PRIMEQUEST1000 シリーズ
ServerView Mission Critical Option

Version 2.4

ユーザマニュアル

2017 年 1 月版

© Copyright Fujitsu Limited 2011-2017

All hardware and software names used are trademarks of their respective manufacturers.

All rights, including rights of translation, reproduction by printing, copying or similar methods, in part or in whole, are reserved.

Offenders will be liable for damages.

All rights, including rights created by patent grant or registration of a utility model or design, are reserved.

Delivery subject to availability. Right of technical modification reserved.

目　次

1　製品概要 1
1.1　PRIMEQUEST における監視の仕組み 1
1.1.1　システム全体 1
1.1.2　ServerView Suite 4
1.1.3　VMware vSphere 5/6 におけるサーバ監視 5
1.2　ServerView Mission Critical Option (SVmco) 7
1.2.1　SVmco/SVmcovm の機能 7
1.2.2　ハード異常監視の仕組み 8

2　導入手順 9
2.1　SVmco の設定（Linux：Red Hat Enterprise Linux） 9
2.1.1　PSA-MMB 間通信 LAN の設定 13
2.1.2　管理 LAN の設定確認 19
2.1.3　SELinux 機能の設定確認 19
2.1.4　ファイアーウォール機能の確認 (ポートの開放) 20
2.1.5　管理 LAN IP アドレスの設定 29
2.1.6　パーティションからのトラップ送信先の設定 31
2.1.7　複製ディスク使用時の SNMP 設定 35
2.1.8　SVmco のアップデートインストール 39
2.1.9　SIRMS のアップデートインストール 43
2.1.10　SVmco のアンインストール 44
2.1.11　SIRMS のアンインストール 44
2.1.12　SVmco のバックアップ 45
2.1.13　SVmco のリストア 46
2.2　SVmco の設定 (Windows Server 2008/2012) 48
2.2.1　PSA-MMB 間通信 LAN の設定 53
2.2.2　管理 LAN の設定確認 58
2.2.3　PSHED Plugin ドライバのインストール 59
2.2.4　Windows ファイアーウォールの設定 61
2.2.5　管理 LAN IP アドレスの設定 71
2.2.6　パーティションからのトラップ送信先の設定 73
2.2.7　STOP エラー (致命的なシステムエラー) 発生後の Watchdog Timer 監視設定 75
2.2.8　SVmco のアップデートインストール 76
2.2.8.1　SVmco のアップデートインストール 77
2.2.8.2　PSHED Plugin ドライバのアップデートインストール 78

2.2.9 SIRMS のアップデートインストール 82
2.2.10 SVmco のアンインストール 83
2.2.11 SIRMS のアンインストール 84
2.3 SVmco の設定 (VMware 4) 86
2.3.1 SVmco のインストール 86
2.3.2 SIRMS のインストール 87
2.3.3 SVmco インストール後の設定 88
2.3.4 ネットワークの設定 89
2.3.5 ファイアーウォールの設定 98
2.3.6 デフォルトゲートウェイの設定 99
2.3.7 パーティションの再起動 102
2.3.8 VMware SVmco 保守情報取得 102
2.3.9 VMware SVmco 留意事項 103
2.4 SVmcovm のインストール/アンインストール 103
2.4.1 インストール手順 103
2.4.2 SVmcovm のインストール前の確認/設定 104
2.4.2.1 ネットワーク構成例 1 105
2.4.2.2 ネットワーク構成例 2 105
2.4.2.3 PSA-MMB 間通信 LAN が割り当たっている物理アダプタ(vmnic)の確認 106
2.4.2.3.1. VMware vSphere Client の場合 106
2.4.2.3.2. VMware vSphere Web Client の場合 114
2.4.2.4 仮想マシンへの PSA-MMB 間通信 LAN の割り当て 115
2.4.2.4.1. VMware vSphere Client の場合 115
2.4.2.4.2. VMware vSphere Web Client の場合 132
2.4.2.5 ESXi からの情報取得用ネットワークの設定 142
2.4.2.5.1. VMware vSphere Client の場合 142
2.4.2.5.2. VMware vSphere Web Client の場合 160
2.4.2.5.3. Linux(Red hat Enterprise Linux)の場合 175
2.4.2.5.4. Windows(Windows Server 2008/2012)の場合 178
2.4.2.6 仮想マシンの自動起動設定 183
2.4.2.6.1. VMware vSphere Client の場合 184
2.4.2.6.2. VMware vSphere Web Client の場合 187
2.4.3 インストール（Linux：Red Hat Enterprise Linux） 189
2.4.3.1 SVmcovm 動作に必要なパッケージ 189
2.4.3.1.1 パッケージ(RHEL5) 189
2.4.3.1.2 パッケージ(RHEL6) 190
2.4.3.2 SVmcovm のインストール 190
2.4.4 インストール後の設定（Linux：Red Hat Enterprise Linux） 191
2.4.4.1 SElinux 機能の設定確認 191
2.4.4.2 PSA-MMB 間通信 LAN の設定 192
2.4.4.2.1. VMware vSphere Client の場合 193

2.4.4.2.2. VMware vSphere Web Client の場合 ... 202
2.4.4.3 ファイアーウォールの機能の確認 ... 210
2.4.4.4 ESXi へのアクセス情報の設定 ... 216
2.4.4.4.1. VMware vSphere Client の場合 ... 217
2.4.4.4.2. VMware vSphere Web Client の場合 ... 229
2.4.4.5 仮想 OS へのログ転送の設定(ログ受信側) ... 239
2.4.4.5.1. ログデーモンの設定 ... 239
2.4.4.5.2. ログ転送用のファイアウォールの設定 ... 241
2.4.4.5.2.1. VMware vSphere Client の場合 ... 241
2.4.4.5.2.2. VMware vSphere Web Client の場合 ... 244
2.4.4.6 仮想 OS へのログ転送の設定(ログ送信側) ... 247
2.4.4.6.1. VMware vSphere Client の場合 ... 247
2.4.4.6.2. VMware vSphere Web Client の場合 ... 250
2.4.4.7 MMB 経由の Trap 送信の設定 ... 253
2.4.5 仮想マシンの再起動 ... 256
2.4.6 SVmcovm のアップデートインストール ... 257
2.4.7 SVmcovm のアンインストール ... 258
2.4.8 VMware SVmcovm 保守情報取得 ... 259
2.4.9 インストール(Windows Server 2008/2012) ... 260
2.4.10 インストール後の設定(Windows Server 2008/2012) ... 262
2.4.10.1 PSA-MMB 間通信 LAN の設定 ... 263
2.4.10.1.1. VMware vSphere Client の場合 ... 264
2.4.10.1.2. VMware vSphere Web Client の場合 ... 272
2.4.10.2 ファイアーウォールの機能の確認 ... 281
2.4.10.3 ESXi へのアクセス情報の設定 ... 287
2.4.10.3.1. VMware vSphere Client の場合 ... 287
2.4.10.3.2. VMware vSphere Web Client の場合 ... 300
2.4.10.4 仮想マシンへのログ転送の設定(ログ受信側) ... 309
2.4.10.4.1 ログ転送設定 1(Syslog Collector が使用出来る場合) ... 310
2.4.10.4.1.1. Syslog Collector のインストール ... 310
2.4.10.4.1.1.1. VMware vCenter Server 5.x の場合 ... 311
2.4.10.4.1.1.2. VMware vCenter Server 6.x の場合 ... 320
2.4.10.4.1.2. ログ転送のためのファイアウォールの設定 ... 325
2.4.10.4.1.2.1. VMware vSphere Client の場合 ... 325
2.4.10.4.1.2.2. VMware vSphere Web Client の場合 ... 328
2.4.10.4.2 ログ転送設定 2(Syslog Collector を使わない場合) ... 331
2.4.10.5 仮想マシンへのログ転送の設定(ログ送信側) ... 332
2.4.10.5.1 Syslog Collector を使用している場合 ... 332
2.4.10.5.1.1. VMware vSphere Client の場合 ... 332
2.4.10.5.1.2. VMware vSphere Web Client の場合 ... 335
2.4.10.5.2 Syslog Collector を使用しない場合 ... 338

2.4.10.6 MMB 経由の Trap 送信の設定 339
2.4.11 仮想マシンの再起動 342
2.4.12 SVmcovm のアップデートインストール 344
2.4.13 SVmcovm のアンインストール 347
2.4.14 VMware SVmcovm 保守情報取得 348

3 SVmco/SVmcovm の CLI 349
3.1 SVmco/SVmcovm の CLI 349
3.1.1 CLI コマンド一覧 349
3.1.2 ディスク操作コマンド (diskctrl) 351
3.1.3 SVmco 起動／停止コマンド (y30SVmco) 363
3.1.4 SVmco 調査資料収集コマンド (getosvmco) 366
3.1.5 SNMP セキュリティ設定コマンド (setsnmpsec) 367
3.1.6 PCI カード操作コマンド(fjpciswap) 368
3.1.7 管理 LAN 用インターフェース向けファイアーウォール設定コマンド (setmlanfw.sh) 382
3.1.8 PSA-MMB 通信 LAN 設定コマンド(setpsalan) 390
3.1.9 iptables **設定ツール** 392
3.2 SVMcovm の CLI 394
3.2.1 CLI コマンド一覧 394
3.2.2 SVmcovm 起動／停止コマンド (y30SVmco) 396
3.2.3 SVmcovm 調査資料収集コマンド (getosvmco) 397
3.2.4 SVmcovm 用 iptables 設定ツール 399
3.2.5 ESXi へのアクセス情報設定コマンド(setuserinfo) 400

4 ハードディスクの活性交換 402
4.1 ハードディスクの活性交換の概要 402
4.2 ディスクの追加・削除・交換 405
4.2.1 追加の手順 405
4.2.2 削除の手順 407
4.2.3 交換の手順 (ハードディスクが無応答となる故障以外の場合) 409
4.2.4 交換の手順 (ハードディスクが無応答となる故障の場合) 412

5 Windows における PCI カードの活性保守 416
5.1 活性保守の概要 416
5.1.1 全体の流れ 417
5.2 PCI カードのホットプラグの共通手順 418
5.2.1 交換の手順 418
5.2.2 追加の手順 420
5.2.3 削除について 421
5.3 NIC のホットプラグ 422

5.3.1 チーミングに組み込まれている **NIC** のホットプラグ 422
5.3.2 冗長化されていない **NIC** のホットプラグ 429
5.3.3 **NIC** の追加手順 431
5.4 **FC** カードのホットプラグ 432
5.4.1 **ETERNUS** マルチパスドライバに組み込まれている **FC** カードのホットプラグ 432
5.4.2 **FC** カードの追加手順 437
5.5 **Windows** の **iSCSI (NIC)** の活性交換 437
5.5.1 **MPD** の組込み確認 438
5.5.2 **MPD** の切離し作業 446
5.5.3 **MPD** 組込み作業 450

6 **SVmco** の手動インストール・アンインストール **..... 451**
6.1 **SVmco** の手動インストール **(Linux: Red Hat Enterprise Linux)** 451
6.1.1 インストールの流れ 451
6.1.2 **SVmco** インストール前の確認 452
6.1.2.1 **PSA-MMB** 間通信 **LAN** の設定確認 452
6.1.2.2 **iptables** の状態確認 452
6.1.3 **SVmco** のインストール 453
6.1.3.1 **SVmco** 動作に必要なパッケージ 453
6.1.3.2 **SVmco** のインストール 454
6.1.4 **SVmco** インストール時の自動設定 454
6.1.5 **SIRMS** のインストール 456
6.1.6 パーティション再起動 456
6.1.7 **SVmco** インストール後の設定 457
6.1.7.1 **SELinux** 機能の設定確認 457
6.1.7.2 ファイアーウォール機能の確認 **(**ポートの開放**)** 457
6.1.7.3 **PSA-MMB** 間通信 **LAN** 用インターフェース 458
6.1.7.4 パーティションからのトラップ送信先の設定 464
6.1.7.5 複製ディスク使用時の **SNMP** 設定 464
6.1.7.6 管理 **LAN** の設定確認 464
6.1.8 **SVmco** のアップデートインストール 465
6.1.9 **SIRMS** のアップデートインストール 465
6.1.10 **SVmco** のアンインストール 465
6.1.11 **SIRMS** のアンインストール 465
6.2 **SVmco** の手動インストール **(Windows Server 2008/2012)** 465
6.2.1 インストールの流れ 466
6.2.2 インストール前の確認 467
6.2.2.1 **PSA-MMB** 間通信 **LAN** の設定確認 468
6.2.2.2 **SVmco** 動作のための必須サービスの確認 468
6.2.3 **SVmco** のインストール 470

6.2.4 SVmco インストール時の自動設定 471
6.2.5 SIRMS のインストール 472
6.2.6 SVmco インストール後の設定 477
6.2.6.1 パーティションからのトラップ送信先の設定 477
6.2.6.2 Windows ファイアーウォールの設定 477
6.2.6.3 STOP エラー(致命的なシステムエラー)発生後の Watchdog 監視設定 477
6.2.6.4 PSHED Plugin ドライバのインストール 478
6.2.6.5 管理 LAN の設定確認 478
6.2.7 SVmco のアップデートインストール 478
6.2.8 SIRMS のアップデートインストール 478
6.2.9 SVmco のアンインストール 478
6.2.10 SIRMS のアンインストール 479

7 SVmcovm の手動インストール 480

8 VMware5/6 における PCI カード故障箇所の特定手順 481
8.1 LAN カードの特定手順 483
8.2 FC カードの特定手順 487
8.3 RAID カードの特定手順 488
8.4 SAS 配下のテープ装置の特定手順 490
8.5 VMware6.x で FC カードの故障箇所が Unknown または誤った箇所で通報された場合の故障箇所特定方法について 490

1　製品概要

1.1　PRIMEQUEST における監視の仕組み

1.1.1　システム全体

PRIMEQUEST における監視の仕組みを以下に説明します。

PRIMEQUEST のハードウェアは MMB(Management Board)によって管理されます。

MMB は、PRIMEQUEST に搭載されている各コンポーネント(SB、電源、ファン、LAN など)やパーティションを管理し、システムクロック、管理 LAN、および PCI ボックスを制御します。

また、ビデオリダイレクション、テキストコンソールリダイレクション、Memory Mirror Mode の設定など、各種動作を設定します。これらの機能は、MMB Web-UI から操作できます。

ServerView Agent(SVagent)、ServerView RAID(SV RAID)、ServerView Mission Critical Option (SVmco)は、パーティション上のハードウェア異常監視、構成管理などを行うソフトウェアです。各パーティションの OS 上で、アプリケーションとして稼動します。

MMB および ServerView Suite(SVS)は、専用のコンソールを使うことなく、管理 LAN に接続した汎用の PC から MMB Web-UI、または ServerView Operation Manager(SVOM) Web-UI を使って操作できます。

システムを管理するための各種操作・設定は、MMB、または SVOM の Web-UI を通じて行います。また、異常監視については、SVOM の Web-UI で、MMB の監視対象を含め、システム全体の統合監視が可能です。

注意：

PRIMEQUEST1000 と PRIMEQUEST1000x2 以降で、以下のソフトについては、パーティション上にインストールするソフトが変わります。

PRIMEQUEST1000：PRIMEQUEST Server Agent (PSA) *1

PRIMEQUEST1000x2 以降：SVmco

尚、SVIM を使用してインストールする場合は、SVIM が機種を自動判別し、必要なソフトをインストールします。

*1: PSA は PRIMEQUEST.専用のシステム管理ソフトウェアです。

PSA の詳細は、「PQ1000 シリーズ 製品概説マニュアル」を参照下さい。

また、VMware ESXi5/6 の場合、PSA,SVmco をインストールせず、ESXi に CIM Provider、Guest OS 上に SVmcovm をインストールします。

［サーバ監視ソフトのインストール可否］

監視対象サーバ		VMware ESXi 5/6	VMware ESX 4	Windows	Linux
ソフトウェア名称	ServerView Agents	×	○	○	○
	ServerView Mission Critical Option (*1)	×	○	○	○
	PRIMEQUEST Server Agent(*2)	×	○	○	○
	ServerView ESXi CIM Provider(*3)	○	×	×	×
	ServerView Mission Critical Option for VM (*4)	○	×	×	×
	ServerView	×	×	○	○

	Operations Manager （SVOM）				

○：インストール可

×：インストール不可

※VMware ESX/ESXi を含むシステムで SVOM を利用する場合は、別途管理サーバ（Windows/Linux 上で動くサーバ、ゲスト OS でも可）を準備してください。

*1: PRIMEQUEST 1400S2Lite/1400S2/1400E2/1400L2/1800E2/1800L2 の場合のみ

*2: PRIMEQUEST 1400S/1400E/1400L/1800E/1800L の場合のみ

*3: 全 PRIMEQUEST(1400S/1400E/1400L/1800E/1800L/1400S2Lite/1400S2/1400E2/1400L2/1800E2/1800L2)が該当。ESXi 上にインストール。

*4: 全 PRIMEQUEST(1400S/1400E/1400L/1800E/1800L/1400S2Lite/1400S2/1400E2/1400L2/1800E2/1800L2)が該当。VMware ESXi5/6 上のゲスト OS にインストールしてください(詳細は 2.4 章参照)。Vmware ESXi 5/6 以外にはインストールしないで下さい。

1.1.2 ServerView Suite

パーティション内における各 ServerView コンポーネントの役割は以下の通りです。

・ServerView Operation Manager (SVOM)

各パーティション上の構成情報、異常検知の情報を表示します。

・ServerView Agent(SVagent)

パーティション上のハード構成情報、異常検知を行います。

・ServerView RAID(SV RAID)

パーティション上の各ディスクデバイス、SAS/RAID カードの構成情報、異常検知を行います。

・ServerView Mission Critical Option(SVmco)

SVagent/SVraid で検知したイベントを MMB と連携し、REMCS/Mail 通報を行います(Linux/Windows)。また、PRIMECLUSTER/PRIMESOFT 連携機能を提供します(Linux 版のみ)。

・ServerView Mission Critical Option for VM(SVmcovm)

SVraid で検知したイベントを MMB と連携し、REMCS/Mail 通報を行います。

ハード異常が発生するとイベントの内容に応じて、以下のアクションを行います。

・REMCS 通報：MMB から送信されます。

(SVOM からの REMCS 通報は PRIMEQUEST では使用できません。)

・メール通報：MMB、又は SVOM から送信されます。

・Trap 通報：SVagent、又は SV RAID から送信されます。

尚、PQ1000 でサポートしていた MMB からの Trap 送信機能はサポートしていません。

・シスログ、イベントログ出力：SVagent、又は SV RAID からログ出力されます。

1.1.3 VMware vSphere 5/6 におけるサーバ監視

PRIMEQUEST において、VMware vSphere 5/6 を使用するに当たっては、パーティション内で検出したハード故障を MMB に対して通知・中継する為、ServerView をインストールするゲスト OS が必要です。

また、本ゲスト OS は、ESXi が稼働するパーティション毎に必要です。

本ゲスト OS を選定するに当たっては、以下の条件に該当するゲスト OS を選定してください。

1) Guest OS と同一パーティション内の ESXi との通信が必要です。
2) MMB-PSA 間 LAN を使用した通信が必要です。

   (手順は、本マニュアル 2.4 章を参照ください)
3) SVmcovm は常に該当パーティション上で稼働する必要がある為、vSphere High Availability・vMotion 等の ESXi ホスト間に跨る移行や移動を行わない Guest OS を選択してください。
4) パーティション内で SAS アレイディスクユニットや SAS アレイコントローラカードを使用する場合は、本ゲスト OS に ServerView RAID を導入してください。
5) Guest OS の OS 種別が Redhat 5, Redhat 6, Windows2008, Windows2012 である事。

[留意事項]

・本ゲスト OS は、他のゲスト OS と異なり、ESXi との間で通信を行います。

その為、ネットワークセキュリティを考慮し、ESXi-ゲスト OS 間の通信には、本通信専用の仮想スイッチの構築を推奨します。

・ゲスト OS が Redhat 5, Redhat 6 の場合、VMware の標準機能を使用して、ESXi 上のログをゲスト OS のシスログへ出力させます。これにより、ゲスト OS 上の SVmcovm がハード故障を検知出来る様にになります。

・パーティション内で SAS アレイディスクユニットや SAS アレイコントローラカードを使用する場合は、本ゲスト OS に ServerView RAID も導入してください。

・ゲスト OS の監視については、VMware 社提供の vSphere Client、又は vCenter Server で確認できます。

また、SVOM V6.0 から SVOM に VMware サーバなどを登録した場合、その上で動作しているゲスト OS のステータスが表示されます。

1.2 ServerView Mission Critical Option (SVmco)

SVmco の製品概要を説明します。

1.2.1 SVmco/SVmcovm の機能

ServerView Mission Critical Option (SVmco) 及び ServerView Mission Critical Option for VM (SVmcovm) は、PRIMEQUEST 向け保守連携用ソフトです。

ServerView Agent(SVagent) /ServerView RAID(SVraid)、及び Management Board(MMB)と連携し、パーティション上で発生したハード異常の検知、および通報を行います。

SVmco/SVmcovm の主な機能は以下のとおりです。

・MMB 連携機能

SVagent と連携、又は ESXi 上のドライバが出力したログからハード故障を検知し、REMCS/Mail 通報を行う為に必要なハード異常の情報を MMB に通知します。

これにより、MMB から REMCS/Mail 通報が送信されます。

・DISK 保守操作

パーティション上での DISK 活性交換機能をサポートします。

・REMCS 機能

REMCS に対応するパーティションからのイベント／ハード情報を収集／通報します。

・PRIMECLUSTER/PRIMESOFT 連携

PRIMECLUSTER/PRIMESOFT に対応するサービスを提供します。

注：SVmcovm は、上記機能の内、MMB 連携機能のみをサポート。

1.2.2 ハード異常監視の仕組み

SVagent では、シスログ(Linux,VMware)、イベントログ(Windows)に出力されるログを監視し、SVagent 内のフィルタ定義をもとに、各種発生イベントのフィルタリングを行い、SVagent 及び SVmco がその結果から各種アクション(メール通報、REMCS 通報、Trap 通報、ログ出力)の実施を行います。

メール/REMCS 通報においては、SVmco が PSA-MMB 間専用 LAN を介して、MMB と連携を行い、MMB 経由で通報を送信します。

注意

VMware ESX 4 の場合、Console OS シスログに出力される以下のハードウェアのメッセージが監視対象となります。カッコ内は、『７．２．SVagent のメッセージ』のタイトルを示しています。メッセージの詳細については、これらの項を参照してください。

・LAN (「LAN 関連メッセージ[Linux]」)

・FC (「ファイバーチャネルメッセージ[Linux]」)

・SCSI (「SCSI メッセージ[Linux]」)

ただし、SCSI 共通層や Linux と異なる VMware 固有のドライバメッセージ、また vmkernel や vmkwarning などは、監視対象外です。

VMware ESXSi 5 の場合、以下のメッセージが監視対象となります。

・LAN (「LAN 関連メッセージ[Linux]」)

・FC (「ファイバーチャネルメッセージ[Linux]」)

・SCSI (「SCSI メッセージ[Linux]」)

・ServerView RAID メッセージ [Linux]

・ServerView RAID 関連メッセージ [Windows]

2　導入手順

2.1　SVmco の設定（Linux：Red Hat Enterprise Linux）

SVmco インストール後、SVmco を動作させるために必要な設定の確認と、使用できる機能について説明します。設定は root 権限で作業を行ってください。

SVmco 動作に必要な設定確認と使用できる機能

必須／必要に応じて	設定項目	自動設定 (*1)／手動設定 (*2)	参照先
必須	PSA-MMB 間通信 LAN の設定	自動設定	2.1.1　PSA-MMB 間通信 LAN の設定
	管理 LAN の設定確認	手動設定	2.1.2　管理 LAN の設定確認
	SELinux 機能の設定確認	自動設定	2.1.3　SELinux 機能の設定確認
	ファイアーウォール機能の確認 (ポートの開放)	自動設定	2.1.4　ファイアーウォール機能の確認 (ポートの開放)
	管理 LAN IP アドレスの設定	手動設定	2.1.5 管理 LAN IP アドレスの設定
必要に応じて	パーティションからのトラップ送信先の設定	手動設定	2.1.6 パーティションからのトラップ送信先の設定

必須／必要に応じて	設定項目	自動設定 (*1)／手動設定 (*2)	参照先
	複製ディスク使用時の SNMP 設定	手動設定	2.1.7 複製ディスク使用時の SNMP 設定
	SVmco のアップデートインストール	対象外	2.1.8　SVmco のアップデートインストール
	SIRMS のアップデートインストール	対象外	2.1.9　SIRMS のアップデートインストール
	SVmco のアンインストール	対象外	2.1.10　SVmco のアンインストール
	SIRMS のアンインストール	対象外	2.1.11　SIRMS のアンインストール

*1：自動設定：SVmco インストール時に自動設定されています。自動設定の内容の変更が必要な場合があるので、上記表の参照先を確認してください。

*2：手動設定：SVmco インストール時には設定されません。上記表の参照先のとおり設定してください。

*3：PRIMEQUEST 1000x2 シリーズ以降の運用時は、必ず SVmco をインストールしてください。SVmco をアンインストールすると、以下の制限があります。

- REMCS 契約時にパーティション上の異常が通知されない。
- ハードディスクの活性保守ができない。必ずパーティション停止保守となる。
- PRIMECLUSTER 連携が使用できない。

備考

- SVIM を使用して OS をインストールするときに、SVmco も同時にインストールされます。SVIM について詳しくは、『ServerView Suite ServerView Installation Manager』を参照してください。
- SVmco を手動でインストールする場合について詳しくは、「6.　SVmco の手動インストール・アンインストール」を参照してください。
- SVmco インストール時に、SVmco 動作のための設定が以下のように自動的に追記または変更されます。

SVmco インストール時に自動追記／変更される設定

対象	動作	備考
snmpd.conf ファイル	設定追記	
snmptrapd.conf ファイル	設定追記	※SVmco1.4 版以降を使用していて、IPv6 を無効にする場合、設定を削除する必要があります。下記の注意 2 に従って設定を削除して下さい。
snmptrapd の起動オプション	変更	
snmpd の起動オプション	変更	
PSA-MMB 間専用 LAN インターフェース	IP アドレス設定	「2.1.1　PSA-MMB 間通信 LAN の設定」を参照し、必要に応じて変更する。
iptables 設定	設定追加	
SELinux 設定ファイル (/etc/selinux/conf)	変更	RHEL5 の場合のみ、SELinux が無効化される。ただし、すでに無効化されている場合は変更しない
SELinux 設定	設定追加	RHEL６．０以降の場合のみ、ポリシーモジュールが追加される。ただし、SELinux が Disable 設定時は本ポリシーモジュールは動作しない。なお、PRIMEQUEST としては、SELinux 有効化での運用はＲＨＥＬ６．２以降となっている。

注意

1. MMB 側の PSA-MMB 間専用 LAN の IP アドレス、またはパーティション側の PSA-MMB 間専用 LAN の IP アドレスを変更した場合は、必ず SVmco を再起動してください。再起動しないと SVmco で検出するエラーが通知できません。
2. SVmco1.4 版以降を使用しており、IPv6 を無効にする場合、以下の snmptrapd の設定ファイルから設定の削除が必要です。

設定を削除しない場合、Trap を受信することが出来ない状態となり、例えば PRIMECLUSTER 連携をしている場合、他ノードからの Trap を受信できない問題などがあります。

以下の手順に従って設定を削除して下さい。

1. /etc/snmp/snmptrapd.conf を開き、以下の”**udp6:162**”を削除する。

   修正前：

```
snmpTrapdAddr udp:162,udp6:162
```

   修正後：

```
snmpTrapdAddr udp:162
```

2. snmptrapd の状態を確認した上で、正常に起動することを確認します。

   ■ snmptrapd が停止している状態

```
#/etc/init.d/snmptrapd status
snmptrapd は停止しています
#/etc/init.d/snmptrapd start
snmptrapd を起動中:                    [  OK  ]
#
```

   ■ snmptrapd が起動している状態

```
#/etc/init.d/snmptrapd status
snmptrapd (pid  xxxx) を実行中...
#/etc/init.d/snmptrapd restart
snmptrapd を停止中:                    [  OK  ]
snmptrapd を起動中:                    [  OK  ]
#
```

2.1.1 PSA-MMB 間通信 LAN の設定

ここでは、PSA-MMB 間通信 LAN の設定の確認について説明します。

SVmco が MMB と通信するためには、PSA-MMB 間通信 LAN に接続されたネットワークインターフェースカード (NIC) が活性化されている必要があります。

PSA-MMB 間通信 LAN は、通常 SVmco インストール時に自動的に以下の値に設定されます。

<IP アドレス>

172.30.0.<パーティション ID + 2>/24

例) パーティション ID が 2 の場合

172.30.0.4/24

<通信設定>

Auto Negotiation off

Speed 100Mbps

Duplex full

以下の場合に限り、IP アドレスの設定を変更してください。

1. 自動設定される IP アドレスが、業務ネットワークや管理ネットワークで使用する IP アドレスやサブネットと重なってしまう
2. 別パーティションから複製したディスクを使用して新たにパーティションを構築した
3. あるパーティションでインストールしたディスクを別のパーティションに移して使用するなどで、パーティション ID が変更となる

IP アドレスの設定は、以降の手順で変更してください。なお、上記の 1.の理由で設定を変更する場合は、同一筐体に存在する全パーティション、および MMB 側の PSA-MMB 間通信 LAN の IP アドレスも同一サブネットの IP アドレスに変更する必要があります。MMB 側の IP アドレスは、MMB Web-UI から設定してください。

注意

- 通信設定については、自動的に設定された値から変更しないでください。変更した場合、PSA-MMB 間の通信が不通となり、SVmco の機能を使用できなくなることがあります。
- PSA-MMB 間 LAN 設定は、SVmco インストール後に変更してください。SVmco インストール前に変更した場合、インストール時に設定が上書きされます。
- MMB Web-UI の [Network Configuration] - [Network Interface] 画面にて [MMB-PSA IP Address] の [Interface] が Disable の場合、イベント通報機能が使用できません。なお、Disable から Enable に変更するさいには、変更後に OS の再起動が必要です。

■ PSA-MMB 間通信 LAN 用の NIC の確認

以下の手順で、PSA-MMB 間通信 LAN の NIC に割り当てられたインターフェース名を確認します。

- 操作手順

1. ifconfig コマンドを実行して、システムで認識されているネットワークインターフェースの一覧を表示し、インターフェース名を確認します。

【入力形式】

```
/sbin/ifconfig -a
```

【表示例】

左に表示された eth0、eth1、lo がインターフェース名です。

```
#  /sbin/ifconfig -a
eth0   Link encap:Ethernet HWaddr 00:D0:B7:53:89:C3
       inet addr:10.24.17.149 Bcast:10.24.17.255 Mask:255.255.255.0
       inet6 addr:  fe80::2d0:b7ff:fe53:89c3/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST MTU:1500  Metric:1
       RX packets:1107704 errors:0  dropped:0 overruns:0 frame:0
       TX packets:2653820 errors:0  dropped:0 overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:390009908 (371.9 MiB) TX bytes:809006934 (771.5 MiB)

eth1   Link encap:Ethernet HWaddr 00:0E:0C:21:83:97
       inet addr:192.168.0.162 Bcast:10.24.17.255 Mask:255.255.255.0
       inet6 addr:  fe80::20e:cff:fe21:8397/64 Scope:Link
       UP BROADCAST RUNNING MULTICAST MTU:1500  Metric:1
       RX packets:1538726 errors:0  dropped:0 overruns:0 frame:0
       TX packets:356 errors:0 dropped:0  overruns:0 carrier:0
       collisions:0 txqueuelen:1000
       RX bytes:341051195 (325.2 MiB)  TX bytes:22862 (22.3 KiB)
       Base address:0x5cc0  Memory:fbfe0000-fc000000

lo     Link encap:Local Loopback
       inet addr:127.0.0.1 Mask:255.0.0.0
       inet6 addr: ::1/128 Scope:Host
       UP LOOPBACK RUNNING MTU:16436  Metric:1
       RX packets:3865 errors:0 dropped:0  overruns:0 frame:0
```

2. ethtool コマンドを実行して PSA-MMB 間通信 LAN 用 NIC を探します。手順 1. で表示された各インターフェースに対して、以下のコマンドをそれぞれ実施して確認します。

   PSA-MMB 間通信 LAN 用 NIC は、bus-info(SEG:BUS:DEV.FUNC 番号) が 0000:00:19.0 になります。

【入力形式】

```
/sbin/ethtool -i <インターフェース名>
```

【表示例】

eth0 に対して実施した結果、PSA-MMB 間通信 LAN 用 NIC と一致した例です。

```
# /sbin/ethtool -i eth0
driver: e100
version: 3.0.27-k2-NAPI
firmware-version: N/A
bus-info: 0000:00:19.0 (PSA-MMB 間通信 LAN 向け NIC と一致)
```

■ PSA-MMB 間通信 LAN 用の NIC の設定

以下の手順で、PSA-MMB 間通信 LAN 用の NIC を設定します。

■ 操作手順

1. /etc/sysconfig/network-scripts 配下の該当するインターフェースに対する ifcfg ファイルを編集します。

○ PSA-MMB 間通信 LAN 用 NIC インターフェース用：ifcfg-<NIC インターフェース名>

例. ifcfg-eth0

該当するインターフェースに対する ifcfg ファイルを編集し、IP アドレスを変更します。

PSA-MMB 間通信 LAN 用 NIC インターフェース用 ifcfg ファイルの編集例を、以下に示します。

```
# vi  /etc/sysconfig/network-scripts/ifcfg-<NIC インターフェース名>


以下の行を変更します。
BROADCAST=<PSA-MMB 間通信 LAN 向け BROADCAST アドレス>
IPADDR=<PSA-MMB 間通信 LAN 向け IP アドレス>
NETMASK=<PSA-MMB 間通信 LAN 向けサブネットマスク>
```

注意

- 設定を変更する前に、ifcfg ファイルが SVmco インストール時の自動設定の値になっているかを確認してください。自動設定の値になっていない場合、SVmco がインストールされていない可能性があります。必ず SVmco をインストールした後に設定を変更してください。
- 変更が必要な項目 (BROADCAST、IPADDR、NETMASK) 以外は、コメント行を含め変更しないでください。変更した場合、PSA-MMB 間の通信が不通となり、SVmco が提供する機能を使用できなくなるだけでなく、SVmco アップデート時に自動設定の値に上書きされる可能性があります。
- IP アドレスは同一筐体内で重複しない値を設定して下さい。

2. **その後、network サービスの restart により、ネットワークインターフェースが起動します。**

【入力形式】

```
/sbin/service  network restart
```

注意

SVmco 1.9 版以降を使用している場合、以下の手順 3 は自動で設定されるため必要ありません。手順 4 で SVmco を再起動して下さい。

3. SVmco の設定ファイルに、PSA-MMB 間通信 LAN の IP アドレスを設定します。

ファイル格納場所：/etc/fujitsu/SVmco/usr/tommbipsetup.conf

設定値：手順 1.で設定した IP アドレスを入力する。

<設定例>

```
[NETWORK]
TOMMBIP=172.30.0.4 （手順 1 で設定した IP アドレス）
```

4. PSA-MMB 間通信 LAN 用 NIC の設定を反映させるため、SVmco を再起動します。

【入力形式】

```
/sbin/service  y30SVmco stop
/sbin/service  y30SVmco start
```

2.1.2 管理 LAN の設定確認

管理 LAN ネットワークの設定、および必要に応じて PRIMECLUSTER GLS または bonding などによる二重化設定を行ってください。

また、上記管理 LAN のネットワーク設定完了後、「2.1.5 管理 LAN IP アドレスの設定」を実施してください。

注意

PRIMEQUEST 環境では、MMB との通信に使用する管理 LAN に接続するスイッチの STP 機能を OFF にする必要があります。

2.1.3 SELinux 機能の設定確認

PRIMEQUEST1000 シリーズでは、RHEL6.2 以降から SE Linux の有効化での運用が

サポートされている為、SVmco をインストールするパーティション OS が RHEL5,

RHEL6.0 および RHEL6.1 の場合は、SELinux を無効にして下さい。

RHEL6.2 以降の場合は SELinux 機能の有効/無効のいずれでも運用することができます。

上記理由により、RHEL5 , RHEL6.0 または RHEL6.1 の場合は、SELinux 機能が無

効に設定されていることを確認してください。有効に設定されている場合は、

SELinux 機能を無効にします。なお、RHEL5 の場合のみ、SVmco インストール時に自動的に無効に設定されます。

以下のように[disabled] になっていることを確認します。[disabled] 以外の値が表示された場合は、コンフィグファイル(/etc/selinux/config) を修正して[disabled] にします。

- 設定の確認

```
#cd /etc/selinux/
#more config
.....
.....
SELINUX=disabled ← ここを確認します。
```

■ 設定の修正

```
# vi /etc/selinux/config
.....
.....
SELINUX=disabled ← ここを修正します。
```

2.1.4 ファイアーウォール機能の確認 (ポートの開放)

ファイアーウォール設定でパーティションのポートが開放されていないときは、SVmco が動作するために必要なポートを開放します。管理 LAN 用のインターフェースと PSA-MMB 間通信 LAN 用インターフェースに対して設定します。

PSA-MMB 間通信 LAN 用インターフェースに関する設定は必須です。通常、SVmco インストール時に自動設定されます (*1)。

管理 LAN 用インターフェースに関する設定は、PRIMECLUSTER との連携を行う場合にのみ必要となります。ポート開放は、提供されている設定用シェルスクリプトを実行して設定するか、iptables コマンドなどを使って手動で設定してください (*2)。

*1： SVIM から SVmco が自動インストールされた場合のみ、ポートが設定されます。

*2：設定用のシェルスクリプト (setmlanfw.sh) を実行すると、管理 LAN 用のチェイン (MMLAN) のみ作成されます。Iptables の INPUT または OUTPUT に、管理 LAN 用のチェインへのジャンプ設定を追加してください。詳細は「■設定用シェルスクリプト (setmlanfw.sh) を使った設定」を参照してください。

■ 管理 LAN 用インターフェース

管理 LAN 用のインターフェースに関して、以下のポートを開放します。

設定を行う前に「2.1.2 管理 LAN IP アドレスの設定」を行ってください。ポート開放は、設定用シェルスクリプト (setmlanfw.sh) を使うか、iptables コマンドなどを使って手動で設定してください。

管理 LAN 用のインターフェースで開放するポート

ポート	ポート番号	説 明	備 考
snmptrap ポート	udp/snmptrap または 162	ポートはクラスタ連携 (PCL など) を使用する場合にのみ開放する。	IP アドレス指定は、全クラスタノードに属する MMB の MMB Physical IP Address (MMB#0/MMB#1) を指定
rmcp+ポート	udp/7000～7100		

■ **設定用シェルスクリプト (setmlanfw.sh) を使った設定**

1. 「2.1.2 管理 LAN IP アドレスの設定」が行われていることを確認します。

2. 設定ファイルを用意します。

   設定ファイルのサンプルは以下に配置してあります。

   ```
   /opt/fujitsu/SVmco/sh/sample_conf_setmlanfw.txt
   ```

備考

上記ファイルはサンプルファイルのため、SVmco アップデート時に上書きされます。
実際に使用した設定ファイルを保持しておきたい場合は、別途保存してください。

設定ファイルでは、 [PCL] とだけ記載した行に続けて、PRIMECLUSTER で定義された全クラスタノードに属する MMB の物理 IP (MMB Physical IP Address <MMB#0/MMB#1>)、または上記 MMB の物理 IP を含むネットワーク IP を 1 行 1 項目単位で記載します。

管理 LAN で使用している通信プロトコルによって設定が異なります。

➢ **IPv4 で使用している時**

設定ファイル記載例：

[PCL]

