0 Status:Normal; Ver:0201h; Serial:PP0641X324  ;
        + FRU-Part-Number:CA06620-D301 A6                         ;
                :
    CLKU_B#0 Status:Normal; Ver:0101h; Serial:PP0542M679  ;
        + FRU-Part-Number:CA06629-D042 A1                         ;
                :
    OPNL#0 Status:Normal; Ver:0101h; Serial:PP06058246  ;
        + FRU-Part-Number:CA06629-D061 A1                         ;
    PSU#0 Status:Normal; Serial:;
        + FRU-Part-Number:CA01022-0690;
        + Power_Status:On;
                :
    FANBP_A#0 Status:Normal; Ver:0101h; Serial:PP0607D266  ;
        + FRU-Part-Number:CA21123-B54X 003AC                      ;
        FAN_A#0 Status:Normal; Serial:PA0605B287;
            + FRU-Part-Number:CA06501-D023 A2   /371-2222-00          ;
                :
        FAN_A#15 Status:Normal; Serial:PA0605B303;
            + FRU-Part-Number:CA06501-D023 A2   /371-2222-00          ;
                :
    FANBP_B#0 Status:Normal; Ver:0201h; Serial:PP0607D270  ;
        + FRU-Part-Number:CA21123-B55X 003AC                      ;
        FAN_A#4 Status:Normal; Serial:PA0605B297;
            + FRU-Part-Number:CA06501-D023 A2   /371-2222-00          ;
                :
        FAN_A#9 Status:Normal; Serial:PA0605B300;
            + FRU-Part-Number:CA06501-D023 A2   /371-2222-00          ;
                :
    SWBP#0 Status:Normal; Ver:0101h; Serial:PP0607E759  ;
        + FRU-Part-Number:CA20394-B16X 001AA                      ;
    MEDBP#0 Status:Normal; Ver:0101h; Serial:PP06058497  ;
        + FRU-Part-Number:CA20394-B17X 002AB                      ;
```

EXAMPLE 4 Displays the number of installed FRUs in the M9000 server.

```
XSCF> showhardconf -u
SPARC Enterprise M9000; Memory_Size:240 GB
 +-----------------------------------+------------+
 |              FRU                  |  Quantity  |
 +-----------------------------------+------------+
 | CMU                               |       4    |
```

```
|     Type:A;                        |   (   2)   |
|     Type:B;                        |   (   1)   |
|     Type:C;                        |   (   1)   |
|     CPU                            |      16    |
|         Freq:2.280 GHz;            |   (   8)   |
|         Freq:2.880 GHz;            |   (   8)   |
|     MEM                            |     112    |
|         Type:1A; Size:1 GB;        |   (  48)   |
|         Type:2B; Size:2 GB;        |   (  32)   |
|         Type:4B; Size:4 GB;        |   (  32)   |
| IOU                                |       8    |
|     Type:A;                        |   (   6)   |
|     Type:B;                        |   (   2)   |
| XSCFU_B                            |       2    |
| XBU_B                              |       8    |
| CLKU_B                             |       2    |
| OPNL                               |       1    |
| PSU                                |      15    |
| FANBP_A                            |       1    |
| FANBP_B                            |       1    |
|     FAN_A                          |      16    |
| SWBP                               |       1    |
| MEDBP                              |       1    |
+------------------------------------+------------+
```

EXAMPLE 5 Displays the information of the FRUs in the M3000 server (in case of AC power supply).

```
XSCF> showhardconf
SPARC Enterprise M3000;
    + Serial:BE80601016; Operator_Panel_Switch:Service;
    + Power_Supply_System:Single; SCF-ID:XSCF#0;
    + System_Power:Off; System_Phase:Cabinet Power Off;
    Domain#0 Domain_Status:Powered Off;

    MBU_A Status:Normal; Ver:0101h; Serial:7867000269  ;
        + FRU-Part-Number:CF00541-0493 0040 /541-0493-00-40       ;
        + CPU Status:Normal;
            + Freq:2.520 GHz; Type:32;
            + Core:4; Strand:2;
        + Memory_Size:8 GB;
        MEM#0A Status:Normal;
            + Code:00000000000000c14572T128000HR3.7A   2b25-20541204;
            + Type:1A; Size:1 GB;
                 :
```

```
        MEM#3B Status:Normal;
            + Code:00000000000000c14572T128000HR3.7A   2b25-21341204;
            + Type:1A; Size:1 GB;
        PCI#0 Name_Property:pci; Card_type:Other;
        PCI#1 Name_Property:pci; Card_type:Other;
        PCI#2 Name_Property:pci; Card_type:Other;
        PCI#3 Name_Property:pci; Card_type:Other;
    OPNL Status:Normal; Ver:0101h; Serial:7867000076  ;
        + FRU-Part-Number:CF00541-0850 0040 /541-0850-00-40       ;
    PSU#0 Status:Normal; Serial:0000000-ASTECB20  ;
        + FRU-Part-Number:CF00300-1898 0002 /300-1898-00-02;
        + Power_Status:Off;
        + Type:AC;
    PSU#1 Status:Normal; Serial:0000000-ASTECB17  ;
        + FRU-Part-Number:CF00300-1898 0002 /300-1898-00-02;
        + Power_Status:Off;
        + Type:AC;
    FANBP_B Status:Normal; Ver:0101h; Serial:7867000053  ;
        + FRU-Part-Number:CA06629-D051 001AA
        FAN_A#0 Status:Normal;
        FAN_A#1 Status:Normal;
```

EXAMPLE 6 Displays the information of the FRUs in the M3000 server (in case of DC power supply).

```
XSCF> showhardconf
SPARC Enterprise M3000;
    + Serial:BE80601016; Operator_Panel_Switch:Service;
    + Power_Supply_System:Single; SCF-ID:XSCF#0;
    + System_Power:Off; System_Phase:Cabinet Power Off;
    Domain#0 Domain_Status:Powered Off;

    MBU_A Status:Normal; Ver:0101h; Serial:7867000269  ;
        + FRU-Part-Number:CF00541-0493 0040 /541-0493-00-40       ;
        + CPU Status:Normal;
            + Freq:2.750 GHz; Type:32;
            + Core:4; Strand:2;
        + Memory_Size:8 GB;
        MEM#0A Status:Normal;
            + Code:00000000000000c14572T128000HR3.7A   2b25-20541204;
            + Type:1A; Size:1 GB;
                :
        MEM#3B Status:Normal;
            + Code:00000000000000c14572T128000HR3.7A   2b25-21341204;
            + Type:1A; Size:1 GB;
```

```
        PCI#0 Name_Property:pci; Card_type:Other;
        PCI#1 Name_Property:pci; Card_type:Other;
        PCI#2 Name_Property:pci; Card_type:Other;
        PCI#3 Name_Property:pci; Card_type:Other;
    OPNL Status:Normal; Ver:0101h; Serial:7867000076  ;
        + FRU-Part-Number:CF00541-0850 0040 /541-0850-00-40       ;
    PSU#0 Status:Normal; Serial:EA09320015 ;
        + FRU-Part-Number:CA01022-0730 01A  /300-2278-01;
        + Power_Status:Off;
        + Type:DC;
    PSU#1 Status:Normal; Serial:EA09320016 ;
        + FRU-Part-Number:CA01022-0730 01A  /300-2278-01;
        + Power_Status:Off;
        + Type:DC;
    FANBP_B Status:Normal; Ver:0101h; Serial:7867000053  ;
        + FRU-Part-Number:CA06629-D051 001AA
        FAN_A#0 Status:Normal;
        FAN_A#1 Status:Normal;
```

EXAMPLE 7 Displays the number of installed FRUs in the M3000 server.

```
XSCF> showhardconf -u
SPARC Enterprise M3000; Memory_Size:8 GB;
 +-----------------------------------+------------+
 |              FRU                  |  Quantity  |
 +-----------------------------------+------------+
 | MBU_A                             |       1    |
 |     CPU                           |   (   1)   |
 |         Freq:2.520 GHz;           |   (   1)   |
 |     MEM                           |       8    |
 |         Type:1A; Size:1 GB;       |   (   8)   |
 | OPNL                              |       1    |
 | PSU                               |       2    |
 | FANBP_B                           |       1    |
 |     FAN_A                         |       2    |
 +-----------------------------------+------------+
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

NAME

showhostname - display the current host name for the XSCF unit

SYNOPSIS

showhostname [-a | *xscfu*]

showhostname -h

DESCRIPTION

showhostname(8) command displays the current host name for the XSCF unit.

The host name is displayed in Fully Qualified Domain Name (FQDN) format.

Privileges

You must have one of the following privileges to run this command:

useradm, platadm, platop, auditadm, auditop, domainadm, domainmgr, domainop, fieldeng

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-a	Displays the current host names for all XSCF units. If an XSCF unit name is specified with the -a option, the XSCF unit name is ignored.
-h	Displays usage statement. When used with other options or operands, an error occurs.

OPERANDS

The following operand is supported:

xscfu Specifies the XSCF unit name to be displayed. One of the following values can be specified. If *xscfu* is specified with the -a option, *xscfu* is ignored.

xscf#0	XSCF unit 0
xscf#1	XSCF unit 1 (In the M8000/M9000 servers)

EXTENDED DESCRIPTION

- In the M8000/M9000 servers, a defect occurred on standby XSCF unit shows a message.
- The sethostname(8) command sets a host name for an XSCF unit.

EXAMPLES

EXAMPLE 1 Displays the current host names for all XSCF units.

```
XSCF> showhostname -a
xscf#0: scf0-hostname.example.com
xscf#1: scf1-hostname.example.com
```

EXAMPLE 2 Displays the host name for XSCF unit 0.

```
XSCF> showhostname xscf#0
xscf#0: scf0-hostname.example.com
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

sethostname(8)

NAME

showhttps - display the status of the HTTPS service set for the XSCF network

SYNOPSIS

showhttps

showhttps -h

DESCRIPTION

The showhttps(8) command displays the status of the HTTPS service currently set for the XSCF network.

With this command, whether the HTTPS service is operating and the installation status of the information that is necessary for authentication can be checked. If it is installed, the installation date is also displayed.

The following states are displayed:

HTTPS Status	Indicates whether the HTTPS service is operating
Server key	Indicates whether the private key of the web server has been installed
CA key	Indicates whether the private key of the certification authority has been installed
CA cert	Indicates whether the certificate of the certification authority has been installed
CSR	Requests the certificate of the web server

Privileges

You must have one of the following privileges to run this command:

useradm, platadm, platop, auditadm, auditop, domainadm, domainmgr, domainop, fieldeng

Refer to setprivileges(8) for more information.

OPTIONS

The following option is supported:

-h	Displays usage statement.

EXTENDED DESCRIPTION

The sethttps(8) command make settings for the HTTPS service in the XSCF network.

EXAMPLES

EXAMPLE 1 Displays the status of the HTTPS service.

```
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 200
CA cert: installed in Apr 24 12:00:34 JST 200
CSR:
```

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBwjCCASsCAQAwgYExCzAJBgNVBAYTAmpqMQ4wDAYDVQQIEwVzdGF0ZTERMA8G
A1UEBxMIbG9jYWxpdHkxFTATBgNVBAoTDG9yZ2FuaXphdGlvbjEPMA0GA1UECxMG
b3JnYW5pMQ8wDQYDVQQDEwZjb21tb24xFjAUBgkqhkiG9w0BCQEWB2VlLm1haWww
gZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJ5D57X/k42LcipTWBWzv2GrxaVM
5GEyx3bdBW8/7WZhnd3uiZ9+ANlvRAuw/YYy7I/pAD+NQJesBcBjuyj9x+IiJl9F
MrI5fR8pOIywVOdbMPCar09rrU45bVeZhTyi+uQOdWLoX/Dhq0fm2BpYuh9WukT5
pTEg+2dABg8UdHmNAgMBAAGgADANBgkqhkiG9w0BAQQFAAOBgQAux1jH3dyB6Xho
PgBuVIakDzIKEPipK9qQfC57YI43uRBGRubu0AHEcLVue5yTu6G5SxHTCq07tV5g
38UHSg5Kqy9QuWHWMri/hxm0kQ4gBpApjNb6F/B+ngBE3j/thGbEuvJb+0wbycvu
5jrhB/ZV9k8X/MbDOxSx/U5nF+Zuyw==
-----END CERTIFICATE REQUEST-----
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

sethttps (8)

NAME

showldap - display the Lightweight Directory Access Protocol (LDAP) configuration for the Service Processor

SYNOPSIS

showldap

showldap [-c]

showldap -h

DESCRIPTION

showldap(8) displays the Service Processor LDAP configuration. When invoked without options, showldap displays all LDAP configuration except for the certificate chain and the password used when binding to the LDAP server.

Privileges

You must have useradm or fieldeng privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-c Displays the LDAP server certification chain.

-h Displays usage statement.

When used with other options or operands, an error occurs.

EXAMPLES

EXAMPLE 1 Displaying All LDAP Configuration Data

```
XSCF> showldap
Bind Name: user
Base Distinguishing Name: ou=people,dc=company,dc=com
LDAP Search Timeout: 60
Bind password: Set
LDAP Servers: ldap://company.com:389
CERTS: None
```

EXAMPLE 2 Displaying All LDAP Configuration Data

```
XSCF> showldap -c
There are no certificates configured.
```

EXIT STATUS

The following exit values are returned:

0 Successful completion.

>0 An error occurred.

SEE ALSO

setldap(8)

NAME

showldapssl - show LDAP/SSL configuration and messages

SYNOPSIS

showldapssl

showldapssl `cert` [`-v`] [`-i` *n*]

showldapssl `log` [`-M`] [`-C`] [`-S` *start_record_number*] [`-E` *end_record_number*]

showldapssl `log -f`

showldapssl `group administrator` [`-i` *n*]

showldapssl `group operator` [`-i` *n*]

showldapssl `group custom` [`-i` *n*]

showldapssl `userdomain` [`-i` *n*]

showldapssl `usermap`

showldapssl `defaultrole`

showldapssl `server` [`-i` *n*]

showldapssl `-h`

DESCRIPTION

`showldapssl`(8) displays the LDAP/SSL configuration and diagnostic messages.

Privileges

You must have `useradm` privileges to run this command.

Refer to `setprivileges`(8) for more information.

OPTIONS

The following options are supported:

`-f`	Displays diagnostic messages in real time. When this option is used, the command does not terminate. Each diagnostic message is displayed when it is registered. To stop the real-time display, press `Ctrl-C`.
`-h`	Displays usage statement. When used with other options or operands, an error occurs.
`-i` *n*	Sets an index marker, value 1 - 5. When executed without `-i`, or with `-i` and no value, `showldapssl` walks sequentially through items 1 through 5. Exceptions: When used without `-i`, the command `showldapssl cert` displays the certificate information for the Primary server, and `showldapssl server` displays the Primary server configuration.
`-v`	Specifies verbose output. Used only with the cert operand to display the full certificate.

-C	Appends to end of output the number of records in the log.
-E	Specifies the last record number to display, where end_record_number can be any record number in the log. Use -C to obtain the number of records in the log.
-M	Displays text by page, like the more(1) command does.
-S	Specifies the first record to display, where start_record_number can be any record number in the log. Use -C to obtain the number of records in the log.

OPERANDS

The following operands are supported:

cert	Display current server certificates.
log	Display diagnostic messages.
group administrator	Display current group configurations.
group operator	Display current group configurations.
group custom	Display current group configurations.
userdomain	Display current userdomain settings.
usermap	Display current user mapping settings.
defaultrole	Display current defaultrole setting.
server	Display current LDAP/SSL server settings.

EXAMPLES

EXAMPLE 1 Displays the current state of LDAP/SSL.

```
XSCF> showldapssl
usermapmode: enabled
state: enabled
strictcertmode: enabled
timeout: 4
logdetail: none
```

EXAMPLE 2 Displays certificate information for the Primary server.

```
XSCF> showldapssl cert
Primary Server:
certstatus = certificate present
issuer = C=US, ST=California, L=San Diego, O=aCompany,
OU=System Group, CN=John User serial number = 0 (00000000)
subject = C=US, ST=California, L=San Diego, O=aCompany,
OU=System Group, CN=John User serial number = 0 (00000000)
```

```
valid from = Apr 18 05:38:36 2009 GMT
valid until = Apr 16 05:38:36 2019 GMT
version = 3 (0x02)
```

EXAMPLE 3 Displays specified diagnostic messages.

```
XSCF> showldapssl log -S 5 -E 10
Thu Sep 2 01:43 2009 (LdapSSL): -error- authentication status: auth-ERROR
Thu Sep 2 01:44 2009 (LdapSSL): -error- authentication status: auth-ERROR
Thu Sep 2 01:47 2009 (LdapSSL): -error- authentication status: auth-ERROR
Thu Sep 2 01:51 2009 (LdapSSL): -error- authentication status: auth-ERROR
Thu Sep 2 01:52 2009 (LdapSSL): -error- authentication status: auth-ERROR
Thu Sep 2 01:55 2009 (LdapSSL): -error- authentication status: auth-ERROR
```

EXAMPLE 4 Displays configuration for administrator group 3.

```
XSCF> showldapssl group administrator -i 3
Administrator Group 3
name: CN=pSuperAdmin,OU=Groups,DC=sales,DC=company,DC=com
```

EXAMPLE 5 Displays alternate server 1 setting. A port number of 0 indicates that the default port for LDAP/SSL is used.

```
XSCF> showldapssl server -i 1
Alternate Server  1
address: (none)
port: 0
```

EXAMPLE 6 Displays the optional user mapping settings.

```
XSCF> showldapssl usermap
attributeInfo: (&(objectclass=person)(uid=<USERNAME>))
binddn: cn=Manager,dc=company,dc=com
bindpw: Set
searchbase: ou=people,dc=company,dc=com
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

setldapssl(8)

NAME

showlocale - display the current setting for the XSCF locale

SYNOPSIS

showlocale

showlocale -h

DESCRIPTION

The showlocale(8) command displays the current setting for the XSCF locale.

Either of the following is displayed:

C	English
ja_JP.UTF-8	Japanese

Privileges

You must have one of the following privileges to run this command:

useradm, platadm, platop, auditadm, auditop, domainadm, domainmgr, domainop

Refer to setprivileges(8) for more information.

OPTIONS

The following option is supported:

-h	Displays usage statement.

EXTENDED DESCRIPTION

The setlocale(8) command sets a locale for the XSCF.

EXAMPLES

EXAMPLE 1 Displays the current setting for the XSCF locale (when English is set).

```
XSCF> showlocale
C
```

EXAMPLE 2 Displays the current setting for the XSCF locale (when Japanese is set).

```
XSCF> showlocale
ja_JP.UTF-8
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

setlocale(8)

NAME

showlocator - display the state of the CHECK LED on the operator panel

SYNOPSIS

showlocator

showlocator -h

DESCRIPTION

showlocator(8) command displays the blink state of the CHECK LED on the operator panel.

The one of the following state is displayed:

Off	Indicates normal operation, which means either the circuit breaker is off or power is not being supplied.
Blinking	Indicates that the unit is a maintenance target.
On	Indicates that an error was detected in the main unit.

Privileges

You must have one of the following privileges to run this command:

useradm, platadm, platop, fieldeng

Refer to setprivileges(8) for more information.

OPTIONS

The following option is supported:

-h	Displays usage statement.

EXTENDED DESCRIPTION

The setlocator(8) command can be used to specify the blink state of the CHECK LED.

EXAMPLES

EXAMPLE 1 Displays the CHECK LED state.

```
XSCF> showlocator
Locator LED status:Blinking
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

setlocator(8)

NAME

showloginlockout - display the account lockout setting

SYNOPSIS

showloginlockout

showloginlockout -h

DESCRIPTION

The showloginlockout(8) command displays the amount of time, in minutes, that a user is prevented from logging in after three failed attempts.

Privileges

You must have useradm privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following option is supported:

-h Displays usage statement. When used with other options or operands, an error occurs.

EXTENDED DESCRIPTION

A user is allowed three consecutive attempts to login. After the third failed attempt the system prevents further attempts for the amount of time determined by the setloginlockout(8) command. showloginlockout displays that amount of time in minutes.

After the set amount of time has elapsed, the user may try again.

EXAMPLES

EXAMPLE 1 Display The Lockout time

```
XSCF> showloginlockout
90 minutes
```

EXIT STATUS

The following exit values are returned:

0 Successful completion.

>0 An error occurred.

SEE ALSO

setloginlockout(8)

NAME

showlogs - display the specified log

SYNOPSIS

showlogs [-t *time* [-T *time*] | -p *timestamp*] [-v | -V | -S] [-r] [-M] error

showlogs [-t *time* [-T *time*] | -p *timestamp*] [-v] [-r] [-M] event

showlogs [-t *time* [-T *time*]] [-r] [-M] {power | env}

showlogs [-r] [-M] monitor

showlogs -d *domain_id* [-t *time* [-T *time*]] [-r] [-M] {console | ipl | panic}

showlogs -h

DESCRIPTION

The showlogs(8) command displays the specified log.

Log data is displayed in the order of timestamps, starting from the oldest data by default. Depending on the target for the log collection, the following logs can be specified:

For Field Replaceable Unit (FRU)

- Error log (sometimes includes scan log)
- Power log
- Event log
- Temperature and humidity record
- Monitoring message log

For domain

- Console message log
- Panic message log
- IPL message log

Privileges

You must have one of the following privileges to run this command:

- Error log, Event log, Temperature and humidity record, and Monitor message log:

  platadm, platop, fieldeng

- Power log:

  platadm, platop, domainadm, domainmgr, fieldeng

- Scan log:

  fieldeng

- Console message log, Panic message log, and IPL message log:

  platadm, platop, domainadm, domainmgr, domainop, fieldeng

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

`-d` *domain_id*
: Specifies the ID of a domain to be displayed. This option can be specified for domain specific log. *domain_id* can be `0–23` depending on the system configuration.

`-h`
: Displays usage statement. When used with other options or operands, an error occurs.

`-M`
: Displays text by page.

`-p` *timestamp*
: Specifies a *timestamp* in a log when one log is to be displayed. This option can be specified for an error log or event log.

  timestamp is specified in one of the following formats:

  yyyy-mm-dd,hh:mm:ss

  The *timestamp* is specified in the '*year-month-day*, *hour*:*minute*:*second*' format.

  mm/dd/yy,hh:mm:ss

  The *timestamp* is specified in the '*month*/*day*/*year*, *hour*:*minute*:*second*' format.

  Monddhh:mm:ssyyyy

  The *timestamp* is specified in the '*month-name*, *day*, *hour*:*minute*:*second*, *year*' format.

`-r`
: Displays a log in the order of timestamps, starting from the latest timestamp. By default, the display of log data in the order of timestamps starts from the oldest data.

`-S`
: Displays a scan log attached to an error log. Only a user having the `fieldeng` privilege can specify this operand. This cannot be specified together with the`-v` option or `-V` option.

`-t` *time*

Specifies the start date and time of the display range for log data. It is specified in one of the following formats:

yyyy-mm-dd,hh:mm

The *timestamp* is specified in the '*year-month-day*, *hour*:*minute*' format.

mm/dd/yy,hh:mm

The *timestamp* is specified in the '*month*/*day*/*year*, *hour*:*minute*' format.

Monddhh:mmyyyy

The *timestamp* is specified in the '*month-name*, *day*, *hour*:*minute*, *year*' format.

yyyy-mm-dd,hh:mm:ss

The *timestamp* is specified in the '*year-month-day*, *hour*:*minute*:*second*' format.

mm/dd/yy,hh:mm:ss

The *timestamp* is specified in the '*month*/*day*/*year*, *hour*:*minute*:*second*' format.

Monddhh:mm:ssyyyy

The *timestamp* is specified in the '*month-name*, *day*, *hour*:*minute*:*second*, *year*' format.

Even if the `-r` option is specified together with this option, the specified `-t` and `-T` options are not reversed. The `-t` option cannot be used for the monitoring message log.

`-T` *time*

Specifies the end date and time of the display range for log data. It is specified in one of the following formats:

yyyy-mm-dd,hh:mm

The *timestamp* is specified in the '*year-month-day*, *hour*:*minute*' format.

mm/dd/yy,hh:mm

The *timestamp* is specified in the '*month*/*day*/*year*, *hour*:*minute*' format.

Monddhh:mmyyyy

The *timestamp* is specified in the '*month-name*, *day*, *hour*:*minute*, *year*' format.

yyyy-mm-dd,hh:mm:ss

The *timestamp* is specified in the '*year-month-day*, *hour*:*minute*:*second*' format.

mm/dd/yy,hh:mm:ss

The *timestamp* is specified in the '*month*/*day*/*year*, *hour*:*minute*:*second*' format.

Monddhh:mm:ssyyyy

The *timestamp* is specified in the '*month-name*, *day*, *hour*:*minute*:*second*, *year*' format.

Even if the `-r` option is specified together with this option, the specified `-t` and `-T` options are not reversed. The `-T` option cannot be used for the monitoring message log.

`-v`

Displays a log in detail. Details of `Diagnostic Codes UUID` and `MSG-ID`, which are used by the `fmadm`(8) and `fmdump`(8) commands, are also displayed in addition to the items normally displayed. This option cannot be specified together with the `-S` or `-V` option. This option can be specified for an error log or event log.

`-V`

Displays a log in greater detail. If detailed log information on machine administration and OBP console log information have already been collected, they are also displayed in addition to the information displayed by the `-v` option. This option cannot be specified together with the `-S` or the `-v` option. This option can be specified for an error log.

OPERANDS

The following operands are supported:

`error`	Displays the error log. (sometimes includes scan log)
`power`	Displays the power log.
`event`	Displays the event log.
`env`	Displays the temperature and humidity record.
`monitor`	Displays the monitoring message log.
`console`	Displays the console message log.
`panic`	Displays the panic message log.
`ipl`	Displays the IPL message log.

EXTENDED DESCRIPTION

Logs are displayed in the following formats:

- Error log

  Default

```
Date: Mar 30 17:45:31 JST 2005   Code: xxxxxxxx-xxxxxxxx-xxxxxxxxxxxxxxxx
Status: Alarm                  Occurred: Mar 30 17:45:31.000 JST 2005
FRU: PSU#1,PSU#2,*
Msg: ACFAIL occurred (ACS=3)(FEP type = A1)
```

  Case where the `-v` option is specified

```
Date: Mar 30 17:45:31 JST 2005    Code: xxxxxxxx-xxxxxxxx-xxxxxxxxxxxxxxxx
Status: Alarm                  Occurred: Mar 30 17:45:31.000 JST 2005
FRU: PSU#1,PSU#2,*
Msg: ACFAIL occurred (ACS=3)(FEP type = A1)
Diagnostic Code:
   xxxxxxxx xxxxxxxx xxxxxxxx
   xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx
   xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx
UUID: bf36f0ea-9e47-42b5-fc6f-c0d979c4c8f4 MSG-ID:FMD-8000-11
```

  Case where the `-V` option is specified

```
Date: Mar 30 17:45:31 JST 2005   Code: xxxxxxxx-xxxxxxxx-xxxxxxxxxxxxxxxx
Status: Alarm                  Occurred: Mar 30 17:45:31.000 JST 2005
FRU: PSU#1,PSU#2,*
Msg: ACFAIL occurred (ACS=3)(FEP type = A1)
Diagnostic Code:
   xxxxxxxx xxxxxxxx xxxxxxxx
   xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx
   xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx
```

```
UUID: bf36f0ea-9e47-42b5-fc6f-c0d979c4c8f4 MSG-ID:FMD-8000-11
Diagnostic Messages:
      :
      :
```

Case where the `-S` option is specified

```
Date: Mar 30 17:45:31 JST 2005     Code: xxxxxxxx-xxxxxxxx-xxxxxxxxxxxxxxx
Status: Alarm                  Occurred: Mar 30 17:45:31.000 JST 2005
FRU: PSU#1,PSU#2,*
Msg: ACFAIL occurred (ACS=3)(FEP type = A1)
Diagnostic Code:
   xxxxxxxx xxxxxxxx xxxxxxxx
   xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx
   xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx
UUID: bf36f0ea-9e47-42b5-fc6f-c0d979c4c8f4 MSG-ID:FMD-8000-11
Detail log: SCAN MINOR RC 2K
   0000: xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx
   0010: xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx
      :
      :
```

`Date`: Log collection date and time (month day hour:minute:second time-zone year)

The displayed time is the local time.

`Code`: Error code

Data is displayed in 16-byte format.

`Occurred`: Date (Month Day Hour: Minute: Second TimeZone Year) when an error occurred.

This date is displayed as the local time.

`Status`: Error status

One of the following states is displayed:

`Warning`	Partial degradation of the unit or warning about the FRU
`Alarm`	FRU failure or error
`Information`	Notification
`Notice`	System state notification

FRU:	Suspected faulty unit The suspected faulty units that are displayed and delimited by a "," (comma) are the units most likely and second most likely to be faulty. If there are three suspected faulty units, an "*" is displayed next to the unit third most likely to be faulty. Display of more than two suspected faulty units depends on whether more than two suspected faulty units are detected.
Msg:	Error description
Diagnostic Code:	Detailed error code The displayed code is a hexadecimal number.
UUID:	Abbreviation for Universal Unique Identifier This is a globally unique ID that is a 32-digit hexadecimal number.
MSG-ID:	Unique message ID
Diagnostic Messages:	Detailed message If the log has a detailed message, it is displayed.
Detail log:	Scan log code This code is displayed when the log includes a scan log. Address: Displayed in hexadecimal notation.

- Power log

```
Date                          Event             Cause          DID  Switch
Mar 30 17:25:31 JST 2005     System Power Off  Pow.Fail/Recov.--   Service
Mar 30 17:35:31 JST 2005     System Power On   Pow.Fail/Recov.--   Locked
Mar 30 17:45:31 JST 2005     Domain Power On   Panel          00   Locked
Mar 30 17:50:31 JST 2005     Domain Power Off  Operator       10   Service
       :
       :
```

`Date`: Log collection date and time (month day hour:minute:second time-zone year)

The displayed time is the local time.