192.168.0.0/24

192.168.1.5

1. ファイアーウォールの状態確認

以下のコマンドを実行し、iptables の状態を確認します。

```
#/sbin/service iptables status
```

“ファイアーウォールは停止”など iptables が停止しているメッセージが表示された場合は、以下のコマンドで iptables を起動してください。

起動しないと、設定ツールが必要な設定を行えません。

```
#/sbin/service iptables start
```

2. 設定用シェルスクリプトを実行します。

手順 2.で用意した設定ファイルのパスを、第一引数に指定します。

設定ファイルの内容を確認するメッセージが表示されるので、「Y」と入力します。

実行例： (カレントディレクトリに設定ファイル"fwconf.txt"が

準備されているものとします。)

/opt/fujitsu/SVmco/sh/setmlanfw.sh ./fwconf.txt

Management LAN IP address:

192.168.0.1

Source IPs for PRIMECLUSTER Service:

192.168.0.0/24

192.168.1.5.

```
Press "Y" to confirm above settings, "N" to cancel all settings
                              Y
#####################################################################
# Created the MMLAN chain on your firewall(iptables)              #
# For more detail on how to set firewall, refer to the Installation Manual.#
#####################################################################
The setting was completed
```

3. iptables -L -n コマンドを実行し、設定チェイン "MMLAN" が存在することを確認します。

```
実行例：
# iptables -L -n
Chain INPUT (policy DROP)
target   prot  opt source       destination
MMLAN    all -- 0.0.0.0/0      0.0.0.0/0

Chain FORWARD (policy DROP)
target   prot  opt source       destination

Chain OUTPUT (policy DROP)
target   prot  opt source       destination
MMLAN    all -- 0.0.0.0/0      0.0.0.0/0

Chain MMLAN (2 references)
target  prot  opt source       destination
ACCEPT  udp  -- 192.168.0.0/24 192.168.0.1  udp dpts:7000:7100
ACCEPT  udp  -- 192.168.0.1   192.168.0.0/24 udp spts:7000:7100
ACCEPT  udp  -- 192.168.0.0/24 192.168.0.1  udp dpt:162
ACCEPT  udp  -- 192.168.0.1   192.168.0.0/24 udp spt:162
ACCEPT  udp  -- 192.168.1.5   192.168.0.1  udp dpts:7000:7100
ACCEPT  udp  -- 192.168.0.1   192.168.1.5   udp spts:7000:7100
ACCEPT  udp  -- 192.168.1.5   192.168.0.1  udp dpt:162
ACCEPT  udp  -- 192.168.0.1   192.168.1.5   udp spt:162
```

注意

管理 LAN 用インターフェースの IP アドレスを変更した場合、いったん設定を削除してから、再度設定してください。設定の削除については、「3.1.7　管理 LAN 用インターフェース向けファイアーウォール設定コマンド (setmlanfw.sh)」の「(8) 設定削除手順」を参照してください。

4. 設定チェイン "MMLAN" を INPUT および OUTPUT チェインに追加します。このとき、INPUT および OUTPUT チェインにある既存の REJECT 設定や、ユーザー定義のチェインに遮断されないように、注意して設定してください。

実施例： INPUT、FORWARD に REJECT 設定がある場合

```
# iptables –L
Chain INPUT (policy ACCEPT)
target    prot  opt source          destination
ACCEPT     all   --  0.0.0.0/0           0.0.0.0/0  state RELATED,ESTABLISHED
ACCEPT     icmp  --  0.0.0.0/0             0.0.0.0/0
ACCEPT     all   --  0.0.0.0/0           0.0.0.0/0
ACCEPT     tcp   --  0.0.0.0/0            0.0.0.0/0  state NEW tcp dpt:22
REJECT     all   --  0.0.0.0/0           0.0.0.0/0  reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
target   prot  opt source        destination
REJECT     all   --  0.0.0.0/0           0.0.0.0/0  reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
target   prot  opt source        destination

Chain MMLAN (2 references)
target    prot  opt source          destination
ACCEPT     udp  --  192.168.0.0/24       192.168.0.1    udp dpts:7000:7100
ACCEPT     udp  --  192.168.0.1          192.168.0.0/24  udp spts:7000:7100
ACCEPT     udp  --  192.168.0.0/24       192.168.0.1     udp dpt:162
ACCEPT     udp  --  192.168.0.1          192.168.0.0/24  udp spt:162
ACCEPT     udp  --  192.168.1.5          192.168.0.1     udp dpts:7000:7100
ACCEPT     udp  --  192.168.0.1          192.168.1.5     udp spts:7000:7100
ACCEPT     udp  --  192.168.1.5          192.168.0.1     udp dpt:162
ACCEPT     udp  --  192.168.0.1          192.168.1.5     udp spt:162
```

5. "MMLAN" を INPUT チェインの 5 番目 (REJECT 設定の前) および OUTPUT チェインに追加します。(iptables のオプションの詳細は man マニュアルを参照してください。)

```
# /sbin/iptables –I INPUT 5 –j MMLAN
# /sbin/iptables –A OUTPUT –j MMLAN
```

6. iptables -L コマンドを実行し、INPUT チェインおよび OUTPUT チェインについて、追加した MMLAN チェインが、その前の REJECT、DROP などにより遮断されていないことを確認します。

設定例：

```
# iptables –L
Chain INPUT (policy ACCEPT)
target   prot  opt source           destination
ACCEPT     all   --  0.0.0.0/0          0.0.0.0/0  state RELATED,ESTABLISHED
ACCEPT     icmp  --  0.0.0.0/0          0.0.0.0/0
ACCEPT     all   --  0.0.0.0/0          0.0.0.0/0
ACCEPT     tcp   --  0.0.0.0/0          0.0.0.0/0  state NEW tcp dpt:22
MMLAN      all   --  0.0.0.0/0          0.0.0.0/0
REJECT     all   --  0.0.0.0/0          0.0.0.0/0  reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
target   prot  opt source       destination
REJECT     all   --  0.0.0.0/0          0.0.0.0/0  reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
target   prot  opt source       destination
MMLAN      all   --  0.0.0.0/0          0.0.0.0/0
```

```
Chain MMLAN (2 references)
target    prot  opt source         destination
ACCEPT    udp   -- 192.168.0.0/24      192.168.0.1  udp dpts:7000:7100
ACCEPT    udp   -- 192.168.0.1        192.168.0.0/24 udp spts:7000:7100
ACCEPT    udp   -- 192.168.0.0/24      192.168.0.1  udp dpt:162
ACCEPT    udp   -- 192.168.0.1        192.168.0.0/24 udp spt:162
ACCEPT    udp   -- 192.168.1.5        192.168.0.1  udp dpts:7000:7100
ACCEPT    udp   -- 192.168.0.1        192.168.1.5   udp spts:7000:7100
ACCEPT    udp   -- 192.168.1.5        192.168.0.1  udp dpt:162
ACCEPT    udp   -- 192.168.0.1        192.168.1.5   udp spt:162
```

7. ファイアーウォールの設定を保存します。

```
# /sbin/service iptables save
```

■ PSA-MMB 間通信 LAN 用インターフェース

PSA-MMB 間通信 LAN 用インターフェースに関して、以下のポートを開放します。
通常、SVmco インストール時に自動的にポート開放が設定されます (*)。

* : SVIM から SVmco がインストールされた場合のみ、自動的にポートが設定されます。

PSA-MMB 間通信 LAN 用インターフェースで開放するポート

ポート	ポート番号	説 明	備 考
snmp ポート	udp/snmp または 161		送受信双方

ポート	ポート番号	説 明	備 考
psa-mmb 通信ポート	tcp/MMB 側 5000	MMB 側の 5000 番ポートに対する通信。 本通信では、パーティション側はクライアントとして動作するため、パーティション側で使用されるポート番号は、不定 (tcp/1025 ～ 65535 のいずれか 1 ポート)。 パーティションからの接続開始許可が設定されている場合や、パーティションとの接続が確立したものに通信許可などが設定されている場合は、5000 番ポートに対する設定は不要。 5000 番ポートに対する設定が不要な例： iptables -A OUTPUT -m state --state NEW,ESTABLISH -j ACCEPT iptables -A INPUT -m state --state ESTABLISH -j ACCEPT	送受信双方
icmp	echo-request		送信のみ
icmp	echo-reply		受信のみ

【入力形式】

```
/sbin/iptables -L
```

ポートの開放は、iptables コマンドなどで実施してください。使用方法は、コマンドの man などを参照してください。

【入力形式】

```
/usr/bin/man iptables
```

2.1.5 管理 LAN IP アドレスの設定

SVmco にパーティション上の管理 LAN の IP アドレスを設定します。

[注意]

SVmco1.3 版以前からのアップデートでは、PRIMECLUSTER 連携の為の IPv4 用管理 LAN IP アドレスの設定ファイル ipsetup.conf 内にあるパラメータ”IPVersion”の設定項目は追加されません。

1. eecd プロセスが起動している事を確認します。

```
ps ax | grep eecd
```

起動していなかった場合には、ServerView Agent を起動します。

【入力形式】

```
/usr/sbin/srvmagt start
```

2. 設定ファイルを編集します。

   設定内容は管理 LAN で使用している通信プロトコルによって異なります。

- **IPv4 で使用している場合**

1. /etc/fujitsu/SVmco/usr/ipsetup.conf ファイルを編集します。

```
# vi /etc/fujitsu/SVmco/usr/ipsetup.conf
以下の行を変更します。
[NETWORK]
ManagementIP=<管理 LAN 用 IP アドレス>

以下の行は変更不要です。
IPVersion=0
```

【入力形式】

```
[NETWORK]
ManagementIP=192.168.0.1

IPVersion=0
```

2. 下記コマンドを実施してください。

【入力形式】

```
/usr/sbin/eecdcp -c oc=E002 oe=000C ¥'$IPADDRESS¥'
```

例

```
/usr/sbin/eecdcp -c oc=E002 oe=000C ¥'192.168.0.1¥'
```

3. 管理 LAN 用 IP アドレスの設定を反映させるため、SVmco を再起動します。

【入力形式】

```
/sbin/service  y30SVmco stop
```

```
/sbin/service  y30SVmco start
```

2.1.6 パーティションからのトラップ送信先の設定

備考

- 本設定は、必要な場合のみ実施してください。
- 運用管理ソフトウェアがパーティションごとにイベントを管理する場合には、本設定が必要です。

■ snmpd.conf の編集

```
# vi /etc/snmp/snmpd.conf


使用したい SNMP のバージョンに応じて、以下の行を追加します。
定義順は自由です。
trapsink HOST [COMMUNITY [PORT]]      # SNMPv1 トラップの設定
trap2sink HOST [COMMUNITY [PORT]]     # SNMPv2 トラップの設定
trapsess SNMPCMD_ARGS HOST[:PORT]     # SNMPv3 トラップの設定
```

設定の詳細について以降で説明します。

■ SNMPv1/SNMPv2 トラップの設定

```
trapsink HOST [COMMUNITY [PORT]]      # SNMPv1 トラップの設定
trap2sink HOST [COMMUNITY [PORT]]     # SNMPv2 トラップの設定
```

トラップを受信する (通知を送る先の) ホストを定義します。

- ホストを定義すると snmpd 起動時に Cold Start トラップを送ります。パーティションからの SNMP トラップ送信が設定されている場合は、認証が失敗したときにもトラップを送ります。
- trapsink、trap2sink 行を複数指定すれば、複数の送信先を指定することができます。

COMMUNITY が指定されていない場合は、trapcommunity で指定した文字列が使われます。trapcommunity は、トラップを送るときに使う初期値のコミュニティ文字列を定義するコマンドです。trapcommunity でコミュニティ文字列を定義するときは、trapsink, trap2sink 行より前に指定してください。

```
trapcommunity STRING          #コミュニティ名設定
```

- PORT が指定されていない場合は、一般的な SNMP トラップポート (162) が使われます。

  IP アドレスが"192.168.0.162"の 162 ポートのマネージャに対して、コミュニティ名が"public"で、トラップを送信可能とする場合の例

```
trapsink 192.168.0.162 public 162      ##SNMPv1 トラップの設定
trap2sink 192.168.0.162 public 162     ##SNMPv2 トラップの設定
```

■ SNMPv3 トラップの設定

```
trapsess SNMPCMD_ARGS HOST[:PORT]# SNMPv3 トラップの設定
```

トラップを受信する(通知を送る先の) ホストを定義します。PORT が指定されていない場合は、一般的な SNMP トラップポート(162) が使われます。

SNMPCMD_ARGS で指定する主なオプションについて説明します。

-v version：

SNMP バージョンを指定します。SNMPv3 の場合は 3 を指定します。

-e engineID：

トラップ送信元の/var/net-snmp/snmpd.conf ファイル内の oldEngineID の値を設定します。

-u secName：

SNMPv3 用のアカウントです。マネージャ側の設定と同期を取る必要があります。

-l secLevel：

SNMPv3 メッセージのセキュリティレベルに応じて、下図に示すいずれかの値を設定します。

secLevel の設定

設定値	認証	暗号化
noAuthNoPriv	設定しない	設定しない
authNoPriv	設定する	設定しない
authPriv	設定する	設定する

-a authProtocol：

SNMPv3 メッセージを認証するためのプロトコルで MD5 または SHA を指定します。SHA を使用するためにはインストールされている openssl を使ってパッケージを作成しなければなりません。-l オプションでセキュリティレベルに認証が含まれる場合に有効となり、認証が含まれない場合は省略可能です。

-A authPassword：

認証パスワード(8 文字以上)。マネージャ側の設定と同期を取る必要があります。-l オプションでセキュリティレベルに認証が含まれる場合に有効となり、認証が含まれない場合は省略可能です。

-x privProtocol：

SNMPv3 メッセージを暗号化するためのプロトコル。現在のところプライバシープロトコルがサポートされているのは DES のみです。-l オプションでセキュリティレベルに暗号化が含まれる場合に有効となり、暗号化が含まれない場合は省略可能です。

-X privPassword：

暗号化パスワード (8 文字以上)。マネージャ側の設定と同期を取る必要があります。-l オプションでセキュリティレベルに暗号化が含まれる場合に有効となり、暗号化が含まれない場合は省略可能です。

IP アドレスが "192.168.0.162" の 162 ポートのマネージャに対して、[PRIMEQUEST] というアカウントで認証・暗号化を有効にし、SNMPv3 トラップを送信可能とする場合の例

```
#trapsess -v 3 -e 0x800007e58026577a9f421950a4 -u PRIMEQUEST -l ¥
authPriv -a MD5
-A 00000000 -x DES -X 11111111 192.168.0.162:162   ¥
##SNMPv3 トラップの設定
```

¥：改行しないことを表す。

トラップ送信先の設定後、下記コマンドにより、snmpd を再起動します。

```
#/etc/rc.d/init.d/snmpd restart
```

■　トラップ送信先設定確認方法について

トラップ送信先設定確認をするには、snmpd を再起動するさいの、net-snmp 標準トラップを利用します。このトラップの受信可否により、正しく設定されているかを確認できます。

備考

トラップ送信先では、トラップ受信用のアプリケーションや管理マネージャが動作していて、net-snmp 標準トラップが受信できる必要があります。

トラップ送信元マシン上では、下記コマンドにより、snmpd を再起動します。

```
# /etc/rc.d/init.d/snmpd restart
```

本操作により、トラップ送信先では、トラップ受信用のアプリケーションに、「ColdStart」の net-snmp 標準トラップが通知されます。

例として、トラップ送信先が Linux マシンの場合を示します。トラップ送信先が Linux マシンの場合、[snmptrapd] でトラップ受信したときに、以下のようなメッセージがシステムログに表示されます。トラップが正しく受信できることを確認してください。

```
Aug 17 12:00:53 pq-server  snmptrapd[2600]: 2005-08-17 12:00:53 ¥
pq-server.
fujitsu.com  [192.168.0.162](via 192.168.0.162) TRAP, SNMP v1, ¥
community
public  NET-SNMP-MIB::netSnmpAgentOIDs.10 Cold Start Trap (0) ¥
Uptime: 0:00:00.17
```

¥：改行しないことを表す。

2.1.7 複製ディスク使用時の SNMP 設定

ここでは、複製したディスクを使用した場合に必要な設定について説明します。

備考

本設定は、必要な場合のみ実施してください。

同一筐体内のパーティションから複製したディスクを使用して、新たにパーティションを構築することができます。この場合には、SVmco の内部通信で使用する SNMPv3 の EngineID を手動で変更する必要があります。

以下に変更手順を示します。本手順は、root 権限で実施してください。

■ 操作手順

1. ps コマンドで、SVmco が起動しているかを確認します。

【入力形式】

```
ps ax | grep mco
```

【表示例】

以下のように/opt/fujitsu/SVmco/bin/配下のプロセスが表示される場合は、SVmco が稼動中です。

```
# ps ax | grep mco

4562 ?    S   0:00 /opt/fujitsu/SVmco/bin/pm -o 70 /etc/opt/¥
SVmco/global/pmmco.conf
4563 ?    S   0:18 /opt/fujitsu/SVmco/bin/pcx -p /
4564 ?    S   0:06 /opt/fujitsu/SVmco/bin/pcxipmi -p /
4565 ?    S   0:00 /opt/fujitsu/SVmco/bin/mmbm -p /
4566 ?    S   0:01 /opt/fujitsu/SVmco/bin/mmbs -p /
21670 pts/5 S+   0:00 grep mco
```

¥：改行しないことを表す。

2. SVmco が起動中の場合は、service コマンドで SVmco を停止します。

【入力形式】

```
/sbin/service y30SVmco stop
```

3. ps コマンドにより、snmpd が起動しているか確認します。

【入力形式】

```
ps ax | grep snmpd
```

【表示例】

以下のように/usr/sbin/snmpd が表示される場合は、snmpd が起動中です。

```
# ps ax | grep snmpd
32611 ?    S   0:04 /usr/sbin/snmpd -Lsd -Lf /dev/null -p ¥
var/run/snmpd -a
```

¥：改行しないことを表す。

4. snmpd が起動中の場合は、service コマンドで snmpd を停止させます。

【入力形式】

```
/sbin/service snmpd stop
```

5. /var/net-snmp/snmpd.conf ファイルに定義されている oldEngineID の値を変更します。

※

16 進表記で 34 桁以内の任意の数値に変更してください。ただし、同一筐体内の他パーティションで定義されている値とは異なる値にする必要があります。

oldEngineID の値を 0x19760523 に書き替える場合の例

```
#vi  /var/net-snmp/snmpd.conf
oldEngineID 0x19760523
```

6. service コマンドで snmpd を起動します。

【入力形式】

```
/sbin/service snmpd start
```

7. SVmco 内部通信で使用する SNMPv3 用パスワードを再生成するために、/opt/fujitsu/Svmco/sh ディレクトリへ移動します。

   【入力形式】

   ```
   cd /opt/fujitsu/Svmco/sh
   ```

8. 上記ディレクトリ内で、snmpsetup.sh を実行します。

   snmpsetup.sh を実行すると、SVmco 内部通信で使用する SNMPv3 用パスワードが自動生成されます。

   【入力形式】

   ```
   ./snmpsetup.sh install
   ```

9. SVmco を起動します。

   【入力形式】

   ```
   /sbin/service y30SVmco start
   ```

2.1.8 SVmco のアップデートインストール

Red Hat Enterprise Linux での SVmco のアップデートインストール方法について説明します。

以下の説明は、作業ディレクトリ (以下、$WORK_DIR と呼びます) 内に SVmco のパッケージ (SVmco-$VER-$REL.tar.gz) が展開されてディレクトリ "SVmco" が作成されていることを前提としています。 本作業は root 権限で行ってください。

また、アップデートの前後で ServerView Agents の停止・起動を行う必要があります。実施しないと、一部のファイルが置き換わらない場合があります。

また、SVmco のアップデートインストールを実施する前に、バックアップ手順を実施してください。バックアップ手順について詳しくは、「2.1.12 SVmco のバックアップ」を参照してください。

また、SVmco-1.6.0-0 版以前からのアップデートインストールかつ

PSA-MMB 間通信 LAN の IP をデフォルト設定※1 から変更している環境の場合、

アップデートインストール後にネットワークインターフェースのファイルを手動で

再設定する必要があります。

※1 PSA-MMB 間通信 LAN の IP のデフォルト設定

<IP アドレス>

172.30.0.<パーティション ID + 2>

例) パーティション ID が 2 の場合

172.30.0.4

1. ServerView Agents サービスを停止します。

```
# srvmagt stop
```

2. SVmco サービスを停止します。

```
# /sbin/service y30SVmco stop
```

3. 作業ディレクトリ内のディレクトリ "SVmco" に移動します。

```
# cd $WORK_DIR/SVmco
```

4. 以下のコマンドを実行し、インストールを実施します。

```
# ./INSTALL.sh
```

5. 環境に応じて、「環境により必要な設定手順」の 1)、2)を実施してください。

6. SVmco サービスを起動します。

```
# /sbin/service y30SVmco start
```

7. ServerView Agents サービスを起動します。

```
# srvmagt start
```

環境により必要な設定手順

1) SVmco1.4 版以降へのアップデートインストールかつ、

IPv6 を無効にしている場合、以下の snmptrapd の設定ファイルから設定の削除が必要です。

設定を削除しない場合、Trap を受信することが出来ない状態となり、例えば PRIMECLUSTER 連携をしている場合、他ノードからの Trap を受信できない問題などがあります。

以下の手順に従って設定を削除して下さい。

1. /etc/snmp/snmptrapd.conf を開き、以下の”**udp6:162**”を削除する。

修正前：

```
snmpTrapdAddr udp:162,udp6:162
```

修正後：

```
snmpTrapdAddr udp:162
```

2. snmptrapd の状態を確認した上で、正常に起動することを確認します。

■ snmptrapd が停止している状態

```
# /sbin/service snmptrapd status
snmptrapd は停止しています
# /sbin/service snmptrapd start
snmptrapd を起動中:                                [  OK  ]
#
```

■ snmptrapd が起動している状態

```
# /sbin/service snmptrapd status
snmptrapd (pid  xxxx) を実行中...
# /sbin/service snmptrapd restart
snmptrapd を停止中:                        [  OK  ]
snmptrapd を起動中:                        [  OK  ]
#
```

2) SVmco-1.6.0-0 版以前からのアップデートかつ

PSA-MMB 間通信 LAN の IP をデフォルト設定から変更している環境の場合、下記の設定ファイルの修正が必要になります。

以下の手順に従って設定を修正して下さい。

1. /etc/sysconfig/network-scripts/ifcfg-ethx を開き、バックアップしたファイルと同じ内容に修正します。なお、文頭の PSA-MMB LAN に関してのコメント行は修正しないでください。

   * ifcfg-ethx の末尾の x は PSA-MMB 間通信 LAN のネットワークインターフェースの番号です。

2. ネットワークを再起動します。

```
# /sbin/service network restart
```

SVmco アップデート時の注意事項

- PRIMECLUSTER のシステムにおける SVmco のアップデートを行う際は、PRIMECLUSTER 導入運用手引書に従い、該当ノードの PRIMECLUSTER を停止した上　で実施してください。
- SVmco アップデート、及び SVmco 再起動時には SVmco の PRIMECLUSTER 連携機能が一時停止するため、以下の 2 種類の PRIMECLUSTER のメッセージの何れかが出力されることがあります。

  7210 An error was detected in MMB.

  SA SA_mmbp.so to test host <nodename> failed

- SVmco アップデート時に以下のメッセージが出力されることがありますが、動作上問題はありません。

  /sbin/ldconfig: <ライブラリ名> is not a symbolic link

- SVmco1.3 版以前からのアップデートでは、PRIMECLUSTER 連携の為の IPv4 用管理 LAN IP アドレスの設定ファイル ipsetup.conf 内にあるパラメータ”IPVersion”の設定項目は追加されません。

  パラメータを追加しない場合は、管理 LAN の IP 種別は IPv4 として動作します。

2.1.9 SIRMS のアップデートインストール

Red Hat Enterprise Linux での SIRMS のアップデートインストール方法について説明します。

以下のコマンドで SIRMS 関連のパッケージのアップデートインストールを実行します。

【入力形式】

```
/bin/rpm -Uvh sirms-X.X.X-X.i386.rpm (*)
```

*：X.X.X-X は版数です。

2.1.10 SVmco のアンインストール

Red Hat Enterprise Linux での SVmco のアンインストール方法について説明します。

以下のコマンドの順番で、SVmco のサービスを停止してから、SVmco パッケージをアンインストールします。

また、SVmco のアンインストールを実施する前に、バックアップ手順を実施してください。バックアップ手順について詳しくは、「2.1.12 SVmco のバックアップ」を参照してください。

【入力形式】

```
/sbin/service y30SVmco stop
/bin/rpm -e SVmco
```

注意

- iptables が停止状態の場合、インストール時に iptables に追加した SVmco 用の設定が削除されません。手動で削除して下さい。

2.1.11 SIRMS のアンインストール

Red Hat Enterprise Linux での SIRMS のアンインストール方法について説明します。

以下のコマンドで SIRMS 関連のパッケージをアンインストールします。

【入力形式】

```
/bin/rpm -e  sirms
```

2.1.12 SVmco のバックアップ

ここでは、SVmco の設定ファイル・ファイアウォール設定のバックアップ手順を説明します。バックアップのデータは、トラブル復旧時に必要です。SVmco のアップデートインストール及び SVmco のアンインストールを実施する前にバックアップすることを推奨します。

下記手順に従って、SVmco の設定ファイル・ファイアウォール設定を退避します。また、下記手順では例として/home/tmp/SVmco_backup/を退避ディレクトリとしています。退避前に作成してください。

```
# iptables-save > /home/tmp/SVmco_backup/iptables_backup                ※1
# cp -pr /etc/fujitsu/SVmco/usr/ /home/tmp/SVmco_backup/
# cp -p /etc/fujitsu/SVmco/local/set.node /home/tmp/SVmco_backup/       ※2
# cp -p /etc/snmp/snmptrapd.conf /home/tmp/SVmco_backup/
# cp -p /etc/sysconfig/snmptrapd /home/tmp/SVmco_backup/
# cp -p /etc/sysconfig/network-scripts/ifcfg-ethx /home/tmp/SVmco_backup/ ※3
```

※1：iptables-save コマンドは、iptables の設定を表示するコマンドです。

※2：set.node ファイルは PRIMECLUSTER/PRIMESOFT 環境のみ存在します。

※3：ifcfg-ethx の末尾の x は PSA-MMB 間 LAN のネットワークインターフェースの番号です。PSA-MMB 間通信 LAN 用ネットワークインターフェースの bus-info(SEG:BUS:DEV.FUNC 番号) が以下になります。PSA-MMB 間通信 LAN を判別する方法について詳しくは、「2.1.1 PSA-MMB 間通信 LAN の設定」を参照してください。

```
0000:00:19.0
```

2.1.13 SVmco のリストア

ここでは、トラブル発生時（例：SVmco のアップデートインストール時に失敗する場合）、SVmco のリストア手順を説明します。

以下の説明は、作業ディレクトリ (以下、$WORK_DIR と呼びます) 内に SVmco のパッケージ (バックアップした SVmco と同じ版数) が展開され、ディレクトリ "SVmco" が作成されていることを前提としています。 本作業は root 権限で行ってください。

また、下記手順では例として/home/tmp/SVmco_backup/を退避ディレクトリとし、バックアップのデータが既に取得されていることを前提としています。バックアップ手順について詳しくは、「2.1.12 SVmco のバックアップ」を参照してください。

1. SVmco をアンインストールします。

```
# rpm -e SVmco
```

2. 以下ディレクトリが存在しないことを確認します。

```
/etc/fujitsu/SVmco
/opt/fujitsu/SVmco
/var/fujitsu/SVmco
```

   上記ディレクトリが存在する場合、該当ディレクトリを手動で削除します。

   例：/opt/fujitsu/SVmco にファイル・ディレクトリが残る場合

```
# rm -fr /opt/fujitsu/SVmco
```

3. SVmco の作業ディレクトリ内に移動します。

```
# cd $WORK_DIR/SVmco
```

4. SVmco を新規インストールします。

```
# ./INSTALL.sh
```

5. 退避した設定ファイル・ファイアウォール設定をリストアします。

```
# iptables-restore /home/tmp/SVmco_backup/iptables_backup          ※1
# service iptables save
# \cp -prf /home/tmp/SVmco_backup/usr /etc/fujitsu/SVmco/           ※2
# cp -pf /home/tmp/SVmco_backup/set.node /etc/fujitsu/SVmco/local/  ※3
# \cp -pf /home/tmp/SVmco_backup/snmptrapd.conf /etc/snmp/          ※2
# \cp -pf /home/tmp/SVmco_backup/snmptrapd /etc/sysconfig/          ※2
# \cp -pf /home/tmp/SVmco_backup/ifcfg-ethx /etc/sysconfig/network-scripts/
                                                                    ※4
```

※1: iptables-restore コマンドは iptables のルールをリストアするためのコマンドです。

※2: cp コマンドの先頭に「\」（バックスラッシュ）を付けている理由は、ファイルの上書き警告を出力しないようにするためです。

※3: set.node ファイルは PRIMECLUSTER/PRIMESOFT 環境のみ存在します。

※4: ifcfg-ethx の末尾の x は PSA-MMB 間 LAN のネットワークインターフェースの番号です。

6. OS を再起動します。

```
# reboot
```

7. SVmco の起動確認をします。

   シスログに下記のメッセージが出力されることを確認します。

```
SVmco: I 00502 MMBA MMB connected
SVmco: I 00069 SVPM startup succeeded
 (/etc/fujitsu/SVmco/global/pmsvmco.conf)
```

8. インストール成功後、退避ファイルを手動で削除します。

```
# rm -fr /home/tmp/SVmco_backup
```

2.2 SVmco の設定 (Windows Server 2008/2012)

OS インストール後、SVmco を動作させるため必要な設定の確認と、使用できる機能について説明します。設定は Administrator 権限で作業を行ってください。

SVmco 動作に必要な設定確認と使用できる機能

必須／必要に応じて	設定項目	自動設定 (*1)／手動設定 (*2)	参照先
必須	PSA-MMB 間通信 LAN の設定	手動設定	2.2.1　PSA-MMB 間通信 LAN の設定
	管理 LAN の設定確認	手動設定	2.2.2　管理 LAN の設定確認
	PSHED Plugin ドライバのインストール	手動設定	2.2.3PSHED Plugin ドライバのインストール
	Windows ファイアーウォールの設定	手動設定	2.2.4　Windows ファイアーウォールの設定

必須／必要に応じて	設定項目	自動設定 (*1)／手動設定 (*2)	参照先
	管理 LAN IP アドレスの設定	手動設定	2.2.5　管理 LAN IP アドレスの設定 (*3)
必要に応じて	トラップ送信先の設定	手動設定	2.2.6 パーティションからのトラップ送信先の設定
	STOP エラー (致命的なシステムエラー) 発生後の Watchdog 監視設定	手動設定	2.2.7 STOP エラー (致命的なシステムエラー) 発生後の Watchdog 監視設定
	SVmco のアップデートインストール	対象外	2.2.8 SVmco のアップデートインストール
	SIRMS のアップデートインストール	対象外	2.2.9　SIRMS のアップデートインストール
	SVmco のアンインストール (*4)	対象外	2.2.10　SVmco のアンインストール
	SIRMS のアンインストール	対象外	2.2.11　SIRMS のアンインストール

*1：自動設定：SVmco インストール時に自動設定されています。自動設定の内容の変更が必要な場合があるので、上記表の参照先を確認してください。

*2：手動設定：SVmco インストール時には設定されていません。上記表の参照先のとおり設定してください。

*3：ServerView Agents v6.20 版以降では、管理 LAN 設定コマンドを実行するユーザーが ServerView SNMP agents のセキュリティ設定で設定したユーザグループに属している事が必要な場合があります。

ユーザーグループの設定値は、Agent Configuration ツールの「セキュリティ設定」タブのユーザーグループで確認して下さい。

ユーザーグループ	対処
FUJITSU SVUSER	手動でグループを作成してから管理 LAN 設定コマンドを実行するユーザーをグループメンバーとして追加

	して下さい。
空欄	対処は必要無し。
FUJITSU SVUSER 以外	手動でグループを作成してから管理 LAN 設定コマンドを実行するユーザーをグループメンバーとして追加して下さい。
無効(グレースケール) ※パスワードによる保護が無効の場合	対処は必要無し。

手動でのユーザーグループの作成方法については、『ServerView Agents インストールガイド』3.6.1 章 ”管理ユーザー”を参照して下さい

*4：PRIMEQUEST 1000x2 シリーズ運用時は、必ず SVmco をインストールしてください。SVmco をアンインストールすると、以下の制限があります。

- REMCS 契約時にパーティション上の異常が通知されません。
- PCI カードの活性保守ができない。必ずパーティション停止保守となる。

備考

- SVIM を使用して OS をインストールするときに、SVmco も同時にインストールされます。SVIM について詳しくは、『ServerView Installation Manager』を参照してください。
- SVmco をインストールすると、OS 側の REMCS 機能として必要なコンポーネントがインストールされます。REMCS の設定は当社技術員が実施します。SVmco インストール時に、SVmco 動作のための設定が以下のように自動的に追記または変更されます。

注意

SVmco インストール時に自動追記／変更された設定については、設定変更を行わないでください。SVmco が正常に動作できなくなる場合があります。

SVmco インストール時に自動追記／変更される設定

項目	説明
1. サービスの設定	● ServerView Mission Critical Option ● PRIMEQUEST PEM Command Service PRIMEQUEST Environment Control Service
2. 環境変数の設定	● PATH 変数：既存の PATH 変数に SVmco が使用する値が追加される。 ● SVmco_INSTALLPATH 変数：新規に変数が追加される。

項目	説明
3. SNMP のセキュリティ設定	PRIMEQUEST の場合、SVagent が MMB からの SNMP パケットを受け付ける必要があるため、SNMP Service のセキュリティを設定する。 SVmco インストール時に、[SNMP Service] の[プロパティ] 画面のセキュリティタブで選択されている項目により処理が異なる。 ● [すべてのホストから SNMP パケットを受け付ける] が選択されている場合： SNMP のセキュリティ設定はしない。 ● [これらのホストから SNMP パケットを受け付ける] が選択されている場合：MMB の IP アドレスと、localhost が設定されていない場合に、localhost を SNMP のセキュリティで設定する。
4. WMI (Windows Management Instrumentation) の設定	SVmco は Windows に標準でインストールされる WMI を利用して、MMB に対して、IPMI 経由で PCI カード情報を通知する。 このとき、RAID 装置などの LUN 数が多い場合、WMI が収集するために使用するメモリサイズや内部ハンドル数が不足することがあるため、以下の値に設定を変更する。 ● 使用メモリ上限サイズ：536,870,912 byte (OS 初期値) ● 内部ハンドルの上限数：65,536

備考

- 以下の場合は、SNMP セキュリティ設定コマンド (setsnmpsec) を実行します。コマンドについて詳しくは、「3.5 SNMP セキュリティ設定コマンド (setsnmpsec)」を参照してください。
  - SVmco インストール後に SNMP Service のセキュリティ設定を [すべてのホストから SNMP パケットを受け付ける] から [これらのホストから SNMP パケットを受け付ける] に変更する場合
  - MMB の IP アドレスを変更する場合

- MMB の IP アドレスおよびパーティション側の管理 LAN の IP アドレスを変更した場合は、必ず SVmco を再起動してください。再起動しない場合、SVagent で検出するエラーの通知ができません。

■ Windows Server 2008/2012 設定時の注意

- イベントビューアのシステムログ、アプリケーションログのプロパティで [ログサイズが最大値に達した時の操作] を [イベントを上書きしない] に変更しないでください。ログサイズが最大値に達した場合、それ以降にエラーが発生してもログに出力されないため、SVagent で検出できません。
- 以下のレジストリの値を 20000 (20 秒) 未満に設定すると、OS のシャットダウン時にハングアップする可能性があります。このためレジストリの値は、必ず 20000 (20 秒) 以上に設定してください。

```
HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control"
WaitToKillServiceTimeout" (種類: REG_DWORD / Default:20000)
```

上記のレジストリで、シャットダウン時にサービスを終了させるまでの待ち時間 (ms) を指定できます。

2.2.1 PSA-MMB 間通信 LAN の設定

ここでは、PSA-MMB 間通信 LAN の設定の確認について説明します。

SVmco が MMB と通信するため、パーティション側の PSA-MMB 間通信 LAN に接続されたネットワークインターフェースカード (NIC) が活性化されている必要があります。

PSA-MMB 間通信 LAN の設定は、以下の手順を実施してください。

注意

下記の場合、イベント通報機能が使用できません。

- MMB Web-UI の [Network Configuration] - [Network Interface] 画面にて、[MMB-PSA IP Address] の [Interface] が Disable の場合
- 以下の操作 (PSA-MMB 間通信 LAN 設定コマンドの実行) を行わない場合

1. PSA-MMB 間通信 LAN 設定コマンドを実行します。

   [SVmco インストール先フォルダ] ¥opt¥fujitsu¥SVmco¥sh¥setpsalan.bat

注意

- SVmco インストール後に OS を再起動しないと、手順 1 の PSA-MMB 間通信 LAN 設定コマンドが失敗します。

  OS を再起動してから、PSA-MMB 間通信 LAN 設定コマンドを実行してください。

- PSA-MMB 間 LAN のネットワークインターフェース”SVMCONIF”が既に存在している場合、PSA-MMB 間 LAN の設定が実行されません。再設定が必要な場合は、ネットワークインターフェース名前を”SVMCONIF”以外の名前に変更して PSA-MMB 間通信 LAN 設定コマンドを実行して下さい。

2. OS を再起動します。

   注意

   続けて「2.2.3 PSHED Plugin ドライバのインストール」を行う場合は、ここで OS を再起動する必要はありません。2.2.3 のインストール完了時に OS を再起動してください。

上記の手順を行うと、以下の値が設定されます。

<IP アドレス>

172.30.0.<パーティション ID + 2>/24

例) パーティション ID が 2 の場合

172.30.0.4/24

<通信設定>

Auto Negotiation off

Speed 100Mbps

Duplex full

<ネットワークインターフェース>

PSA-MMB 間通信 LAN のネットワークインターフェース名を”SVMCONIF”に変更

以下の場合に限り、IP アドレスの設定を変更してください。

- 自動設定される IP アドレスが、業務ネットワークや管理ネットワークで使用する IP アドレスやサブネットと重なってしまう
- 別パーティションから複製したディスクを使用して新たにパーティションを構築した
- あるパーティションでイントールしたディスクを別のパーティションに移して使用するなどで、パーティション ID が変更となる
- Windows クラスタ(MSCS)を "筐体間クラスタ／同一パーティション番号" 間でクラスタ構成を構築する (同じ IP アドレスが割り振られるため、構成チェックで「重複 IP アドレスが見つかりました」というエラーが発生する。)

IP アドレスの設定は、以降の手順で変更してください。なお、上記の 1.の理由で設定を変更する場合は、同一筐体に存在する全パーティション、および MMB 側の PSA-MMB 間通信 LAN の IP アドレスも同一サブネットの IP アドレスに変更する必要があります。MMB 側の IP アドレスは、MMB Web-UI から設定してください。

注意

- 通信設定については、自動的に設定された値から変更しないでください。変更した場合、PSA-MMB 間の通信が不通となり、SVmco の機能を使用できなくなることがあります。
- PSA-MMB 間 LAN 設定は、SVmco インストール後に変更してください。SVmco インストール前に変更した場合、インストール時に設定が上書きされます。

■ PSA-MMB 間通信 LAN 用のネットワークアダプターの設定

以下の手順で、ネットワークアダプターを設定します。

操作手順

1. [コントロールパネル] - [ネットワーク接続] の順に選択します。

   →ネットワークの一覧が表示されます。

2. 表示された一覧から [SVMCONIF] を選択し、マウスの右クリックメニューから [プロパティ] を選択します。

注意

- 名前が[SVMCONIF] となっている接続が存在しない場合、SVmco がインストールされていない可能性があります。必ず SVmco をインストールした後に設定を変更してください。
- 接続名 [SVMCONIF] は変更しないでください。変更した場合、SVmco アップデート時に自動設定の値に上書きされる可能性があります。