`Event`: Power status

One of the following states is displayed:

`Domain Power On`	The domain power is on.
`Domain Power Off`	The domain power is off.
`System Power On`	The system power is on.
`System Power Off`	The system power is off.
`SCF Reset`	XSCF is in the reset state.
`Domain Reset`	The domain is in the reset state.
`XIR`	The domain CPU is in the reset state.

`Cause`: Factor that caused this Status

One of the following factors is displayed:

`Self Reset`, `Power On`, `System Reset`, `Panel`, `Scheduled`, `RCI`, `Pow.Fail/Recov.`, `Operator`, `SW Request`, `Alarm`, `Fatal`, `Panic`

`DID`: Domain ID

domain_id can be `00–23` depending on the system configuration.

`Switch`: Status of the mode switch of the operator panel

One of the following states are displayed:

`Locked`	Normal operation mode
`Service`	Service mode

- Event log

  Default

```
Date                          Message
Mar 30 17:45:31 JST 2005      System power on
Mar 30 17:55:31 JST 2005      System power off
      :
      :
```

Case where the -v option is specified

```
Date                          Message
Mar 30 17:45:31 JST 2005      System power on
  Switch= Service
  Code=xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx
        xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx
```

`Date`: Log collection date and time (month day hour:minute:second time-zone year)

The displayed time is the local time.

`Message`: Event message

`Switch`: Status of the mode switch of the operator panel

One of the following states are displayed:

`Locked`	Normal operation mode
`Service`	Service mode

`Code`: Detailed event information

The displayed information is in hexadecimal format

- TEMPERATURE AND HUMIDITY RECORD

```
Date                          Temperature  Humidity  Power
Mar 30 17:45:31 JST 2005      32.56(C)     60.20%    System Power On
Mar 30 17:55:31 JST 2005      32.56(C)     60.25%    System Power Off
      :
      :
```

`Date`: Log collection date and time (month day hour:minute:second time-zone year)

The displayed time is the local time.

`Temperature`: Intake air temperature

Decimal numbers are displayed to two decimal places. The unit is degree Celsius (C).

`Humidity`: Humidity

The displayed numbers are percentages (%). Humidity is displayed on the M8000/M9000 servers only.

`Power`: Power state of the main unit

Either of the following states is displayed:

`System Power ON`	The main unit power is on.
`System Power OFF`	The main unit power is off.

- Monitoring message log

```
Mar 30 17:45:31 JST 2005      monitor message
Mar 30 17:55:31 JST 2005      monitor message
      :
```

Each line of display has a date and time paired with a monitoring message. The time in the displayed log collection date and time (month day hour:minute:second time-zone year) is the local time.

- Console message log

```
DomainID: 00
Mar 30 17:45:31 JST 2005      console message
Mar 30 17:55:31 JST 2005      console message
      :
```

[First line]

`DomainID`: Domain ID

domain_id can be `00–23` depending on the system configuration.

[Second and subsequent lines]

Each line of display has a date and time paired with a console message.

The time in the displayed log collection date and time (month day hour:minute:second time-zone year) is the local time.

- Panic message log

```
<<panic>>
Date: Mar 30 18:45:31 JST 2005      DomainID: 00
Mar 30 17:45:31 JST 2005      panic message
Mar 30 17:55:31 JST 2005      panic message
      :
```

[Second line]

`Date`: Panic occurrence date and time (month day hour:minute:second time-zone year)

The displayed time is the local time.

`DomainID`: Domain ID

domain_id can be `00`–`23` depending on the system configuration.

[Third and subsequent lines]

Each line of display has a date and time paired with a panic message.

The time in the displayed log collection date and time (month day hour:minute:second time-zone year) is the local time.

- IPL message log

```
<<ipl>>
Date: Mar 30 18:45:31 JST 2005      DomainID: 00
Mar 30 17:45:31 JST 2005      ipl message
Mar 30 17:55:31 JST 2005      ipl message
      :
```

[Second line]

`Date`: IPL date and time (month day hour:minute:second time-zone year)

The displayed time is the local time.

`DomainID`: Domain ID

domain_id can be `00`–`23` depending on the system configuration.

[Third and subsequent lines]

Each line of display has a date and time paired with an IPL message.

The time in the displayed log collection date and time (month day hour:minute:second time-zone year) is the local time.

EXAMPLES

EXAMPLE 1 Displays an error log.

```
XSCF> showlogs error
Date: Mar 30 12:45:31 JST 2005     Code: 00112233-44556677-8899aabbcceeff0
  Status: Alarm                   Occurred: Mar 30 17:45:31.000 JST 2005
  FRU: IOU#0/PCI#3
  Msg: offline(vendor=FUJITSU, product=MAJ3182MC)
Date: Mar 30 15:45:31 JST 2005     Code: 00112233-44556677-8899aabbcceeff0
  Status: Warning                 Occurred: Mar 30 17:45:31.000 JST 2005
  FRU: PSU#1,PSU#2
  Msg: ACFAIL occurred (ACS=3)(FEP type = A1)
Date: Mar 30 17:45:31 JST 2005     Code: 00112233-44556677-8899aabbcceeff0
  Status: Alarm                   Occurred: Mar 30 17:45:31.000 JST 2005
  FRU: PSU#1,PSU#2,*
  Msg: ACFAIL occurred (ACS=3)(FEP type = A1)
```

EXAMPLE 2 Displays an error log in detail for the times of the specified timestamp (-v).

```
XSCF> showlogs error -p Mar3012:45:312005 -v
Date: Mar 30 12:45:31 JST 2005     Code: 00112233-44556677-8899aabbcceeff0
  Status: Alarm
  Component: IOU#0/PCI#3
  Msg: offline(vendor=FUJITSU, product=MAJ3182MC)
  Diagnostic Code:
    00112233 44556677 8899aabb
    00112233 44556677 8899aabb ccddeeff
    00112233 44556677 8899aabb ccddeeff
UUID: bf36f0ea-9e47-42b5-fc6f-c0d979c4c8f4 MSG-ID: FMD-8000-11
```

EXAMPLE 3 Displays an error log in greater detail for the times of the specified timestamp (-V).

```
XSCF> showlogs error -p Mar3012:45:312005 -V
Date: Mar 30 12:45:31 JST 2005     Code: 00112233-44556677-8899aabbcceeff0
  Status: Alarm                   Occurred: Mar 30 17:45:31.000 JST 2005
  FRU: IOU#0/PCI#3
  Msg: offline(vendor=FUJITSU, product=MAJ3182MC)
  Diagnostic Code:
    00112233 44556677 8899aabb
    00112233 44556677 8899aabb ccddeeff
    00112233 44556677 8899aabb ccddeeff
  UUID: bf36f0ea-9e47-42b5-fc6f-c0d979c4c8f4 MSG-ID: FMD-8000-11
  Diagnostic Messages
  Jul 11 16:17:42 plato10 root: [ID 702911 user.error] WARNING: /
pci@83,4000/scsi@2/sd@0,0 (sd47):
  Jul 11 16:17:42 plato10 root: [ID 702911 user.error]   incomplete write-
giving up
```

EXAMPLE 4 Displays a power log.

```
XSCF> showlogs power
Date                          Event              Cause         DID  Switch
Mar 30 17:25:31 JST 2005      System Power Off   Pow.Fail/Recov.-- Service
Mar 30 17:35:31 JST 2005      System Power On    Pow.Fail/Recov.-- Locked
Mar 30 17:45:31 JST 2005      Domain Power Off   Operator        00 Locked
Mar 30 17:50:31 JST 2005      Domain Power On    Operator        00 Service
```

EXAMPLE 5 Displays a power log in the order of timestamps, starting from the latest timestamp.

```
XSCF> showlogs power -r
Date                          Event              Cause         DID Switch
Mar 30 17:50:31 JST 2005      Domain Power On    Operator       00  Service
Mar 30 17:45:31 JST 2005      Domain Power Off   Operator       00  Locked
Mar 30 17:35:31 JST 2005      System Power On    Pow.Fail/Recov.--  Locked
Mar 30 17:25:31 JST 2005      System Power Off   Pow.Fail/Recov.--  Service
```

EXAMPLE 6 Displays the specified range of a power log.

```
XSCF> showlogs power -t Mar3017:302005 -T Mar3017:492005
Date                          Event              Cause         DID  Switch
Mar 30 17:35:31 JST 2005      System Power On    Pow.Fail/Recov.-- Locked
Mar 30 17:45:31 JST 2005      Domain Power Off   Operator        00 Locked
```

EXAMPLE 7 Displays the specified range of a power log. The log is displayed in the order of timestamps, starting from the latest timestamp.

```
XSCF> showlogs power -t Mar3017:302005 -T Mar3017:492005 -r
Date                          Event              Cause         DID  switch
Mar 30 17:45:31 JST 2005      Domain Power Off   Operator       00  Locked
Mar 30 17:35:31 JST 2005      System Power On    Pow.Fail/Recov.--  Locked
```

EXAMPLE 8 Displays the specified date of a power log. Data with this date or later in the log is displayed.

```
XSCF> showlogs power -t Mar3017:302005
Date                          Event              Cause         DID  switch
Mar 30 17:35:31 JST 2005      System Power On    Pow.Fail/Recov.--  Locked
Mar 30 17:45:31 JST 2005      Domain Power Off   Panel           00   Locked
Mar 30 17:50:31 JST 2005      Domain Power On    Operator        00   Service
```

EXAMPLE 9 Displays a console message log of the domain ID 0.

```
XSCF> showlogs console -d 00
DomainID:00
```

```
Mar 30 17:45:31 JST 2005      Executing last command: boot
Mar 30 17:55:31 JST 2005      Boot device: /pci@83,4000/FJSV,ulsa@2,1/
disk@0,0:a  File and args:
Mar 30 17:55:32 JST 2005      SunOS Release 5.10 Version Generic 64-bit
```

Note: The codes or messages shown here may differ from those actually displayed.

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

NAME

showlookup - display the configuration for authentication and privileges lookup

SYNOPSIS

showlookup

showlookup -h

DESCRIPTION

showlookup(8) displays configuration settings for authentication and privileges.

Privileges

You must have useradm or fieldeng privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following option is supported:

-h Displays usage statement.

EXAMPLES

EXAMPLE 1 Displaying Settings for Authentication and Privileges

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

EXIT STATUS

The following exit values are returned:

0 Successful completion.

>0 An error occurred.

SEE ALSO

setlookup(8)

NAME

showmonitorlog - display the contents of monitoring messages in real time

SYNOPSIS

showmonitorlog

showmonitorlog -h

DESCRIPTION

The showmonitorlog(8) command displays the contents of monitoring messages in real time.

When executed, the showmonitorlog(8) command will not terminate in order to display the monitoring message log, and the XSCF shell is occupied for the display. When a monitoring message is registered, the contents of the message are displayed.

To stop the real-time display, press the "Ctrl" and "C" key combination.

Privileges

You must have one of the following privileges to run this command:

platadm, platop, fieldeng

Refer to setprivileges(8) for more information.

OPTIONS

The following option is supported:

-h	Displays usage statement.

EXAMPLES

EXAMPLE 1 Displays the contents of a monitoring message in real time.

```
XSCF> showmonitorlog
Apr 13 12:32:16 XXXXX Alarm: /CMU#1,/CMU#0/DDC#0:ANALYZE:SC-IOU I/F fatal
error 0x00000000;
  :
  :
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

NAME

shownameserver - display the registered domain name system (DNS) servers and the DNS search paths specified on the XSCF network

SYNOPSIS

shownameserver

shownameserver -h

DESCRIPTION

shownameserver(8) command displays the registered DNS servers and the DNS search paths in the XSCF network.

Privileges

You must have one of the following privileges to run this command:

useradm, platadm, platop, auditadm, auditop, domainadm, domainmgr, domainop, fieldeng

Refer to setprivileges(8) for more information.

OPTIONS

The following option is supported:

-h Displays usage statement.

EXTENDED DESCRIPTION

The setnameserver(8) command sets the DNS servers and the DNS search paths used in the XSCF network.

EXAMPLES

EXAMPLE 1 Displays the DNS serversand the DNS search paths currently set for the XSCF network. The following example shows that three DNS servers and five DNS search paths have been set:

```
XSCF> shownameserver
nameserver 192.168.1.2
nameserver 10.18.108.10
nameserver 10.24.1.2
search     example1.com
search     example2.com
search     example3.com
search     example4.com
search     example5.com
```

EXAMPLE 2 Displays the DNS servers and the DNS search paths currently set for the XSCF network. The following example shows that no DNS server and the DNS search path are set:

```
XSCF> shownameserver
nameserver ---
search     ---
```

EXIT STATUS

The following exit values are returned:

`0`	Successful completion.
`>0`	An error occurred.

SEE ALSO

setnameserver`(8)`

NAME

shownetwork - display information of network interfaces for XSCF

SYNOPSIS

shownetwork [-M] {-a | -i | *interface*}

shownetwork -h

DESCRIPTION

shownetwork(8) command displays current information of network interfaces for XSCF.

Information on the specified network interface or all the network interfaces can be displayed. The following information is displayed:

xscf#x-y	XSCF network interface name
HWaddr	MAC address (hexadecimal notation)
inet addr	IP address
Bcast	Broadcast
Mask	Netmask
UP/DOWN	Whether the network interface is enabled

Privileges

You must have one of the following privileges to run this command:

useradm, platadm, platop, auditadm, auditop, domainadm, domainmgr, domainop, fieldeng

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-a	Displays information for all XSCF network interfaces.
-h	Displays usage statement. When used with other options or operands, an error occurs.
-M	Displays text by page. This option provides a function that is the same as that of the more command.

OPERANDS

The following operands are supported:

interface

Specifies the network interface whose information is to be displayed. One of the following values can be specified, depending on the system configuration. If this operand is specified with the `-a` option, the operand is ignored.

- In the M3000/M4000/M5000 servers:

For XSCF unit 0 :

`xscf#0-lan#0`	XSCF-LAN#0
`xscf#0-lan#1`	XSCF-LAN#1

For abbreviation:

`lan#0`	an abbreviation of XSCF-LAN#0
`lan#1`	an abbreviation of XSCF-LAN#1

- In the M8000/M9000 servers:

For XSCF unit 0 :

`xscf#0-lan#0`	XSCF-LAN#0
`xscf#0-lan#1`	XSCF-LAN#1
`xscf#0-if`	Interface between XSCF units (Inter SCF Network; ISN)

For XSCF unit 1:

`xscf#1-lan#0`	XSCF-LAN#0
`xscf#1-lan#1`	XSCF-LAN#1
`xscf#1-if`	ISN

For takeover IP address:

`lan#0`	takeover IP address for XSCF-LAN#0
`lan#1`	takeover IP address for XSCF-LAN#1

EXTENDED DESCRIPTION

- In the M8000/M9000 servers, a takeover IP address can be used without a need to determine whether XSCF has been switched. By setting the LAN ports of the active XSCF unit as `lan#0` and `lan#1`, they can be accessed with the names `lan#0` and `lan#1`.

- In the M3000/M4000/M5000 servers, the value of the `lan#0` is fixed with `xscf#0-lan#0`, and the `lan#1` is fixed with `xscf#0-lan#1`.
- In the M8000/M9000 servers and when the takeover IP address has been disabled by `setnetwork`(8) command, nothing will be displayed even though the takeover IP address is specified by the `shownetwork`(8) command.
- The `setnetwork`(8) command configures a network interface used by the XSCF.

EXAMPLES

EXAMPLE 1 Displays the information for XSCF-LAN#0 on XSCF unit 0.

```
XSCF> shownetwork xscf#0-lan#1
xscf#0-lan#1
 Link encap:Ethernet  HWaddr 00:00:00:12:34:56
 inet addr:192.168.10.11  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
```

EXAMPLE 2 Displays the information for XSCF-LAN#1 on XSCF unit 0 in the M3000/M4000/M5000 server.

```
XSCF> shownetwork lan#1
xscf#0-lan#1
 Link encap:Ethernet  HWaddr 00:00:00:12:34:56
 inet addr:192.168.10.11  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
```

EXAMPLE 3 Displays the information for ISN on the XSCF unit 0.

```
XSCF> shownetwork xscf#0-if
xscf#0-if
 Link encap:Ethernet  HWaddr 00:00:00:12:34:56
 inet addr:192.168.10.128 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:(0.0 B)  TX bytes:17010 (16.6 KiB)
 Base address:0x1000
```

EXAMPLE 4 Displays the information for XSCF-LAN#0 on XSCF Unit 0.

```
XSCF> shownetwork xscf#0-lan#0
xscf#0-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:14541827 (13.8 MiB)  TX bytes:1459769 (1.3 MiB)
 Base address:0x1000
```

EXAMPLE 5 Displays the information for the takeover IP address for XSCF-LAN#0.

```
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
```

EXAMPLE 6 Displays the current settings of XSCF network.

```
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
```

EXAMPLE 7 Displays the information for XSCF unit 0 and XSCF unit 1 in the M8000/M9000 servers.

```
XSCF> shownetwork -a
xscf#0-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

xscf#0-lan#1
 Link encap:Ethernet  HWaddr 00:00:00:12:34:57
 inet addr:192.168.10.11  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

xscf#0-if  Link encap:Ethernet  HWaddr 00:00:00:00:00:00
 inet addr:192.168.10.128  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:0 (0.0 B)  TX bytes:17010 (16.6 KiB)
 Base address:0x1000

xscf#1-lan#0
 HWaddr 00:00:00:12:34:59
 inet addr:192.168.10.12  Mask:255.255.255.0

xscf#1-lan#1
 HWaddr 00:00:00:12:34:60

xscf#1-if
 HWaddr 00:00:00:12:34:61
XSCF>
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

setnetwork (8)

NAME

shownotice - display copyright and license information for the XSCF Control Package (XCP)

SYNOPSIS

shownotice [-c {copyright | license}]

shownotice -h

DESCRIPTION

The shownotice(8) command displays by page the copyright and, if available, license files for the XCP. When used without an option, shownotice displays copyright information and any available license information. You can display only the copyright or the license file by specifying the -c option.

Privileges

No privileges are required to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-c {copyright|license}

Specifies for display by page either the copyright file or the license file for the XCP.

copyright Specifies for display only the copyright file.

license Specifies for display only the license file, if a license file is available for your platform. If the license file for your platform is not available for the shownotice command, the license argument is not supported.

-h

Displays usage statement. When used with other options or operands, an error occurs.

EXAMPLES

EXAMPLE 1 Display Only Copyright Information

```
XSCF> shownotice -c copyright
[Copyright text displays.]
```

EXAMPLE 2 Display Copyright and License Information

```
XSCF> shownotice
[Copyright text displays.]
[License text displays (if available).]
```

NAME

showntp - display the NTP information which currently set for XSCF

SYNOPSIS

showntp {-l | -a | *address* | -s | -m}

showntp -h

DESCRIPTION

The showntp(8) command displays the NTP information currently set for XSCF.

The showntp(8) command can display the following information:

- NTP servers which have been registered to the XSCF network
- Status of synchronization with the NTP servers
- Stratum value which has been set to XSCF
- Designation of preferred server
- Clock address of the local clock which is set in XSCF

Privileges

You must have one of the following privileges to run this command:

useradm, platadm, platop, auditadm, auditop, domainadm, domainmgr, domainop, fieldeng

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-a — Displays all the NTP servers currently set for the XSCF network.

-h — Displays usage statement. When used with other options or operands, an error occurs.

-l — Displays whether synchronization with an NTP server is being maintained.

-m — Displays whether a preferred server has been designated (prefer), and displays the clock address of the local clock (localaddr).

In prefer, either of the following is displayed:

on — Preferred server has been designated.

off — Preferred server not designated.

In localaddr, the least significant byte of the clock address of the local clock 127.127.0.*x* is displayed in a numeric from 0 to 3.

-s — Displays the stratum value which has been set to XSCF.

OPERANDS

The following operand is supported:

address

Specifies the IP address or the XSCF host name of an NTP server to be displayed. If the `-a` option is specified, the operand is ignored.

A specified IP address is a set of four integer values delimited by the "." (period). The following address form is accepted:

xxx.xxx.xxx.xxx

where:

xxx

An integer from 0–255. Zero suppression can be used to specify the integer.

The host name can be specified in the format that complies with RFC 1034.

EXTENDED DESCRIPTION

- When the preferred server not designated, the NTP server in the output of the `showntp`(8) command does not come with the prefer information.
- The `setntp`(8) command sets the NTP servers used in the XSCF network.
- When you use the `showntp`(8) command after the `setntp`(8) command, it will display the pending modifications performed by `setntp`(8), which might not yet be effective. If not yet effective, the setting will not match the actual NTP settings currently in operation. To view the NTP settings currently in operation, execute `showntp`(8) command with the `-l` option.

EXAMPLES

EXAMPLE 1 Displays all NTP servers currently being set (in a case that the preferred server designated).

```
XSCF> showntp -a
server ntp1.example.com prefer
server ntp2.example.com
```

EXAMPLE 2 Confirms synchronization with an NTP server and displays the results.

```
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
```

EXAMPLE 3 Displays the stratum value which has been set to XSCF.

```
XSCF> showntp -s
stratum : 5
```

EXAMPLE 4 Displays whether a preferred server has been designated, and displays the clock address of the local clock.

```
XSCF> showntp -m
prefer : on
localaddr : 0
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

setntp(8)

NAME

showpacketfilters - show the IP packet filtering rules that are set in the XSCF network

SYNOPSIS

showpacketfilters {-a | -l} [-M]

showpacketfilters -h

DESCRIPTION

showpacketfilters(8) command shows the IP packet filtering rules that are set in the XSCF network.

Privileges

No privileges are required to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-a	Shows the IP packet filtering rules that are set in XSCF.
-h	Displays usage statement. When used with other options or operands, an error occurs.
-l	Shows the operation status of the IP packet filtering rules that are set in XSCF.
-M	Displays text by page.

EXTENDED DESCRIPTION

The setpacketfilters(8) command can be used to set the IP filtering rules.

EXAMPLES

EXAMPLE 1 On M8000/M9000 servers, shows the IP packet filtering rules that are set in the XSCF network.

```
XSCF> showpacketfilters -a
-s 172.16.0.0/255.255.0.0 -i xscf#0-lan#0 -j DROP
-s 172.16.0.0/255.255.0.0 -i xscf#1-lan#0 -j DROP
-s 10.10.10.10/255.255.255.255 -j DROP
-s 192.168.100.0/255.255.255.0 -i xscf#0-lan#1 -j ACCEPT
-s 192.168.100.0/255.255.255.0 -i xscf#1-lan#1 -j ACCEPT
-i xscf#0-lan#1 -j DROP
-i xscf#1-lan#1 -j DROP
```

EXAMPLE 2 On M8000/M9000 servers, shows the operation status of the IP packet filtering rules in the XSCF network.

```
XSCF> showpacketfilters -l
 pkts bytes target     prot in            source
 0     0 DROP       all  xscf#0-lan#0  172.16.0.0/255.255.0.0
 0     0 DROP       all  *             10.10.10.10
 0     0 ACCEPT     all  xscf#0-lan#1  192.168.100.0/255.255.255.0
```

```
  0     0 DROP       all  xscf#0-lan#1  0.0.0.0/0.0.0.0

  pkts bytes target     prot in            source
  0     0 DROP       all  xscf#1-lan#0  172.16.0.0/255.255.0.0
  0     0 DROP       all  *             10.10.10.10
  0     0 ACCEPT     all  xscf#1-lan#1  192.168.100.0/255.255.255.0
  0     0 DROP       all  xscf#1-lan#1  0.0.0.0/0.0.0.0
 XSCF>
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

setpacketfilters (8)

NAME

showpasswordpolicy - display the current password settings

SYNOPSIS

showpasswordpolicy

showpasswordpolicy -h

DESCRIPTION

showpasswordpolicy(8) displays the password policy settings. These include default password expiration settings for new accounts, pam_cracklib parameters, and the number of passwords to keep in password history for each user.

Privileges

You must have useradm privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following option is supported:

-h Displays usage statement.

EXAMPLES

EXAMPLE 1 Displaying Password Policy Settings

```
XSCF> showpasswordpolicy
Mindays:  0
Maxdays:  99999
Warn:     7
Inactive: -1
Expiry:   0
Retry:    3
Difok:    10
Minlen:   9
Dcredit:  1
Ucredit:  1
Lcredit:  1
Ocredit:  1
Remember: 3
```

EXIT STATUS

The following exit values are returned:

0 Successful completion.

>0 An error occurred.

SEE ALSO

setpasswordpolicy(8)

NAME

showpowerupdelay - display the current settings for the warm-up time of the system and wait time before system startup

SYNOPSIS

showpowerupdelay

showpowerupdelay -h

DESCRIPTION

The showpowerupdelay(8) command displays the current settings for the warm-up time of the system and wait time before system startup.

The following settings are displayed:

warmup time	Warm-up time
wait time	Wait time before system startup

Privileges

You must have one of the following privileges to run this command:

platadm, platop, domainadm, domainmgr, domainop, fieldeng

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-h	Displays usage statement.

EXTENDED DESCRIPTION

The setpowerupdelay(8) command sets the warm-up time of the system and a wait time before system startup.

EXAMPLES

EXAMPLE 1 Displays the warm-up time of the system and wait time before system startup.

```
XSCF> showpowerupdelay
warmup time : 10 minute(s)
wait time    : 20 minute(s)
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

setpowerupdelay(8)

NAME

showresult - display the exit status of the most recently executed command

SYNOPSIS

showresult

showresult -h

DESCRIPTION

The showresult(8) command displays the exit status of the most recently executed command.

showresult(8) is convenient for a remote control program to confirm whether the most recently executed command is successfully completed.

Privileges

No privileges are required to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-h Displays usage statement.

EXTENDED DESCRIPTION

If you stop a running command by an operation such as Ctrl-C and then execute the showresult(8) command, the exit status that is displayed, zero or non-zero, depends on the cmmand that was stopped.

EXAMPLES

EXAMPLE 1 display the exit status of setupfru(8).

```
XSCF> setupfru -x 1 sb 0
XSCF> showresult
0
```

EXIT STATUS

The following exit values are returned:

0 Successful completion.

>0 An error occurred.

NAME

showroute - display routing information for an XSCF network interface

SYNOPSIS

showroute [-M] [-n] {-a | *interface*}

showroute -h

DESCRIPTION

showroute(8) command displays the current routing information for an XSCF network interface.

Routing information for the specified network interface or all the network interfaces can be displayed. The following information is displayed:

Destination	Destination IP address	
Gateway	Gateway address	
Netmask	Netmask address	
Flags	Flag which indicates the status of specified routing	
	U	route is up
	H	target is host
	G	use gateway
	R	reinstate route for dynamic routing
	C	cache entry
	!	reject route
Interface	XSCF network interface name	

Privileges

You must have one of the following privileges to run this command:

useradm, platadm, platop, auditadm, auditop, domainadm, domainmgr, domainop, fieldeng

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-a	Displays routing information that is set for all XSCF network interfaces.

`-h`	Displays usage statement. When used with other options or operands, an error occurs.
`-M`	Displays text by page. This option provides a function that is the same as that of the `more` command.
`-n`	Displays IP address without the name resolution of host name.

OPERANDS

The following operand is supported:

interface

Specifies the network interface whose information is to be displayed. One of the following values can be specified, depending on the system configuration. If this operand is specified with the `-a` option, the operand is ignored.

- In the M3000/M4000/M5000 servers:

For XSCF unit 0:

`xscf#0-lan#0`	XSCF-LAN#0
`xscf#0-lan#1`	XSCF-LAN#1

For abbreviation:

`lan#0`	XSCF-LAN#0
`lan#1`	XSCF-LAN#1

- In the M8000/M9000 servers:

For XSCF unit 0:

`xscf#0-lan#0`	XSCF-LAN#0
`xscf#0-lan#1`	XSCF-LAN#1

For XSCF unit 1 :

`xscf#1-lan#0`	XSCF-LAN#0
`xscf#1-lan#1`	XSCF-LAN#1

EXTENDED DESCRIPTION

The `setroute`(8) command sets routing information for the XSCF network.

EXAMPLES

EXAMPLE 1 Displays routing information for XSCF-LAN#0 on XSCF unit 0.

```
XSCF> showroute xscf#0-lan#0
Destination     Gateway         Netmask         Flags Interface
192.168.10.0    0.0.0.0         255.255.255.0   U     xscf#0-lan#0
default         192.168.10.1    0.0.0.0         UG    xscf#0-lan#0
```

EXAMPLE 2 Displays routing information for XSCF-LAN#0 on XSCF unit 0 without the name resolution of host name.

```
XSCF> showroute -n xscf#0-lan#0
Destination     Gateway         Netmask         Flags Interface
192.168.10.0    0.0.0.0         255.255.255.0   U     xscf#0-lan#0
0.0.0.0         192.168.10.1    0.0.0.0         UG    xscf#0-lan#0
```

EXAMPLE 3 Displays all routing information for XSCF unit 0 and XSCF unit 1 in the M8000/M9000 server.

```
XSCF> showroute -a
Destination     Gateway         Netmask         Flags Interface
192.168.10.0    *               255.255.255.0   U     xscf#0-lan#0
default         192.168.10.1    0.0.0.0         UG    xscf#0-lan#0

Destination     Gateway         Netmask         Interface
192.168.10.0    *               255.255.255.0   xscf#1-lan#0
default         192.168.10.1    0.0.0.0         xscf#1-lan#0
XSCF>
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

setroute(8)

NAME

showshutdowndelay - display the shutdown wait time at power interruption of the uninterruptible power supply (UPS)

SYNOPSIS

showshutdowndelay

showshutdowndelay -h

DESCRIPTION

The showshutdowndelay(8) command displays the wait time before the start of system shutdown for when power interruption occurs in a system connected to the UPS.

The time set by the setshutdowndelay(8) command is displayed. The default time set is 10 seconds.

Privileges

You must have one of the following privileges to run this command:

platadm, platop, domainadm, domainmgr, domainop, fieldeng

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-h	Displays usage statement.