3. [インターネットプロトコル バージョン 4(TCP/IP)] を選択し、[プロパティ] ボタンをクリックします。

   → [インターネットプロトコル バージョン 4 (TCP/IP)のプロパティ] が表示されます。

4. IP アドレス、サブネットマスクを設定します。

注意

- MMB-PSA 間 LAN は、筐体内部通信用のネットワークのため、DNS の設定は不要です。エラーメッセージが表示された場合も無視して次に進んでください。
- IP アドレスは同一筐体内で重複しない値を設定して下さい。

5. SVmco の設定ファイルに、PSA-MMB 間通信 LAN の IP アドレスを設定します。

ファイル格納場所：[SVmco インストール先フォルダ]
¥etc¥fujitsu¥SVmco¥usr¥tommbipsetup.conf

設定値：手順 4.で設定した IP アドレスを入力する。

<設定例>

```
[NETWORK]
TOMMBIP=172.30.0.4 （手順 4 で設定した IP アドレス）
```

注意

[NETWORK]および TOMMBIP=の前に;でコメントアウトされている場合には、;を削除して設定してください。

6. PSA-MMB 間通信 LAN 用 NIC の設定を反映させるため、以下の手順で SVmco を再起動します。

   [コントロールパネル] - [管理ツール] - [サービス] の順に選択します。

   右ウィンドウで [ServerView Mission Critical Option]を右クリックし、[再起動] を選択します。

・ リモートデスクトップ接続で設定

リモートデスクトップ接続を使用して PSA-MMB 間通信 LAN を設定する場合は、コンソールセッションに接続する必要があります。以下の手順で接続してください。

1. [スタート] - [ファイル名を指定して実行] を選択します。

   → [ファイル名を指定して実行] ダイアログボックスが表示されます。

2. [名前] ボックスに "mstsc /v:<servername/ip address> /console" を入力して [OK] ボタンをクリックします。

<servername/ip address>には、接続先サーバ名または IP アドレスを指定してください。(クラスタの仮想 IP アドレスは指定できません。)
mstsc のオプションの詳細は、mstsc /?を入力して確認できます。

注意

PRIMEQUEST 環境では、MMB との通信に使用する管理 LAN に接続するスイッチの STP 機能を OFF にする必要があります。

2.2.2 管理 LAN の設定確認

Systemwalker などの上位ソフトウェアとの連携を行う場合は、パーティション上の管理 LAN の設定が必要です。管理 LAN について詳しくは、『PRIMEQUEST 1000 シリーズ 運用管理マニュアル』(C122-E108) の「1.3 管理 LAN」を参照してください。

管理 LAN ネットワークの設定、および必要に応じてチーミング、GLS などによる二重化設定を行ってください。

また、上記管理 LAN のネットワーク設定完了後、「2.2.5 管理 LAN IP アドレスの設定」を実施してください。

注意

PRIMEQUEST 環境では、MMB との通信に使用する管理 LAN に接続するスイッチの STP 機能を OFF にする必要があります。

2.2.3 PSHED Plugin ドライバのインストール

PSHED Plugin ドライバとは、Windows Hardware Error Architecture (WHEA) の拡張機能のためのドライバです。

本ドライバは、自動でインストールされません。以下のフォルダに格納されているバッチファイル (plugin_install.bat) を使用して、手動でインストールしてください。

- Windows Server 2008/2008 R2 の場合

[SVmco インストール先フォルダ] ¥fjpsaplg¥plugin_install.bat

(例. C:¥Program Files (x86)¥Fujitsu¥ServerView Suite¥SVmco¥fjpsaplg¥plugin_install.bat)

- Windows Server 2012/2012 R2 の場合

[SVmco インストール先フォルダ] ¥fjpsaplg_WS2012¥plugin_install.bat

(例. C:¥Program Files (x86)¥Fujitsu¥ServerView Suite¥SVmco¥fjpsaplg_WS2012¥plugin_install.bat)

備考

本ドライバをインストールしないと以下の機能が動作しません。

- Correctable Error 発生時のイベント ビューア (Windows ログ:システム) へのログ抑止
- ブルースクリーン発生時の Stop Error への状態遷移 (MMB Web-UI の [Power Control] 画面の [System Progress])

注意

- インストール用バッチの実行は複数回実行しないでください。

  複数回実行すると、インストール用のバッチの動作上、実行した回数分だけ PRIMEQUEST PSHED Plugin ドライバがインストールされます。
- インストール用のバッチを誤って複数回実施してしまった場合、動作上問題はありませんが、デバイスマネージャの表示では、PRIMEQUEST PSHED Plugin ドライバが複数表示されます。

この場合は、以下の手順に従って PRIMEQUEST PSHED Plugin ドライバをいったんすべてアンインストールした後、再度インストールを行ってください。再インストール時に、OS の再起動が必要です。

1. デバイス マネージャの [システム デバイス] 上に、[PRIMEQUEST PSHED Plugin Driver] が表示されている数を記録します。
2. 以下の PSHED Plugin ドライバ アンインストール用バッチを、手順 1 で記録した回数分、実行します。

> PSHED Plugin ドライバ アンインストール用バッチ格納場所：
>
> **- Windows Server 2008/2008 R2 の場合**
>
> [SVmco インストール先フォルダ] ¥fjpsaplg¥plugin_uninstall.bat
>
> (デフォルト. C:¥Program Files (x86)¥Fujitsu¥ServerView Suite¥SVmco¥fjpsaplg¥plugin_uninstall.bat)
>
> **- Windows Server 2012/2012 R2 の場合**
>
> [SVmco インストール先フォルダ] ¥fjpsaplg_WS2012¥plugin_uninstall.bat
>
> (デフォルト. C:¥Program Files (x86)¥Fujitsu¥ServerView Suite¥SVmco¥fjpsaplg_WS2012¥plugin_uninstall.bat)

3. OS を再起動します。
4. デバイスマネージャの [システム デバイス] に [PRIMEQUEST PSHED Plugin Driver] が表示されていないことを確認します。
5. 以降の「■　操作手順」に従って、再度 PRIMEQUEST PSHED Plugin ドライバをインストールします。

■ 操作手順

1. 以下のフォルダを開き、[plugin_install.bat] をダブルクリックします。

> **- Windows Server 2008/2008 R2 の場合**
>
> [SVmco インストール先フォルダ] ¥fjpsaplg
>
> (例. C:¥Program Files (x86)¥Fujitsu¥SVmco¥fjpsaplg)

- **Windows Server 2012/2012 R2 の場合**

[SVmco インストール先フォルダ] ¥fjpsaplg_WS2012

(例. C:¥Program Files (x86)¥Fujitsu¥SVmco¥fjpsaplg_WS2012)

2. OS を再起動してください。本ドライバは、OS の再起動後から動作します。
3. **デバイスマネージャのシステムデバイス上に [PRIMEQUEST PSHED Plugin Driver] が表示されていることを確認します。表示されていない場合は、手順 1.から再度実行してください。**

2.2.4 Windows ファイアーウォールの設定

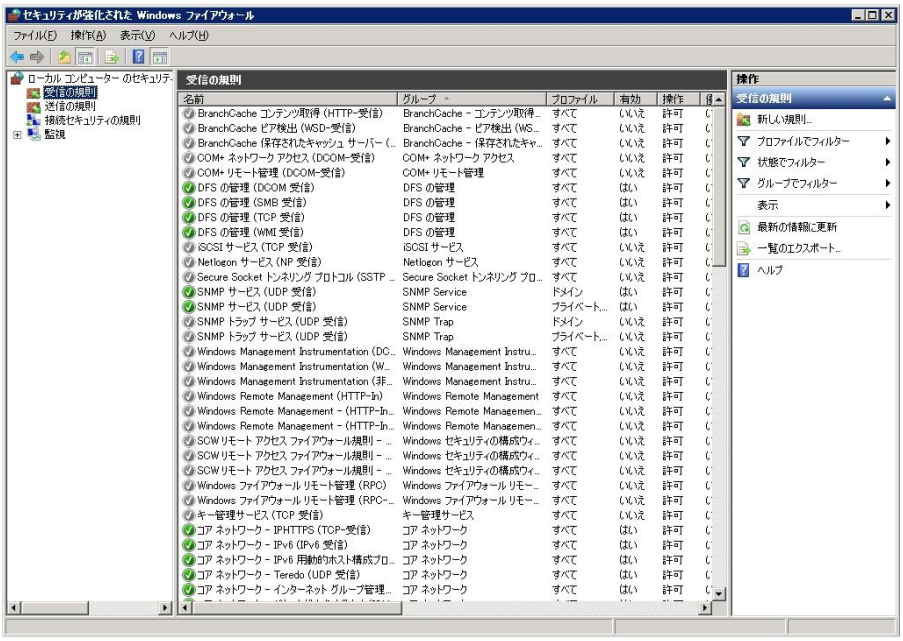
Windows ファイアーウォールを有効にして運用する場合、以下のポートは MMB とのデータ送受信に使用されるため、開放する必要があります。

- SNMP Service が使用する UDP:161 ポート (MMB からの受信)
- svmcommbs.exe が使用する MMB への送信ポート (MMP 側 TCP:5000 ポート用)
- svmcommbs.exe が使用する MMB への ICMP プロトコル

■ 操作手順

1. [スタート] - [管理ツール] - [セキュリティが強化された Windows ファイアウォール] の順に選択します。

2. [セキュリティが強化された Windows ファイアウォール] 画面が表示されます。左ペインから [受信の規則] をクリックすると、中央ペインに [受信の規則] 一覧が表示されます。

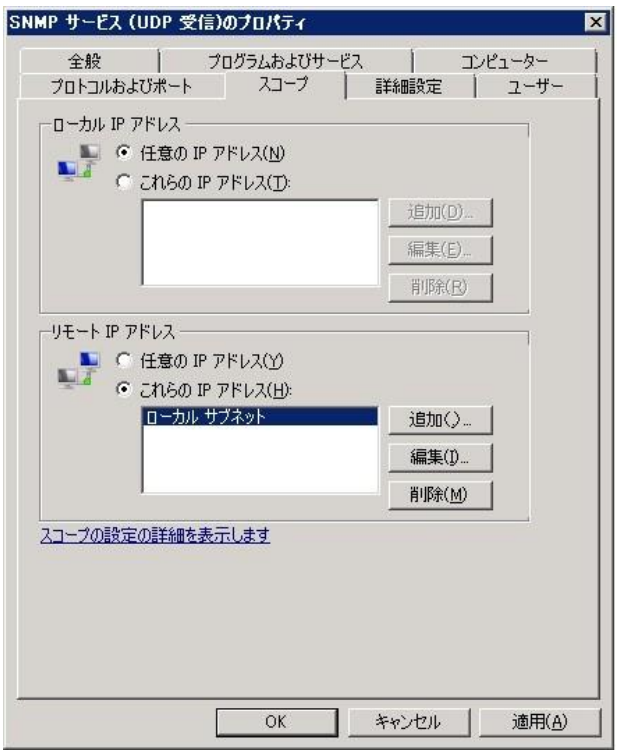


[Windows ファイアウォール] 画面

3. [受信の規則] 一覧の中にある [SNMP サービス (UDP 受信)] を選択して右クリックし、[プロパティ] をクリックします。

   [SNMP サービス (UDP 受信)] は初期値で、プロファイル項が [ドメイン] のものと [プライベート,パブリック] のものの 2 行が存在します。手順 3.～手順 7 は両方の行に対して実施してください。

4. [SNMP サービス (UDP 受信) のプロパティ] ダイアログボックスが表示されます。[全般] タブをクリックし、[全般] 項の中にある [有効] のチェックボックスをオンにします (初期値ではチェックマークが入っています)。

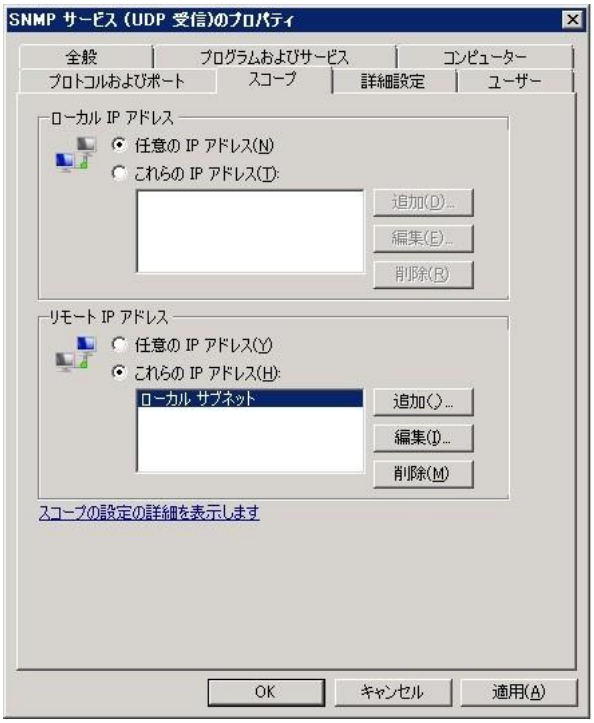


SNMP サービス (UDP 受信) のプロパティ [全般] タブ

5. [スコープ] タブをクリックします。

[ローカル IP アドレス] では [任意の IP アドレス] を選択します。

[リモート IP アドレス] では [これらの IP アドレス] を選択し、[追加] ボタンをクリックします。



SNMP サービス (UDP 受信) のプロパティ [スコープ] タブ

6. [IP アドレス] 画面が表示されます。[事前に定義されたコンピュータセット] を選択します。 リストから [ローカルサブネット] を選択し、[OK] ボタンをクリックします。

[IP アドレス] 画面

7. [OK] ボタンをクリックし、[SNMP サービス (UDP 受信) のプロパティ] ダイアログボックスを閉じます。

8. [セキュリティが強化された Windows ファイアウォール] 画面の左ペインから [送信の規則] をクリックします。

   中央ペインに [送信の規則] 一覧が表示されます。

9. [セキュリティが強化された Windows ファイアウォール] 画面の右ペインから [新しい規則] または [新規の規則] をクリックします。[新規の送信の規則のウィザード] 画面が開き、左上に [規則の種類] と表示されます。[カスタム] を選択し、[次へ] ボタンをクリックします。

10. 左上に [プログラム] と表示されます。[このプログラムのパス] を選択し、[参照] ボタンをクリックします。" svmcommbs.exe" を選択し、[次へ] ボタンをクリックします。

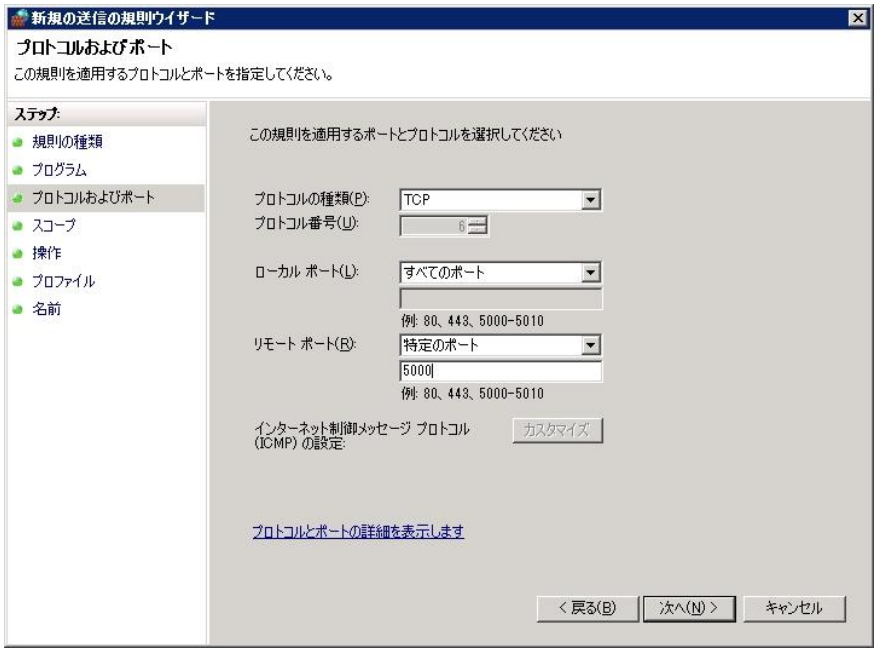
備考

svmcommbs.exe は SVmco のインストールパス配下の opt¥fujitsu¥SVmco¥bin¥にあります。SVmco のインストールパスは初期値で Program Files¥fujitsu¥ServerView Suite¥SVmco¥です。

11. 左上に [プロトコルおよびポート] と表示されます。以下の項目を選択または入力して、[次へ] ボタンをクリックします。

    プロトコルおよびポート] の設定項目

画面項目	選択または入力する値
[プロトコルの種類]	[TCP]
[ローカルポート]	[すべてのポート]
[リモートポート]	[特定のポート]を選択し、下のテキストボックスに「5000」と入力する。



新規の送信の規則ウィザード - プロトコルおよびポート

12. 左上に [スコープ] と表示されます。以下の項目を選択または入力して、[次へ] ボタンをクリックします。

[スコープ] の設定項目

画面項目		選択または入力する値
Windows2008	Windows2008R2 Windows2012	
[この規則はどのローカル IP アドレスに一致しますか?]	この規則を適用するローカル IP アドレスを選択してください。	[任意の IP アドレス]

画面項目		選択または入力する値
Windows2008	Windows2008R2 Windows2012	
[この規則はどのリモート IP アドレスに一致しますか?]	この規則を適用するリモート IP アドレスを選択してください。	[これらの IP アドレス] を選択し、[追加] ボタンをクリックする。 MMB の PSA-MMB 通信 LAN 用 IP アドレスを入力する。

13. 左上に [操作] と表示されます。[接続を許可する] を選択し、[次へ] ボタンをクリックします。

14. 左上に [プロファイル] と表示されます。[ドメイン] 、[プライベート]、[パブリック] すべてのチェックボックスをオンにして、[次へ] ボタンをクリックします。

15. 左上に [名前] と表示されます。[名前[N]:] に「MCOMMBS」と入力し、[完了] ボタンをクリックします。

16. 続けて [セキュリティが強化された Windows ファイアウォール] 画面の右ペインから [新しい規則] または [新規の規則] をクリックします。[新規の送信の規則のウィザード] が開き、左上に [規則の種類] と表示されます。[カスタム] を選択し、[次へ] ボタンをクリックします。

17. 左上に [プログラム] と表示されます。[このプログラムのパス] を選択し、[参照] ボタンをクリックします。[svmcommbs.exe] を選択し、[次へ] ボタンクリックします。

備考

svmcommbs.exe は SVmco のインストールパス配下の opt¥fujitsu¥SVmco¥bin¥にあります。SVmco のインストールパスは初期値で Program Files¥fujitsu¥ServerView Suite¥SVmco¥です。

18. 左上に [プロトコルおよびポート] と表示されます。[プロトコルの種類] で [ICMPv4] を選択し、[次へ] ボタンをクリックします。

新規の送信の規則ウィザード - プロトコルおよびポート

19. 左上に [スコープ] と表示されます。以下の項目を選択または入力して、[次へ] ボタンをクリックします。

    [スコープ] の設定項目

画面項目		選択または入力する値
Windows2008	Windows2008R2 Windows2012	
[この規則はどのローカル IP アドレスに一致しますか?]	この規則を適用するローカル IP アドレスを選択してください。	[任意の IP アドレス]
[この規則はどのリモート IP アドレスに一致しますか?]	この規則を適用するリモート IP アドレスを選択してください。	[これらの IP アドレス] を選択し、[追加] ボタンをクリックする。 MMB の PSA-MMB 通信 LAN 用 IP アドレスを入力する。

20. 左上に [操作] と表示されます。[接続を許可する[A]] を選択し、[次へ] ボタンをクリックします。

21. 左上に [プロファイル] と表示されます。[ドメイン]、[プライベート]、[パブリック] すべてのチェックボックスをオンにして、[次へ] ボタンをクリックします。

22. 左上に [名前] と表示されます。[名前[N]:] に「MCOICMP」と入力し、[完了] ボタンをクリックします。

2.2.5 管理 LAN IP アドレスの設定

パーティション上の管理 LAN の IP アドレスを設定します。

注意： 使用している ServerView Agents が v6.20 版以降の場合:

管理 LAN 設定コマンドを実行するユーザーが ServerView SNMP agents のセキュリティ設定で設定したユーザグループに属している事が必要な場合があります。

ユーザーグループの設定値は、Agent Configuration ツールの「セキュリティ設定」タブのユーザーグループで確認して下さい。

ユーザーグループ	対処
FUJITSU SVUSER	手動でグループを作成してから管理 LAN 設定コマンドを実行するユーザーをグループメンバーとして追加して下さい。
空欄	対処は必要無し。
FUJITSU SVUSER 以外	手動でグループを作成してから管理 LAN 設定コマンドを実行するユーザーをグループメンバーとして追加して下さい。
無効(グレースケール) ※パスワードによる保護が無効の場合	対処は必要無し。

手動でのユーザーグループの作成方法については、『ServerView Agents インストールガイド』3.6.1 章 ”管理ユーザー”を参照して下さい。

以下、管理 LAN IP アドレスの設定手順です。

1. "ServerView Server Control"サービスが起動している事を確認してください。

起動していない場合は、下記の手順で、SVagent を起動してください。

■ SVagent の起動

1. [スタートメニュー] → [管理ツール] → [サービス] の順にクリックします。
2. 右側のウィンドウで [ServerView Server Control] を選択します。
3. メニューバーから [操作] → [起動] の順にクリックし、[ServerView Server Control]を起動します。

2. 設定ファイルを編集します。

設定内容は管理 LAN で使用している通信プロトコルによって異なります。

➢ **IPv4 で使用している場合**

1. [SVmco インストール先フォルダ] ¥etc¥fujitsu¥SVmco¥usr¥ipsetup.conf ファイルを編集します。

エディタなどを使用し、以下の IP アドレスを修正します。

【入力形式】

```
[NETWORK]
ManagementIP=<管理 LAN 用 IP アドレス>
```

【入力例】

```
[NETWORK]
ManagementIP=192.168.0.1
```

2. 下記コマンドを実行してください。

```
MgmtIP.exe -f
```

コマンド実行後、以下のメッセージが出力されれば完了です。

```
MgmtIP: new management IP address “管理 LAN 用 IP アドレス” stored
```

2.2.6 パーティションからのトラップ送信先の設定

パーティションから直接、SVagent, SV RAID のトラップを送信する場合は、以下の手順でトラップ送信先の設定を行います。

備考

- Windows の場合、SNMPv3 は未サポートです。
- 本設定は、必要な場合のみ実施してください。運用管理ソフトウェアがパーティションごとにイベントを管理する場合には本設定が必要になります。

  SNMP トラップをつかったハードウェアの異常監視については、下記のマニュアルを参照して下さい。

  「PRIMEQUEST 1000 シリーズ Windows ネットワーク設計ガイド」付録 C ”SNMP トラップを使ったハードウェア異常監視”

- トラップ送信先では、トラップ受信用のアプリケーションや管理マネージャが動作していて、SNMP サービスの標準トラップが受信できる必要があります。

■ 操作手順

1. [スタートメニュー] → [管理ツール] → [サービス] の順にクリックします。
2. 右側のウィンドウで [SNMP Service] をダブルクリックします。

→ [SNMP Service] 画面が表示されます。

3. [トラップ] タブをクリックします。
4. [コミュニティ名] に設定するコミュニティ名を入力し、[一覧に追加] をクリックします。
5. [トラップ送信先] の [追加] をクリックします。
6. トラップを受信する (通知を送る先の) サーバのホスト名または IP アドレスを入力し、[追加] をクリックします。
7. [OK] をクリックします。
8. [操作] - [再起動] の順に選択し、SNMP Service を再起動します。

■ トラップ送信先設定確認方法について

トラップ送信先設定を確認するには、上記の手順 10.で SNMP サービスを再起動するときの、SNMP サービス標準トラップを使用します。このトラップの受信可否により、正しく設定されているかを確認できます。

備考

トラップ送信先では、トラップ受信用のアプリケーションや管理マネージャが動作していて、SNMP サービスの標準トラップが受信できる必要があります。

トラップ送信元マシン上では、手順 10.を実行することにより、SNMP サービスを再起動します。

本操作により、トラップ送信先では、トラップ受信用のアプリケーションに、"ColdStart" の SNMP Service 標準トラップが通知されます。

参考に、トラップ送信先が Linux マシンの場合、[snmptrapd] でトラップ受信したときに、以下のようなメッセージがシステムログに表示されます。

```
Aug 17 14:50:03 pq-server snmptrapd[2600]: 2005-08-17 14:50:03 ¥
pq-server.fujitsu.com
[192.168.0.162] (via 192.168.0.162) TRAP,  SNMP v1, community ¥
public SNMPv2-SMI::
```

```
enterprises.211.1.31.1.2.100.3 Cold Start Trap (0) Uptime: 0:00:00.00
```

¥：改行しないことを表す。

2.2.7 STOP エラー (致命的なシステムエラー) 発生後の Watchdog Timer 監視設定

システムで STOP エラー (致命的なシステムエラー) が発生した場合は、以下の状態になります。

- MMB の Web-UI の [Partition] - [Power Control] で、該当パーティションの System Progress が "Stop Error" 表示
- OS がメモリダンプの取得処理を実行

上記の場合、何らかの理由によりシステムがフリーズなどの無応答となった場合を回避するために、Watchdog Timer による監視を設定することができます。

設定時間を経過すると、MMB により Hard Reset が実行され、OS のリブートが実行されます。

■ 操作手順

1. 以下のファイルを開きます。

[SVmco インストール先フォルダ] ¥etc¥fujitsu¥SVmco¥usr¥pnwatchdog.conf

(例. C:¥fujitsu¥ServerView Suite¥SVmco¥etc¥fujitsu¥SVmco¥usr¥pnwatchdog.conf)

2. 次のキーの値を設定します。初期値は "0" です。

セクション：[WATCHDOG]

キー：[TIMER]

設定値 (単位：秒) 0 (Watchdog Timer 未使用)

1～6000 (Watchdog Timer 監視時間)

備考

設定値は、適用するパーティションで、メモリダンプに要する時間を測定して決定してください。6000 秒 (1 時間 40 分) を超える時間を要する場合は未使用としてください。

設定値がメモリダンプ処理よりも短い時間の場合、Watchdog Timer がタイムアウトし、Hard Reset されるため、メモリダンプが正しく取得できません。

2.2.8 SVmco のアップデートインストール

SVmco のアップデートインストールについて説明します。

備考

- インストールされている SVmco のバージョンと同じバージョンの修正プログラムの場合、確認メッセージ画面で [OK] ボタンをクリックすると、SVmco が一度アンインストールされ、その後再度インストールされます。アンインストールしない場合は、[プログラムの削除] 画面で [キャンセル] ボタンをクリックしてください。

- 修正プログラムの入手については、製品を購入されたさいの販売会社、または担当営業員に問い合わせてください。

2.2.8.1 SVmco のアップデートインストール

SVmco のアップデートインストール手順を説明します。

作業ディレクトリに SVmco のアップデートパッケージファイル

（ServerViewMissionCriticalOption_Win.exe）が格納されていることを前提に説明します。

また、アップデートの前後で ServerView Agents の停止・起動を行う必要があります。

実施しないと、一部のファイルが置き換わらない場合があります。

本作業は Administrator 権限で作業を行ってください。

1. [管理ツール]－[サービス]を起動します。

2. [SNMP Service]を選択して停止を行います。

3. [ServerView Virtualization Management Agent]を選択して停止を行います。

   ※ServerView Agents V6.00.04 以降を使用している場合、本操作は

   必要ありません。

4. [ServerView Server Control]を選択して停止を行います。

5. エクスプローラから作業ディレクトリを開きます。

6. [ServerViewMissionCriticalOption_Win.exe]を選択し、ダブルクリックまたはマウスの右クリックメニューから[開く]で起動します。

7. [アップデート画面]が表示されますので、[次へ(N)]をクリックします。

8. インストールが完了すると[InstallShield Wizard の完了画面]が表示されますので、[完了]ボタンをクリックします。

9. [Fujitsu]－[ServerView Suite]－[Agents]－[Diagnostic Tools]－[Restart Agents]を起動します。

10. [SNMP サービスのみ再起動]のチェックを外した状態で、[再起動]を実行します。

尚、SVmco のアップデート後に、OS の再起動が必要な場合があります。

2.2.8.2 PSHED Plugin ドライバのアップデートインストール

PSHED Plugin ドライバのアップデートインストール手順を説明します。

PSHED Plugin ドライバの改版があった場合は手動で入れ替えが必要になります。

注意

PSHED Plugin ドライバの改版がない場合は、本手順は不要です。

改版の有無は README の改版履歴を参照ください。

本作業は SVmco のアップデート後に Administrator 権限で作業を行ってください。

※途中エラーが起きた際には手順 1 から再度実行してください。

■ Windows Server 2008/2008 R2 の場合

1. PSHED Plugin ドライバをアップデートします。

   以下のコマンドを実行してください。

   ```
   >[SVmco インストール先フォルダ]\fjpsaplg\fjpsadc.exe update [SVmco インストール先フォルダ]\fjpsaplg\fjpsaplg.inf" ACPI\PSHEDPI
   ```

   第一引数：update (固定)

   第二引数：[SVmco インストール先フォルダ]\fjpsaplg\fjpsaplg.inf

   (inf ファイル※パス付き)

   第三引数：ACPI\PSHEDPI (固定)

   実行例. (インストール先がデフォルトの場合)

   ```
   >"C:\Program Files (x86)\Fujitsu\ServerView Suite\SVmco\fjpsaplg\fjpsadc.exe" update "C:\Program Files (x86)\Fujitsu\ServerView Suite\SVmco\fjpsaplg\fjpsaplg.inf" ACPI\PSHEDPI


   >
   ```

2. OS を再起動します。

3. デバイスマネージャのシステムデバイス上に [PRIMEQUEST PSHED Plugin Driver] が表示されていることを確認します。表示されていない場合は、手順 1 から再度実行してください。

■ Windows Server 2012/2012 R2 の場合

1. PSHED Plugin ドライバをアンインストールします。

   以下のコマンドを実行してください。

```
>[SVmco インストール先フォルダ] \fjpsaplg_WS2012\plugin_uninstall.bat
```

```
実行例. (インストール先がデフォルトの場合)
>"C:\Program Files (x86)\Fujitsu\ServerView Suite\SVmco\fjpsaplg_WS2012\plugin_uninstall.bat”
 ROOT\SYSTEM\0001            : Removed on reboot
 [SC] DeleteService SUCCESS
>
```

2. OS を再起動します。

3. OS 再起動後、PSHED Plugin ドライバをドライバストアから削除します。

   以下のコマンドを実行してください。

```
>[SVmco インストール先フォルダ]
\fjpsaplg_WS2012\plugin_drvstore_delete.bat
```

```
実行例. (インストール先がデフォルトの場合)
>"C:\Program Files (x86)\Fujitsu\ServerView Suite\SVmco\fjpsaplg_WS2012\plugin_drvstore_delete.bat”

 Successful execution of the command.
>
```

4. PSHED Plugin ドライバをインストールします。

   以下のコマンドを実行してください。

   [SVmco インストール先フォルダ] \fjpsaplg_WS2012\plugin_install.bat

   実行例. (インストール先がデフォルトの場合)

   >"C:\Program Files (x86)\Fujitsu\ServerView Suite\SVmco\fjpsaplg_WS2012\plugin_install.bat"

   #

5. OS を再起動します。

6. デバイスマネージャのシステムデバイス上に [PRIMEQUEST PSHED Plugin Driver] が表示されていることを確認します。表示されていない場合は、手順 1 から再度実行してください。

2.2.9 SIRMS のアップデートインストール

SIRMS のアップデートインストール手順を説明します。

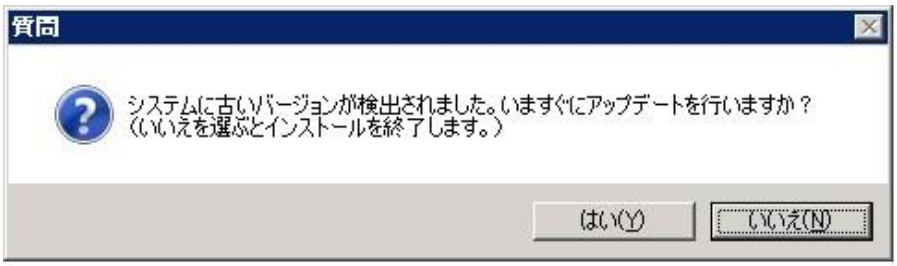
備考

修正プログラムの入手については、製品を購入されたさいの販売会社、または担当営業員に問い合わせてください。

■ 操作手順

1. 修正プログラムを任意のフォルダに格納して解凍します。
2. 解凍したフォルダの「setup.exe」を起動します。
3. 確認メッセージが表示されたら [はい] ボタンをクリックします。

→アンインストールが開始されます。



[確認メッセージ] 画面

アンインストールが完了すると、新しいバージョンのインストールが開始されます。インストール手順について詳しくは、「6.2.5　SIRMS のインストール」の手順 2. から手順 6.を参照してください。

2.2.10 SVmco のアンインストール

SVmco のアンインストール手順を説明します。

備考

SVmco をアンインストールすると、[SVmco インストール先フォルダ] 配下のファイルはすべて削除されます。必要なファイルはアンインストールする前に退避しておいてください。[SVmco インストール先フォルダ] については、環境変数 (SVmco_INSTALLPATH) で確認できます。

■ 操作手順

1. [コントロールパネル] - [プログラムと機能] の順に選択します。

[プログラムと機能] 画面が表示されます。

2. 現在インストールされているプログラムの一覧から [ServerView Mission Critical Option] を選択し、[アンインストール] をクリックします。

[インストールの準備] 画面が表示され、削除の確認メッセージが表示されます。

3. [OK] ボタンをクリックします。

→アンインストールが開始されます。

アンインストールが完了すると、アンインストール完了画面が表示されます。

4. [完了] ボタンをクリックします。

5. PSHED Plugin ドライバを削除するには OS の再起動が必要です。再起動が可能な状態かを確認したうえで、OS を再起動してください。

2.2.11 SIRMS のアンインストール

SIRMS のアンインストール手順を説明します。

■ 操作手順

1. [コントロールパネル] - [プログラムと機能] の順にクリックします。

2. 現在インストールされているプログラムの一覧から [REMCS SIRMS] を選択し、[変更／削除] をクリックします。

削除の確認メッセージが表示されます。

[確認メッセージ] 画面

3. [はい] ボタンをクリックします。

→アンインストールが開始されます。

4. アンインストールが完了したら [完了] ボタンをクリックして終了します。

[アンインストール完了]画面

2.3 SVmco の設定 (VMware 4)

添付ソフトウェアは『ServerView Suite DVD2』に格納されています。
『ServerView SuiteDVD2』からファイルをコピーして使用します。

2.3.1 SVmco のインストール

SVmco のインストールについて説明します。

備考

SVmco は、PRIMEQUEST 1000x2 シリーズ以降で提供しています。

1. ターミナルをルートで起動します。
2. 『ServerView Suite DVD2』をマウントします。
3. SVmco のモジュールを PRIMEQUEST 1000x2 シリーズの任意ディレクトリにコピーし展開します。

```
# cp MNT/SVSLocalTools/Japanese/SVmco/SR_Linux/¥
SVmco-XXXRHEL5.tgz  /tmp
```

*：MNT はマウントポイント

¥：改行しないことを表す。

XXX は版数により異なる。

例では任意ディレクトリを/tmp としています。

```
# cd /tmp
# tar xvzf SVmco-XXXRHEL5.tar.gz
```

4. 以下のコマンドを実行します。

```
# cd SVmco
#  ./INSTALL.sh -SVIM
```

5. SVmco インストール後に設定を行います。設定方法について詳しくは、「2.3.3 SVmco インストール後の設定」を参照してください。

2.3.2 SIRMS のインストール

SRIMS のインストールについて説明します。

1. ターミナルをルートで起動します。
2. 『ServerView Suite DVD2』をマウントします。
3. 以下のコマンドを実行します。

```
# rpm -ivh MNT/SVSLocalTools/Japanese/SIRMS/SR_Linux/¥
sirms-XXX.rpm
```

＊：MNT はマウントポイント

¥：改行しないことを表す。

XXX は版数により異なる。

2.3.3 SVmco インストール後の設定

VMware における SVmco インストール後の設定は、RHEL における設定と一部異なります。本節では、変更箇所のみ説明しています。

RHEL と同一の設定手順については、以下の参照先を参照してください。

SVmco インストール後の設定 (VMware)

SVmco インストール後の設定	**VMware の場合**
PSA-MMB 間通信 LAN の設定	2.3.4 ネットワークの設定
管理 LAN の設定確認	2.3.4 ネットワークの設定
SELinux 機能の設定確認	(設定不要)
ファイアーウォール機能の確認	2.3.5 ファイアーウォールの設定
パーティションからのトラップ送信先の設定	RHEL と同様 2.1.6 パーティションからのトラップ送信先の設定
管理 LAN IP アドレスの設定	RHEL と同様 2.1.5 管理 LAN IP アドレスの設定
複製ディスク使用時の SNMP 設定	RHEL と同様 2.1.7 複製ディスク使用時の SNMP 設定
デフォルトゲートウェイの設定	2.3.6 デフォルトゲートウェイの設定

備考

SVmco は、PRIMEQUEST 1000x2 シリーズ以降で提供しています。

2.3.4 ネットワークの設定

ここでは、SVmco の導入および運用で必要なネットワークの設定について説明します。

以下の流れで操作します。

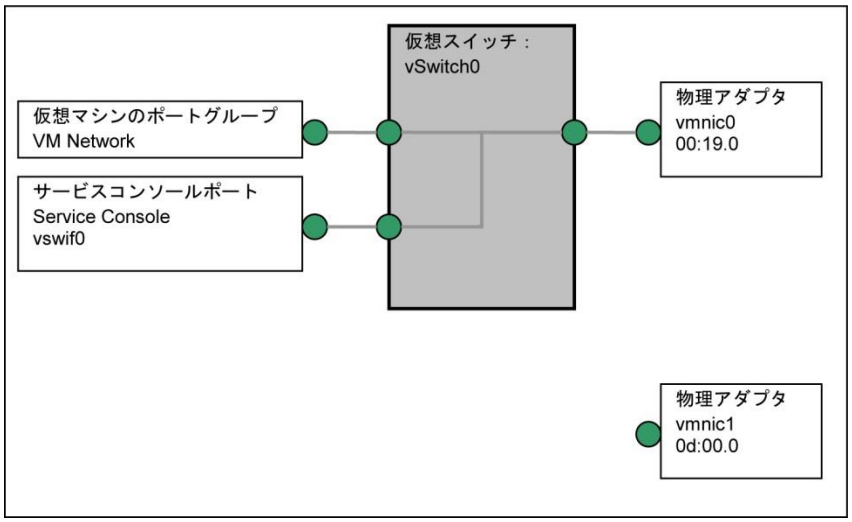
■PSA-MMB 間通信 LAN および管理 LAN の確認

■管理 LAN の設定

■PSA-MMB 間通信 LAN の設定

通常、OS インストール直後のネットワークは、以下のようになっています。

インターフェース名や BUS 番号（Seg/Bus/Dev/Func と同義）などは、環境に合わせて適宜読み替えてください。



以降の設定で使用する各コマンドについて詳しくは、man で確認してください。

注意

OS インストール直後にデフォルトで存在する vswif0 の IP アドレスを設定する前に、ホスト名を設定しないでください。VMware によって/etc/hosts が意図しない値に書き変わる場合があります。

ここでは、管理 LAN に vswif0 を使用することを前提として説明します。

■ PSA-MMB 間通信 LAN および管理 LAN の確認

1. PSA-MMB 間通信 LAN は、BUS 番号が 0000:00:19.0 の物理アダプターを使用します。

   管理 LAN は任意の物理アダプターを使用します。

   esxcfg-nics コマンドで、PSA-MMB 間通信 LAN および管理 LAN で使用する物理アダプターを確認します。

```
# esxcfg-nics -l
Name     PCI       Driver   Link     Speed    Duplex¥
MAC      Address        MTU      Description
vmnic0   00:19.00 e1000e   Up       100Mbps  Half ¥
00:17:42:de:7c:4b 1500 ¥
Intel Corporation 82567LF-2 Gigabit Network Connection
vmnic1   0d:00.00 igb      Up       100Mbps  Full ¥
00:17:42:9b:dc:b4 1500 ¥
Intel Corporation 82576 Gigabit Network Connection
vmnic2   0d:00.01 igb      Down     0Mbps    Half ¥
00:17:42:9b:dc:b5 1500 ¥
Intel Corporation 82576 Gigabit Network Connection
```

   ¥：改行しないことを表す。

   上記例の場合、vmnic0 を PSA-MMB 間通信 LAN、vmnic1 を管理 LAN として使用します。

■ 管理 LAN の設定

1. 管理 LAN のインターフェースには、OS インストール直後にデフォルトで存在する vswif0 を使用します。

   esxcfg-vswif コマンドで、vswif0 の状態を確認します。

```
# esxcfg-vswif -l
Name Port Group/DVPort IP Family IP Address ¥
Netmask Broadcast Enabled TYPE
vswif0 Service Console IPv4 N/A ¥
N/A N/A true NONE
```

   ¥：改行しないことを表す。

   上記の例の場合、Port Group 名「Service Console」に vswif0 が設定されていることがわかります。

2. esxcfg-vswitch コマンドで、仮想スイッチの状態を確認します。

```
# esxcfg-vswitch -l
Switch Name Num Ports Used Ports Configured Ports ¥
MTU Uplinks
vSwitch0    64        2          64 ¥
1500        vmnic0

PortGroup  Name VLAN ID Used Ports Uplinks
VM Network      0       0          vmnic0
Service Console 0       1          vmnic0
```

   ¥：改行しないことを表す。

上記の例の場合、Service Console が vSwitch0 に存在し、物理アダプターが vmnic0 であることがわかります。

3. vSwitch0 の物理アダプターを、管理 LAN で使用する物理アダプターvmnic1 に接続しなおします。

   esxcfg-vswitch コマンドで、vSwitch0 の物理アダプターvmnic0 を取り外します。

```
# esxcfg-vswitch -U vmnic0 vSwitch0
# esxcfg-vswitch -l
Switch Name Num Ports Used Ports Configured Ports ¥
MTU    Uplinks
vSwitch0 64           2          64 ¥
1500

PortGroup Name VLAN ID Used Ports Uplinks
VM Network      0       0
Service Console 0       1
```

   ¥：改行しないことを表す。

4. esxcfg-vswitch コマンドで、vSwitch0 に物理アダプターvmnic1 を接続します。

```
# esxcfg-vswitch -L vmnic1 vSwitch0
# esxcfg-vswitch -l
Switch Name Num Ports Used Ports Configured Ports ¥
MTU    Uplinks
vSwitch0 64           2          64 ¥
1500 vmnic1
```

```
PortGroup Name VLAN ID Used Ports Uplinks
VM Network      0      0          vmnic1
Service Console 0      1          vmnic1
```

¥ : 改行しないことを表す。

4. esxcfg-vswif コマンドで、vswif0 に IP アドレス (192.168.0.2) を割り当てます。

```
# esxcfg-vswif -i 192.168.0.2 -n 255.255.255.0 vswif0
# esxcfg-vswif -l
Name Port Group/DVPort IP Family IP Address ¥
Netmask    Broadcast      Enabled   TYPE
vswif0   Service Console   IPv4   192.168.0.2 ¥
255.255.255.0 192.168.0.255 true STATIC
```

¥ : 改行しないことを表す。

■ PSA-MMB 間通信 LAN の設定

7. esxcfg-vswitch コマンドで、仮想 Switch (vSwitch1) を作成します。

```
# esxcfg-vswitch -a vSwitch1
# esxcfg-vswitch -l
Switch Name Num Ports Used Ports Configured Ports ¥
MTU Uplinks
vSwitch0    64        2          64 ¥
1500 vmnic1

PortGroup Name   VLAN ID      Used Ports      Uplinks
VM Network    0      0        vmnic1
Service Console  0      1        vmnic1

vSwitch1  64  2    64 ¥
1500

PortGroup Name VLAN ID Used Ports Uplinks
```

¥：改行しないことを表す。

8. esxcfg-vswtich コマンドで、仮想 Switch(vSwitch1)に物理アダプターvmnic0 を接続します。

```
# esxcfg-vswitch -L vmnic0 vSwitch1
# esxcfg-vswitch -l
Switch Name Num Ports Used Ports Configured Ports ¥
MTU Uplinks
vSwitch0    64        2          64 ¥
1500 vmnic1
```

```
PortGroup Name VLAN ID Used Ports Uplinks
VM Network      0      0          vmnic1
Service Console 0      1          vmnic1

vSwitch1      64        2          64 ¥
1500 vmnic0

PortGroup Name VLAN ID Used Ports Uplinks
```

¥：改行しないことを表す。

9. 作成した仮想 Switch(vSwitch1)に Port Group (PSA-MMB) を追加します。

```
# esxcfg-vswitch -A PSA-MMB vSwitch1
# esxcfg-vswitch -l
Switch Name Num Ports Used Ports Configured Ports ¥
MTU Uplinks
vSwitch0    64        2          64 ¥
1500 vmnic1

PortGroup Name VLAN ID Used Ports Uplinks
VM Network      0       0         vmnic1
Service Console 0       1         vmnic1

vSwitch1   64     2     64 ¥
1500       vmnic0
```

```
PortGroup Name VLAN ID Used Ports Uplinks
PSA-MMB        0       0          vmnic0
```

¥ : 改行しないことを表す。

10. esxcfg-vswif コマンドで、仮想ポート (vswif1) を作成します。
    設定する IP アドレスは、パーティション番号により異なります。
    以下の表の値を使用してください。

仮想ポートに設定する IP アドレス

パーティション番号	IP アドレス	サブネットマスク
0	172.30.0.2	255.255.255.0
1	172.30.0.3	
2	172.30.0.4	
3	172.30.0.5	

<パーティション番号#2 で PSA-MMB の Port Group を vswif1 とする場合>

```
# esxcfg-vswif -a vswif1 -i 172.30.0.4 -n 255.255.255.0 ¥
-p PSA-MMB
# esxcfg-vswif -l
Name Port Group/DVPort IP Family IP Address ¥
Netmask Broadcast Enabled TYPE
vswif0 Service Console IPv4 192.168.0.2 ¥
255.255.255.0 192.168.0.255 true STATIC
vswif1 PSA-MMB IPv4 172.30.0.4 ¥
255.255.255.0 172.30.0.255 true STATIC
```

¥：改行しないことを表す。

注意：IP アドレスは同一筐体内で重複しない値を設定して下さい。

11. PSA-MMB 間通信 LAN に、以下の設定を追加します。

    Speed：100Mbps

    Duplex：full

    <PSA-MMB 間通信 LAN が vmnic0 の場合>

```
# esxcfg-nics vmnic0 -s 100 -d full
```

12. SVmco の設定ファイルに、PSA-MMB 間通信 LAN の IP アドレスを設定します。

    ファイル格納場所：/etc/fujitsu/SVmco/usr/tommbipsetup.conf

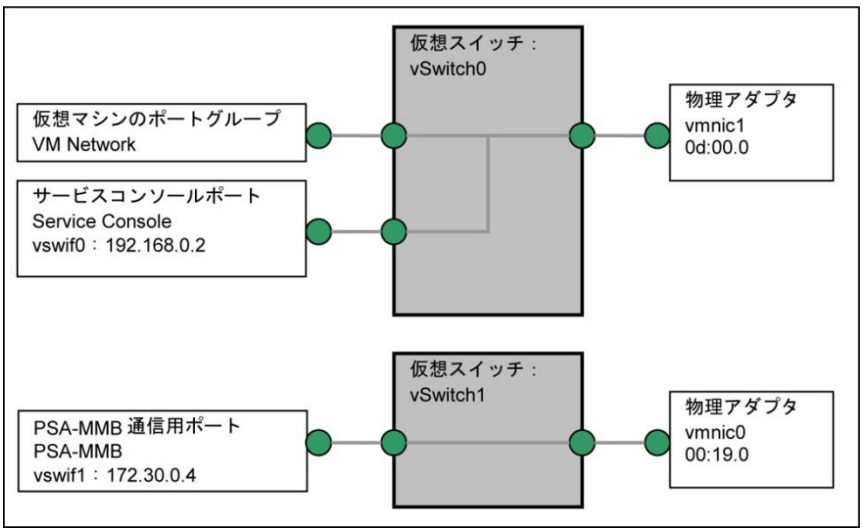
    設定値：手順 4.で設定した IP アドレスを入力する。

    <設定例>

```
[NETWORK]
TOMMBIP=172.30.0.4
```

以上で設定は完了です。

上記設定例では、設定後のネットワークは以下のようになります。



設定後のネットワーク

2.3.5 ファイアーウォールの設定

ここでは、SVmco 運用でのファイアーウォールの設定について説明します。

SVmco では、以下のポートを開放する必要があります。

SVmco 運用でのファイアーウォール設定

№	ポート	ポート番号	説明
1	snmp ポート	Udp/snmp または 161	一般 snmp の通信ポート
3	psa-mmb 通信ポート	tcp/MMB 側 5000	MMB-PSA 間ポート イベントおよび構成情報の通知用

ファイアーウォール設定の実施例

No.	実施例
1	# esxcfg-firewall -o 161,udp,in,SNMP
3	# esxcfg-firewall -o 5000,tcp,out,MCO-MMB

- ファイアーウォール設定の確認

```
#esxcfg-firewall -q
Opened ports:
    SNMP        : port 161 udp.in
    MCO-MMB     : port 5000 tcp.out
```

2.3.6 デフォルトゲートウェイの設定

デフォルトゲートウェイの設定は、OS のインストール時に行います。

何らかの理由によってデフォルトゲートウェイが設定されていない場合は、本設定を行ってください。

1. route コマンドで、一時的なデフォルトゲートウェイを設定します。

```
route add default gw <GATEWAY>
```

例：192.168.0.1 をデフォルトゲートウェイに設定する場合

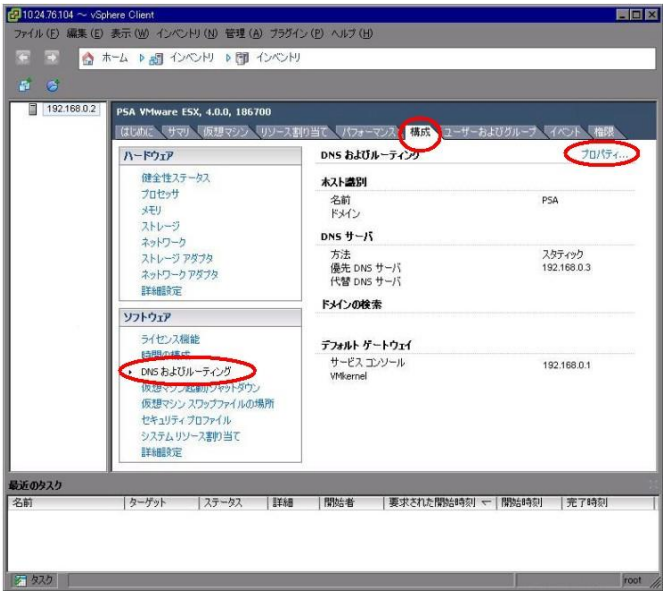
```
# route add default gw 192.168.0.1
```

2. VMware vSphere Client を使用してサービスコンソールに接続し、サービスコンソール側のデフォルトゲートウェイを設定します。
    1. VMware vShpere Client を起動します。

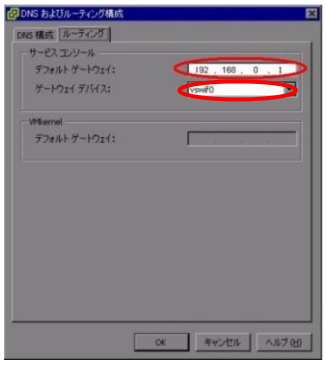
2. [ホーム] → [インベントリ] → [インベントリ] から、[構成] タブをクリックします。

3. 左下にある [ソフトウェア] 内の [DNS およびルーティング] をクリックします。

4. [DNS およびルーティング] 情報が表示された画面の右上にある [プロパティ] をクリックします。



5. [ルーティング] タブをクリックし、[サービスコンソール] の [デフォルト ゲートウェイ] を設定し、[ゲートウェアデバイス]には vswif0 を選択し、[OK] ボタンをクリックします。



[DNS およびルーティング構成] ダイアログボックス

注意

VMware vSphere Client について詳しくは、VMware のマニュアルを参照してください。

2.3.7 パーティションの再起動

以下のコマンドを実行し、パーティションを再起動します。

【入力形式】

```
/sbin/reboot
```

2.3.8 VMware SVmco 保守情報取得

SVmco に関するトラブルが発生した場合、SVmco 調査資料収集コマンド (getosvmco) を実行し、さらに vm-support コマンドを実行します。

1. getosvmco コマンド

```
# /opt/fujitsu/SVmco/sh/getosvmco <ファイル名>
```

2. vm-support コマンド

<実施例>

```
# vm-support
```

備考

VMware ではコアファイルは /var/core 配下に出力され、自動では削除されません。
vm-support コマンド実行後、適宜コアファイルを削除することをお勧めします。

2.3.9 VMware SVmco 留意事項

VMware での SVmco に関する留意事項は、以下のとおりです。

- SVmco は Console OS 上でのみ動作可能で、Console OS 上のデバイスの異常通知を行います。ゲスト OS 上では動作できないため、ゲスト OS にはインストールしないでください。
- OS 起動時に、SVmco の起動に時間がかかる (5 分以上) 場合があります。

2.4 SVmcovm のインストール/アンインストール

SVmcovm の手動単体インストールとアンインストールを行う方法及び、インストール前後の設定について説明します。

2.4.1 インストール手順

SVmcovm は、以下の手順でインストールして下さい。

インストール前の設定は Linux,windows 共通です。

- **SVmcovm のインストール前の確認設定(Linux,windows 共通)**
- **SVmcovm のインストール**
- **SVmcovm のインストール後の設定**
- **仮想マシンの再起動**

【注意】

・SVmcovm を VMware ESXi 5/6 の Guest OS 上にインストールするにあたっては、VMware ESXi 5/6 サーバ上に 特定の仮想マシンを選定し、その仮想マシン上に

SVmcovm をインストールして下さい。
全ての仮想マシンに SVmcovm をインストールする必要はありません。

・ServerView RAID Manager と連携する為、同じ仮想マシン上に ServerView RAID Manager が インストールされている必要があります。
　ServerView RAID Manager のインストールについては、

"PRIMEQUEST 向け ServerView RAID Manager VMware vSphere ESXi 5 インストールガイド"、”PRIMEQUEST 向け ServerView RAID Manager VMware vSphere ESXi 6 インストールガイド”を参照してください。

・管理用仮想マシンは、業務用の仮想マシンと併用でも構いません。
　但し、他のパーティションへ移動(vMotion，vSphereHA 等)しない仮想マシンを選定下さい。
　該当仮想マシンが他のパーティションへ移動されると、正しくイベントの通報がで きなくなる場合があります。

2.4.2 SVmcovm のインストール前の確認/設定

ここでは、SVmcovm のインストールの前に必要なネットワークの設定について説明します。

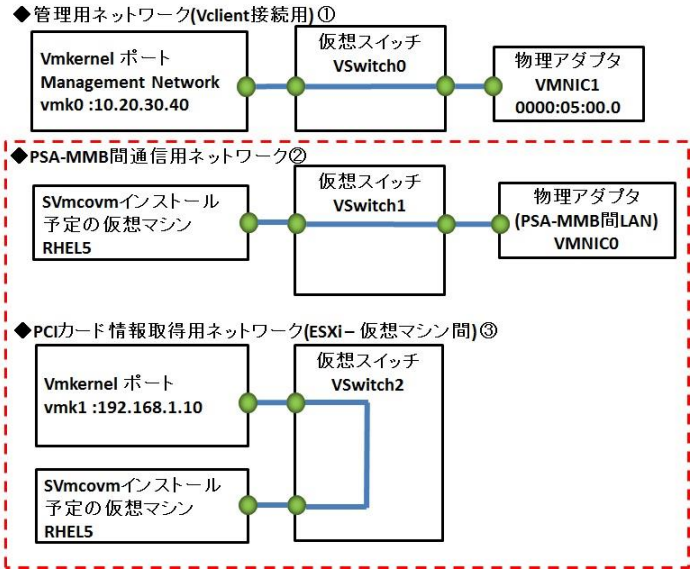
以下の流れで操作します。

1. **PSA-MMB 間通信 LAN が割り当たっている物理アダプタ(vmnic)の確認**
2. **仮想マシンへの PSA-MMB 間通信 LAN の割り当て**
3. **ESXi からの情報取得用仮想ネットワークの設定**
4. **仮想マシンの自動起動設定**

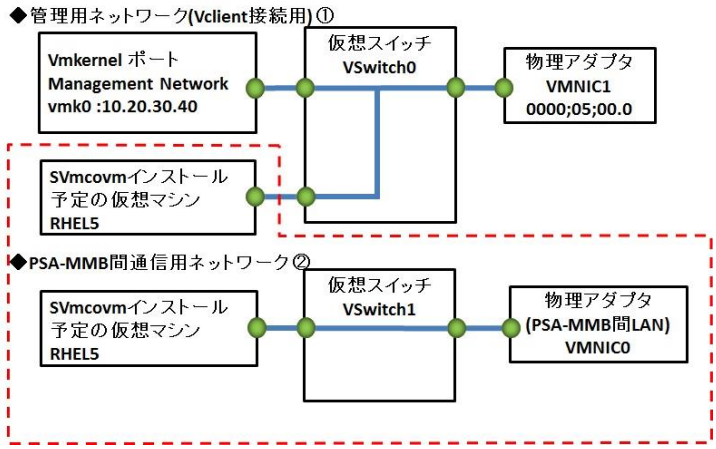
本章では、SVmcovm をインストールする仮想マシンを Red hat Linux5 に選定したと仮定して説明します。構築するネットワーク構成としてセキュリティー上、管理用ネットワーク(ネットワーク構成例 1 の①)とは別に赤の点線で囲んだ部分(ネットワーク構成例 1 の②、③)の新規構築を推奨します。

但し、下記ネットワーク構成例のように、ESXi-仮想 OS 通信ネットワーク(ネットワーク構成例 1 の③)を構築する代わりに、管理用ネットワーク(ネットワーク構成例 2 の①)に仮想マシンを含めた構成でも構いません。

2.4.2.1 ネットワーク構成例 1



2.4.2.2 ネットワーク構成例 2



2.4.2.3 PSA-MMB 間通信 LAN が割り当たっている物理アダプタ (vmnic)の確認

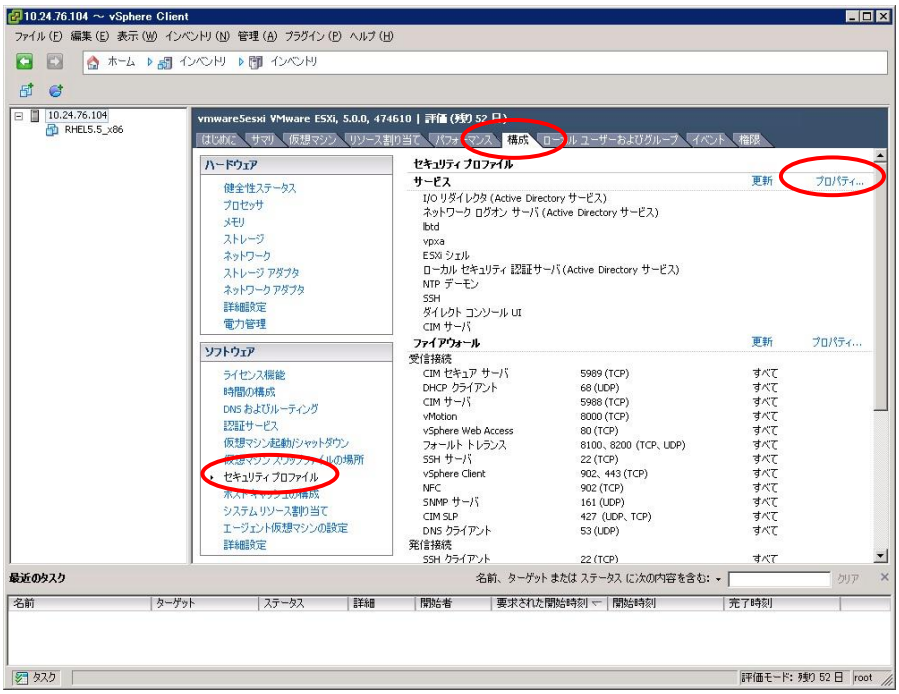
Vmware vSphere ESXi(以下,ESXi)に SSH で接続可能にするために、VMware vSphere Client / VMware vSphere Web Client を使用して、SSH サービスを起動します。

注意 ：VMware vSphere Client / VMware vSphere Web Client について詳しくは、VMware のマニュアルを参照してください。

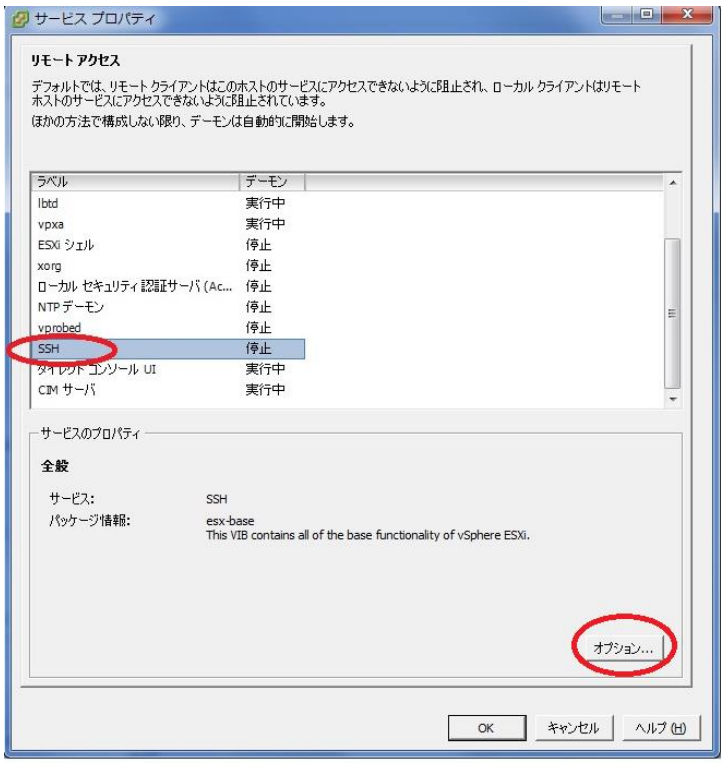
2.4.2.3.1. VMware vSphere Client の場合

1. VMware vShpere Client を起動します。
2. [ホーム] → [インベントリ] → [インベントリ] から、[構成] タブをクリックします。
3. 左下にある [ソフトウェア] 内の [セキュリティプロファイル] をクリックします。

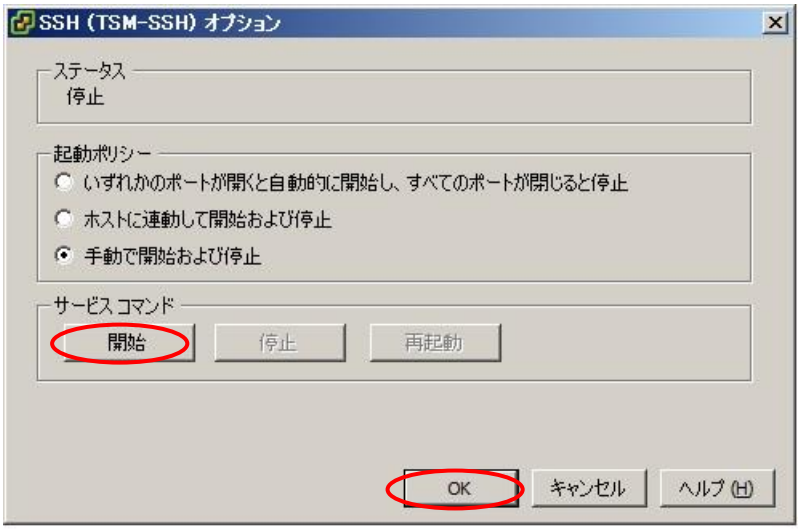
4. [セキュリティプロファイル] 情報が表示された画面の右上にある サービスの [プロパティ] をクリックします。



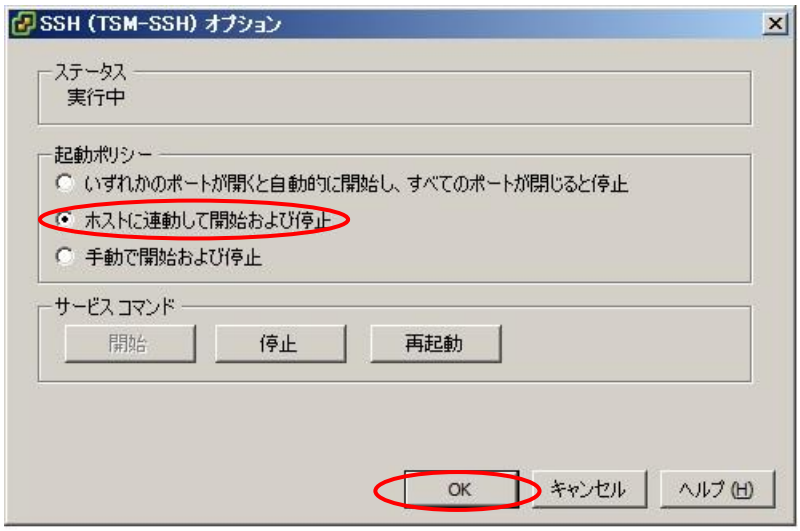
5. [SSH]を選択し、[オプション]ボタンをクリックします。



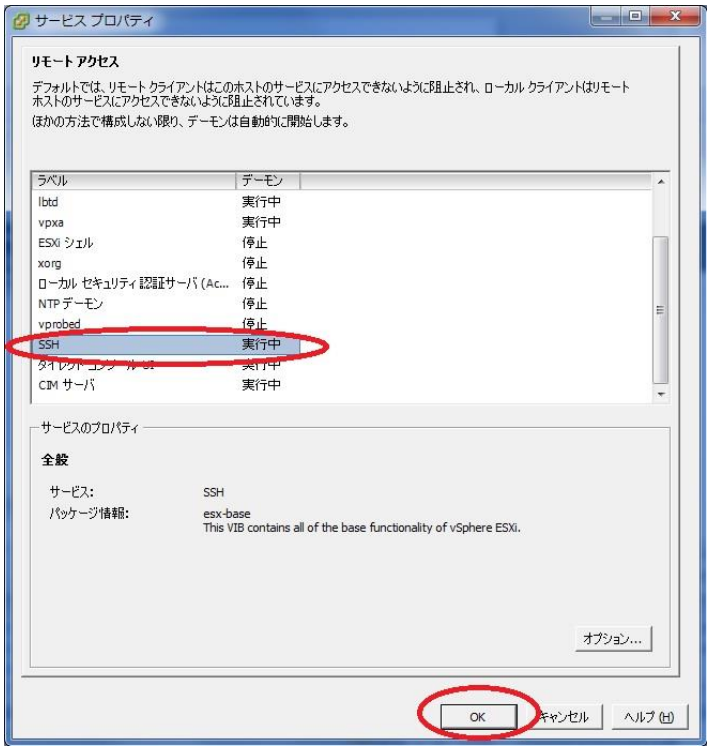
6. [サービスコマンド]で開始をクリックします。



7. 次に[起動ポリシー]の[ホストに連動して開始および停止]を選択し、[OK]をクリックします



8. [SSH]の[デーモン]が実行中になっていることを確認して[OK]をクリックします。



9. [SSH]の[デーモン]が実行中になっていることを確認して[OK]をクリックします。
SSH で ESXi にログインし、以下のコマンドを実行します。

```
# esxcfg-nics -l
```

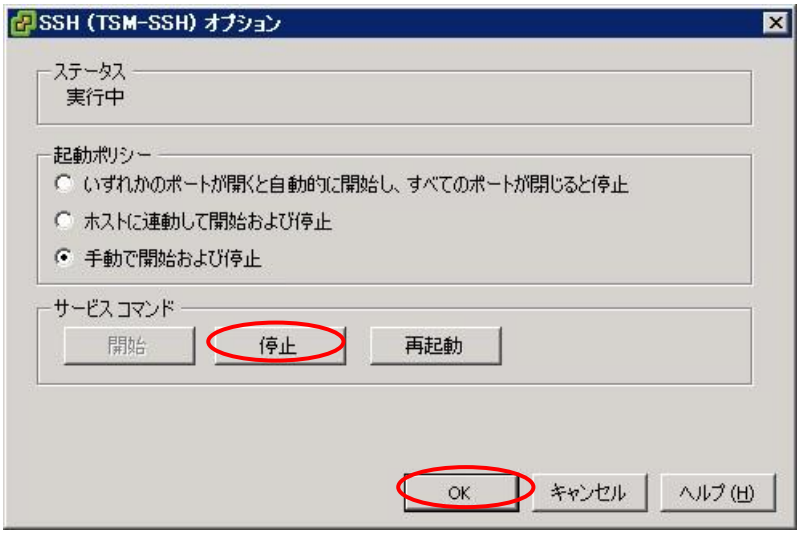
【実行結果(例)】

```
~ # esxcfg-nics -l

Name    PCI           Driver      Link Speed     Duplex MAC Address       MTU
Description

vmnic0  0000:00:19.00 e1000e      Up   100Mbps   Full   00:17:42:de:7c:49 1500
Intel Corporation 82567LF-2 Gigabit Network Connection

vmnic1  0000:05:00.00 igb         Up   100Mbps   Full   00:17:42:9b:dc:b2 1500
Intel Corporation 82576 Gigabit Network Connection

vmnic2  0000:05:00.01 igb         Down 0Mbps     Half   00:17:42:9b:dc:b3 1500
Intel Corporation 82576 Gigabit Network Connection

vmnic3  0000:06:00.00 igb         Down 0Mbps     Half   00:17:42:9b:dc:b0 1500
Intel Corporation 82576 Gigabit Network Connection

vmnic4  0000:06:00.01 igb         Down 0Mbps     Half   00:17:42:9b:dc:b1 1500
Intel Corporation 82576 Gigabit Network Connection

~ #
```

PSA-MMB 間通信 LAN は、BUS 番号が”**0000:00:19.00**”の物理アダプターを使用しますので、“**vmnic0”**に割り当たっている事がわかります。

10. 確認後、SSH のサービスを停止させます。SSH を起動させた時のように、VMware vSphere Client を起動させて、[ホーム]→[インベントリ]→[インベントリ]から[構成]タブをクリックし、左下の[ソフトウェア]内の[セキュリティプロファイル]からプロパティをクリックし、[ファイアウォールのプロパティ]画面で[ssh サービス]を選択し、[オプション]を開きます。

11. 以下のように[サービスコマンド]で[停止]をクリックした後、[OK]をクリックします。



12. [SSH サーバ]のチェックが外れ、[デーモン]が停止になっていることを確認して[OK]をクリックします。

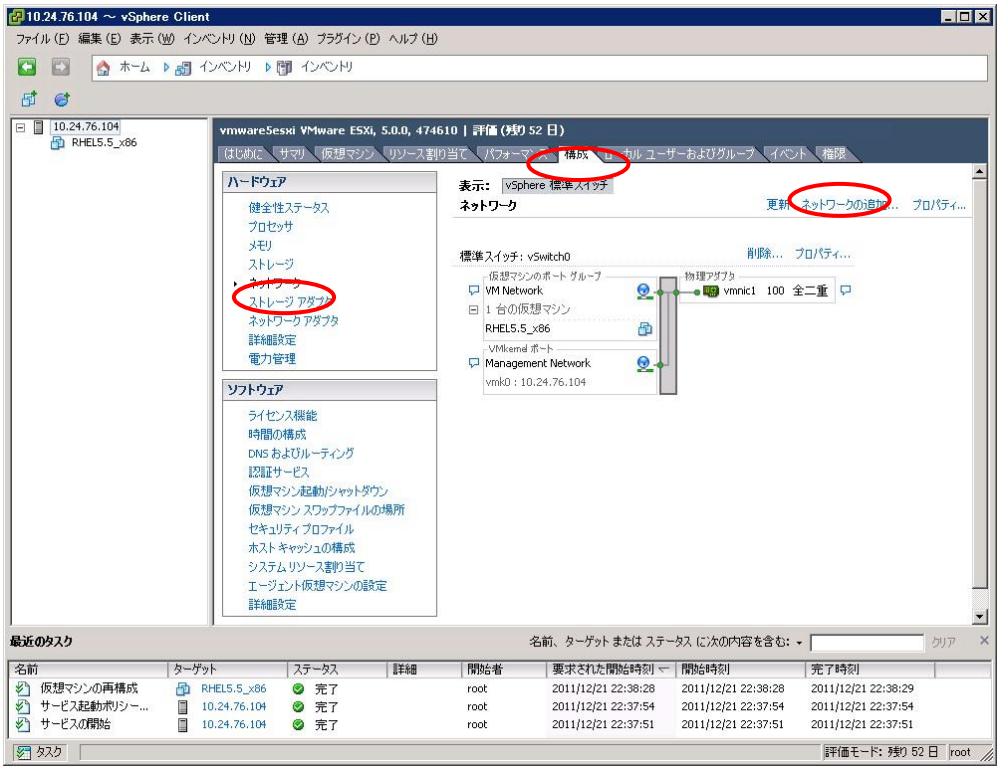
2.4.2.3.2. VMware vSphere Web Client の場合

1. VMware vSphere Web Client の場合は本章の手順は不要です。
   次の章へ進んでください。

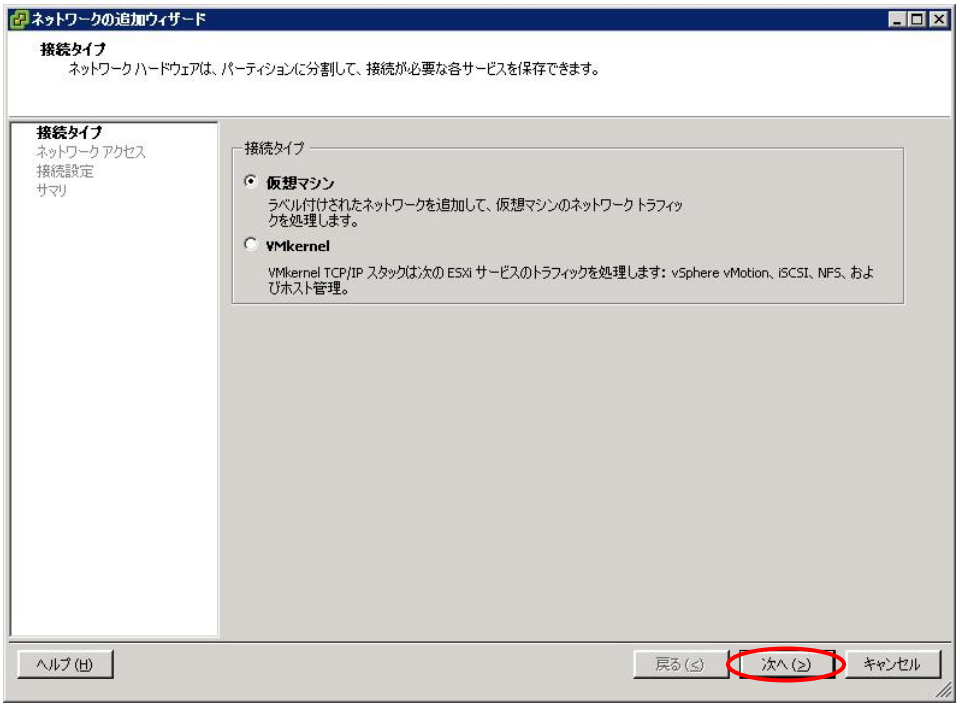
2.4.2.4 仮想マシンへの PSA-MMB 間通信 LAN の割り当て

2.4.2.4.1. VMware vSphere Client の場合

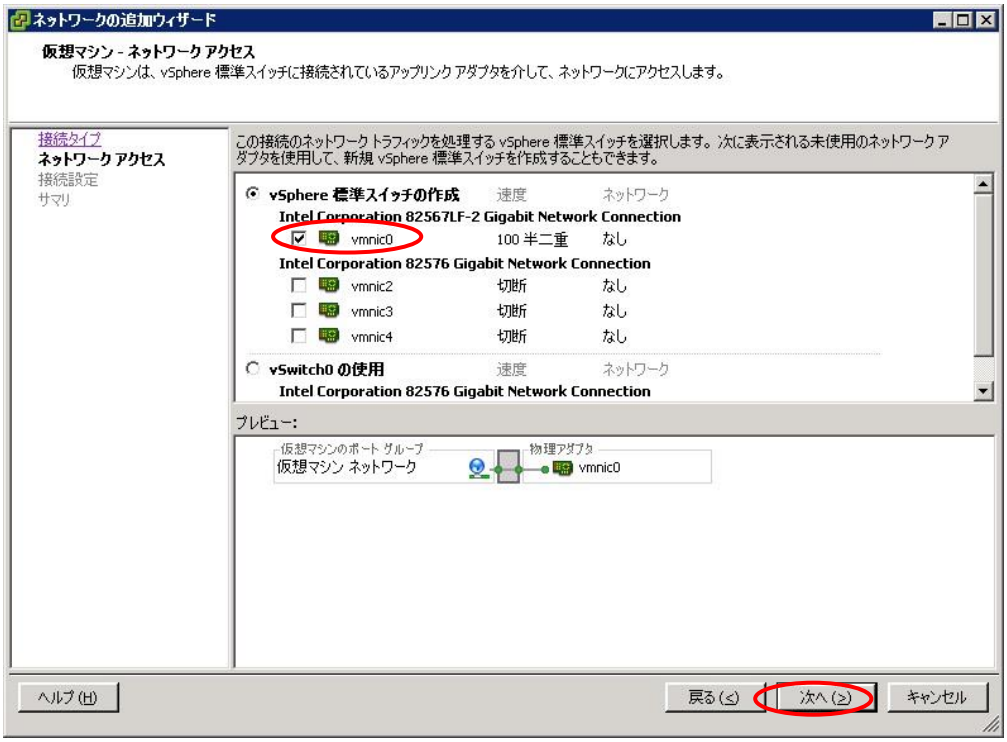
1. VMware vShpere Client を起動します。
2. [ホーム] → [インベントリ] → [インベントリ] から、[構成] タブをクリックします。
3. 左下にある [ハードウェア] 内の [ネットワーク] をクリックします。
4. [ネットワーク]が表示されたら、画面右上にある[ネットワークの追加]をクリックします。