EXAMPLES

EXAMPLE 1 Displays the wait time before the start of shutdown.

```
XSCF> showshutdowndelay
UPS shutdown wait time : 600 second(s)
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

setshutdowndelay(8)

NAME

showsmtp - display the Simple Mail Transfer Protocol (SMTP) configuration information

SYNOPSIS

showsmtp

showsmtp [-v]

showsmtp -h

DESCRIPTION

showsmtp(8) displays the SMTP configuration. When used without options, it displays current SMTP configuration data.

Privileges

You must have platadm or platop privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-h	Displays usage statement. When used with other options or operands, an error occurs.
-v	Specifies verbose output.

EXTENDED DESCRIPTION

SMTP information includes the Mail Server and Reply addresses.

EXAMPLES

EXAMPLE 1 Displaying SMTP configuration

```
XSCF>  showsmtp
Mail Server: 10.4.1.1
Port: 25
Authentication Mechanism: smtp-auth
 User Name: jsmith
 Password: ********
Reply Address: adm@customer.com
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

setsmtp(8)

NAME

showsnmp - display the configuration information and current status of the SNMP agent

SYNOPSIS

showsnmp

showsnmp -h

DESCRIPTION

showsnmp(8) displays the configuration and information and current status of the SNMP agent. This includes: agent status, port, system location, contact and description, traphosts, SNMP version, and any enabled MIB modules.

Privileges

You must have platadm or platop privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following option is supported:

-h Displays usage statement.

EXAMPLES

EXAMPLE 1 Displaying SNMP Information for a System That Has Not Been Set Up

```
XSCF>  showsnmp

Agent Status:       Disabled
Agent Port:         161
System Location:    Unknown
System Contact:     Unknown
System Description: Unknown

Trap Hosts: None
SNMP V1/V2c: None

Enabled MIB Modules: None
```

EXAMPLE 2 Displaying SNMP Information for a Disabled System Set Up With SNMPv3 Trap Host

```
XSCF>  showsnmp

Agent Status:       Disabled
Agent Port:         161
System Location:    SanDiego
System Contact:     bob@jupiter.west
System Description: FF1
```

```
Trap Hosts:
Hostname     Port      Type   Community String  Username  Auth Protocol
--------     ----      ----   ----------------  --------  --------------
host1         162       v3     n/a               jsmith   SHA

SNMP V1/V2c: None

Enabled MIB Modules: None
```

EXAMPLE 3 Displaying SNMP Information for a Enabled System Set Up With SNMPv1/v2c Trap Host

```
XSCF>  showsnmp

Agent Status:       Enabled
Agent Port:         161
System Location:    SanDiego
System Contact:     jsmith@jupiter.west
System Description: FF1

Trap Hosts:
Hostname     Port      Type   Community String  Username  Auth Protocol
--------     ----      ----   ----------------  --------  --------------
host1         162       v1     public            jsmith   SHA
host2         162       v2c    public            n/a      n/a
host3         162       v3     n/a               bob      SHA

SNMP V1/V2c:

Status:           Enabled
Community String: public

Enabled MIB Modules:
SP_MIB
FM_MIB
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

setsnmp(8)

NAME

showsnmpusm - display the current User-based Security Model (USM) information for the SNMP agent

SYNOPSIS

showsnmpusm

showsnmpusm -h

DESCRIPTION

showsnmpusm(8) displays the current USM information for the SNMP agent.

Privileges

You must have platadm or platop privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following option is supported:

-h Displays usage statement.

EXAMPLES

EXAMPLE 1 Displaying SNMP Information for a System

```
XSCF>  showsnmpusm
Username    Auth Protocol
--------    --------------
jsmith      SHA
sue         MD5
```

EXIT STATUS

The following exit values are returned:

0 Successful completion.

>0 An error occurred.

SEE ALSO

setsnmpusm(8)

NAME

showsnmpvacm - display the current View-based Access Control Access (VACM) information for the SNMP agent

SYNOPSIS

showsnmpvacm

showsnmpvacm -h

DESCRIPTION

showsnmpvacm(8) displays the current VACM information for the SNMP agent.

Privileges

You must have platadm or platop privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following option is supported:

-h Displays usage statement.

EXAMPLES

EXAMPLE 1 Displaying SNMP Information for a System

```
XSCF>  showsnmpvacm
Groups:
Groupname   Username
---------   --------
admin       jsmith, bob

Views:
View      Subtree   Mask    Type
----      -------   ----    ----
all_view  .1        ff      include

Access:
View      Group
----      -----
all_view  admin
```

EXIT STATUS

The following exit values are returned:

0 Successful completion.

>0 An error occurred.

SEE ALSO

setsnmpvacm(8)

NAME

showssh - display the settings of the Secure Shell (SSH) service that configured for the XSCF network

SYNOPSIS

showssh [-c hostkey] [-M]

showssh -c pubkey [-u *user_name*] [-M]

showssh -h

DESCRIPTION

showssh(8) command displays the current settings of the SSH service that configured for the XSCF network.

The following information is displayed:

SSH status	Validity of the SSH service
SSH DSCP	Whether the access from domain to the SSH service via the Domain - SP Communication Protocol (DSCP) is permitted
RSA key	Host public key in RSA format
DSA key	Host public key in DSA format
Fingerprint	Host public key in fingerprint format

When specified the display of user public key, the user public key number, which automatically numbered by system, and the user public key are displayed.

Only SSH2 is supported for XSCF.

Privileges

You must have one of the following privileges to run this command:

- To display the user public key of other user account:

  useradm

- To display the information other than above:

  useradm, platadm, platop, auditadm, auditop, domainadm, domainmgr, domainop, fieldeng

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-c hostkey	Displays a host public key. If the -c option is omitted, "-c hostkey" is assumed specified.
-c pubkey	Displays the user public key. If the -c option is omitted, "-c hostkey" is assumed specified

-h	Displays usage statement. When used with other options or operands, an error occurs.
-M	Displays text by page. This option provides a function that is the same as that of the `more` command.
-u *user_name*	Specify the user account name to display the user public key. Should be specified with "`-c pubkey`." When the `-u` option omitted, the user public key of the current login user account will be displayed.

EXTENDED DESCRIPTION

- You can specify the automatically-numbered user public key number to delete the user public key by `setssh`(8) command.
- The `setssh`(8) command makes settings for the SSH service in the XSCF network.

EXAMPLES

EXAMPLE 1 Displays the information of host public keys.

```
XSCF> showssh
SSH status: enabled
SSH DSCP: accept
RSA key:
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAt0IG3wfpQnGr51znS9XtzwHcBBb/
UU0LN08SilUXE6j+
avlxdY7AFqBf1wGxLF+Tx5pTa6HuZ8o8yUBbDZVJAAAAFQCfKPxarV+/5qzK4A43Qaigkqu/
6QAAAIBM
LQl22G8pwibESrh5JmOhSxpLzl3P26ksI8qPr+7BxmjLR0k=
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
AAAAB3NzaC1kc3MAAACBAJSy4GxD7Tk4fxFvyW1D0NUDqZQPY3PuY2IG7QC4BQ1kewDnblB8
/
JEqI+8pnfbWzmOWU37KHL19OEYNAv6v+WZT6RElU5Pyb8F16uq96L8QDMswFlICMZgrn+ilJ
NStr6r8
KDJfwOQMmK0eeDFj2mL40NOvaLQ83+rRwW6Ny/yF1Rgv6PUpUqRLw4VeRb+uOfmPRpe6/
kb4z++lOhtp
WI9bay6CK0nrFRok+z54ez7BrDFBQVuNZx9PyEFezJG9ziEYVUag/23LIAiLxxBmW9pqa/
WxC21Ja4RQ
VN3009kmVwAAAIAON1LR/
9Jdd7yyG18+Ue7eBBJHrCA0pkSzvfzzFFj5XUzQBdabh5p5Rwz+1vriawFI
ZI9j2uhM/3HQdrvYSVBEdMjaasF9hB6T/
uFwP8yqtJf6Y9GdjBAhWuH8F13pX4BtvK9IeldqCscnOuu0
e2rlUoI6GICMr64FL0YYBSwfbwLIz6PSA/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
```

EXAMPLE 2 Displays the user public key of the current login user account.

```
XSCF> showssh -c pubkey
Public key:
 1  ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAzFh95SohrDgpnN7zFCJCVNy+jaZPTjNDxcid
QGbihYDCBttI4151Y0Sv85FJwDpSNHNKoVLMYLjtBmUMPbGgGVB61qskSv/
FeV44hefNCZMiXGItIIpK
P0nBK4XJpCFoFbPXNUHDw1rTD9icD5U/wRFGSRRxFI+Ub5oLRxN8+A8=abcd@example.com
 2  ssh-rsa
CSqGSIb3DQEJARYHZWUubWFpbDCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
nkPntf+TjYtyKlNYFbO/YavFpUzkYTLHdt0Fbz/
tZmGd3e6Jn34A2W9EC7D9hjLsj+kAP41Al6wFwGO7
KP3H4iImX0Uysjl9Hyk4jLBU51sw8JqvT2utTjltV5mFPKL6bDcAgY9=efgh@example.com
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

setssh(8)

NAME

showstatus - display the degraded Field Replaceable Units (FRUs)

SYNOPSIS

showstatus [-M]

showstatus -h

DESCRIPTION

showstatus(8) command displays information about degraded units that are among the FRUs composing the system.

Privileges

You must have one of the following privileges to run this command:

useradm, platadm, platop, domainadm, domainmgr, domainop, fieldeng

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:.

-h	Displays usage statement. When used with other options or operands, an error occurs.
-M	Displays text by page. This option provides a function that is the same as that of the more command.

EXTENDED DESCRIPTION

The showstatus(8) shows the information concerning a unit failed or degraded and the unit on the upper hierarchy, among the FRUs composing the system. "Status:" will be followed by any of the status described below. Beside a unit failed or degraded, placed an "*" indicating the locating fault.

Status	Description
Normal	The component is normally operating.
Faulted	The component is faulty and is not operating.
Degraded	The component is operating. However, either an error has been detected or the component is faulty. As a result, the component might be operating with reduced functionality or performance.
Deconfigured	As a result of another component's faulted or degraded status, the component is not operating. (The component itself is not faulted or degraded.)
Maintenance	The component is under maintenance. A deletefru(8), replacefru(8), or addfru(8) operation is currently underway.

EXAMPLES

EXAMPLE 1 Displays the degraded units. In this example, a CPU module and memory module in a CPU memory unit are degraded because of an error.

```
XSCF> showstatus
  CMU#0;
*       CPUM#0-CHIP#0 Status:Faulted;
*       MEM#00A Status:Faulted;
```

EXAMPLE 2 Displays the degraded units. In this example, a memory module on a memory board is degraded because of an error.

```
XSCF> showstatus
  MBU_B;
   MEMB#0;
*           MEM#0A Status:Faulted;
```

EXAMPLE 3 Displays the degraded units. In this example, a CPU/memory board unit and memory module on a motherboard unit are degraded because of an error.

```
XSCF> showstatus
 MBU_B Status:Normal;
*       MEMB#1 Status:Deconfigured;
*           MEM#3B Status:Deconfigured;
```

EXAMPLE 4 Displays the degraded units. In this example, a CPU/memory board unit is degraded because a crossbar unit is degraded.

```
XSCF> showstatus
 MBU_B Status:Normal;
*       CPUM#1-CHIP#1 Status:Deconfigured;
*   XBU_B#0 Status:Degraded;
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

NAME

showsunmc - show setup information and status of Sun Management Center agent

SYNOPSIS

showsunmc [isenabled]

showsunmc [-h]

DESCRIPTION

This command is used to show the setup information and current status of the Sun Management Center agent. When used with the `isenabled` option, the `showsunmc` command output displays on the agent status: `1` if the agent is enabled, `0` if the agent is disabled.

OPTIONS

The following options are supported.

`isenabled` Displays only the agent status. The value `1` indicates the agent is enabled, `0` indicates the agent is disabled.

`-h` Displays usage statement.

When used with other options or operands, an error occurs.

Privileges

You must have `platadm`, `platop`, or `fieldeng` privileges to run this command.

Refer to `setprivileges`(8) for more information.

OPERANDS

There are no operands for this command.

EXAMPLES

EXAMPLE 1 Show the Status of the Agent: Not Set Up or Enabled

```
XSCF> showsunmc
Agent Status:                    Disabled
Setup Status:                    Not set up
SunMC Server:                    unknown
Security Seed:                   maplesyr
SNMPv1 Community String:         public
Agent Port:                      1161
Host Trap Port:                  162
Host Event Port:                 163
SNMP Agent Port:                 161
Domain Agent Ports:              1161
```

EXAMPLE 2 Show the Status of the Agent: Set Up, But Not Enabled

```
XSCF> showsunmc
Agent Status:                    Disabled
Setup Status:                    Set up
SunMC Server:                    balon
Security Seed:                   maplesyr
SNMPv1 Community String:         double_secret
```

```
Agent Port:                     1161
Host Trap Port:                 162
Host Event Port:                163
SNMP Agent Port:                161
Domain Agent Ports:             1161
```

EXAMPLE 3 Show the Agent Status of an Enabled Agent

```
XSCF> showsunmc isenabled
1
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

setsunmc(8)

NAME

showtelnet - display the current status of the Telnet service for the XSCF network

SYNOPSIS

showtelnet

showtelnet -h

DESCRIPTION

showtelnet(8) command displays the current status of the Telnet service for the XSCF network.

One of the following states is displayed:

enable	The Telnet service is enabled.
disable	The Telnet service is disabled.

Privileges

You must have one of the following privileges to run this command:

useradm, platadm, platop, auditadm, auditop, domainadm, domainmgr, domainop, fieldeng

Refer to setprivileges(8) for more information.

OPTIONS

The following option is supported:

-h	Displays usage statement.

EXTENDED DESCRIPTION

The settelnet(8) command makes settings for the Telnet service in the XSCF network.