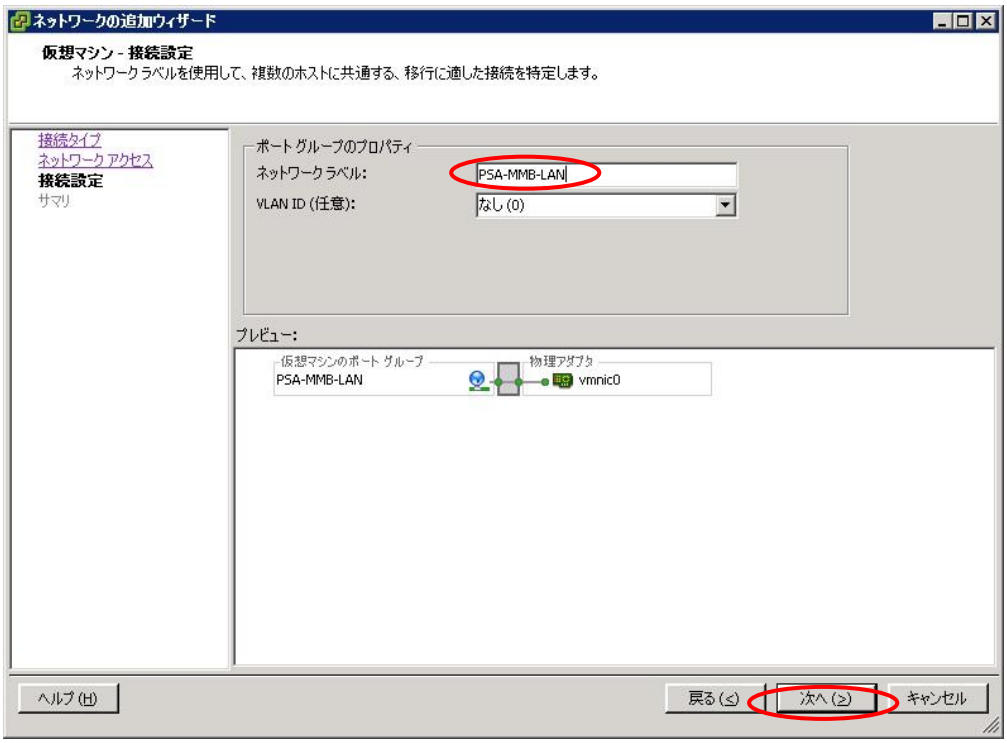
5. [接続タイプ]は仮想マシンをチェックし、[次へ]をクリックします。



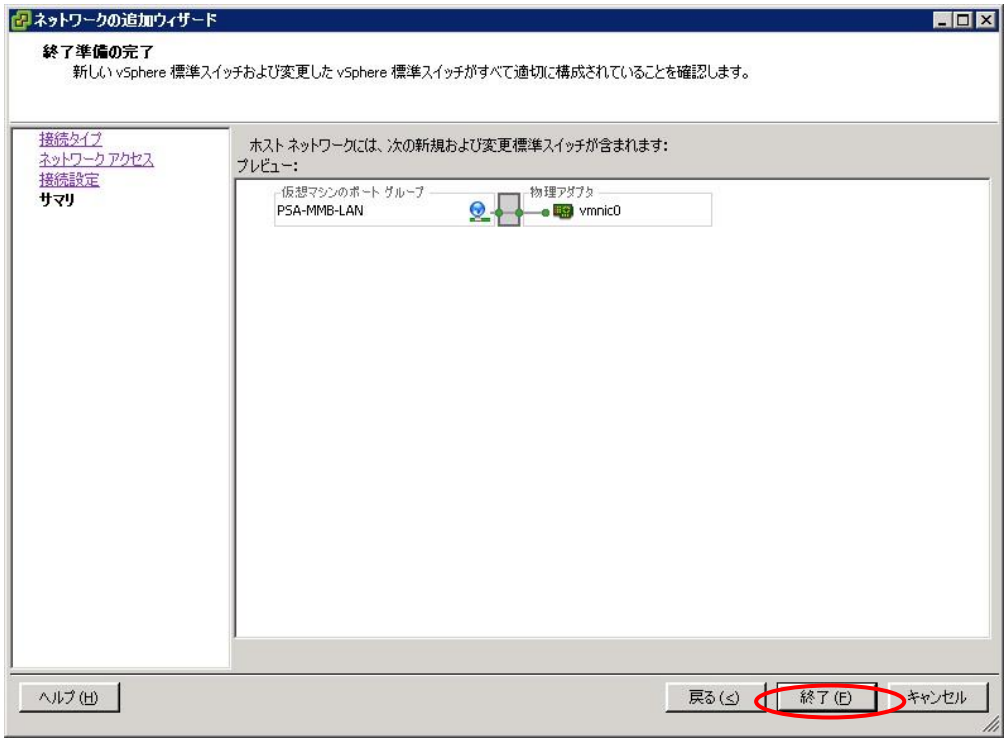
6. [vSphere 標準スイッチ]の作成をチェックし、1 で確認した PSA-MMB 間通信 LAN の物理アダプタ(vmnic0)を選択し、[次へ]をクリックします。



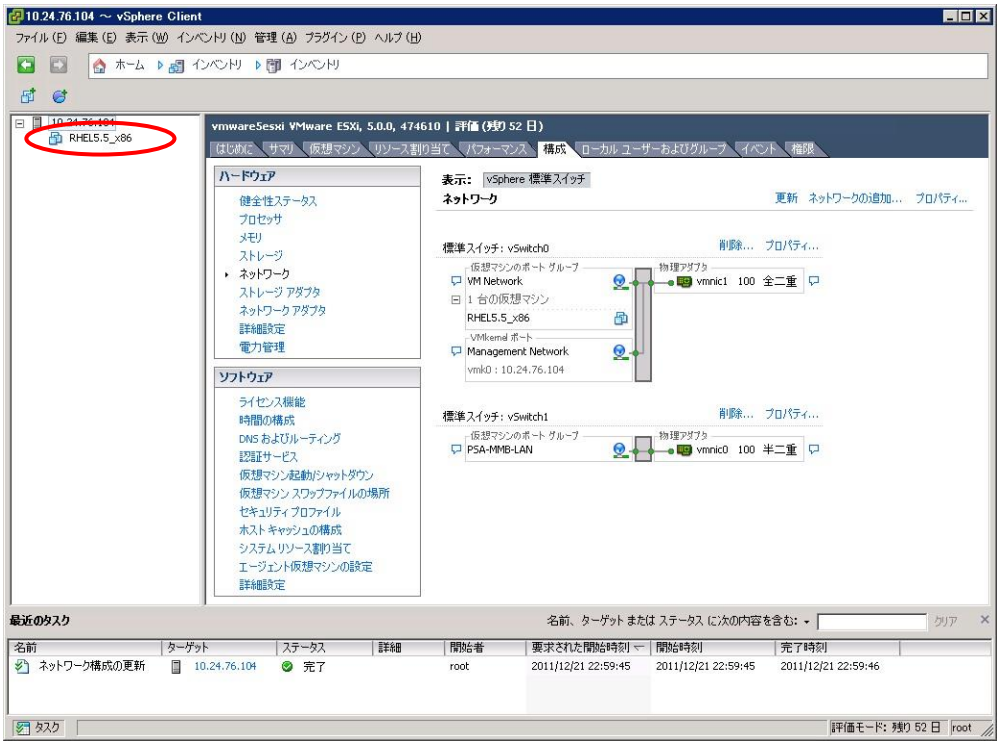
7. [ポートグループのプロパティ]の[ネットワークラベル]に PSA-MMB-LAN を設定し、[次へ]をクリックします。



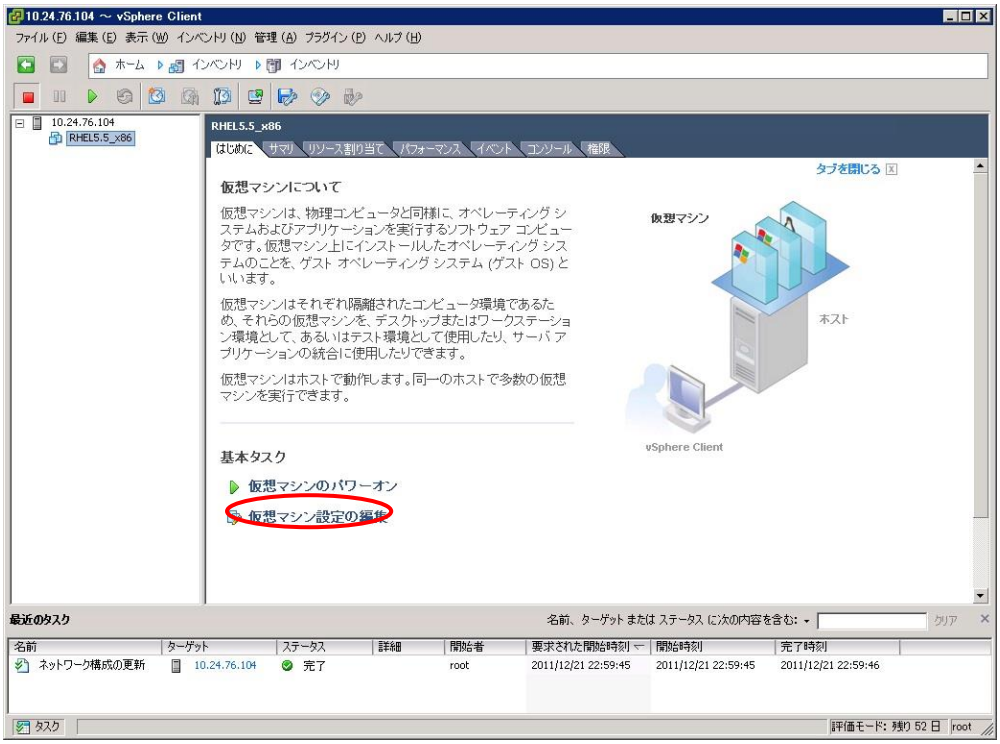
8. [仮想マシンのポートグループ]に PSA-MMB-LAN が設定されており、物理アダプタが正しい事を確認したら、[終了]をクリックします。



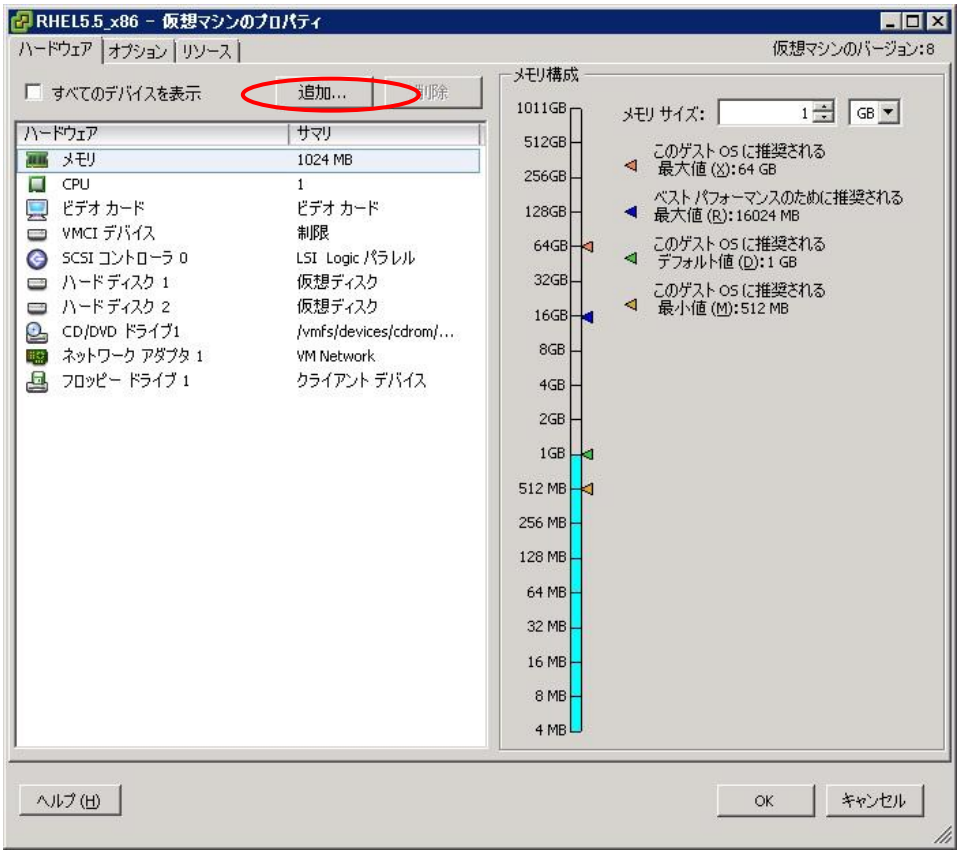
9. [ネットワーク]画面に戻るので、SVmcovm をインストール予定の管理用仮想 OS をクリックします。



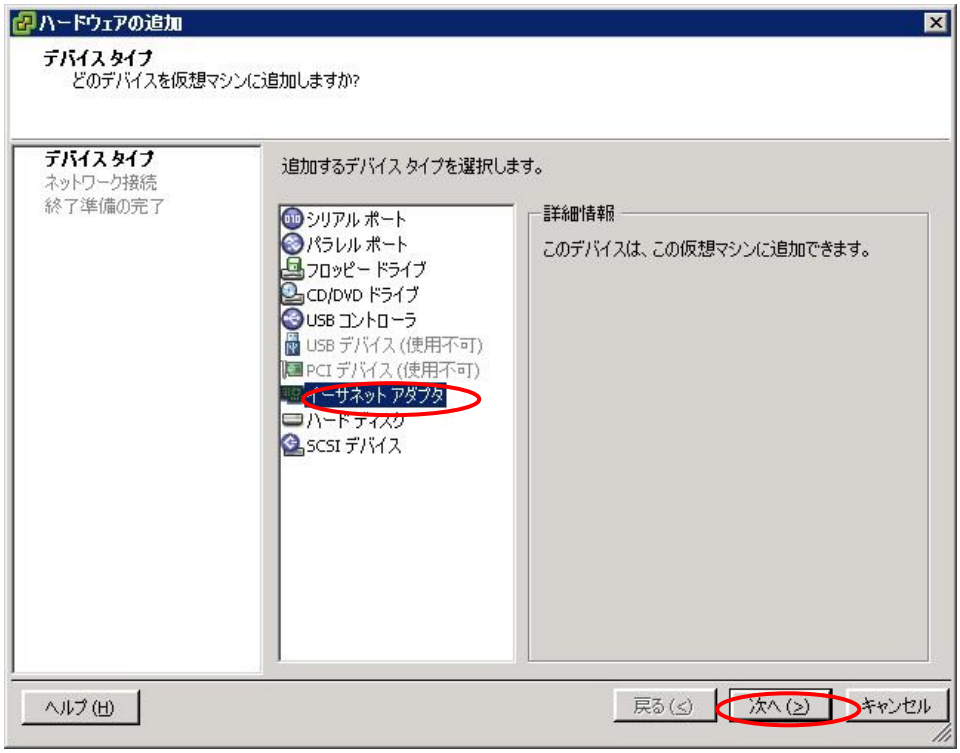
10. [はじめに]のタブから[仮想マシンの設定の編集]をクリックします。



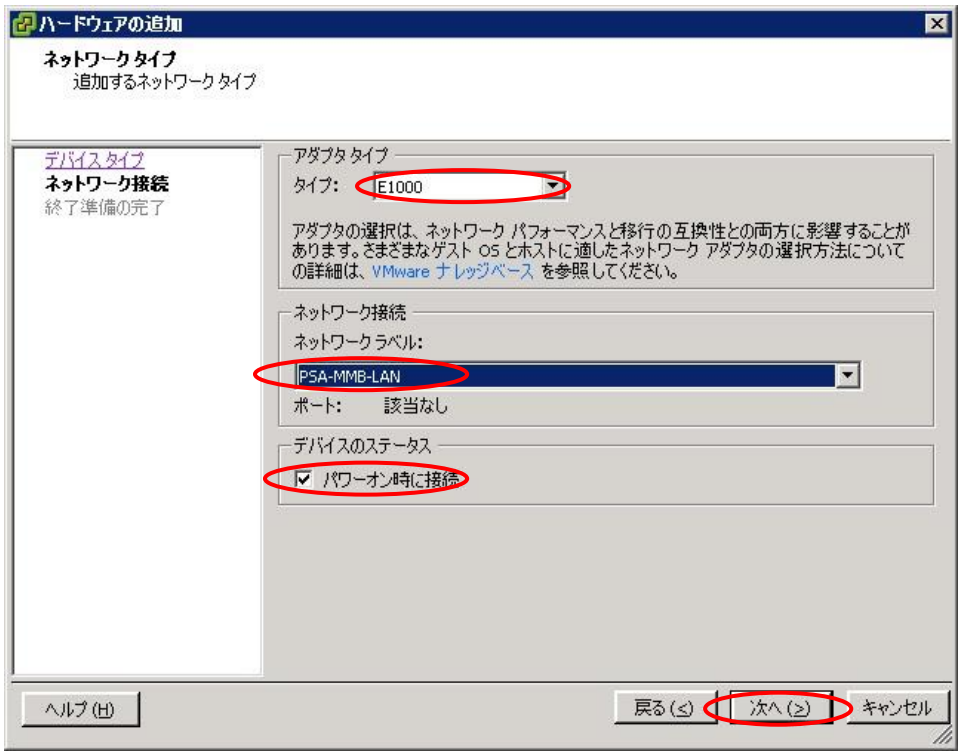
11. [追加]をクリックします。



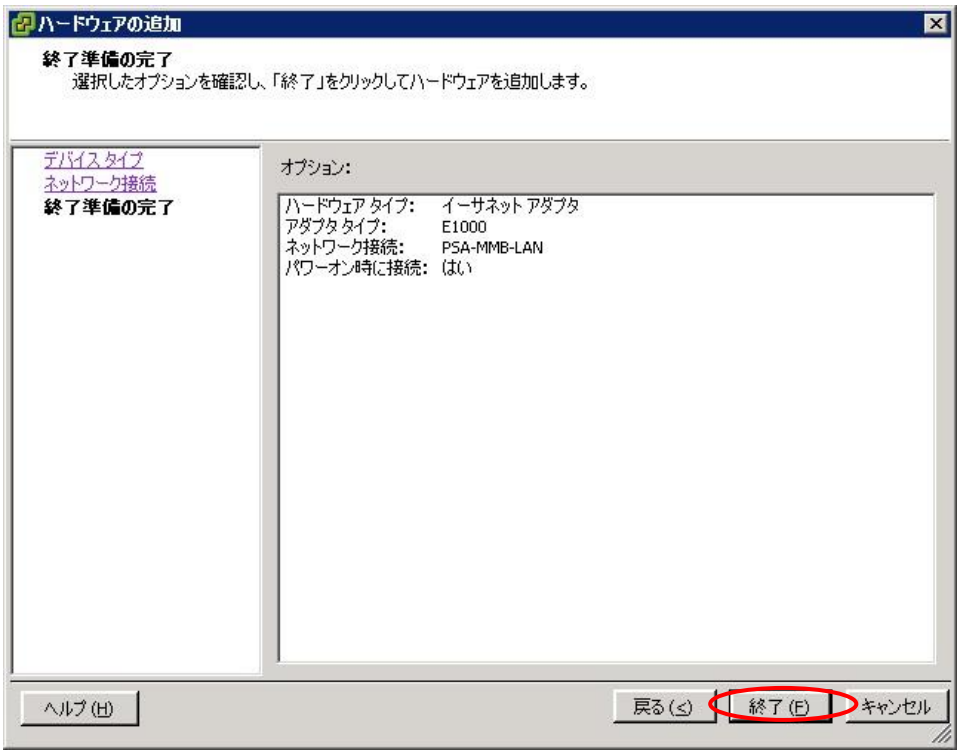
12. 追加するデバイスタイプに[イーサネットアダプタ]を選択し、[次へ]をクリックします。



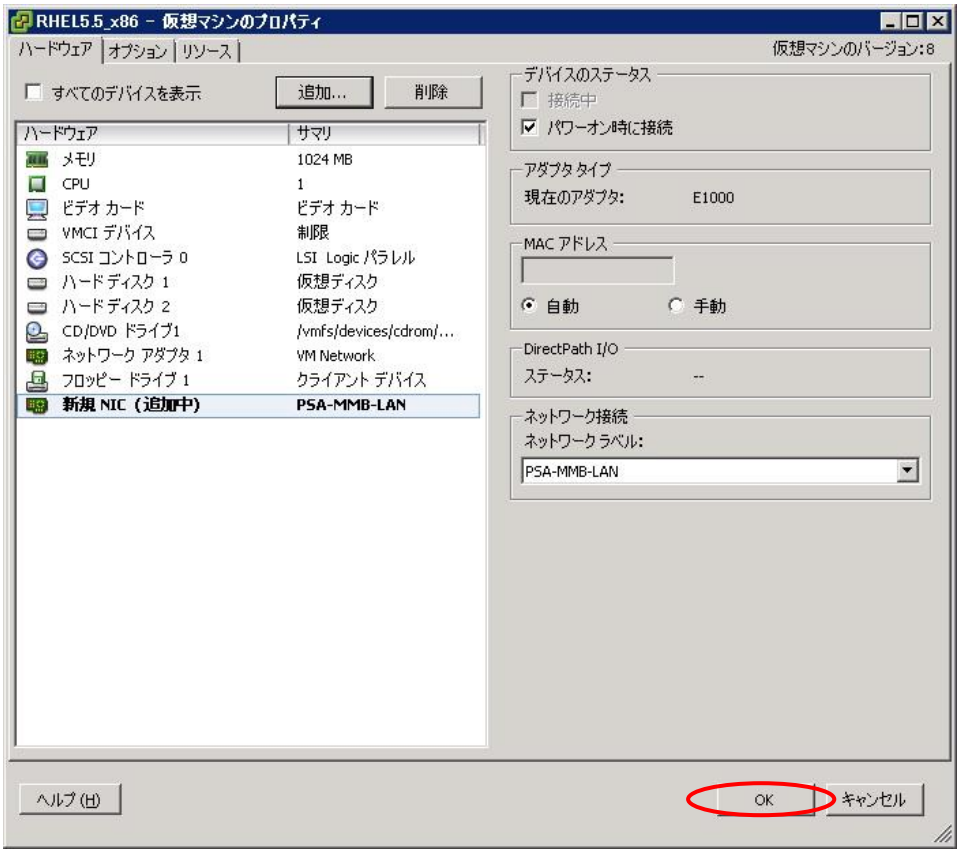
13. [アダプタタイプ]の[タイプ]は E1000 に設定し、[ネットワークラベル]は 8 で作った PSA-MMB-LAN を選択し、パワーオン時に接続にチェックを入れたら、[次へ]をクリックします。



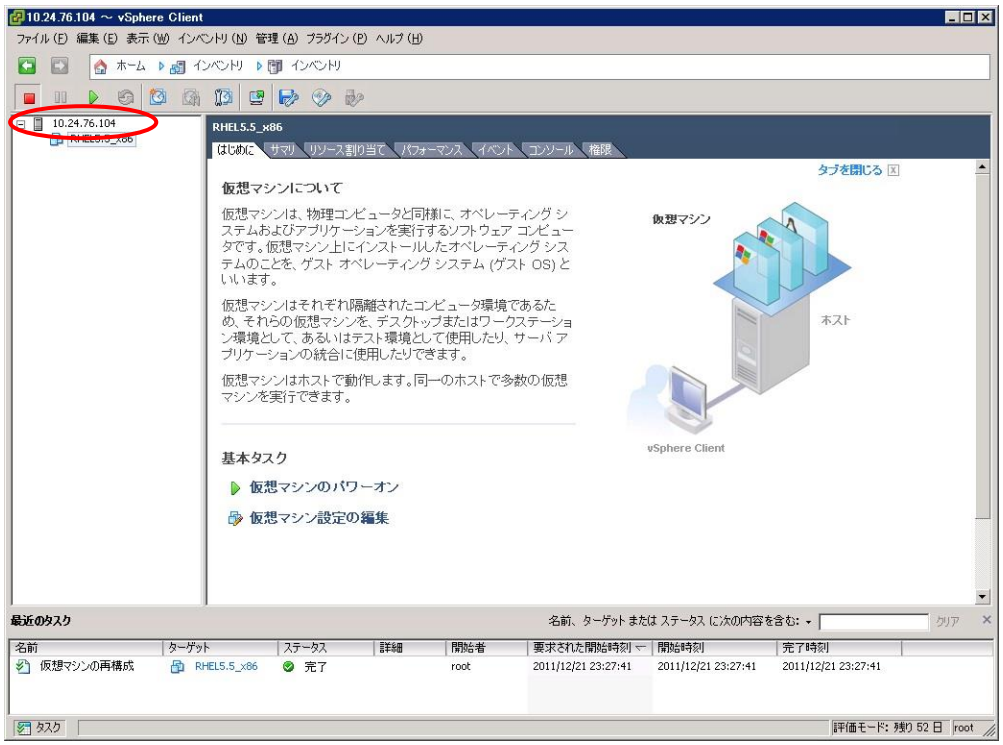
14. ハードウェアタイプが”イーサネットアダプタ”、アダプタタイプが”E1000”、ネットワーク接続が”PSA-MMB-LAN”、パワーオン時に接続が”はい”になっていることを確認したら、[終了]をクリックします。



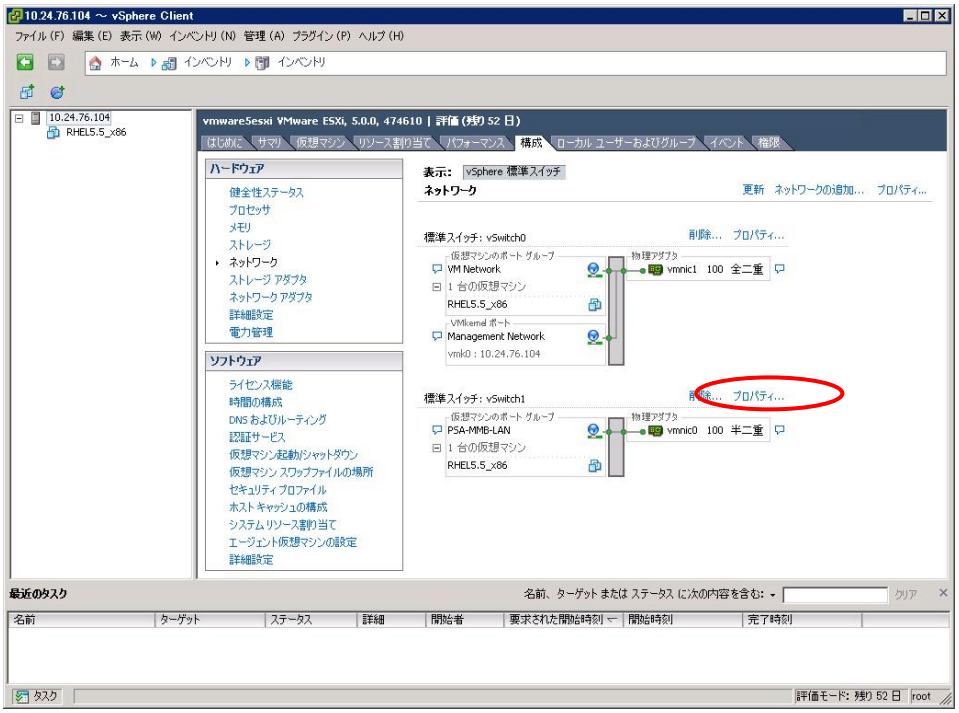
15. 新規 NIC として PSA-MMB-LAN が追加中であることを確認したら、[OK]をクリックします。



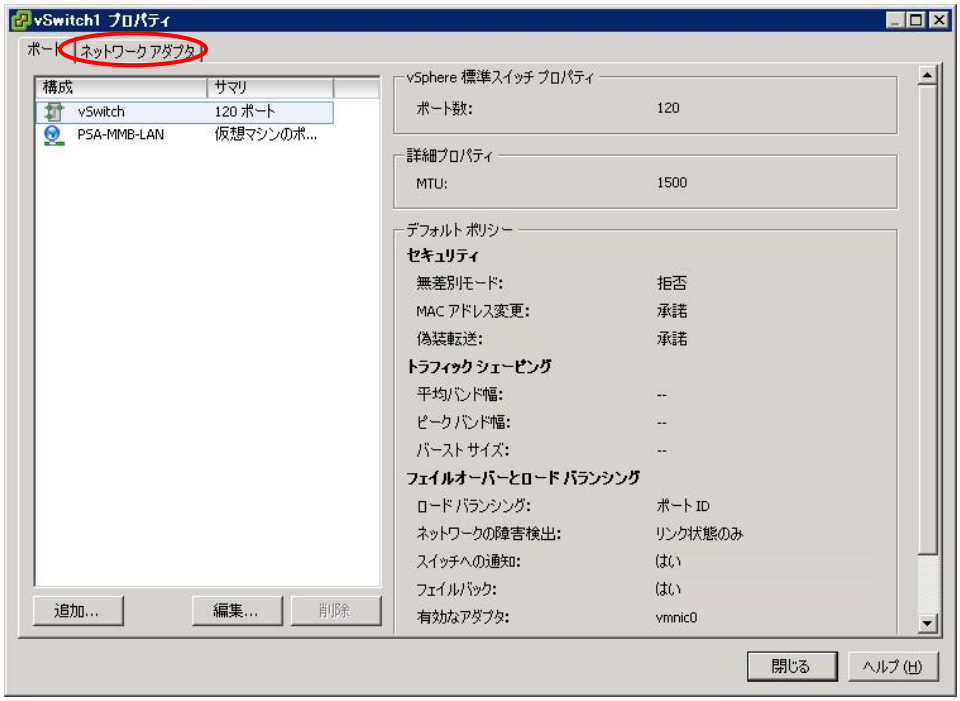
16. PSA-MMB 間通信 LAN の設定変更のため、左上のツリーから ESXi をクリックします。



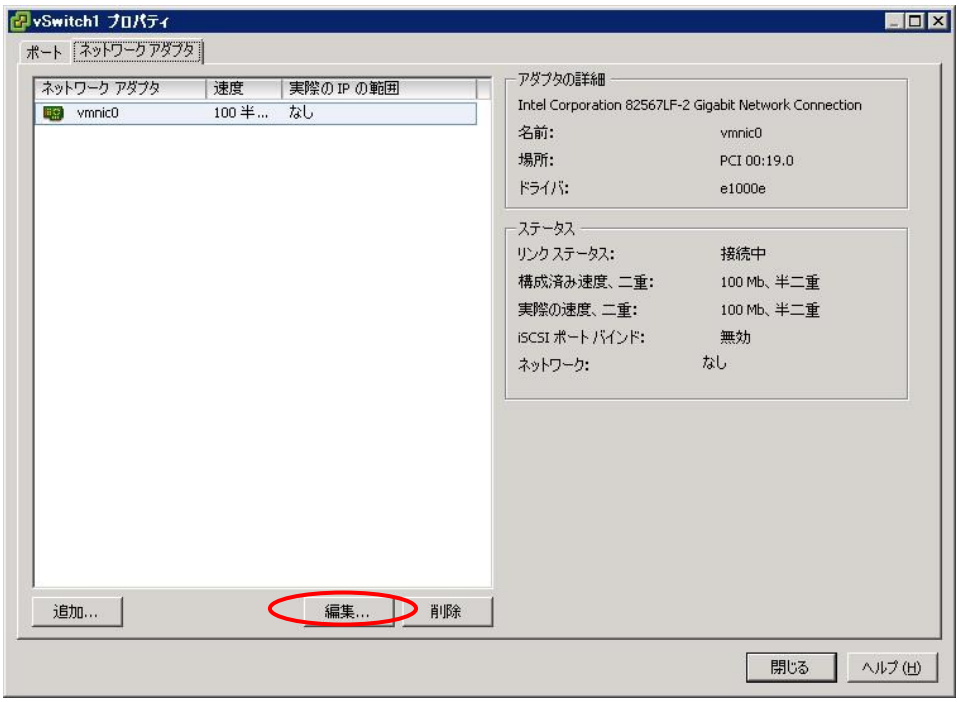
17. [構成]タブを開き、8 で作成した PSA-MMB-LAN の仮想スイッチの[プロパティ]をクリックします。



18. [ネットワークアダプタ]のタブをクリックします。

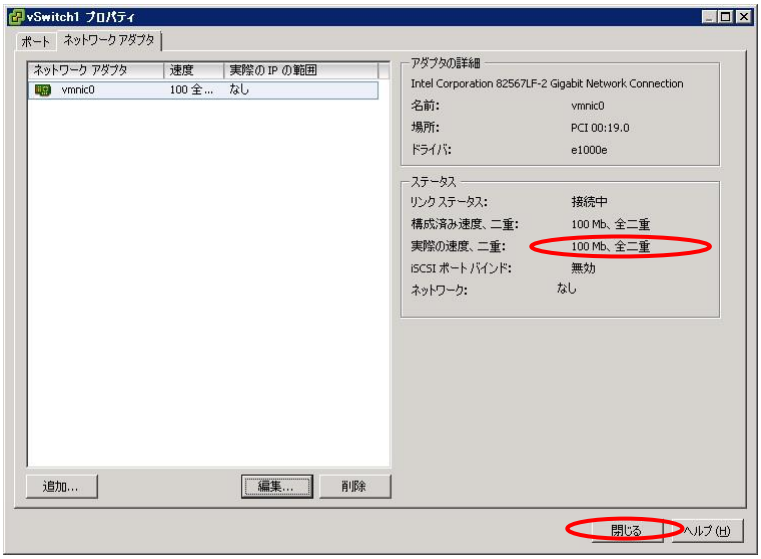


19. PSA-MMB 間通信 LAN の物理アダプタ(vmnic0)を選択し、[編集]をクリックします。



20. [構成済み速度、二重]を”100Mb,全二重”に設定し、[OK]をクリックします。

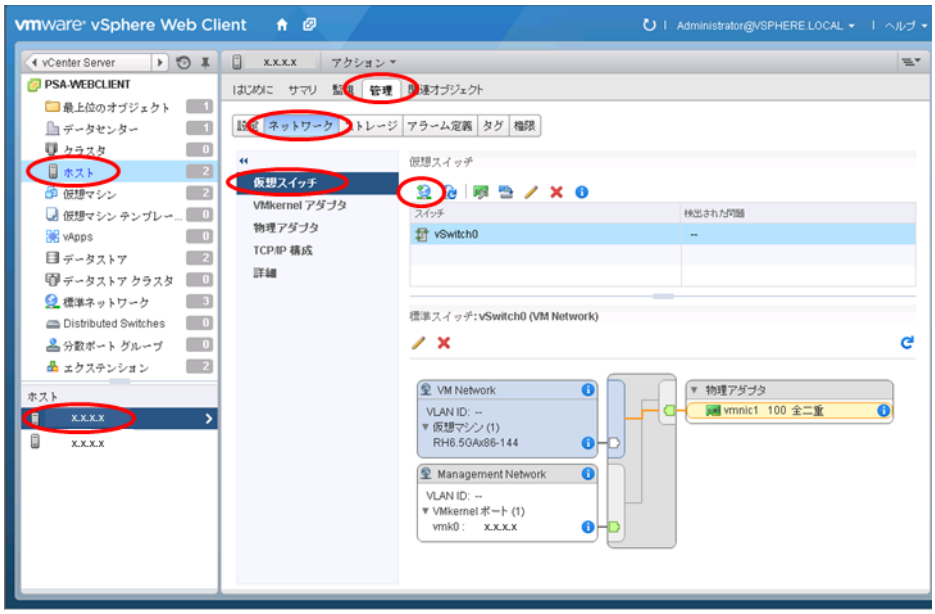
21. [ステータス]の実際の速度、二重が”100Mb,全二重”に設定されている事を確認して、[閉じる]をクリックします。



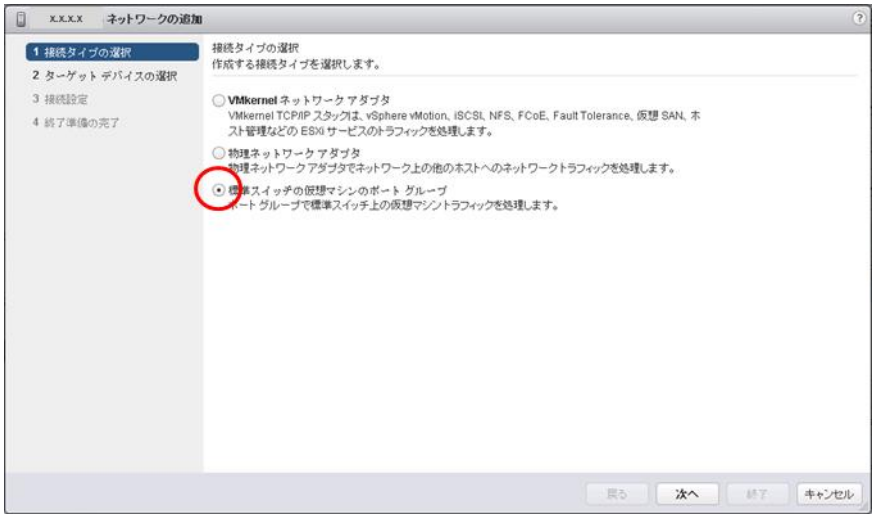
以上で、SVmcovm インストール前の PSA-MMB 間通信 LAN の設定は終了です。

2.4.2.4.2. VMware vSphere Web Client の場合

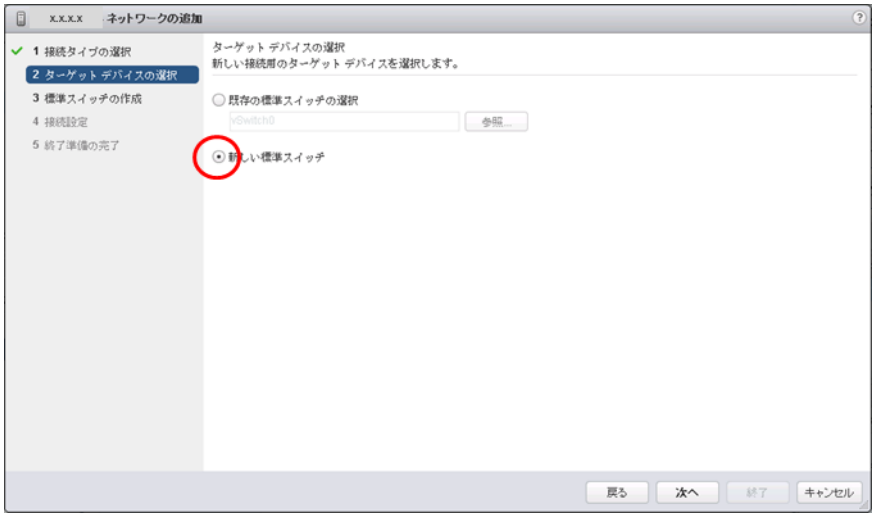
1. VMware vShpere Web Client を起動します。
2. [ホスト] → [対象ホストの IP アドレス] → [管理] タブをクリックします。
3. [ネットワーク]タブ→[仮想スイッチ]を選択します。
4. [仮想スイッチ]画面が表示されたら、 [ホスト、ネットワークを追加します]アイコンをクリックします。