EXAMPLES

EXAMPLE 1 Displays the status of the Telnet service for the XSCF network.

```
XSCF> showtelnet
Telnet status:enabled
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

settelnet(8)

NAME

showtimezone - display the XSCF time zone and Daylight Saving Time information of current settings

SYNOPSIS

showtimezone -c tz

showtimezone -c dst [-m {standard |custom}]

showtimezone -h

DESCRIPTION

The showtimezone(8) command displays the XSCF time zone and Daylight Saving Time information of current settings.

Privileges

You must have one of the following privileges to run this command:

useradm, platadm, platop, auditadm, auditop, domainadm, domainmgr, domainop, fieldeng

Refer to setprivileges(8) for more information.

OPTIONS

The following option is supported:

-c tz — Displays the time zone.

-c dst — Displays the Daylight Saving Time information.

-h — Displays usage statement. When used with other options or operands, an error occurs.

-m {standard | custom} — Specifies the Daylight Saving Time information to be displayed. Either of the following can be specified. If the -m option omitted, it is regarded as "-m custom" specified.

standard

Displays the Daylight Saving Time information that has been set in the current time zone by default.

custom

Displays the Daylight Saving Time information that you set by using the settimezone(8) command. If the Daylight Saving Time is not set, nothing displayed.

EXTENDED DESCRIPTION

- The Daylight Saving Time information is displayed in the following format.
  - When specified custom:

std offset dst[*offset2*] [*from-date*[/*time*] *to-date*[/*time*]]

std	Abbreviations of time zone.
offset	Offset time of time zone and Greenwich mean time (GMT).
	Displayed in minus "–" in case the offset is plus, and displayed in plus "+" in case the offset is minus.
dst	Name of Daylight Saving Time.

offset2

Offset time of Daylight Saving Time and Greenwich mean time (GMT).

Displayed in minus "−" in case the offset is plus, and displayed in plus "+" in case the offset is minus.

from-date[/*time*]

The starting time of Daylight Saving Time.

Any of the following formats displays *from-date*.

`M`*m.w.d*

`M`*m*: Shows the month when Daylight Saving Time starts. Any numeric from `1` to `12` comes in *m*.

w: Shows the week when Daylight Saving Time starts. Any numeric from `1` to `5` comes in, "`1`" for the first week and "`5`" for the last week in the month.

d: Shows the day of the week when Daylight Saving Time starts. Any numeric from `0` to `6` comes in, "`0`" for Sunday and "`6`" for Saturday.

`J`*n*

`J`*n*: The date when Daylight Saving Time starts. Any numeric from `1` to `365` comes in, "`1`" for January 1st. The leap-year day is not counted.

n

n: The date when Daylight Saving Time starts. Any numeric from `1` to `365` comes in, "`1`" for January 2nd. The leap-year day is counted.

In *time*, the time to switch to Daylight Saving Time is shown in the pre-switched time.

hh:mm:ss

Shows the time in "hh:mm:ss" format. The default value is "`02:00:00`."

to-date[/*time*] The termination time of Daylight Saving Time.

Any of the following formats displays *to-date*.

`M`*m.w.d*

`M`*m*: Shows the month when Daylight Saving Time terminates. Any numeric from `1` to `12` comes in *m*.

w: Shows the week when Daylight Saving Time terminates. Any numeric from `1` to `5` comes in, "`1`" for the first week and "`5`" for the last week in the month.

d: Shows the day of the week when start Daylight Saving Time terminates. Any numeric from `0` to `6` comes in, "`0`" for Sunday and "`6`" for Saturday.

`J`*n*

`J`*n*: The date when Daylight Saving Time terminates. Any numeric from `1` to `365` comes in, "`1`" for January 1st. The leap-year day is not counted.

n

n: The date when Daylight Saving Time terminates. Any numeric from `1` to `365` comes in, "`1`" for January 2nd. The leap-year day is counted.

In *time*, the time to switch from Daylight Saving Time is shown in the pre-switched time.

hh:mm:ss Shows the time in "hh:mm:ss" format. The default value is "`02:00:00`."

- When specified `standard`:

  `From:` *ddd MM dd hh:mm:ss yyyy dst*

  `To:` *ddd MM dd hh:mm:ss yyyy dst*

ddd	a day of the week
MM	month
dd	day
hh	hour
mm	minutes
ss	second
yyyy	year
dst	dst name

- The `settimezone`(8) command sets the time zone of the XSCF.

EXAMPLES

EXAMPLE 1 Displays the time zone.

```
XSCF> showtimezone -c tz
Asia/Tokyo
```

EXAMPLE 2 Displays the Daylight Saving Time information as follows: the abbreviation of time zone is JST, the offset from GMT is +9, the name of Daylight Saving Time is JDT, Daylight Saving Time is 1 hour ahead, and the time period is from the last Sunday of March 2:00 to the last Sunday of October 2:00.

```
XSCF> showtimezone -c dst -m custom
JST-9JDT,M3.5.0,M10.5.0
```

EXAMPLE 3 Displays the Daylight Saving Time information as follows: the abbreviation of time zone is JST, the offset from GMT is +9, the name of Daylight Saving Time is JDT, Daylight Saving Time is 1 hour ahead, and the time period is from the first Sunday of April 0:00 to the first Sunday of September 0:00.

```
XSCF> showtimezone -c dst
JST-9JDT-10,M4.1.0/00:00:00,M9.1.0/00:00:00
```

EXAMPLE 4 Displays the Daylight Saving Time information that has been set in the current time zone by default.

```
XSCF> showtimezone -c dst -m standard
From: Sun Mar  9 03:00:00 2008 PDT
To:   Sun Nov  2 01:59:59 2008 PDT
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

setdate(8), **settimezone**(8), **showdate**(8)

NAME

showuser - display user account information

SYNOPSIS

showuser

showuser [[-a] [-M] [-p] [-u] [*user*]]

showuser [[-a] [-l] [-M] [-p] [-u]]

showuser -h

DESCRIPTION

showuser (8) displays XSCF user account information. If the user argument is specified, showuser displays account information for the specified user. If the user argument is not specified, then showuser displays account information for the current user. If the -l option is specified, showuser displays account information for all local users.

When invoked with one or more of the options -a, -p, or-u, showuser displays information as described in the OPTIONS section below. When invoked without any of these options, showuser displays all account information.

Privileges

No privileges are needed for you to view your own account. You must have useradm privileges to run this command for any other user.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-a	Displays password validity and account state information. This is only valid for XSCF user accounts.
-h	Displays usage statement. When used with other options or operands, an error occurs.
-l	Displays information on all local XSCF user accounts sorted by user login name. Cannot be used with the *user* operand.
-M	Displays text by page. This option provides a function that is the same as that of the more command.
-p	Displays all privileges assigned to the user. This is valid for local and remote users.
-u	Displays user ID (UID). This is valid for local and remote users.

OPERANDS

The following operands are supported:

user	Name of an existing user account. Cannot be used with the -l option.

EXAMPLES

EXAMPLE 1 Displays Password and Account Validity Information

```
XSCF>  showuser -a
User Name:          jsmith
Status:             Enabled
Minimum:            0
Maximum:            99999
Warning:            7
Inactive:           -1
Last Change:        Aug 22, 2005
Password Expires:   Never
Password Inactive:  Never
Account Expires:    Never
```

EXAMPLE 2 Displays Privileges Information

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

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

adduser(8), **deleteuser**(8), **disableuser**(8), **enableuser**(8), **password**(8), **setprivileges**(8)

NAME

snapshot - collect and transfer environment, log, error, and FRUID data

SYNOPSIS

snapshot -d *device* [-r] [-e [-P *password*]] [-L {F|I|R}] [-l] [-v] [[-q] -{y|n}] [-S *time* [-E *time*]]

snapshot -t *user@host: directory* [-e [-P *password*]] [-k *host-key*] [-l] [-L {F|I|R}] [-p *password*] [-v] [[-q] -{y|n}] [-S *time* [-E *time*]]

snapshot -T [-D *directory*] [-e [-P *password*]] [-k *host-key*] [-l] [-L {F|I|R}] [-v] [[-q] -{y|n}] [-S *time* [-E *time*]]

snapshot -h

DESCRIPTION

The snapshot(8) command provides a data-collection mechanism that enables rapid, reliable, and flexible retrieval of diagnostic information on the Service Processor. snapshot(8) collects the following data: Configuration, Environmentals, Logs, Errors, and FRUID information. It transfers data to the specified destination.

snapshot opens an output file, the name of which is automatically generated based on the host name and IP address assigned to the Service Processor and the UTC time (in hours, minutes, and seconds) and date on the Service Processor at the time snapshot is invoked. For example: jupiter_10.1.1.1_2006-07-08T22-33-44. snapshot does not support user-specified file names for the output file. As files and command output are collected from the Service Processor, snapshot compresses the output data and writes it in the format of a .zip archive.

snapshot stores the collected data on a remote network host or on an external media device, based upon the use of the -t, -T or -d option. To store the collected data on a remote network host using the -t option, you must specify a host name (or IP address), a target directory on the remote network host, and the user name of a user on the remote host. If you have already set an archive target using setarchiving(8), you can use the -T option to store the data on a remote network host using that same information, or use -T in conjunction with the -D option to change only the target directory. When storing data on a remote network host, snapshot opens a network connection using SSH to act as a data pipe to the remote file.

It is possible to restrict data collection on some larger log files to a specific date range using the options -S and, optionally, -E.

Encrypted network protocols, such as SSH and SSL, are used for transmission of the data across a network connection. The entire .zip archive itself can be encrypted using the -e flag. To decrypt a .zip archive that has been encrypted with this process, use the encryption password given to snapshot with the openssl

command. The following example decrypts the file `jupiter_10.1.1.1_2006-07-08T22-33-44.zip.e`:

```
% openssl aes-128-cbc -d -in jupiter_10.1.1.1_2006-07-08T22-33-
44.zip.e -out jupiter_10.1.1.1_2006-07-08T22-33-44.zip
```

Every `.zip` archive generated by `snapshot` includes two files generated by `snapshot` itself. The first file, called `README`, contains the original name of the `.zip` archive, the name of the configuration file on the Service Processor used to create the `.zip` archive, the version of `snapshot` and whether log-only mode (the `-l` flag) was used to generate the archive. The second file, called `CONFIG`, is a copy of the actual configuration file used by `snapshot` to generate the archive.

The data collected by `snapshot` may potentially be used by Service personnel to diagnose problems with the system. `snapshot` can collect different sets of data for different diagnostic purposes. The three different sets are named `Initial`, `Root Cause`, and `Full`, and are specified through the use of the `-L` option.

Privileges

You must have `platadm` or `fieldeng` privileges to run this command.

Refer to `setprivileges`(8) for more information.

OPTIONS

The following options are supported.

`-D` *directory*

Used with the `-T` option, specifies a value for *directory* instead of the value set using `setarchiving`(8). The directory field must not begin with a "-" or a "~". Refer to the description of the `-T` option for more detailed information.

`-d` *device*

Specifies the external media device to use. The following option is available to `-d`:

`-r`

Removes all files from the external media device prior to data collection. This option is not valid with the `-t` or `-T` options.

`-E` *time*

Specifies the end time for the time period for which data is collected. Used with the `-S` *time* option for the start time, defines the period of time for which log messages are collected by `snapshot`. Only those log entries created before the time specified by `-E` *time* are collected by `snapshot`. Refer also to the description of the `-S` option.

time

Interpreted using `strptime`(3), using one of the following two formats:

```
%Y-%m-%d,%H:%M:%S
%Y-%m-%d_%H-%M-%S
```

`-e` Encrypts the zip archive. Required when using `-P` *password*.

`-h` Displays usage statement.

When used with other options or operands, an error occurs.

`-k` *host-key* Used with the `-t` or `-T` option, sets the public key that the Service Processor uses to log in to the network host. This option is not valid with the `-d` option.

Possible values for *host-key* are as follows:

`none`

This literal value specifies that a public key should not be used to authenticate the network host.

`download`

This literal value specifies that `snapshot` will use `ssh` to download a public host key for the network host and download the key from the host specified in the `-t` argument. `snapshot` displays the key's `md5` fingerprint and prompts for confirmation. If you accept the key, it is used for server authentication. If you reject the key, `snapshot` exits without doing anything. This is the default behavior in SSH Target Mode if `-k` is not specified.

public

The specified public key is used for server authentication. The *host-key* argument should be the complete public key of the network host, beginning with key type (the complete contents of `/etc/ssh/ssh_host_rsa_key.pub` on the network host).

Note – The public key should be enclosed in quotes to ensure that the shell treats it as a single word.

`-L {F|I|R}` Specifies which set of logs will be collected.

`F`	Full log set.
`I`	Initial log set.
`R`	Root Cause log set.

If no log set is specified, the Initial log set is collected by default.

`-l` Specifies collecting only log files. Does not collect command output.

`-n`	Automatically answers "`n`" (no) to all prompts.
`-P` *password*	Used with the `-e` option, sets the encryption password used for encrypting the output file.
`-p` *password*	Specifies the user password used to log in to the host using SSH. This option is valid with the `-t` option, not with the `-d` or `-T` options.
`-q`	Suppresses all messages to stdout, including prompts.

`-S` *time*	Specifies the start time for the time period for which data is collected. Used with the `-E` *time* option for the end time, defines the period of time for which log messages are collected by `snapshot`. If no end time is specified, the target time period ends at the time the snapshot command is launched. Refer also to the description of the `-E` option.
	time — Interpreted using `strptime`(3), using one of the following two formats:
	`%Y-%m-%d,%H:%M:%S`
	`%Y-%m-%d_%H-%M-%S`

`-T`	Specifies executing `snapshot` in SSH target mode using the value for *user@host:directory* previously set using `setarchiving`(8). Can be used with the `-D` option to substitute an alternative value for *directory*. **Note -** The user must create the target directory on the remote host, `snapshot` does not create the target directory.
`-t` *user@host:directory*	Sets the network host and remote directory for data destination. The *host* field specifies the host name or IP address of the network host. The *user* field specifies the user name for the `ssh` login to the archive host. The *directory* field specifies the archive directory on the archive host where the output file should be stored. The directory field must not begin with a "-" or a "~". **Note -** The user must create the target directory on the remote host, `snapshot` does not create the target directory.
`-v`	Specifies verbose output. Displays all actions and commands as they are executed. If this option is specified with the `-q` option, the `-v` option is ignored. **Note -** You may not have the required privileges to run all the commands that are executed by the `snapshot` configuration file. If this occurs, you will see error messages indicating these operations are not permitted.
`-y`	Automatically answers "`y`" (yes) to all prompts.

EXTENDED DESCRIPTION

Modes of Operation

The following is a brief overview of the modes of operation for the `snapshot` command.

The first mode is *SSH Target Mode*. The data collector is run in this mode when it is invoked with the `-t` or `-T` option. In this mode, the data collector opens an `SSH` connection from the Service Processor to the specified target (after appropriate authentication) and sends the zip data archive through the `SSH` connection to the target host. The user must create the target directory on the remote host, snapshot does not create the target directory. The transmission encryption in this mode is provided by `SSH`.

The second mode is *USB Device Mode*. The data collector is run in this mode when it is invoked with the `-d` flag. In this mode, the data collector's output (which is the zip archive) is saved in a file on the USB device. The USB device should be formatted using the FAT32 file system. As in SSH Target mode, you can use the `-e` option to encrypt the zip file in this mode. However, no transmission encryption (such as SSH) occurs in this mode, since the data stays local to the Service Processor.