5. [接続タイプの選択]は[標準スイッチの仮想マシンのポートグループ]をチェックし、[次へ]をクリックします。



6. [新しい標準スイッチ]をチェックし、[次へ]をクリックします。

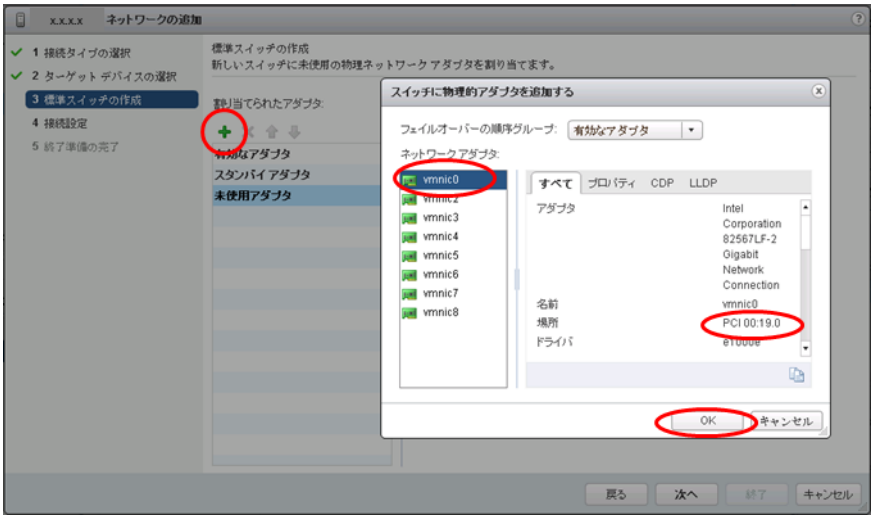


7. [+]アイコンの[アダプタを追加]をクリックします。

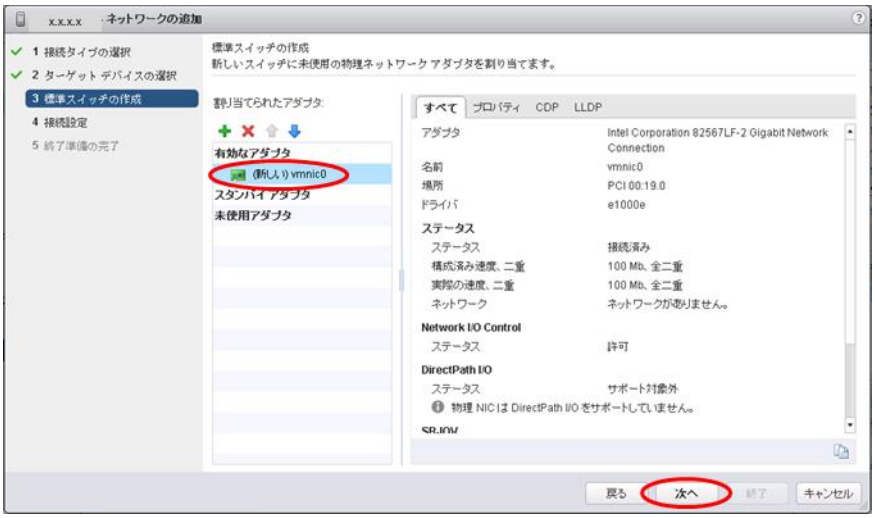
8. [スイッチに物理アダプタを追加する]が表示され、対象のネットワークアダプタを選択し、[OK]を選択します。

※対象のネットワークアダプタ

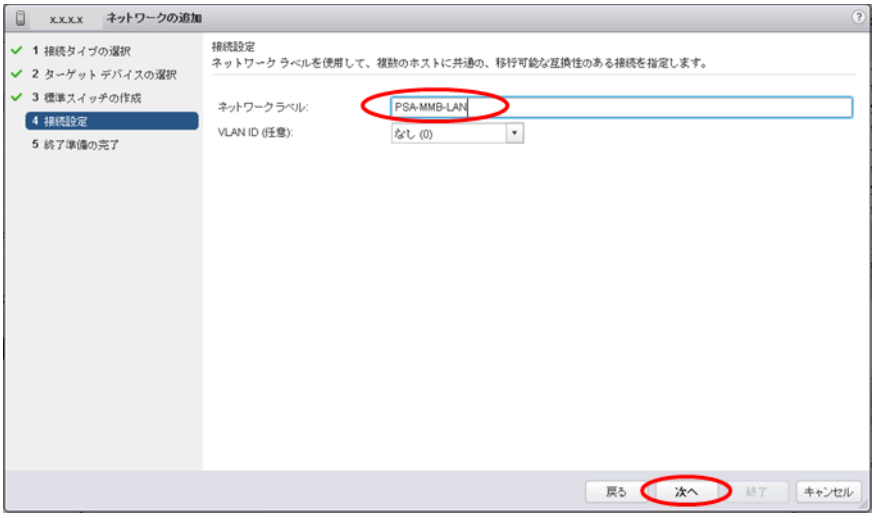
場所の項目から”PCI **00:19.0**”のネットワークアダプタ探します。



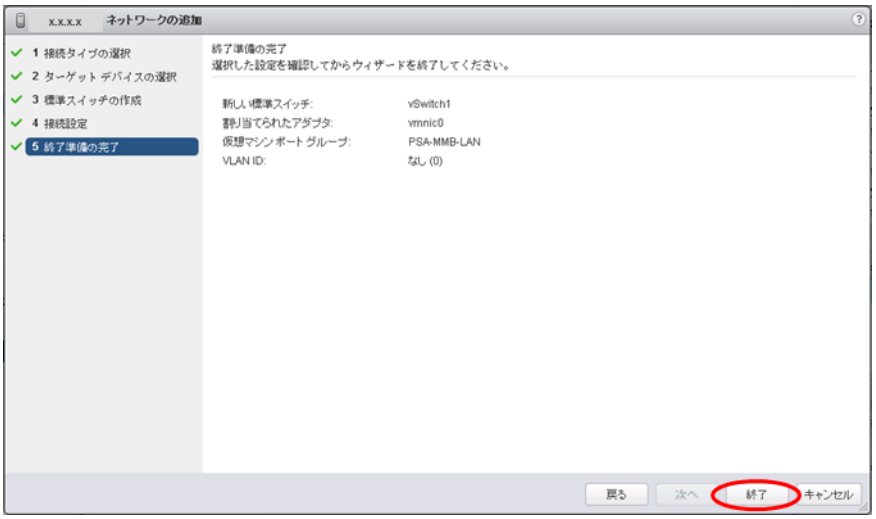
9. 追加されたネットワークアダプタを選択し、[次へ]をクリックします。



10. [ネットワークラベル]に PSA-MMB-LAN を設定し、[次へ]をクリックします。



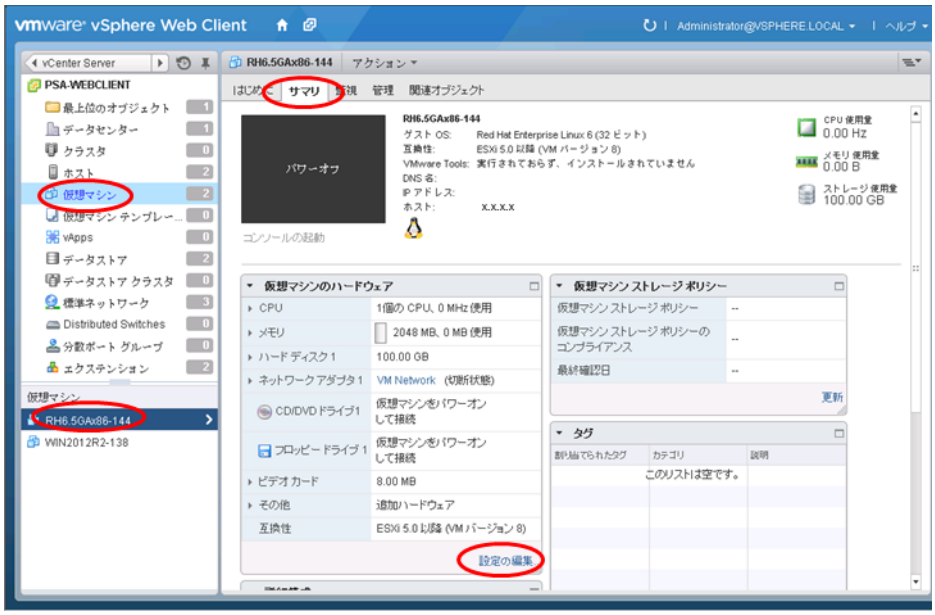
11. 設定内容を確認後、[終了]をクリックします。



12. [仮想マシン]→[対象仮想マシン名]、[サマリ]タブを選択し、[仮想マシンのハードウェア]の[設定の編集]をクリックします。

※対象仮想マシン名

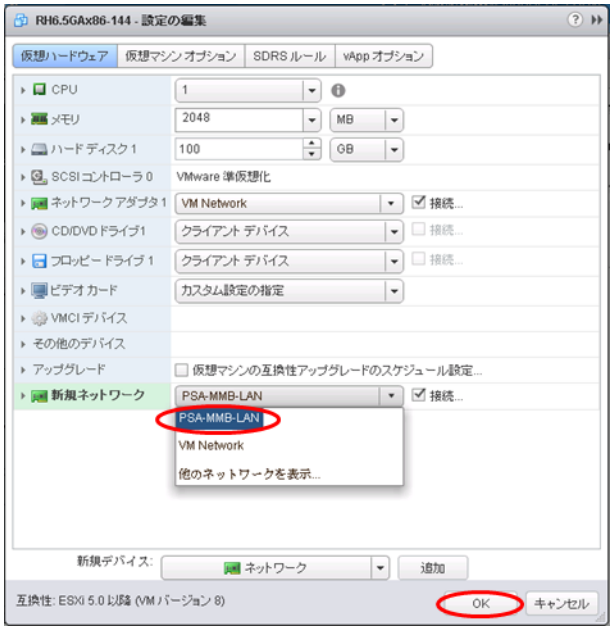
SVmcovm をインストール予定の管理用仮想マシン



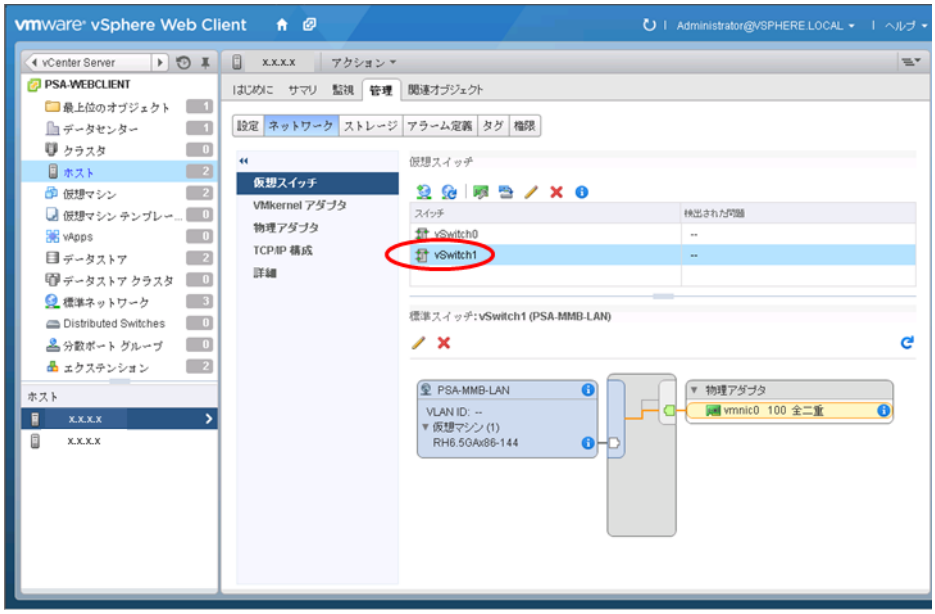
13. 設定の編集画面の[新規デバイス]のプルダウンをクリックし、[ネットワーク]を選択し、[追加]をクリックします。

14. 新規ネットワークが追加されます。

プルダウンより PSA-MMB-LAN を選択し、[OK]をクリックします。

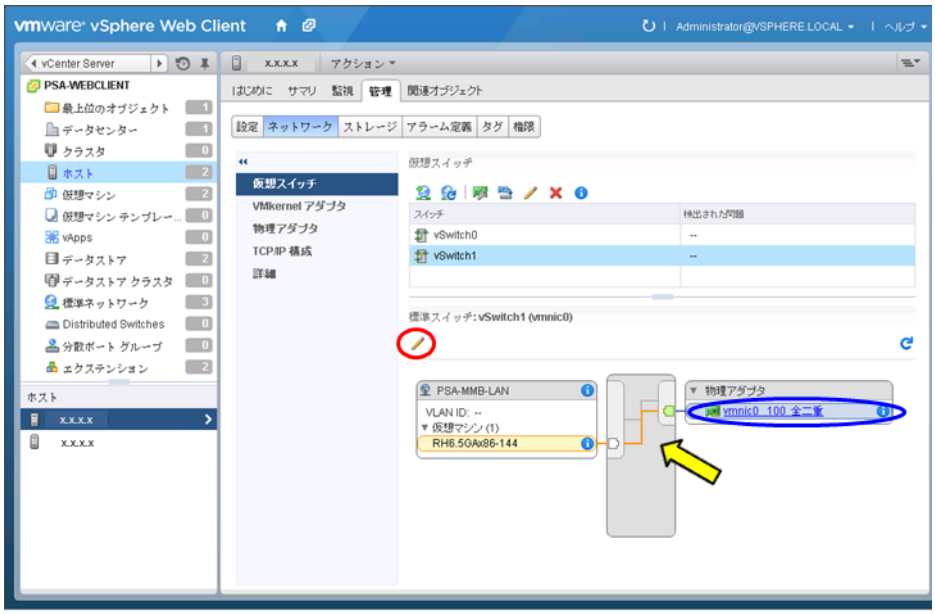


15. PSA-MMB 間通信 LAN の設定変更の為、ホストの仮想スイッチ画面を表示し、追加されたスイッチを選択します。



16. 物理アダプタの仮想ネットワークインタフェース名部分(図の青丸)をクリックし、仮想マシンと物理アダプタが結線されるのを確認します。(図の黄色矢印)

    結線確認後、[アダプタ設定の編集]アイコンをクリックします。(図の赤丸)



17. [構成済み速度、二重]を”100Mb,全二重”に設定し、[OK]をクリックします。

以上で、SVmcovm インストール前の PSA-MMB 間通信 LAN の設定は終了です。

2.4.2.5 ESXi からの情報取得用ネットワークの設定

ESXi から PCI カード情報と SVmcovm が起動する前に出力された PCI カード故障を示すログを採取するために専用のネットワークを設定します。

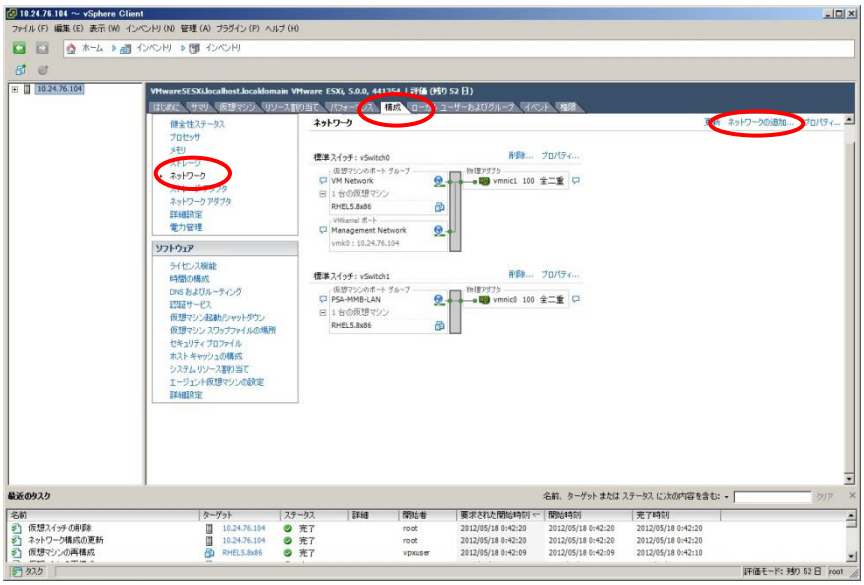
※本 ESXi から情報取得用ネットワークを設定しない場合は、管理通信用に既に作っているネットワークに対象の仮想

マシンを加えて下さい(ネットワーク構成例 2)。

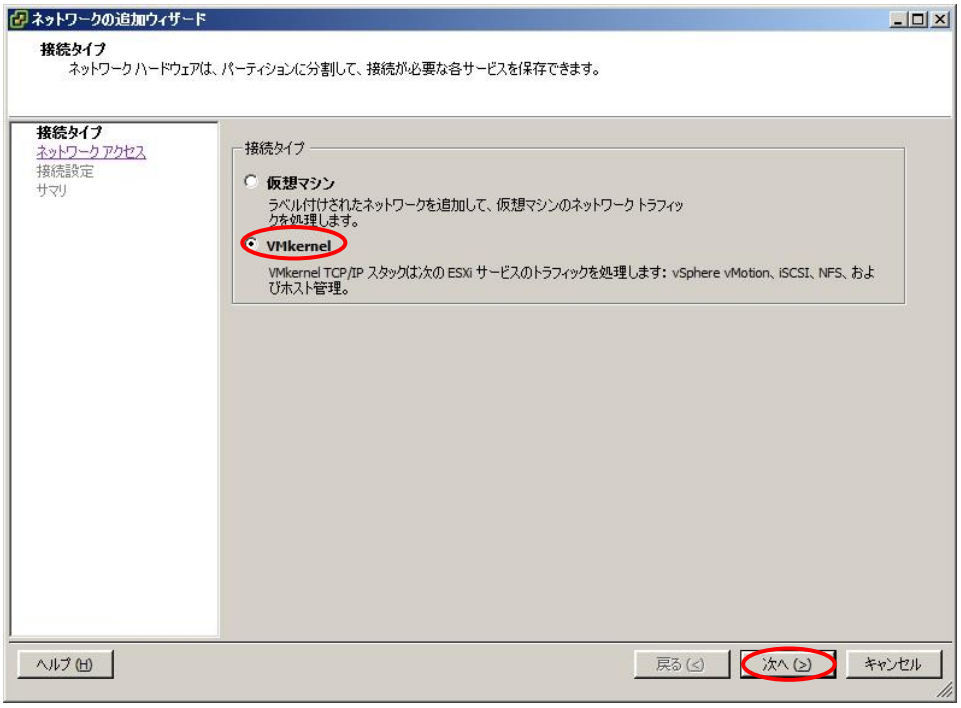
以下に、ESXi からの情報取得用ネットワークを設定する手順を示します。

2.4.2.5.1. VMware vSphere Client の場合

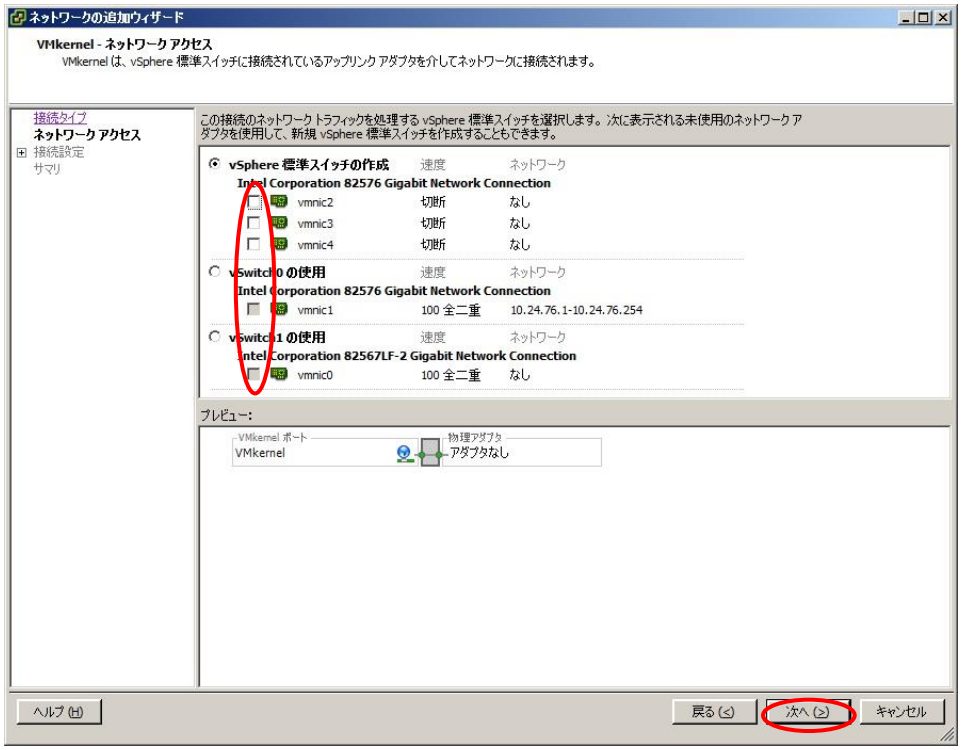
1. VMware vShpere Client を起動します。
2. [ホーム] → [インベントリ] → [インベントリ] から、[構成] タブをクリックします。
3. 左下にある [ハードウェア] 内の [ネットワーク] をクリックします。
4. [ネットワーク]が表示されたら、画面右上にある[ネットワークの追加]をクリックします。



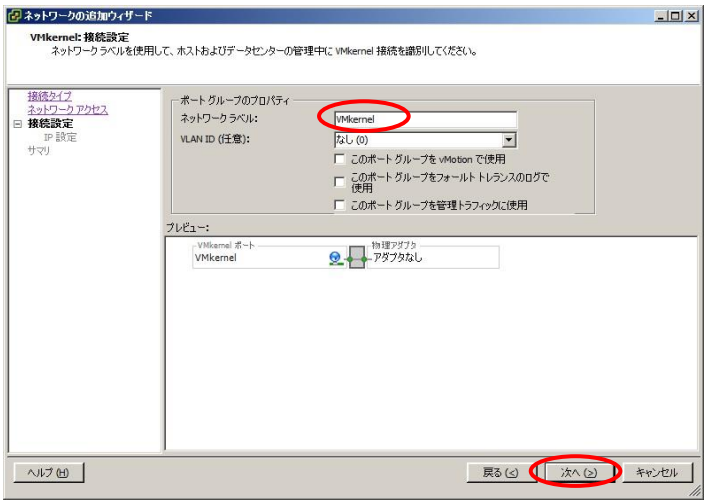
5. [接続タイプ]は VMkernel をチェックし、[次へ]をクリックします



6. 全ての物理 NIC からチェックを外し、 [次へ]をクリックします。

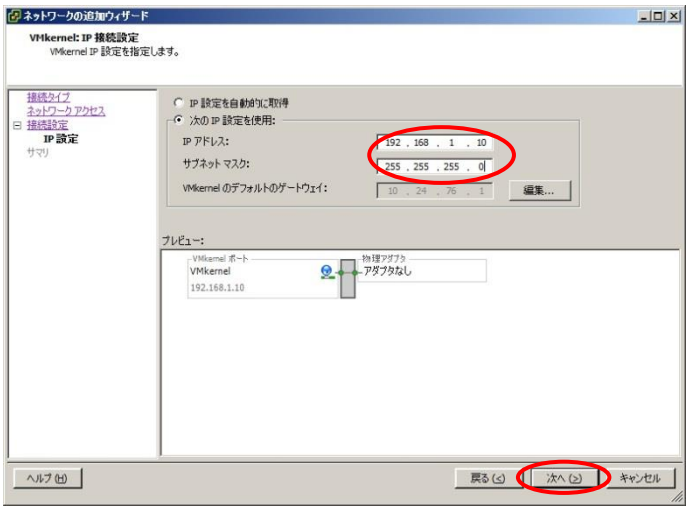


7. 任意のネットワークラベルを設定し[次へ]をクリックします。

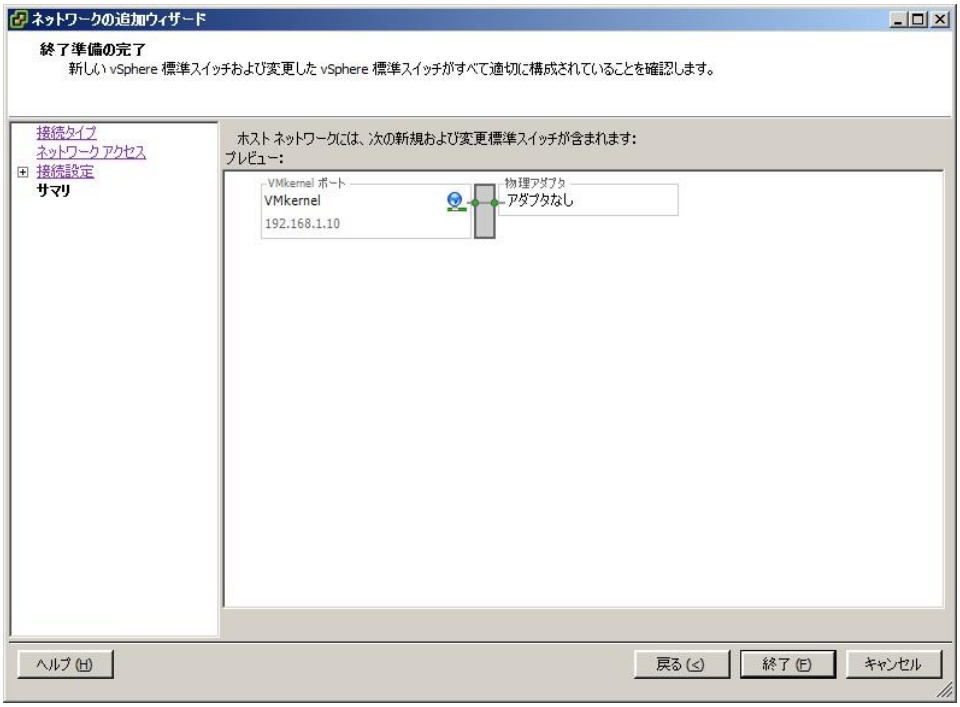


8. 次に IP とネットマスクを設定後、[次へ]をクリックします。(ここでは 192.168.1.10 と設定)

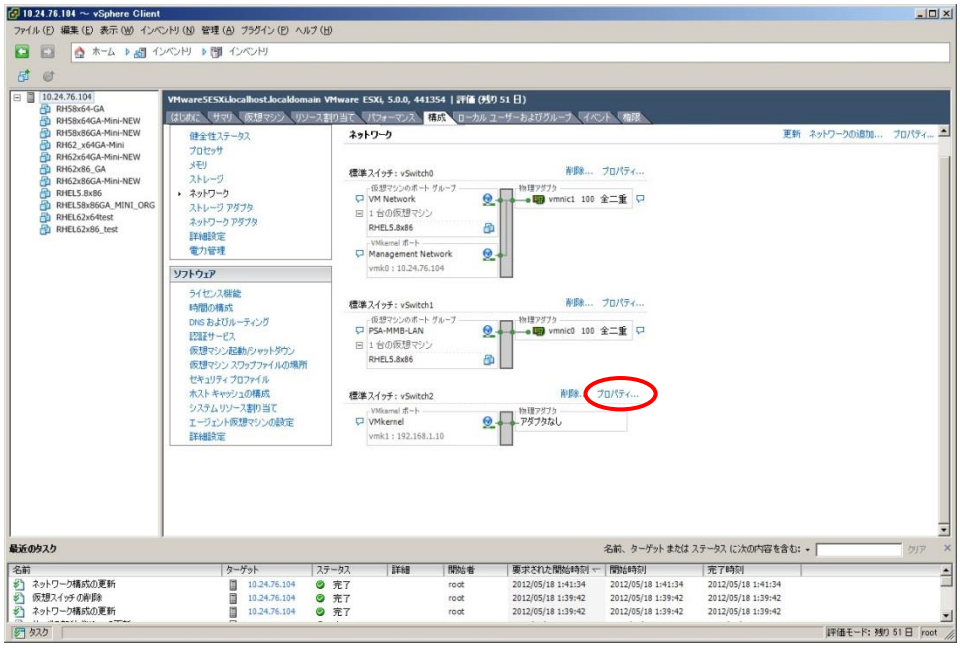
※ゲートウェイの設定を変更すると、管理用ネットワーク(ネットワーク構成例 1 の①)へ通信出来なくなる場合があるためのゲートウェイの値は変更しないで下さい。



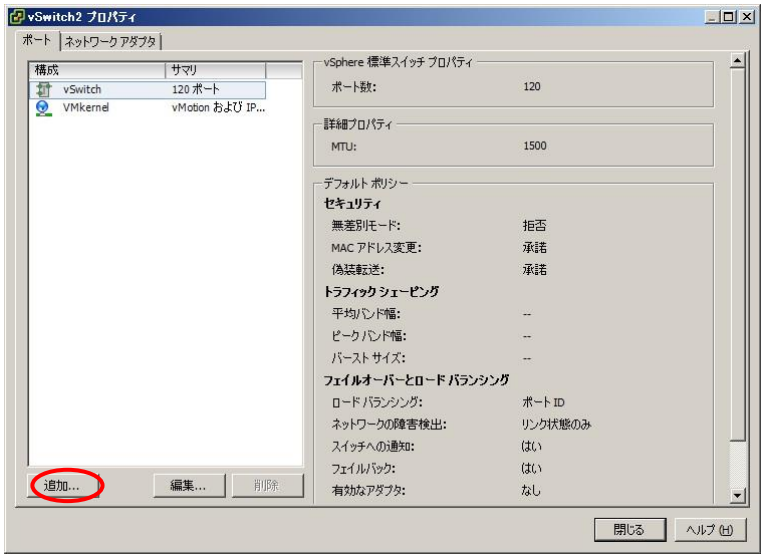
9. [VMkernel ポート]に設定したネットワークアダプタが設定されており、物理アダプタが接続されていないことを確認したら、[終了]をクリックします。



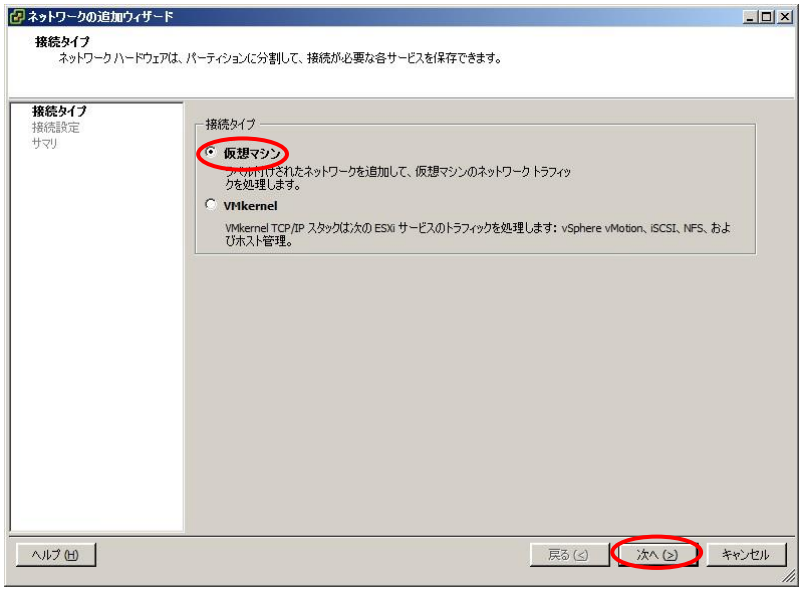
10. 対象のスイッチが作成されていることを確認後、スイッチの[プロパティ]を開きます。



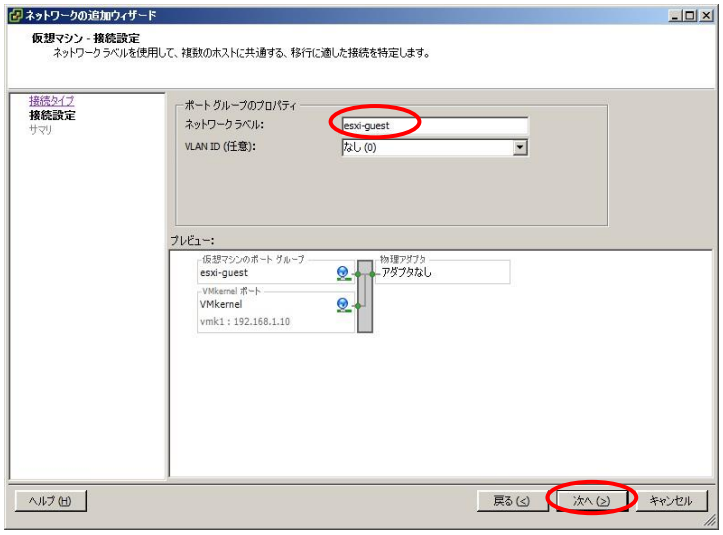
11. 追加をクリックします。



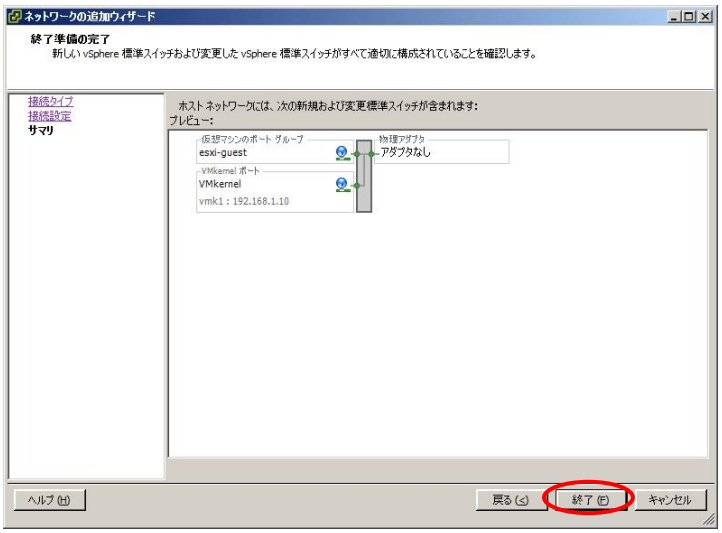
12. 接続タイプは[仮想マシン]を選択して、[次へ]をクリックします。



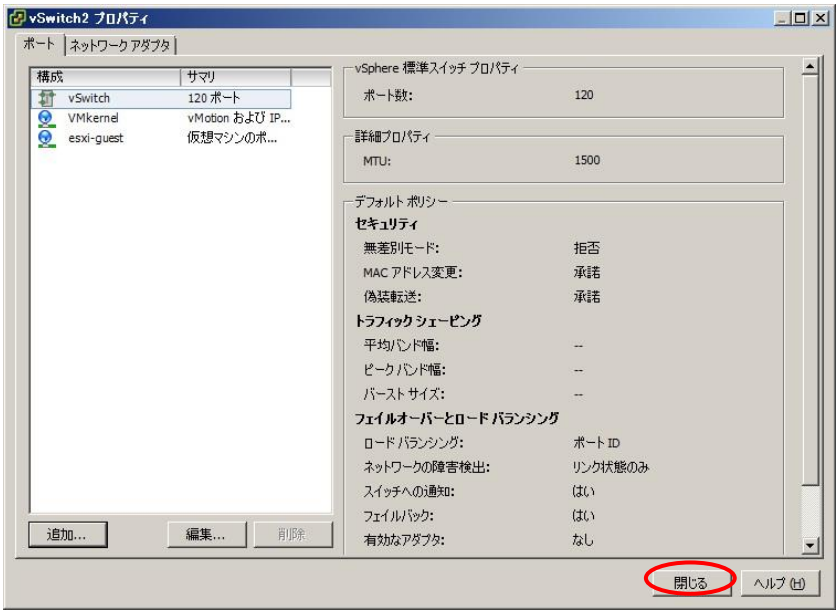
13. 任意のネットワークラベルを設定して[次へ]をクリックします。



14. 正しく設定されていることを確認したら[終了]をクリックします。

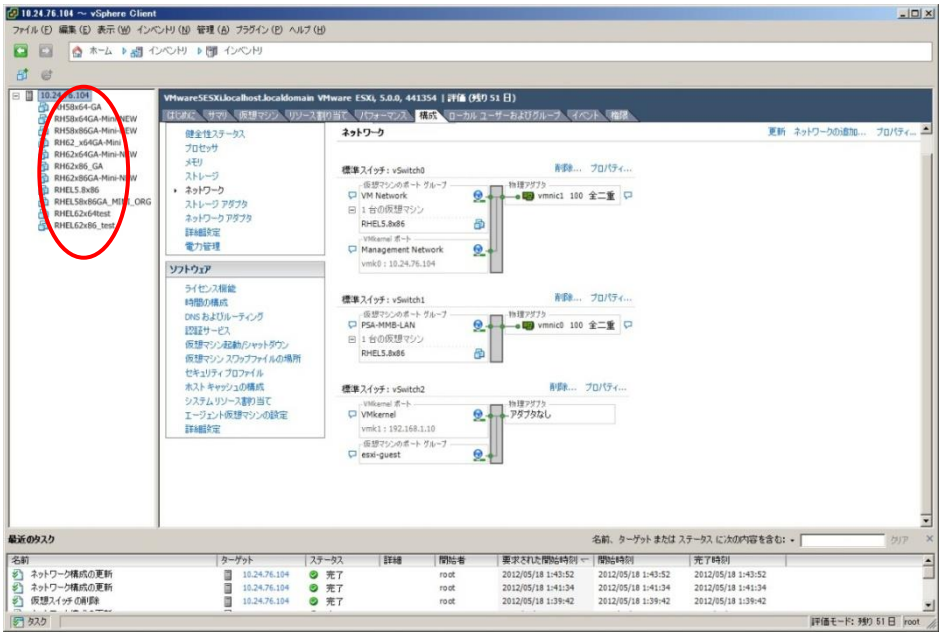


15. 構成に設定した仮想マシンのポートが追加されていることを確認したら、[閉じる]をクリックします。

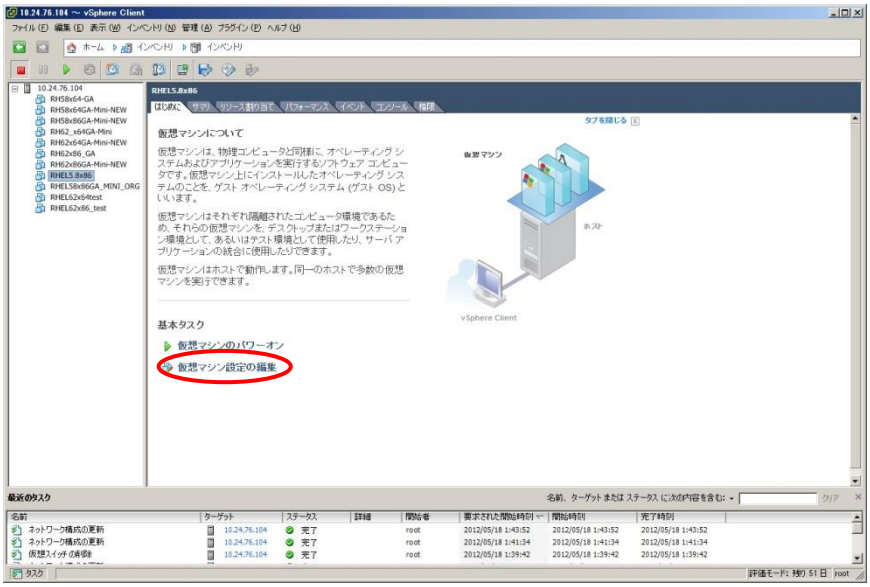


16. 作成した仮想スイッチに仮想マシンを割り当てます。

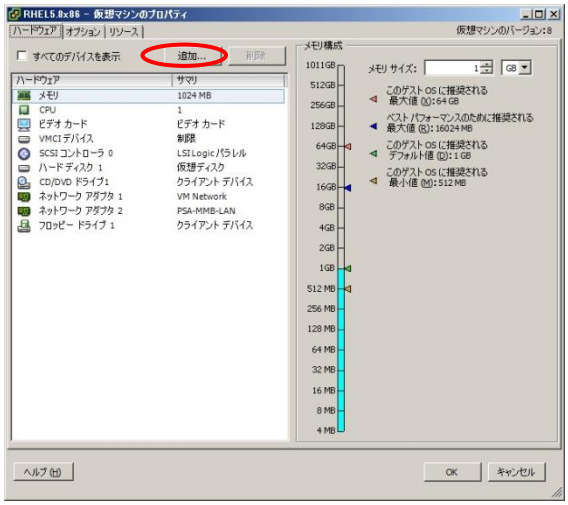
左側の仮想マシンリストから、SVmcovm のインストール予定の仮想マシンをクリックします。



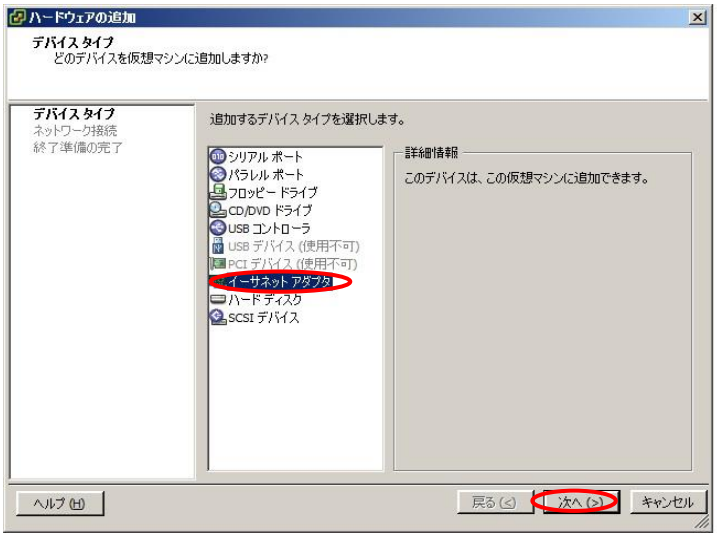
17. [はじめに]にタブから[仮想マシン設定の編集]をクリックします。



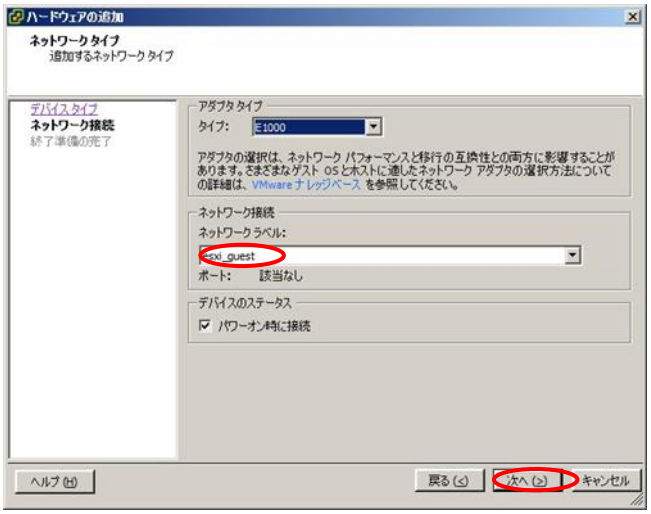
18. 仮想マシンのプロパティに[追加]をクリックします。



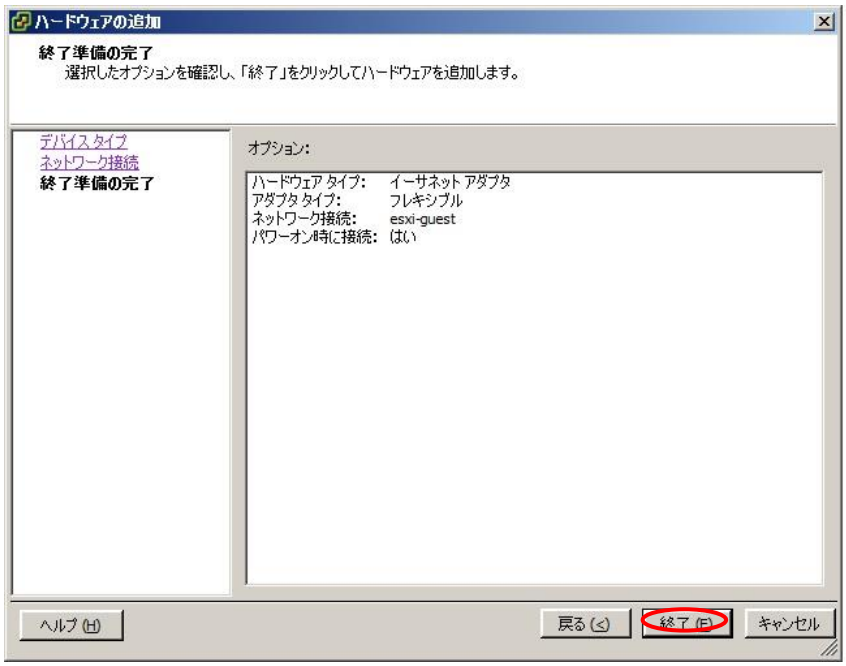
19. デバイスタイプは[イーサネットアダプタ]を選択し、[次へ]をクリックします。



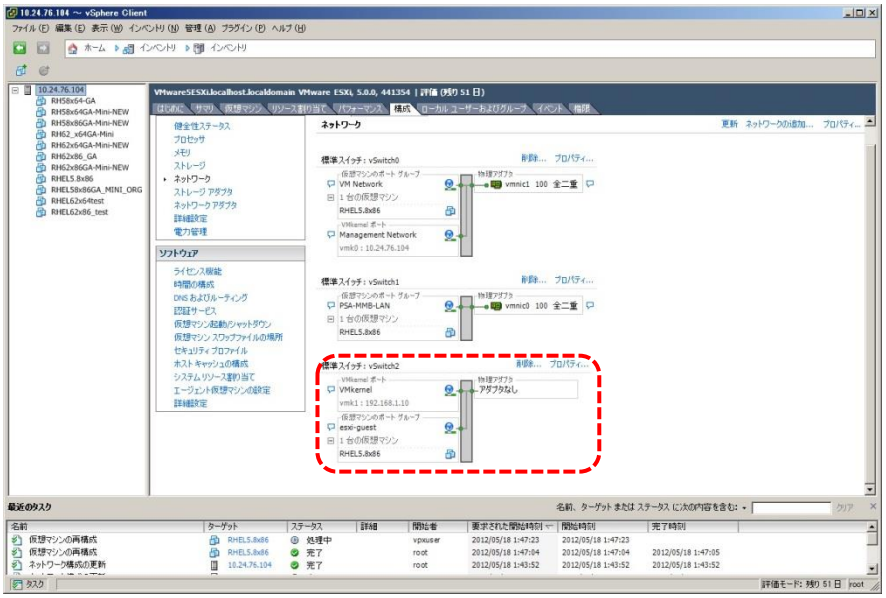
20. ネットワークラベルは、手順 13 で作成したネットワークを指定して、[次へ]をクリックします。



21. ネットワーク接続を確認したら、[終了]をクリックします。

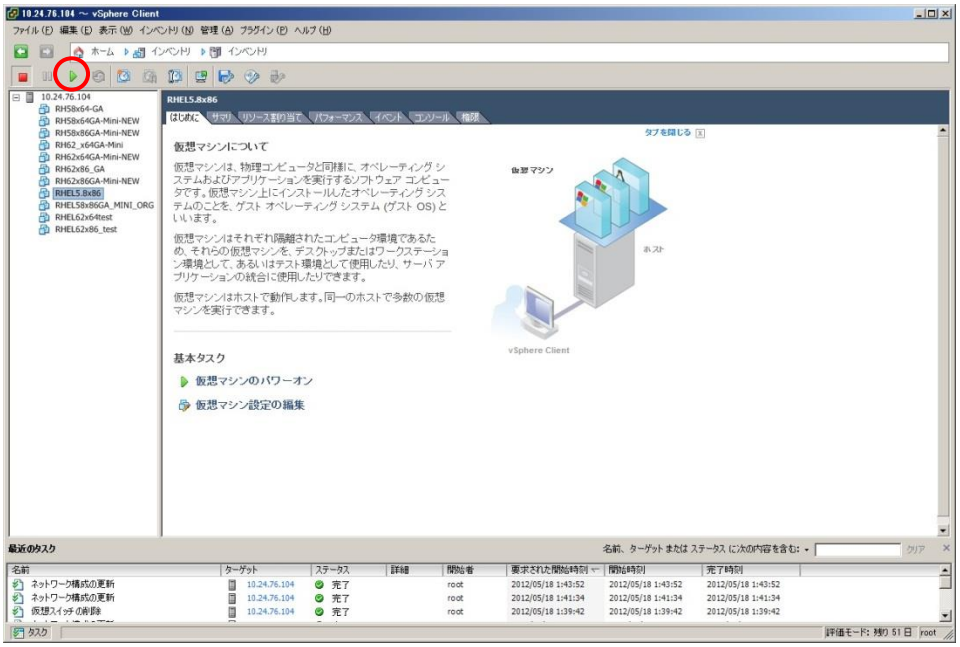


22. 左上から ESXi の IP アドレスを選択して、[構成]タブを選択します。ESXi-仮想マシン通信ネットワークに対象の仮想マシンが割り当たっていれば完了です。

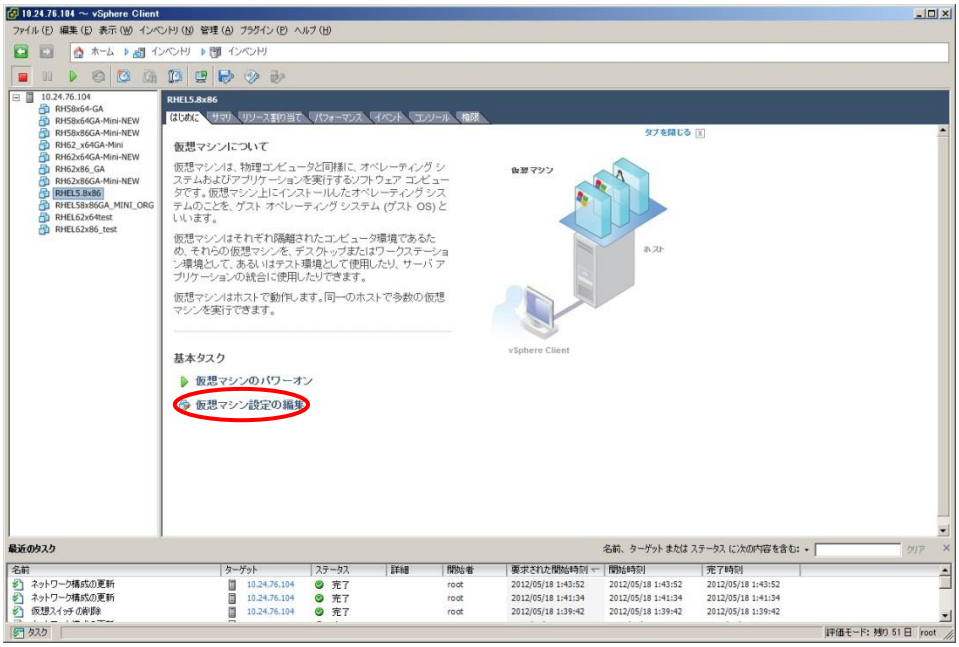


23. 次に以下の手順で仮想マシン上に割り振られた LAN の設定を行います。

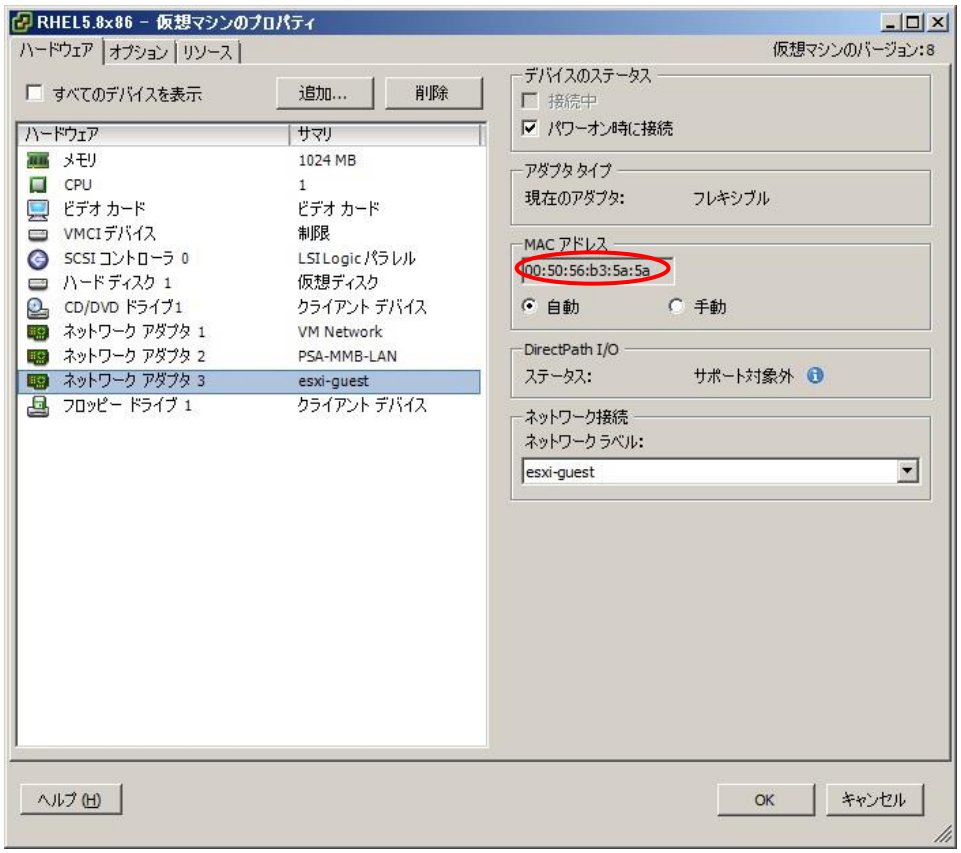
    1. VMware vShpere Client を起動します。
    2. 左上から仮想スイッチを割り当てた仮想マシンをクリックします。
    3. 上部にあるツールバーから[パワーオン]をクリックします。



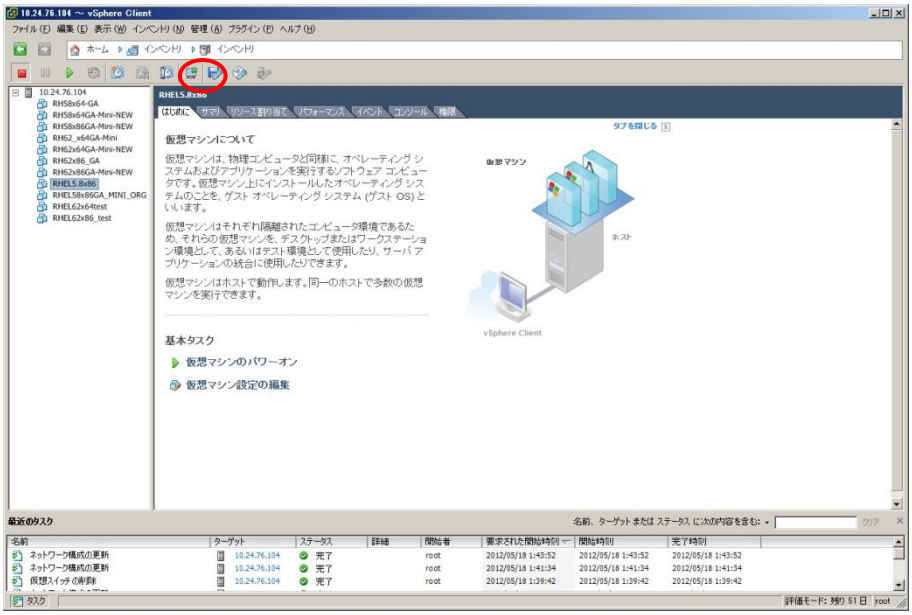
24. 仮想マシンが立ち上がったら、LAN の MAC アドレスを調べるために、[はじめに]タブの[仮想マシン設定の編集]をクリックします。



25. esxi との通信 LAN のネットワークアダプタを選び、[MAC アドレス]を確認します。確認後、[OK]をクリックします。

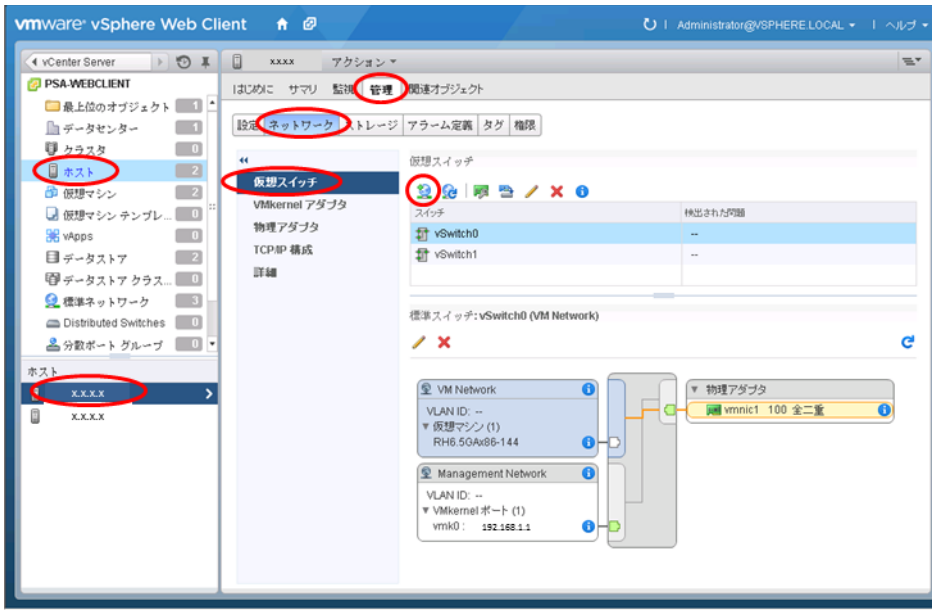


26. 仮想マシンの上部にあるツールバーから[仮想マシンコンソールの起動]をクリックしてコンソールを立ち上げます。

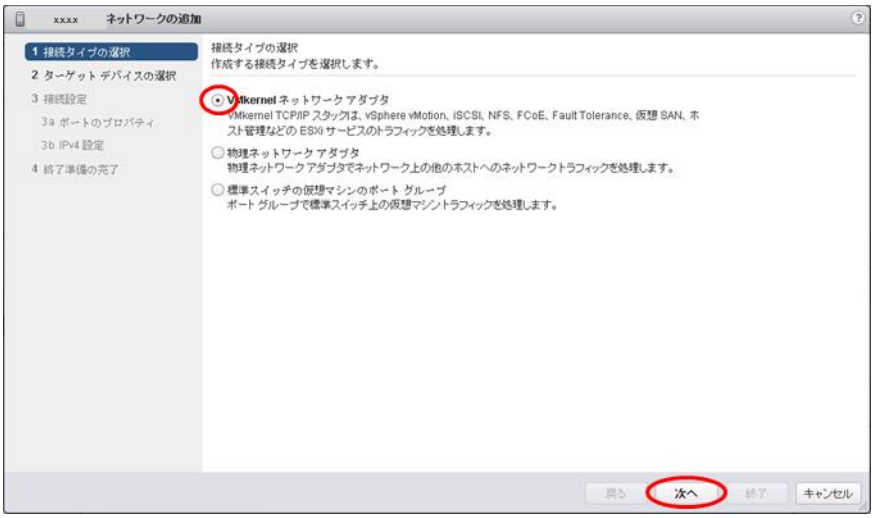


2.4.2.5.2. VMware vSphere Web Client の場合

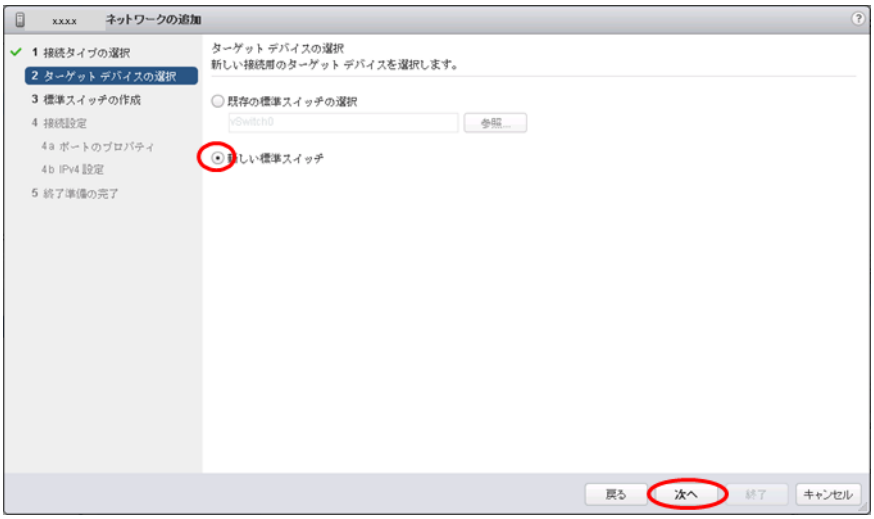
1. VMware vShpere Web Client を起動します。
2. [ホスト] → [対象ホストの IP アドレス] → [管理] タブをクリックします。
3. [ネットワーク]タブ→[仮想スイッチ]を選択します。
4. [仮想スイッチ]が表示されたら、 [ホスト、ネットワークを追加します]アイコンをクリックします。



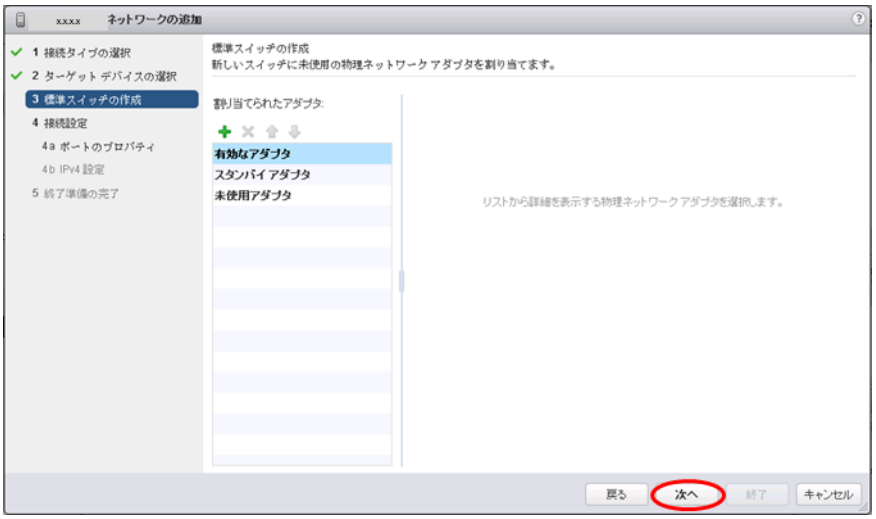
5. [VMkernel ネットワークアダプタ]をチェックし、[次へ]をクリックします



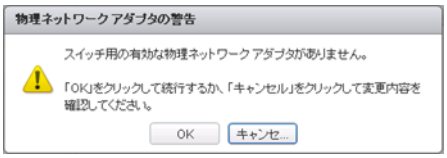
6. [新しい標準スイッチ]をチェックし、 [次へ]をクリックします。



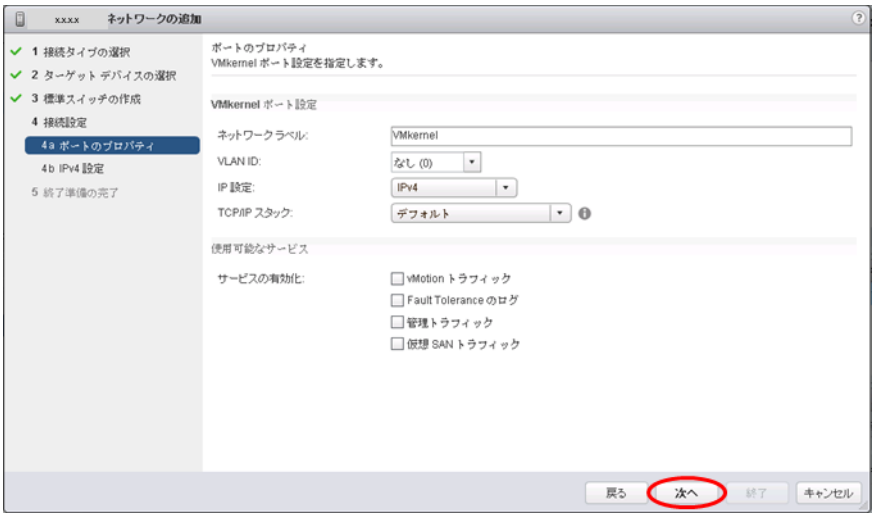
7. アダプタは選択せず、 [次へ]をクリックします。



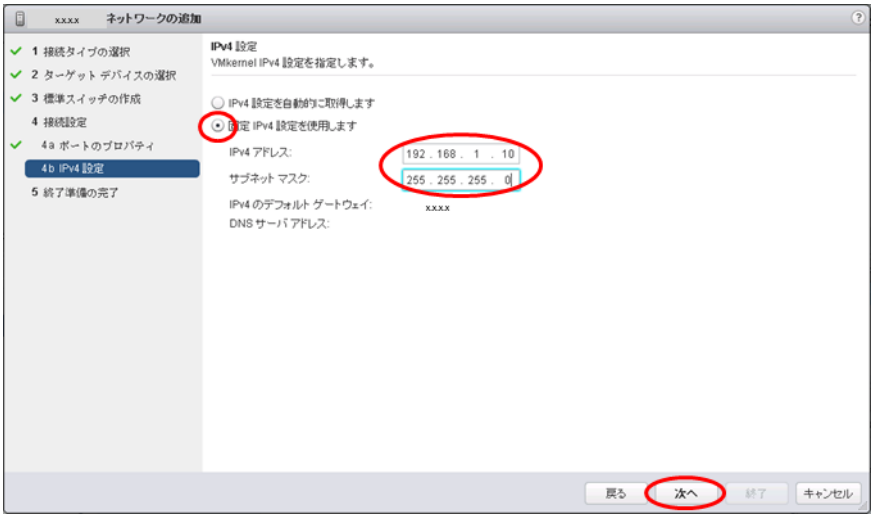
8. 物理ネットワークアダプタの警告が出ますが、 [OK]をクリックします。



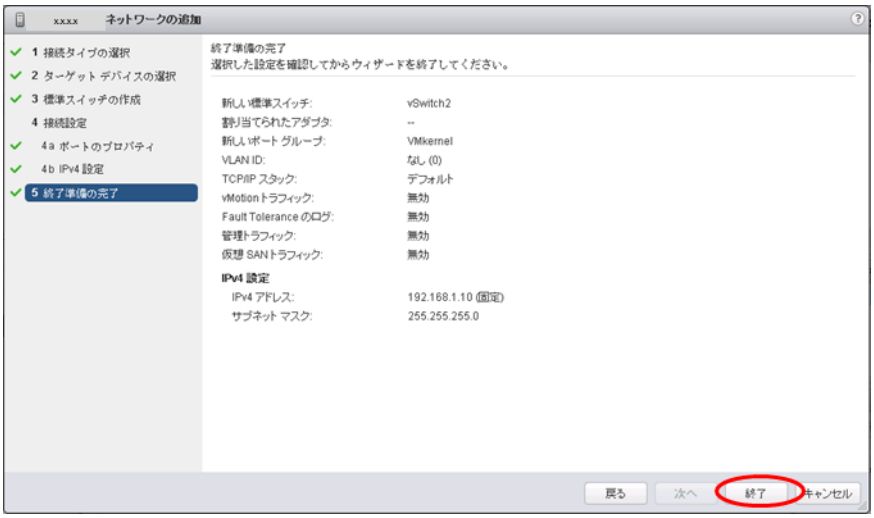
9. 任意のネットワークラベルを設定して[次へ]をクリックします。



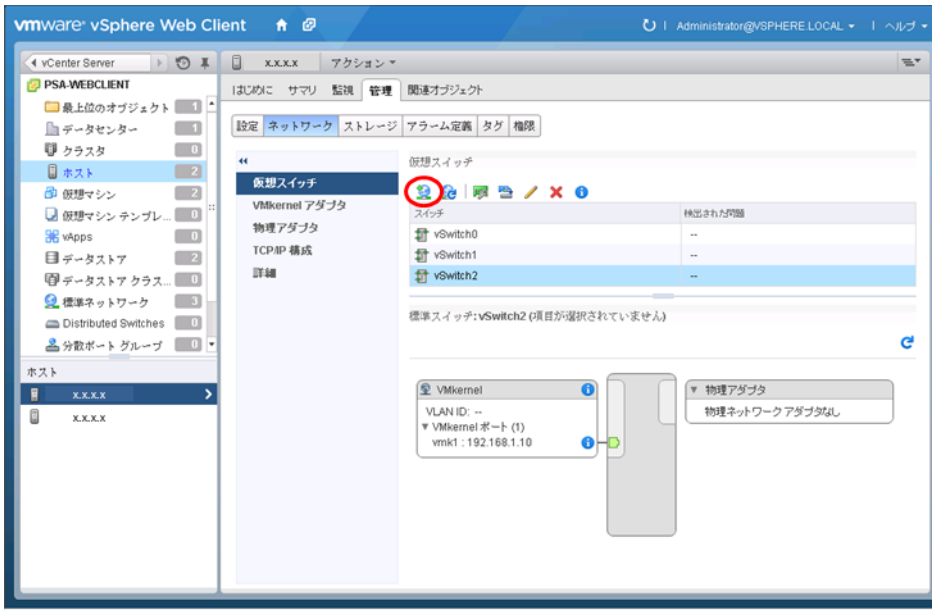
10. 次に IP とネットマスクを設定後、[次へ]をクリックします。(ここでは 192.168.1.10 と設定)



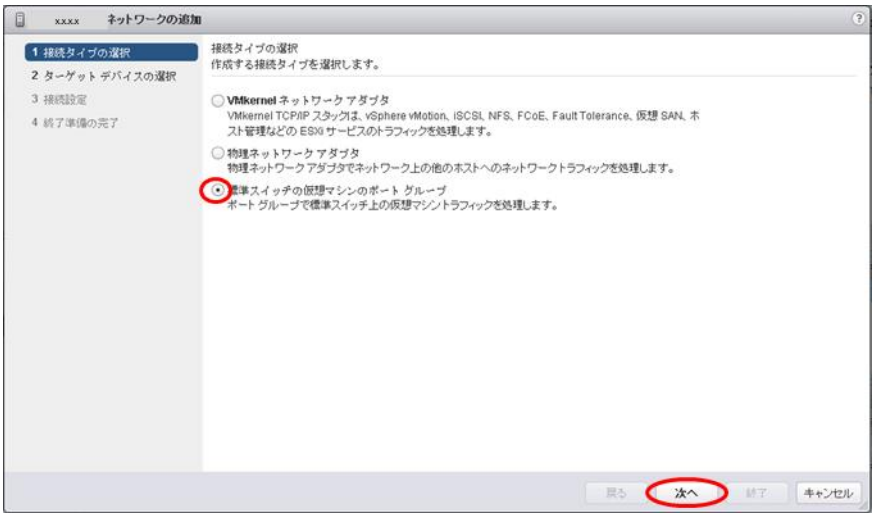
11. 設定内容を確認後、[終了]をクリックします。



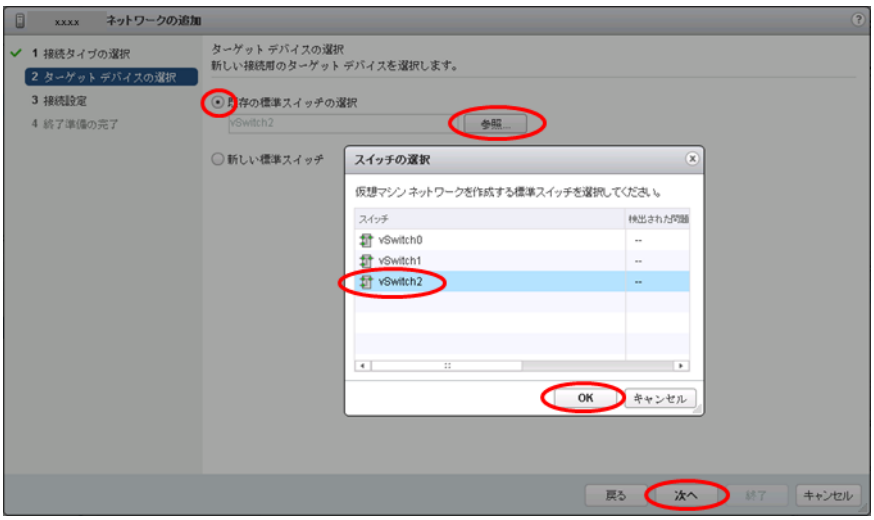
12. [ホストネットワークを追加します]アイコンをクリックします。



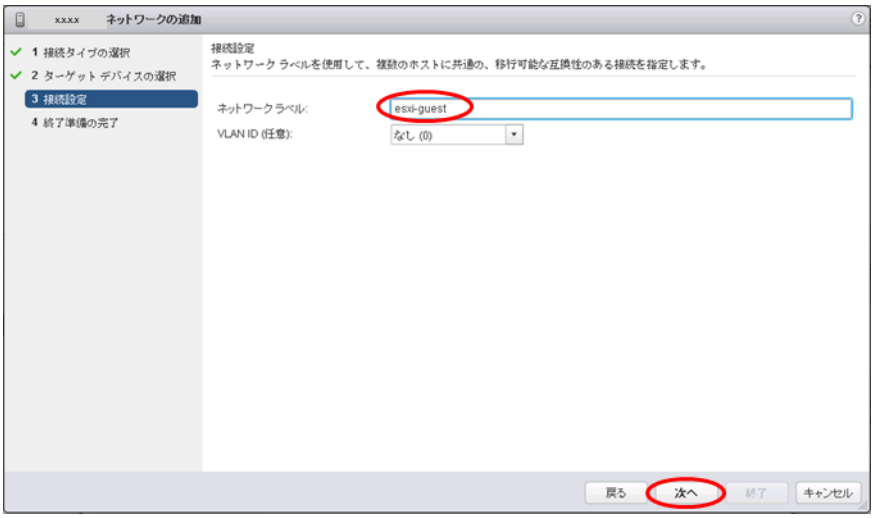
13. [標準スイッチの仮想マシンのポートグループ]を選択し、
[次へ]をクリックします。



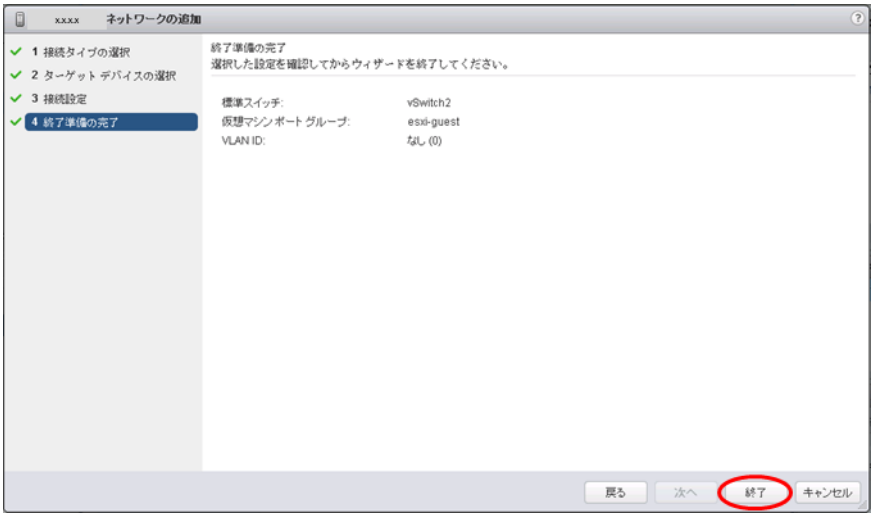
14. [既存の標準スイッチの選択]より手順 11 で作成したスイッチを選択し、
[次へ]をクリックします。



15. 任意のネットワークラベルを設定して[次へ]をクリックします。



16. 設定内容を確認後、 [終了]をクリックします。

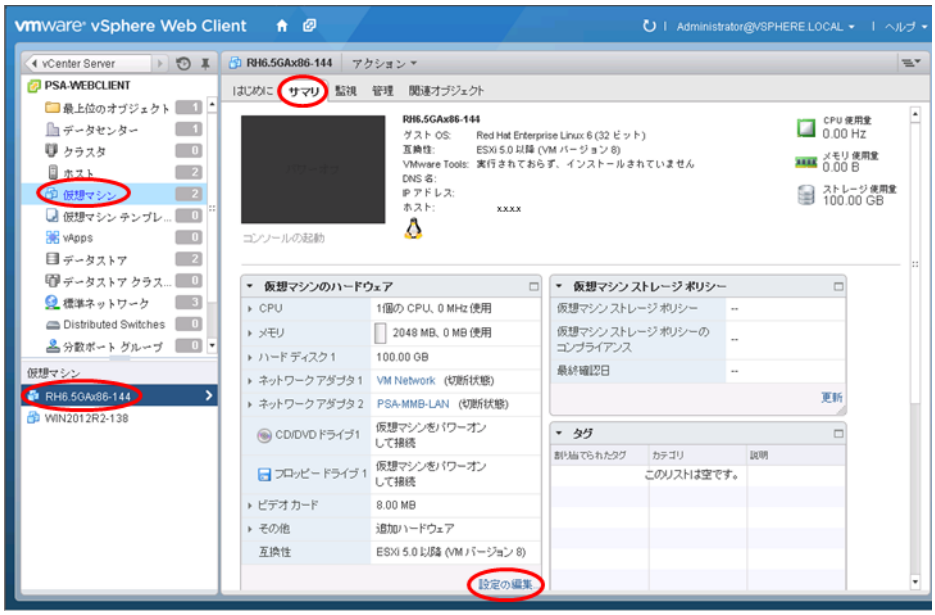


17. 作成した仮想スイッチに仮想マシンを割り当てます。

[仮想マシン]→[対象仮想マシン名]、[サマリ]タブを選択し、[仮想マシンのハードウェア]の[設定の編集]をクリックします。

※対象仮想マシン名

SVmcovm をインストール予定の管理用仮想マシン



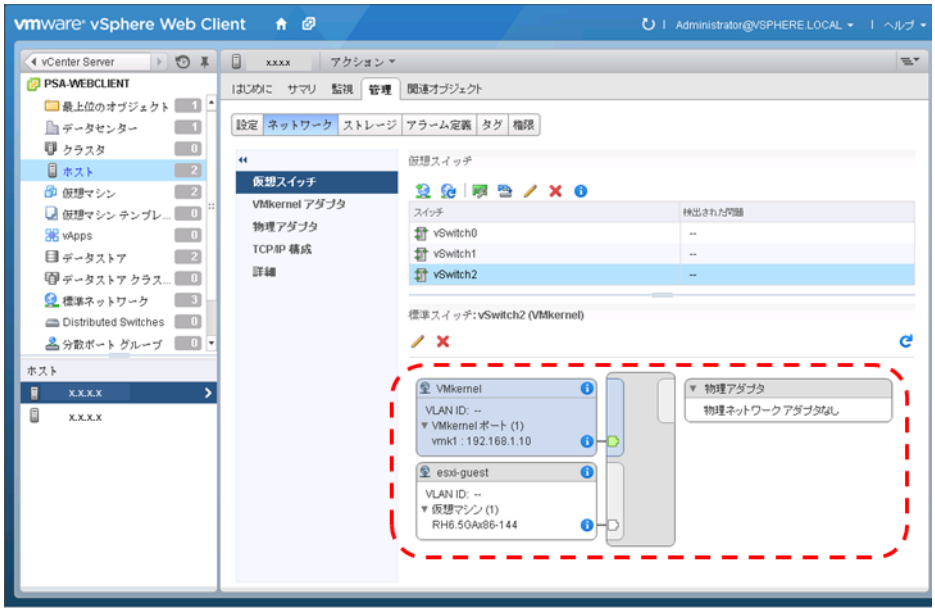
18. 設定の編集画面の[新規デバイス]のプルダウンをクリックし、[ネットワーク]を選択し、[追加]をクリックします。