EXAMPLES

EXAMPLE 1 Downloading a Public Key Using SSH

```
XSCF> snapshot -t joe@jupiter.west:/home/joe/logs/x -k download
Downloading Public Key from 'jupiter.west'...
Key fingerprint in md5: c9:e0:bc+b2:1a:80:29:24:13:d9:f1:13:f5:5c:2c:0f
Accept this public key (yes/no)? y
Enter ssh password for user 'joe' on host 'jupiter.west'
Setting up ssh connection to remote host...
Collecting data into joe@jupiter.west:/home/joe/logs/x/archive.zip
Data collection complete.
```

EXAMPLE 2 Downloading a Host Key

```
XSCF> snapshot -t joe@jupiter.west:/home/joe/logs/x
Downloading Public Key from 'jupiter.west'...
Public Key Fingerprint: c9:e0:bc+b2:1a:80:29:24:13:d9:f1:13:f5:5c:2c:0f
Accept this public key (yes/no)? y
Enter ssh password for user 'joe' on host 'jupiter.west'
Setting up ssh connection to remote host...
Collecting data into joe@jupiter.west:/home/joe/logs/x/archive.zip
Data collection complete.
```

EXAMPLE 3 Downloading With a User-Provided Public Key

```
XSCF> snapshot -t joe@jupiter.west:/home/joe/logs/x -k "ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAwVFiSQNVBFhTTzq0AX5iQqCkkJjd6ezWkVGtmMkJJzzM
jYK0sBlhn6dGEIiHdBSzO8QLAXb8N4Kq8JDOBpLSN4yokUPTcZQNxJaYA0W058Qgxbn"
Enter ssh password for user 'joe' on host 'jupiter.west'
Setting up ssh connection to remote host...
Collecting data into joe@jupiter.west:/home/joe/logs/x/archive.zip
Data collection complete.
```

EXAMPLE 4 Log Files Only Using No Public Key

```
XSCF> snapshot -t bob@mars.east:/home/bob/logs/x -k none -l
Enter ssh password for user 'bob' on host 'mars.east'
Log only mode. No commands will be collected.
Setting up ssh connection to remote host...
Collecting data into joe@jupiter.west:/home/joe/logs/x/archive.zip
Data collection complete.
```

EXAMPLE 5 Downloading Using Encryption With Provided Password and No Public Key

```
XSCF> snapshot -t bob@mars.east:/home/bob/logs/x -k none -e -P password
Output data will be encrypted.
Enter ssh password for user 'bob' on host 'mars.east'
Setting up ssh connection to remote host...
Collecting data into joe@jupiter.west:/home/joe/logs/x/archive.zip
Data collection complete.
```

EXAMPLE 6 Downloading Using No Key to Invalid Directory

```
XSCF> snapshot -t sue@saturn.north:/home/sue/logs/bad_dir -k none
Enter ssh password for user 'sue' on host 'saturn.north'
Setting up ssh connection to remote host...
Failed to create remote file:
/home/sue/logs/bad_dir/archive.zip
Verify adequate disk permissions and disk space on target host
Error opening SSH target
Exiting with error 1
```

EXAMPLE 7 Downloading Public Key With Connectivity Failure

```
XSCF> snapshot -t sue@saturne.west:/home/sue/logs/x -k download
Downloading Public Key from 'saturne.west'...
Error downloading key for host 'saturne.west'
Error opening SSH target
Exiting with error 1
```

EXAMPLE 8 Downloading Public Key and Answering No to All Prompts

```
XSCF> snapshot -v -t jill@earth.east:/home/jill/logs/x -k download -n
Downloading Public Key from 'earth.east'...
Public Key: ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAwVFiSQNVBFhTTzq0AX5iQqCkkJjd6ezWkVGtmMkJJzzM
jYK0sBlhn6dGEIiHdBSzO8QLAXb8N4Kq8JDOBpLSN4yokUPTcZQNxJaYA0W058Qgxbn
Key fingerprint in md5: c9:e0:bc+b2:1a:80:29:24:13:d9:f1:13:f5:5c:2c:0f
Accept this public key (yes/no)? no
Public Key declined
Error opening SSH target
Exiting with error 1
```

EXAMPLE 9 Downloading Public Key Attempted by Unauthorized User

```
XSCF> snapshot -t fakeuser@fakehost.com:/fakedir -p fake-password
Downloading Public Key from 'fakehost.com'...
Error downoading key for host 'fakehost.com'
Error opening SSH target
Exiting with error 1
```

EXAMPLE 10 Downloading to External Media Device

```
XSCF> snapshot -d usb0 -r
Testing writability of USB device....SUCCESS
About to remove all files from device 'usb0'. Continue? [y|n] : y
Collecting data into /media/usb_msd/jupiter_10.1.1.1_2006-04-17T22-41-
51.zip
Data collection complete.
```

EXAMPLE 11 Limiting Data Collection for Certain Logs to a Date Range

```
XSCF> snapshot -d usb0 -S 2007-01-01,01:00:00  -E 2007-01-31_14-00-00
Testing writability of USB device....SUCCESS
Collecting data into /media/usb_msd/jupiter_10.1.1.1_2006-04-17T22-41-
51.zip
Data collection complete.
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

setarchiving(8), **showarchiving**(8), **showlogs**(8)

NAME

switchscf - switch the XSCF unit between the active and standby states

SYNOPSIS

switchscf [[-q] -{y|n}] -t {Active | Standby} [-f]

switchscf -h

DESCRIPTION

The switchscf(8) command switches the XSCF unit that the user is currently logged in to, between the active and standby states.

The switchscf(8) command is available on the M8000/M9000 servers only.

When the active XSCF unit currently logged in to is switched from active to standby or vice versa, the state of the standby XSCF unit is also switched.

Note – When switched, the session of the network which has been connected to the active XSCF is terminated.

Caution – Usually, XSCFs cannot be switched while maintenance work is in progress. If "Switching of XSCF state is disabled due to a maintenance operation. Try again later." is displayed as a result from the switchscf(8) command and XSCFs cannot be switched, check whether the addfru(8), deletefru(8), replacefru(8), or flashupdate(8) maintenance command is being executed. If the command is being executed, wait until the command ends. If XSCFs cannot be switched though none of those maintenance commands is being executed, use the -f option to switch them.

Privileges

You must have platadm or fieldeng privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-f	Switches the state in a case XSCF state can't be changed due to a maintenance operation. **Caution -** Since the -f option forcibly switches XSCF, limit the use of this option to such cases as when switching does not work in normal operations.
-h	Displays usage statement. When used with other options or operands, an error occurs.
-n	Automatically answers "n" (no) to all prompts.
-q	Suppresses all messages to stdout, including prompts.

`-t Active`	Switches the state of the XSCF unit to active.
`-t Standby`	Switches the state of the XSCF unit to standby.
`-y`	Automatically answers "y" (yes) to all prompts.

EXTENDED DESCRIPTION

When the command is executed, a prompt to confirm execution of the command with the specified options is displayed. Enter "**y**" to execute the command or "**n**" to cancel the command.

EXAMPLES

EXAMPLE 1 Switches the state of the XSCF unit that the user is currently logged in to, to standby.

```
XSCF> switchscf -t Standby
The XSCF unit switch between the Active and Standby states. Continue?
[y|n]:y
```

EXAMPLE 2 Switches the state of the XSCF unit that the user is currently logged in to, to standby. Automatically answers "y" to all prompts.

```
XSCF> switchscf -t Standby -y
The XSCF unit switch between the Active and Standby states. Continue?
[y|n]:y
```

EXIT STATUS

The following exit values are returned:

`0`	Successful completion.
`>0`	An error occurred.

NAME

testsb - perform an initial diagnosis of the specified physical system board (PSB)

SYNOPSIS

testsb [[-q] -{y|n}] [-m *diag=mode*] *location*

testsb [[-q] -{y|n}] [-m *diag=mode*] -c {all|expansion}

testsb -v [-y|-n] [-m *diag=mode*] *location*

testsb -v [-y|-n] [-m *diag=mode*] -c {all|expansion}

testsb -h

DESCRIPTION

testsb(8) command performs an initial diagnosis of the specified PSB.

The testsb(8) command is not available on the M3000 server.

The configuration of the PSB and operation of each device mounted on the PSB are checked. After the diagnostics, the result is displayed.

The result also can be seen in "Test" and "Fault" displayed by showboards(8) command.

Privileges

You must have platadm or fieldeng privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:.

`-c {all|expansion}` Specifies the target PSB to be diagnosed. One of the values shown below can be specified:

`all` Diagnoses all the PSB that are mounted.

If the following conditions not satisfied, it leads to an error.

- The system has been powered off.
- All of the target PSB are Uni-XSB.

`expansion` Diagnoses all the PSB that are mounted on the expansion cabinet.

If the following conditions not satisfied, it leads to an error.

- All of the target PSB are not operating on the domain.
- All of the target PSB are Uni-XSB.

`-h` Displays usage statement. When used with other options or operands, an error occurs.

`-m diag=`*mode* Specifies the diagnostic level of initial diagnosis. One of the values shown below can be specified:

`min` Normal (default)

`max` Maximum

`-n` Automatically answers "`n`" (no) to all prompts.

`-q` Suppresses all messages to stdout, including prompts.

`-v` Displays a detailed message of initial diagnosis.

`-y` Automatically answers "`y`" (yes) to all prompts.

OPERANDS

The following operand is supported:

location Specifies only one PSB number. An integer from `00–15` can be specified.

EXTENDED DESCRIPTION

- When the command is executed, a prompt to confirm execution of the command with the specified options is displayed. Enter "`y`" to execute the command or "`n`" to cancel the command.
- The PSB must not be configured in the domain, or the domain in which the PSB is configured must be powered off. To verify that all domains are powered off, execute the `showlogs power` command and look for the value `System Power Off`.

- When the system board (XSB) belonging to the specified PSB is in any status below, the testsb(8) command results in an error.
  - XSB is installed in the domain and this domain is in operation.
  - XSB is installed in the domain and this domain is in OpenBoot PROM (`ok>` prompt) status.
  - XSB is installed in the domain and this domain is power ON status, power OFF status, or reboot status.
  - The `addboard`(8), `deleteboard`(8), or `moveboard`(8) command is executed for XSB.
- In case an XSB which belongs to the specified PSB is in `Unmount` or `Faulted` status, it may be excluded from the target of diagnosis and may not be shown in the diagnosis result. In a case like this, use the `showboards`(8) command to check the diagnosis result.
- In case there are the settings for the warm-up time of the system and the wait time before system startup, a prompt appears to confirm whether or not it can ignore these settings to execute the `testsb`(8) command. Enter "**y**" to execute the command or "**n**" to cancel the command.

- The displayed diagnostic results of the `testsb`(8) command are as follows:

`XSB` XSB numbers belonging to the specified PSBs. One XSB number is displayed for the Uni-XSB type, and four XSB numbers are displayed for the Quad-XSB type.

`Test` Status of the initial diagnosis of XSBs. One of the following status values is displayed:

- `Unmount` No XSB could be recognized because no XSB is mounted or because an error occurred.
- `Unknown` Not tested.
- `Testing` Initial diagnosis is in progress.
- `Passed` Initial diagnosis ended normally.
- `Failed` An error was detected during the initial diagnosis. An XSB cannot be used or is in a degraded state.

`Fault` XSB error. One or more states are displayed:

- `Normal` Normal state.
- `Degraded` One or more components are degraded. Each XSB can operate.
- `Faulted` An XSB cannot operate because an error occurred.

EXAMPLES

EXAMPLE 1 Performs the initial diagnosis on PSB#00.

```
XSCF> testsb 0
Initial diagnosis is about to start, Continue?[y|n] :y
SB#00 power on sequence started.
 0end
Initial diagnosis started. [1800sec]
 0..... 30..... 60..... 90.....120end
Initial diagnosis has completed.
SB power off sequence started. [1200sec]
 0.end
SB powered off.
XSB  Test    Fault
---- ------- --------
00-0 Passed  Normal
00-1 Passed  Normal
00-2 Passed  Normal
00-3 Passed  Normal
```

EXAMPLE 2 Performs an initial diagnosis of PSB#01 with detailed messages displayed.

```
XSCF> testsb -v 1
Initial diagnosis is about to start. Continue? [y|n] :y
SB#01 powered on sequence started.
     :
     :
     :
Initial diagnosis has completed.
{0} ok SB power off sequence started. [1200sec]
 0.end
SB powered off.
XSB  Test    Fault
---- ------- --------
01-0 Passed  Normal
```

EXAMPLE 3 Performs the initial diagnosis on all the PSB that are mounted.

```
XSCF> testsb -c all
Initial diagnosis is about to start. Continue? [y|n] :y
SB power on sequence started.
 0end
Initial diagnosis started. [1800sec]
 0..... 30..... 60..... 90.....120end
Initial diagnosis has completed.
SB power off sequence started. [1200sec]
 0.end
SB powered off.
XSB  Test    Fault
---- ------- --------
00-0 Passed  Normal
01-0 Passed  Normal
02-0 Passed  Normal
03-0 Passed  Normal
```

EXAMPLE 4 Ignores the settings for the warm-up time of the system and the wait time before system startup to perform the initial diagnosis on the PSB that are mounted.

```
XSCF> testsb -c all
Initial diagnosis is about to start. Continue? [y|n] :y
Ignore warmup-time and air-conditioner-wait-time, Continue?[y|n] :y
SB power on sequence started.
 0end
Initial diagnosis started. [1800sec]
 0..... 30..... 60..... 90.....120end
Initial diagnosis has completed.
```

```
SB power off sequence started. [1200sec]
 0.end
SB powered off.
XSB  Test    Fault
---- ------- --------
00-0 Passed  Normal
01-0 Passed  Normal
02-0 Passed  Normal
03-0 Passed  Normal
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

addfru(8), **deletefru**(8), **replacefru**(8), **setupfru**(8), **showboards**(8), **showfru**(8)

NAME

traceroute - display the route packets take to the specified network host or the network device

SYNOPSIS

traceroute [-n] [-r] [-v] [-m *maxttl*] [-p *port*] [-q *nqueries*] [-s *src_addr*] [-w *wait*] *host*

traceroute -h

DESCRIPTION

The traceroute(8) command displays the route packets take to the specified network host or the network device.

The route packets take indicates the router (gateway) which interconnects the specified host or the network device, and indicates what kind of the routers located on the route.

The traceroute(8) command uses the TTL field of IP protocol and tries to elicit the ICMP TIME_EXCEEDED responses from every gateway on the route packets take to the specified network host or the network device.

Privileges

You must have one of the following privileges to run this command:

- To execute the command to "localhost" or to the loopback address (127.0.0.0/8):

  fieldeng

- To execute the command to Inter SCF Network (ISN):

  fieldeng

- The case other than those above:

  No privileges are required.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-h	Displays usage statement. When used with other options or operands, an error occurs.
-m *maxttl*	Specifies the maximum number of hops. It displays the gateways for the number of hops specified. If omitted, it is set to 30.
-n	With no reverse DNS lookup, outputs the IP address.
-p *port*	Specifies the port number of the UDP packet to be used. Valid only in case using the UDP packet. If omitted, it is set to 33434.
-q *nqueries*	Specifies the number of retries to a single gateway. If omitted, it is set to three times.

`-r`	Bypasses the routing table and directly sends the packet to the specified network host or the network device. If the desired host or the network device is not on the same physical network, it results in errors.
`-s` *src_addr*	Specifies the source address to start tracking the route.
`-v`	Displays verbose output. The size of the sending packet will be displayed.
`-w` *wait*	Specifies the timeout period in units of seconds. If omitted, it is set to 3 seconds.

OPERANDS

The following operand is supported:

host	Specifies the network host or the network device to send the packet. Can be specified with host name or IP address. If a DSCP address is specified, an error results.

EXAMPLES

EXAMPLE 1 Displays the route packets take to the host named server.example.com.

```
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
```

EXAMPLE 2 Displays the detailed route packets take to the host named server.example.com. (XSCF-LAN=192.168.100.10)

```
XSCF> traceroute -v server.example.com
traceroute to server.example.com (XX.XX.XX.XX), 30 hops max, 40 byte
packets
 1  XX.XX.XX.1 36 bytes to 192.168.100.10  1.792 ms  1.673 ms  1.549 ms
 2  XX.XX.XX.2 36 bytes to 192.168.100.10  2.235 ms  2.249 ms  2.367 ms
 3  XX.XX.XX.3 36 bytes to 192.168.100.10  2.199 ms  2.228 ms  2.361 ms
 4  XX.XX.XX.4 36 bytes to 192.168.100.10  2.516 ms  2.229 ms  2.357 ms
 5  XX.XX.XX.5 36 bytes to 192.168.100.10  2.546 ms  2.347 ms  2.272 ms
 6  server.example.com 48 bytes to 192.168.100.10  2.172 ms  2.313 ms  2.36
ms
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

NAME

unlockmaintenance - forcibly release the locked status of XSCF

SYNOPSIS

unlockmaintenance [[-q] - {y|n}]

unlockmaintenance -h

DESCRIPTION

unlockmaintenance(8) command releases the locked status of XSCF forcibly.

Normally, while the maintenance command addfru(8), deletefru(8), or replacefru(8) is in execution, XSCF is in the locked status. After the command complete, the lock is released. However, in case an error such as LAN disconnection occurred while executing any of the maintenance command, the XSCF lock may become unable to release. In such a case, you can execute the unlockmaintenance(8) command to forcibly release the locked status of XSCF.

Privileges

You must have fieldeng privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-h	Displays usage statement. When used with other options or operands, an error occurs.
-n	Automatically answers "n" (no) to all prompts.
-q	Suppresses all messages to stdout, including prompts.
-y	Automatically answers "y" (yes) to all prompts.

EXTENDED DESCRIPTION

When the command is executed, a prompt to confirm execution of the command with the specified options is displayed. Enter "y" to execute the command or "n" to cancel the command.

EXAMPLES

EXAMPLE 1 Unlocks the maintenance lock status.

```
XSCF> unlockmaintenance
This command unlocks the maintenance lock which prevents the multiple
execution of maintenance commands.
*Never* use this command, except when the lock state remains by some
reason.
Careless execution of this command causes serious situation because it
interrupts the running command and XSCF might not be able to recognize the
parts.
Continue? [y|n] :y
```

EXAMPLE 2 Unlocks the maintenance lock status. Automatically answers "y" to all prompts.

```
XSCF> unlockmaintenance -y
This command unlocks the maintenance lock which prevents the multiple
execution of maintenance commands.
*Never* use this command, except when the lock state remains by some
reason.
Careless execution of this command causes serious situation because it
interrupts the running command and XSCF might not be able to recognize the
parts.
Continue? [y|n] :y
```

EXAMPLE 3 Unlocks the maintenance lock status. Suppresses prompts, and automatically answers "y" to all prompts.

```
XSCF> unlockmaintenance -q -y
XSCF>
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

addfru(8), **deletefru**(8), **replacefru**(8)

NAME

version - display firmware version

SYNOPSIS

version -c xcp [-v] [-t]

version -c {cmu | xscf} [-v]

version -h

DESCRIPTION

The version(8) command displays firmware version.

The following versions can be displayed:

xcp	The comprehensive version of the XSCF control package (XCP) firmware currently applied to the system.
cmu	The version of OpenBoot PROM firmware.
xscf	The version of XSCF firmware.

Privileges

You must have platadm or fieldeng privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

-c xcp	Displays the XCP version.
-c cmu	Displays the version of OpenBoot PROM firmware.
-c xscf	Displays the version of XSCF firmware.
-h	Displays usage statement. When used with other options or operands, an error occurs.
-t	Displays information of the XCP version that is registered in the XSCF. This option is used together with "-c xcp".
-v	Displays detailed information. Specifying this option with "-c xscf" displays the same information as the usual information.

EXAMPLES

EXAMPLE 1 Displays the XCP version.

```
XSCF> version -c xcp
XSCF#0 (Active)
XCP0 (Current): 1090
XCP1 (Reserve): 1090
XSCF#1 (Standby)
XCP0 (Current): 1090
XCP1 (Reserve): 1090
```

EXAMPLE 2 Displays the details of the XCP version.

```
XSCF> version -c xcp -v
XSCF#0 (Active)
XCP0 (Current): 1082
OpenBoot PROM : 02.09.0000
XSCF          : 01.08.0005
XCP1 (Reserve): 1082
OpenBoot PROM : 02.09.0000
XSCF          : 01.08.0005
XSCF#1 (Standby)
XCP0 (Current): 1082
OpenBoot PROM : 02.09.000
XSCF          : 01.08.0005
XCP1 (Reserve): 1082
OpenBoot PROM : 02.09.0000
XSCF          : 01.08.0005
OpenBoot PROM BACKUP
#0: 02.08.0000
#1: 02.09.0000
```

EXAMPLE 3 Displays the XCP version that is registered in the XSCF.

```
XSCF> version -c xcp -t
XCP: 1090
```

EXAMPLE 4 Displays the details of the XCP version that is registered in the XSCF.

```
XSCF> version -c xcp -v -t
XCP: 1082
OpenBoot PROM : 02.09.0000
XSCF          : 01.08.0005
```

EXAMPLE 5 Displays the version of OpenBoot PROM firmware.

```
XSCF> version -c cmu
DomainID  0: 02.09.0000
DomainID  1: 02.09.0000
DomainID  2: 02.09.0000
DomainID  3: 02.09.0000
   :
DomainID 23: 02.09.0000
```

EXAMPLE 6 Displays the detailed version of OpenBoot PROM firmware.

```
XSCF> version -c cmu -v
DomainID  0: 02.09.0000
DomainID  1: 02.09.0000
```

```
DomainID  2: 02.09.0000
DomainID  3: 02.09.0000
  :
DomainID 23: 02.09.0000
XSB#00-0:  02.09.0000(Current)     02.07.0000(Reserve)
XSB#00-1:  02.09.0000(Current)     02.07.0000(Reserve)
XSB#00-2:  02.09.0000(Current)     02.07.0000(Reserve)
XSB#00-3:  02.09.0000(Current)     02.07.0000(Reserve)
  :
XSB#15-3:  02.09.0000(Current)     02.07.0000(Reserve)
```

EXAMPLE 7 Displays the detailed version of XSCF firmware.

```
XSCF> version -c xscf -v
XSCF#0 (Active )
01.08.0005(Reserve) 01.08.0005(Current)
XSCF#1 (Standby)
01.08.0005(Current) 01.08.0005(Reserve)
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

NAME

viewaudit - display audit records

SYNOPSIS

viewaudit

viewaudit [-A *date-time*] [-B *date-time*] [-C] [-c *classes*] [-D *date-time*] [-E *end-record*] [-e *events*] [-i *audit-ids*] [-l] [-m *del*] [-n] [-p *privilege-results*] [-r *return-values*] [-s *start-record*] [-u *users*] [-x]

viewaudit -h

DESCRIPTION

viewaudit(8) displays audit records. When invoked without options, viewaudit displays all current local audit records. When invoked with options, viewaudit displays only the selected records. By default, records are displayed in text format, one token per line, with a comma as the field separator. The output can be modified using the -C, -E, -l,-m *del*, -n, -S, or -x option.

Privileges

You must have auditadm or auditop privileges to run this command.

Refer to setprivileges(8) for more information.

OPTIONS

The following options are supported:

`-A` *date-time*

Selects records that occurred at or after *date-time*. The *date-time* argument is in local time. the `-A` and `-B` options can be used together to form a range. Valid values for *date-time* are:

Absolute *date-time* : *yyyymmdd*[*hh*[*mm*[*ss*]]]

where:

yyyy = year (`1970` is the earliest valid value)

mm = month (`01–12`)

dd = day (`01–31`)

hh = hour (`00–23`)

mm = minutes (`00–59`)

ss = seconds (`00–59`)

The default value is `00` for *hh*, *mm*, and *ss*.

`-B` *date-time*

Selects records that occurred before *date-time*. The *date-time* argument is in local time. the `-A` and `-B` options can be used together to form a range. Valid values for *date-time* are either absolute or offset:

Absolute *date-time* : *yyyymmdd*[*hh*[*mm*[*ss*]]]

where:

yyyy = year (`1970` is the earliest valid value)

mm = month (`01–12`)

dd = day (`01–31`)

hh = hour (`00–23`)

mm = minutes (`00–59`)

ss = seconds (`00–59`)

Offset *date-time*: +*n d* | *h* | *m* | *s*

where:

n = number of units

d = days

h = hours

m = minutes

s = seconds

Offset is only available with the `-B` option and must be used with `-A`.

(The default value is `00` for *hh*, *mm* and *ss*.)

`-C`

Appends the number of records that matched the selection criteria to the end of the output.

-c *classes*

Selects records in indicated classes. *classes* is a comma-separated list of audit classes. A class may be specified by its numeric value or its name. The ACS_ prefix may be omitted. For example, the class of audit related events can be expressed as ACS_AUDIT, AUDIT or 16.

The following are valid classes:

all	Denotes all classes.
ACS_SYSTEM(1)	System-related events
ACS_WRITE(2)	Commands that can modify a state
ACS_READ(4)	Commands that read a current state
ACS_LOGIN(8)	Login-related events
ACS_AUDIT(16)	Audit-related events
ACS_DOMAIN(32)	Domain management–related events
ACS_USER(64)	User management–related events
ACS_PLATFORM(128)	Platform management–related events
ACS_MODES(256)	Mode-related events

-D *date-time*

Selects records that occurred on a specific day (a 24-hour period beginning at 00:00:00 of the day specified and ending at 23:59:59). The day specified is in local time in the following format: *yyyymmddhhmmss* (year,month,day, hour,minute,second). The time portion of the argument, if supplied, is ignored. Any records with timestamps during that day are selected. If any hours, minutes, or seconds are given, they are ignored. -D cannot be used with -A or -B.

-E *end-record*

Selects the last record matching the selection criteria to display.

`-e` *events*	Selects records of the indicated events. *events* is a comma-separated list of audit events. An event may be specified by its numeric value or its name. The `AEV_` prefix may be omitted. For example, the event for SSH login can be expressed as `AEV_LOGIN_SSH`, `LOGIN_SSH` or `4`. See `showaudit -e all` for a list of valid events.
`-h`	Displays usage statement. When used with other options or operands, an error occurs.
`-i` *audit-ids*	Selects records of the indicated audit session identifier. If you become interested in activity reflected in a particular audit record, you might wish to view all the audit records for that session. An *audit-id* is not persistent and can be reassigned across resets of the Service Processor. *audit-ids* is a comma-separated list of audit session identifiers. The *audit-id* is the number following the label `subject` in an audit file. For example, in the following listing, the *audit-id* is `1` (shown in boldface for emphasis). **`subject,1,bob,normal,telnet 45880 jupiter`**
`-l`	Prints one line per record.
`-m` *del*	Uses *del* as the field delimiter instead of the default delimiter, which is the comma. If *del* has special meaning for the shell, it must be quoted. The maximum size of a delimiter is three characters. The delimiter is not meaningful and is not used with the `-x` option.
`-n`	Specifies that UIDs and IP addresses should not be converted to user names or host names.
`-p` *privilege-results*	Select records according to the indicated *privilege-results*. *privilege-results* is a comma-separated list. *privilege-results* are: `granted`, `denied`, or `error`.
`-r` *return-values*	Selects records according to the indicated return values. *returnvals* is a comma-separated list of the values: `success`, or `failure`. `success` corresponds to a return value of 0. `failure` corresponds to a nonzero return value.

-S *start-record*	Selects the first record matching the selection criteria to display.
-u *users*	Selects records attributed to indicated users. *users* is a comma-separated list of users. A user can be specified by user name or numeric UID.
-x	Prints in XML format.

EXAMPLES

EXAMPLE 1 Displaying Audit Records for December 12, 2005

```
XSCF> viewaudit -D 20051212

file,1,2006-01-11 10:52:30.391 -05:00,20060111155230.0000000000.jupiter
```

EXAMPLE 2 Displaying User Audit Records

```
XSCF> viewaudit -u jsmith

file,1,2006-01-11 10:52:30.391 -05:00,20060111155230.0000000000.jupiter
header,37,1,login - telnet,jupiter,2006-01-11 11:31:09.659 -05:00
subject,1,jsmith,normal,ssh 45880 jupiter
command,showuser
platform access,granted
return,0
```

EXAMPLE 3 Displaying Audit Records for Privileges

```
XSCF> viewaudit -p granted

file,1,2006-01-11 10:52:30.391 -05:00,20060111155230.0000000000.jupiter
header,37,1,login - telnet,jupiter,2006-01-11 11:31:09.659 -05:00
subject,1,jsmith,normal,ssh 45880 jupiter
command,showuser
platform access,granted
return,0
```

EXAMPLE 4 Displaying Audit Records for Successful Access

```
XSCF> viewaudit -r success

file,1,2006-01-11 10:52:30.391 -05:00,20060111155230.0000000000.jupiter
header,37,1,login - telnet,jupiter,2006-01-11 11:31:09.659 -05:00
subject,1,jsmith,normal,ssh 45880 jupiter
command,showuser
platform access,granted
return,0
```

```
header,57,1,command - viewaudit,jupiter.company.com,2006-01-26
16:13:09.128 -05:00
subject,5,sue,normal,ssh 1282 saturn
command,viewaudit
platform access,granted
return,0
...
```

EXAMPLE 5 Displaying Audit Records Within a Range of Two Days

```
XSCF> viewaudit -A 20080108 -B +2d

file,1,2008-01-09 20:12:12.968 -08:00,20080110041212.0000000004.sca-m5k-
0-0
file,1,2008-01-10 21:14:49.481 -08:00,terminated
file,1,2008-01-10 21:14:49.485 -08:00,20080111051449.0000000005.sca-m5k-
0-0
```

EXAMPLE 6 Displaying First 5 Records (of 4238) that Match a Date Range

```
XSCF> viewaudit -l -A 20070515 -B 20080110 -C -S 1 -E 5

file,1,2008-01-09 20:12:12.968 -08:00,20080110041212.0000000004.sca-m5k-
0-0
header,63,1,command - setaudit,sca-m5k-0-0.sfbay.sun.com,2008-01-09
20:12:12.974 -08:00,s ubject,250,opl,normal,ssh 42759 san-e4900-
0.West.Sun.COM,command,setaudit,delete,platform access,granted,return,0
header,37,1,login - ssh,sca-m5k-0-0.sfbay.sun.com,2008-01-09
20:12:14.455 -
08:00,subject, 252,scfroot,normal,ssh 42761 san-e4900-0.West.Sun.COM
header,37,1,logout,sca-m5k-0-0.sfbay.sun.com,2008-01-09 20:12:14.800 -
08:00,subject,250,o pl,normal,ssh 42759 san-e4900-0.West.Sun.COM
header,37,1,login - ssh,sca-m5k-0-0.sfbay.sun.com,2008-01-09
20:12:15.595 -
08:00,subject, 253,scfroot,normal,ssh 42762 san-e4900-0.West.Sun.COM
4238
```

EXIT STATUS

The following exit values are returned:

0	Successful completion.
>0	An error occurred.

SEE ALSO

setaudit(8), **showaudit**(8)