19. 新規ネットワークが追加されます。

プルダウンより手順 16 で作成したネットワークを選択し、

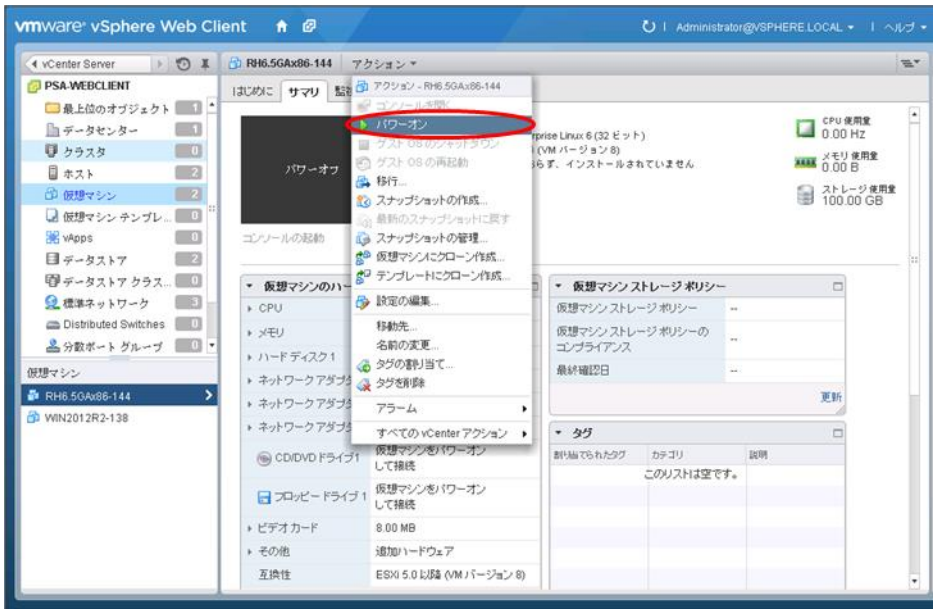
[OK]をクリックします。

20. 対象ホストの仮想スイッチ画面にいきます。ESXi-仮想マシン通信ネットワークに対象の仮想マシンが割り当たっていれば完了です。

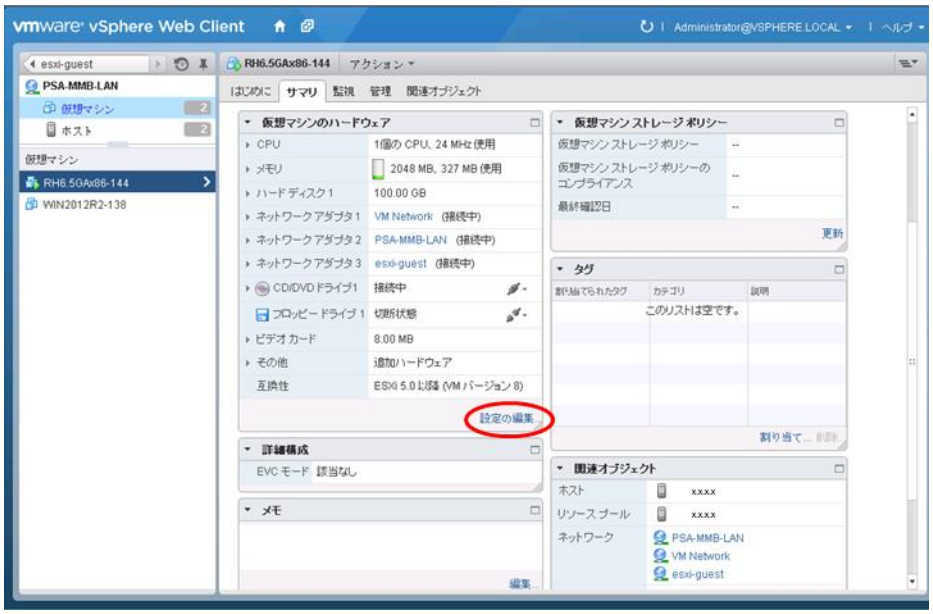


21. 次に以下の手順で仮想マシン上に割り振られた LAN の設定を行います。

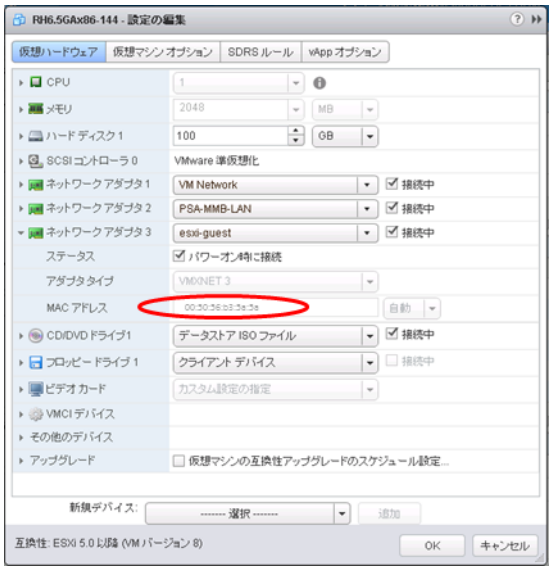
    1. VMware vShpere Web Client を起動します。
    2. 対象ホストを選択し、[アクション]プルダウンより、パワーオンをクリックします。



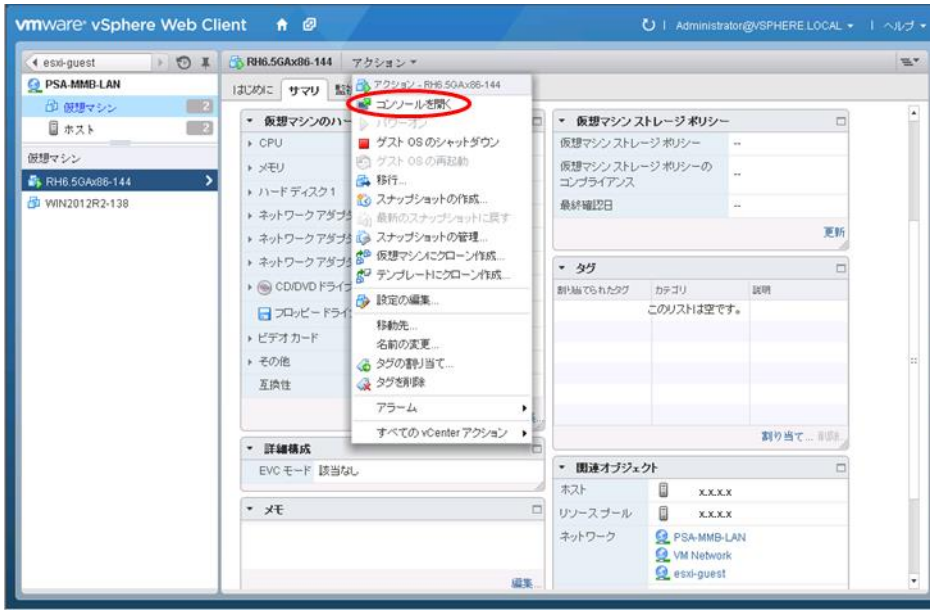
22. 仮想マシンが立ち上がったら、LAN の MAC アドレスを調べるために、対象仮想マシンの[仮想マシンのハードウェア]の[設定の編集]をクリックします。



23. esxi との通信 LAN のネットワークアダプタを選び、[MAC アドレス]を確認します。確認後、[OK]をクリックします。



24. [アクション]プルダウンより、 [コンソールを開く]をクリックしてコンソールを立ち上げます。



2.4.2.5.3. Linux(Red hat Enterprise Linux)の場合

1. 仮想コンソールなどでログインする。

2. ログインしたら、端末を立ち上げて、以下のコマンドを実行し、2.4.2.5.1 章の手順 25 または 2.4.2.5.2 章の手順 23 で確認した MAC アドレスからネットワークインターフェースを探します。

```
# ifconfig –a | grep –i <esxi-仮想マシン間通信 LAN の MAC アドレス>
```

【実行結果(例)】

```
# ifconfig –a | grep –i 00：50：56：b3：5a：5a
eth2 Link encap:Ethernet Hwaddr 00：50：56：b3：5a：5a
#
```

実行結果より、”eth2”が esxi-仮想マシン間通信 LAN ということが確認できました。

3. 以下のディレクトリに移動します。

```
# cd /etc/sysconfig/network-scripts
```

4. エディターなどで、対象のネットワークインターフェースの設定を開きます。
ここでは、eth2 の設定ファイルを開いています。

```
# vi ifcfg-eth2
```

5. 設定ファイルを編集します。IP アドレスは 2.4.2.5.1 章の手順 8 または 2.4.2.5.2 章の手順 10 で設定した ESXi からの情報取得用 IP と同じサブネットの IP を設定してください。

<IP を 192.168.1.20 と設定した場合>

【編集前】

```
DEVICE = eth2
BOOTPROTO = dhcp
ONBOOT = yes
HWADDR = 00：50：56：b3：5a：5a
```

【編集後】

```
DEVICE = eth2
BOOTPROTO = static
ONBOOT = yes
HWADDR = 00：50：56：b3：5a：5a
IPADDR = 192.168.1.20
NETMASK = 255.255.255.0
```

6. 設定反映のためにネットワークを再起動します。

```
# /sbin/service network restart
```

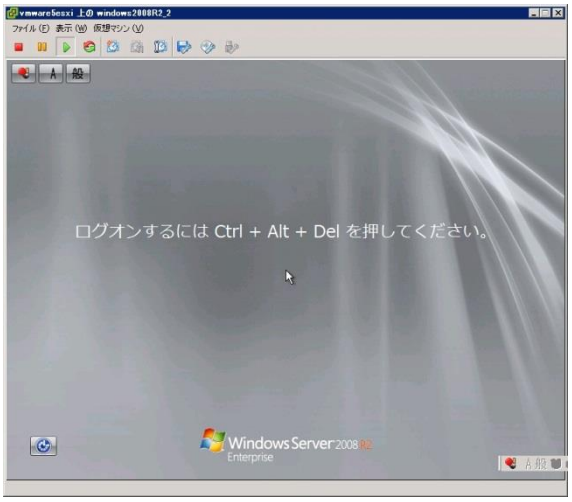
7. ESXi(ここでは 192.168.1.10)に対して、Ping 応答があることを確認します。

```
# ping 192168.1.10
```

以上で ESXi-仮想マシン間のネットワーク設定は終了です。

2.4.2.5.4. Windows(Windows Server 2008/2012)の場合

1. 仮想コンソールなどで、仮想 OS にログインします。

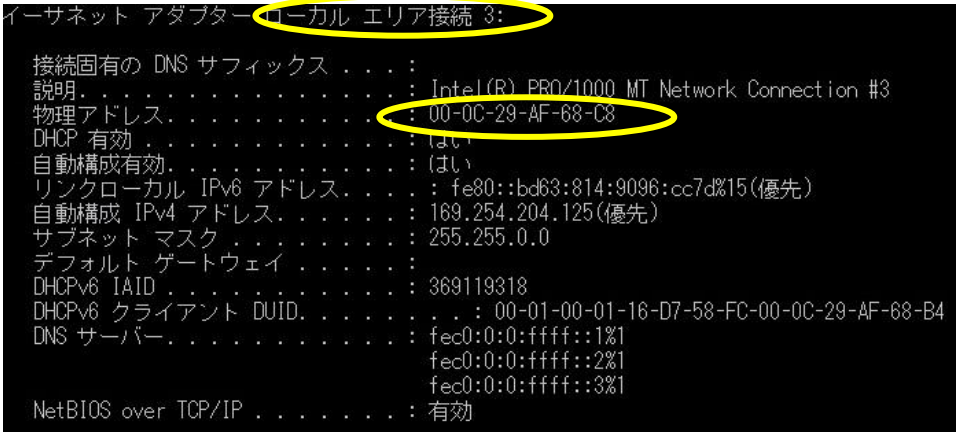


2. ログインしたら、コマンドプロンプトを立ち上げて、以下のコマンドを実行し、esxi-仮想マシン通信 LAN が割り当たっているネットワークインターフェースを調べます。検索には MAC アドレスは 2.4.2.5.1 章の手順 25 または 2.4.2.5.2 章の手順 23 で確認した値を使います。

```
> ipconfig /all
```

【実行結果(例)】

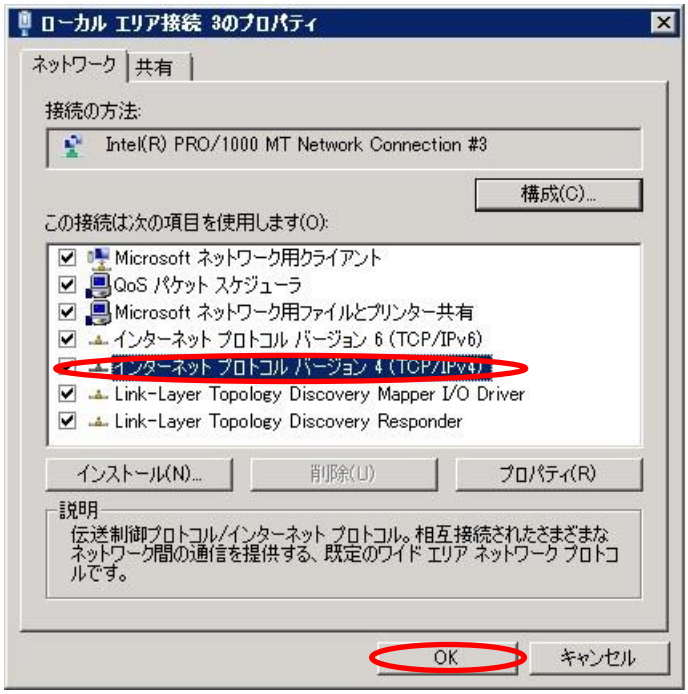
(esxi-仮想マシン通信 LAN の MAC アドレスが 00:0C:29:AF:68:C8 の場合)



実行結果より、”ローカルエリア接続 3”が esxi-仮想 OS 間通信 LAN ということが確認できました。

3. [コントロールパネル] -> [ネットワークとインターネット] -> [ネットワークの共有センター]を開き、手順 2 で確認した LAN(ここでは、ローカルエリア接続 3)を選びます。

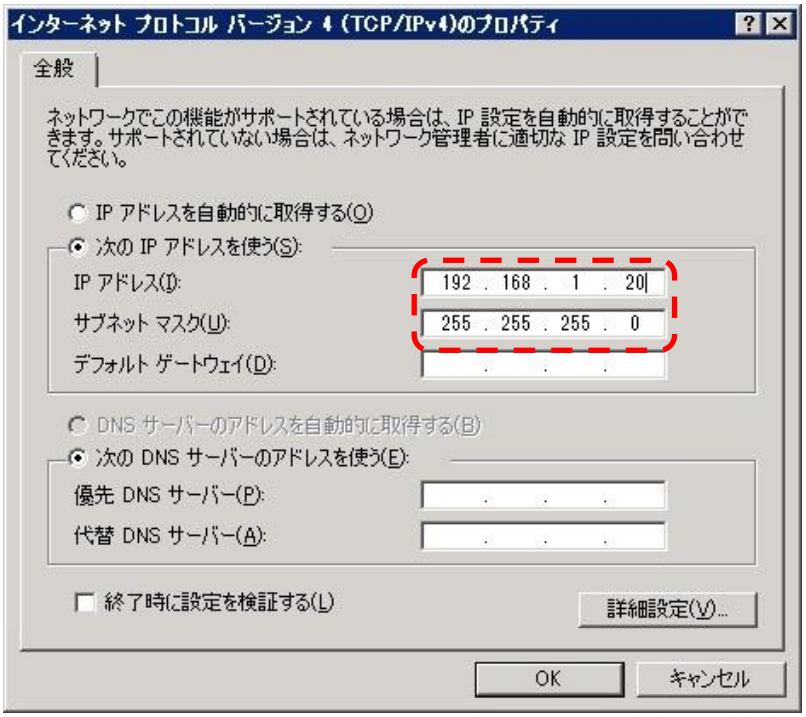
4. ローカルエリア接続 3 の[プロパティ]から[インターネットプロトコルバージョン 4(TCP/IPv4)]を選んだ状態で、[プロパティ]をクリックします。



5. IP アドレスを設定します。2.4.2.5.1 章の手順 8 または 2.4.2.5.2 章の手順 10 で設定した ESXi からの情報取得用 IP アドレスと同じサブネットにして下さい。

ここで設定した IP アドレスは、SVmcovm インストール後の設定 2.4.10.4.1 ログ転送設定 1(Syslog Collector が使用出来る場合)で使用します。

例：ESXi 側に割り当てている IP が 192.168.1.10 の場合



6. ESXi(ここでは 192.168.1.10)に対して、Ping 応答があることを確認します。

```
# ping 192.168.1.10
```

以上で ESXi-仮想マシン間のネットワーク設定は終了です。

2.4.2.6 仮想マシンの自動起動設定

SVmcovm がインストールされている仮想マシンは、ESXi 起動と同期して SVmcovm が異常監視を開始することを推奨します。

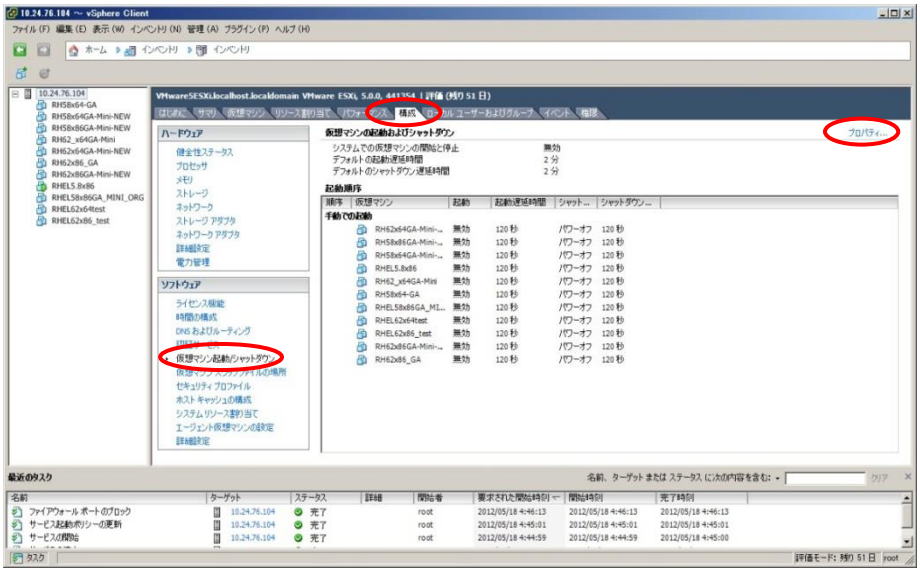
ただし、自動起動しない場合は、以下の故障検出が遅れます。

1. PCI カード/ディスクの故障検出： SVmcovm 起動後に検出開始。
2. MMB の PCI レーン縮退監視： システムステータスが OS Running に変更後に検出開始。

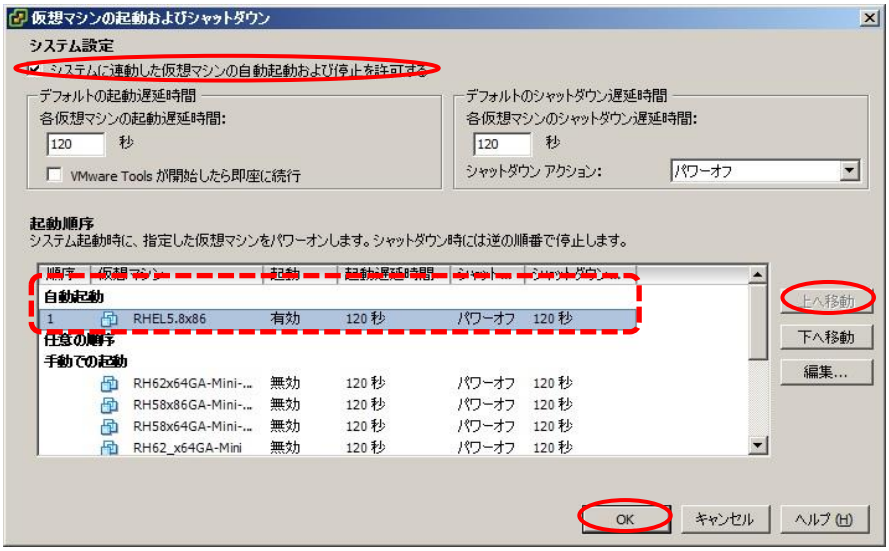
以下では、仮想マシンを自動起動する手順を示します。

2.4.2.6.1. VMware vSphere Client の場合

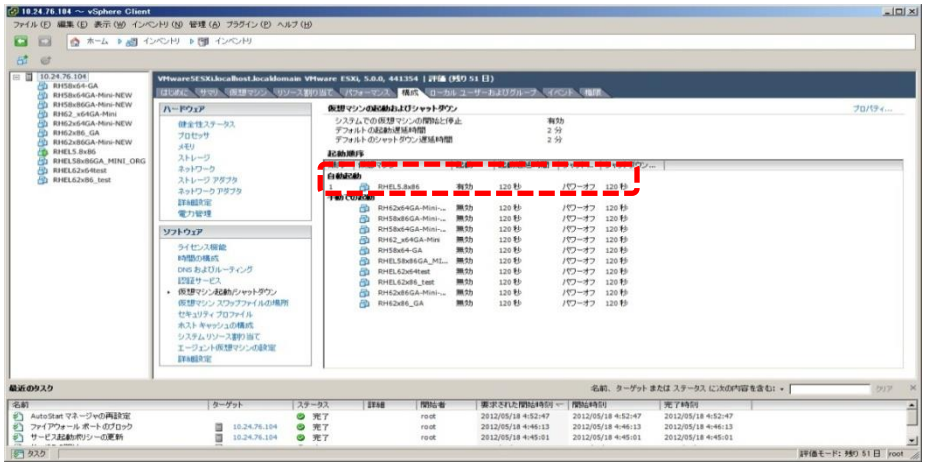
1. VMware vShpere Client を起動します。
2. [ホーム] → [インベントリ] → [インベントリ] から、[構成] タブをクリックします。
3. [仮想マシン起動/シャットダウン]をクリックします。
4. 右側に表示された項目から[プロパティ]をクリックします。



5. システム設定の”システムに連動した仮想マシンの自動起動および停止を許可する”にチェックを入れた後、対象の仮想 OS を選択し、以下のように”自動起動”に入るまで”上へ移動”をクリックします。
設定が終わったら、[OK]をクリックします。

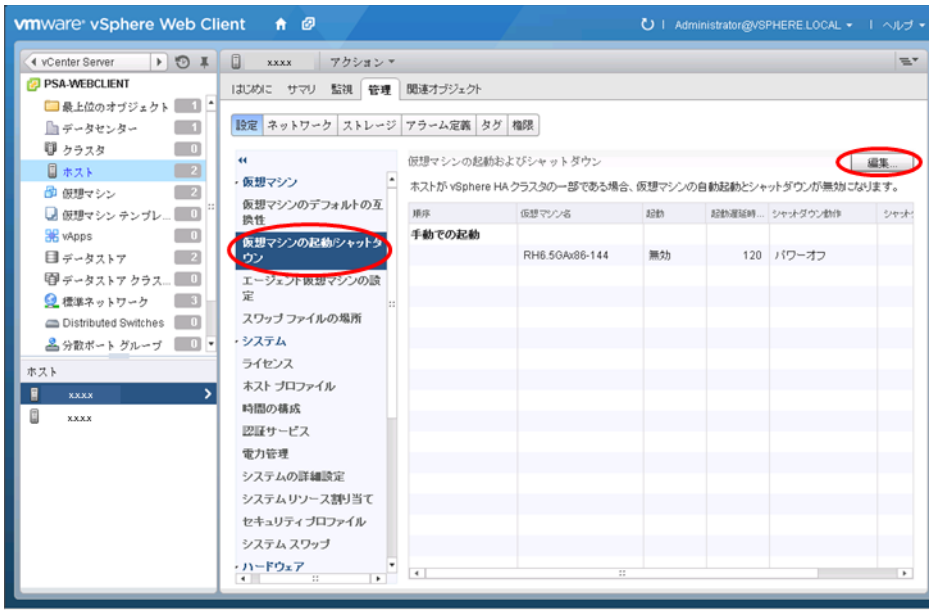


6. 以下のように、対象の仮想マシンが”自動起動”の順番に存在すれば設定完了です。

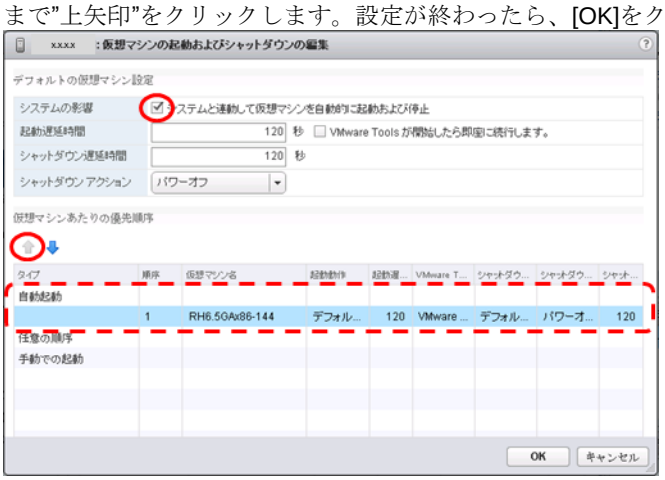


2.4.2.6.2. VMware vSphere Web Client の場合

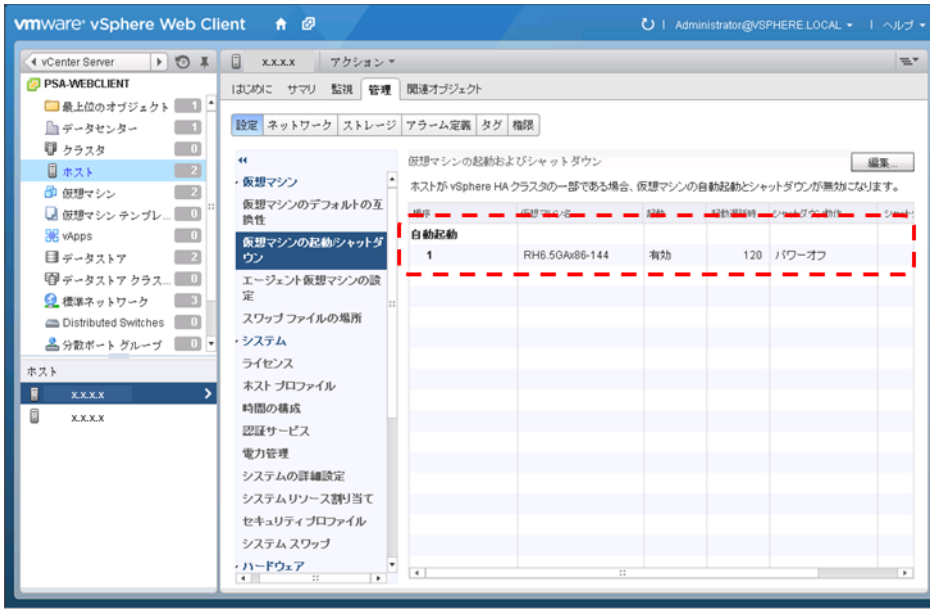
1. VMware vShpere Web Client を起動します。
2. [ホスト] → [対象ホストの IP アドレス] から、[管理] タブをクリックします。
3. 管理画面表示後、[設定]タブから [仮想マシンの起動/シャットダウン] をクリックし、[編集]をクリックします。



4. システム設定の”システムに連動した仮想マシンの自動起動および停止”にチェックを入れた後、対象の仮想マシンを選択し、以下のように”自動起動”に入るまで”上矢印”をクリックします。設定が終わったら、[OK]をクリックします。



5. 以下のように、対象の仮想マシンが”自動起動”に存在すれば設定完了です。



2.4.3 インストール（Linux：Red Hat Enterprise Linux）

Linux 環境への SVmcovm のインストールについて説明します。

備考

SVmcovm は、PRIMEQUEST1000 Type1/Type2 対応の仮想マシン専用のパッケージです。

2.4.3.1 SVmcovm 動作に必要なパッケージ

SVmcovm の動作のためには、以下のパッケージが必要です。

SVmcovm インストール前に各パッケージがインストールされていることを rpm コマンドで確認してください。

注意：

RHEL5,RHEL6 共通して、X64 環境にインストールする時は、**openssl の 32bit パッケージ(openssl-x.x.x-x.x.i686)**を必ずインストールしてください。

また、RHEL6 の x64 環境のみ glibc の 32bit パッケージ(glibc-x.x-x.x.i686)をインストールが必要です。

インストールされていない場合は、SVmcovm が正常に起動出来ません。

2.4.3.1.1 パッケージ(RHEL5)

X86	X64
gdb-x.x-x.x.i386	gdb-x.x-x.x.x86_64
tcl-x.x.x-x.i386	tcl-x.x.x-x.x86_64
	openssl-x.x.x-x.x.i686
expect-x.x.x-x.x.i386	expect-x.x.x-x.x.x86_64
openssh-clients-x.x-x.x.i386	openssh-clients-x.x-x.x.x86_64

2.4.3.1.2　パッケージ(RHEL6)

X86	X64
gdb-x.x-x.x.i686	gdb-x.x-x.x.x86_64
	glibc-x.x-x.x.i686
tcl-x.x.x-x.i686	tcl-x.x.x-x.x86_64
	openssl-x.x.x-x.x.i686
openssh-clients-x.x-x.x.i686	openssh-clients-x.x-x.x.x86_64
expect-x.x.x-x.x.i686	expect-x.x.x-x.x.x86_64

2.4.3.2　SVmcovm のインストール

1. DVD ドライブに『ServerView Suite DVD2』をセットし、以下のディレクトリから対象のモジュールを任意の場所にコピーします。

```
SVSLocalTools/Japanese/SVmcovm/SR_Linux/SVmcovm-XXX.tar.gz
```

2. ターミナルをルートで起動します。
3. SVmcovm のモジュールを PRIMEQUEST 1000/1000x2 シリーズ上で展開します。

```
# tar xvzf SVmcovm-XXX.tar.gz
```

XXX は版数により異なる。

4. 以下のコマンドを実行します。

```
# cd SVmcovm
#  ./INSTALL.sh
```

5. SVmcovm インストール後に設定を行います。設定方法について詳しくは、『2.4.4 SVmcovm インストール後の設定』を参照してください。

2.4.4 インストール後の設定（Linux：Red Hat Enterprise Linux）

SVmcovm インストール後の設定は以下の手順で行ってください。

1. SElinux 機能の設定確認
2. PSA-MMB 間通信 LAN の設定
3. ファイアーウォール機能の確認
4. ESXi へのアクセス情報の設定
5. 仮想マシンへのログ転送の設定(ログ受信側)
6. 仮想マシンへのログ転送の設定(ログ送信側)
7. MMB 経由の Trap 送信の設定

2.4.4.1 SElinux 機能の設定確認

SVmcovm における SElinux の設定については、『2.1.3 SELinux 機能の設定確認』を参照してください。

2.4.4.2 PSA-MMB 間通信 LAN の設定

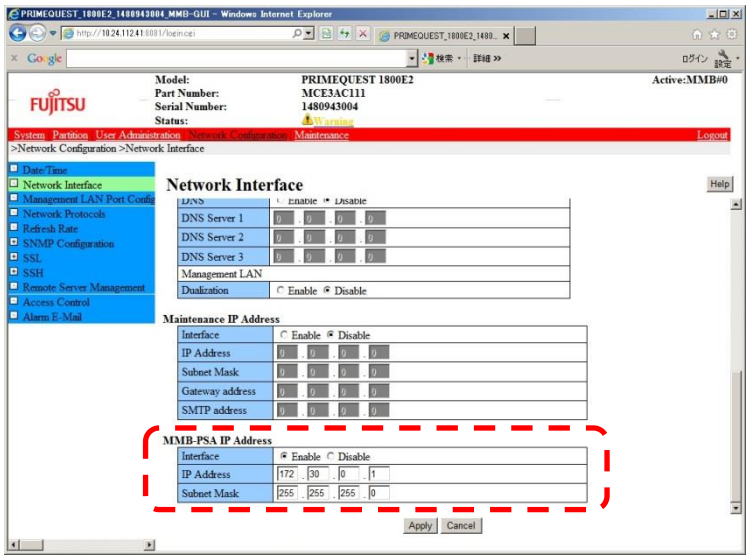
ここでは SVmcovm が MMB と通信するための PSA-MMB 間通信 LAN の設定について説明します。

【注意】：

- SVmcovm が MMB と通信するためには、仮想マシンに PSA-MMB 間通信 LAN の物理アダプタが割り当たっている必要があります。

  割り当てる方法については、2.4.2 SVmcovm のインストール前の確認/設定を参照してください。

- 設定する IP アドレスは、MMB 側の PSA-MMB 間通信 LAN の IP アドレスと同一のサブネットの IP である必要があります。MMB 側の IP アドレスは、MMB Web-UI から設定してください。



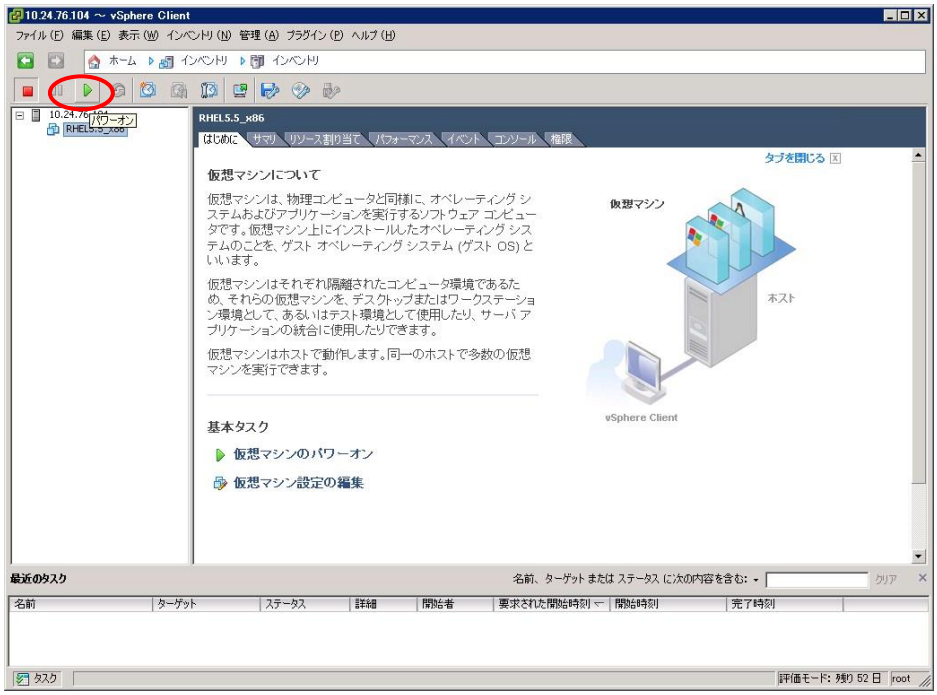
- MMB Web-UI の[Network Configuration]-[Network Interface]画面にて、[MMB-PSA IP Address]の[Interface]が Disable の場合、イベント通報機能が使用出来ません。尚、Disable から Enable に変更した場合、変更後に OS の再起動が必要です。

■ PSA-MMB 間通信 LAN の設定

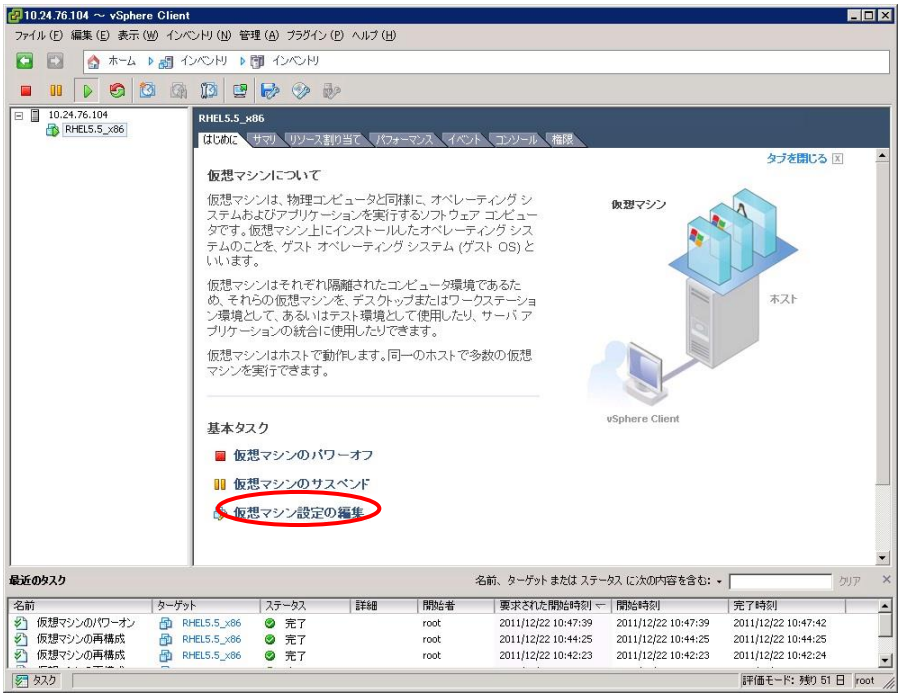
以下の手順で、PSA-MMB 間通信 LAN の設定を行います。

2.4.4.2.1. VMware vSphere Client の場合

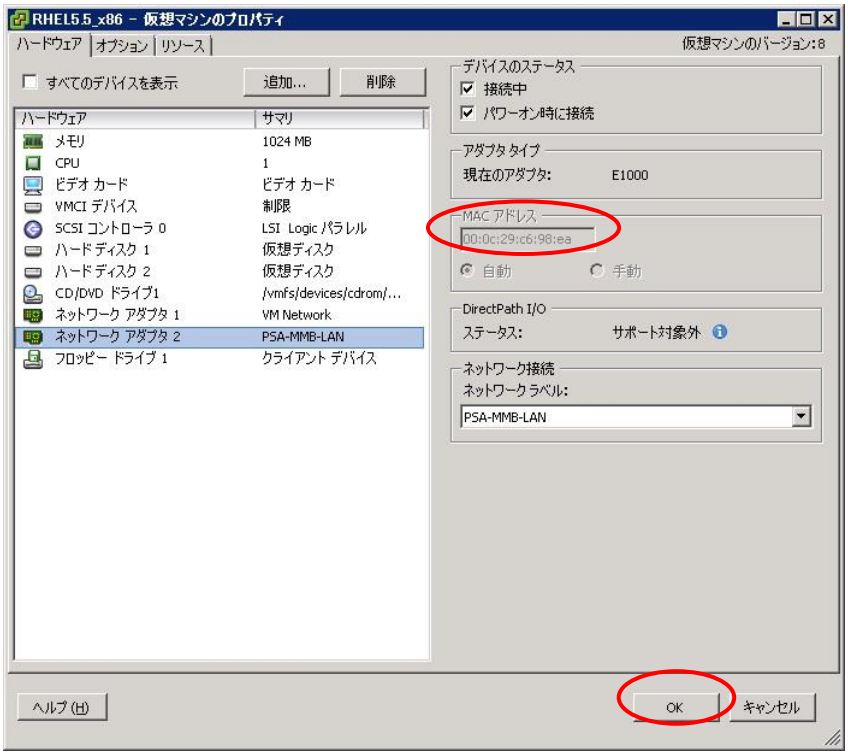
1. VMware vShpere Client を起動します。
2. 上から『2.4.2SVmcovm のインストール前の確認/設定』で PSA-MMB-LAN の仮想スイッチを割り当てた仮想マシンをクリックします。
3. 上部にあるツールバーから[パワーオン]をクリックします。



4. 仮想マシンが立ち上がったら、PSA-MMB 間通信 LAN の MAC アドレスを調べるために、[はじめに]タブの[仮想マシン設定の編集]をクリックします。

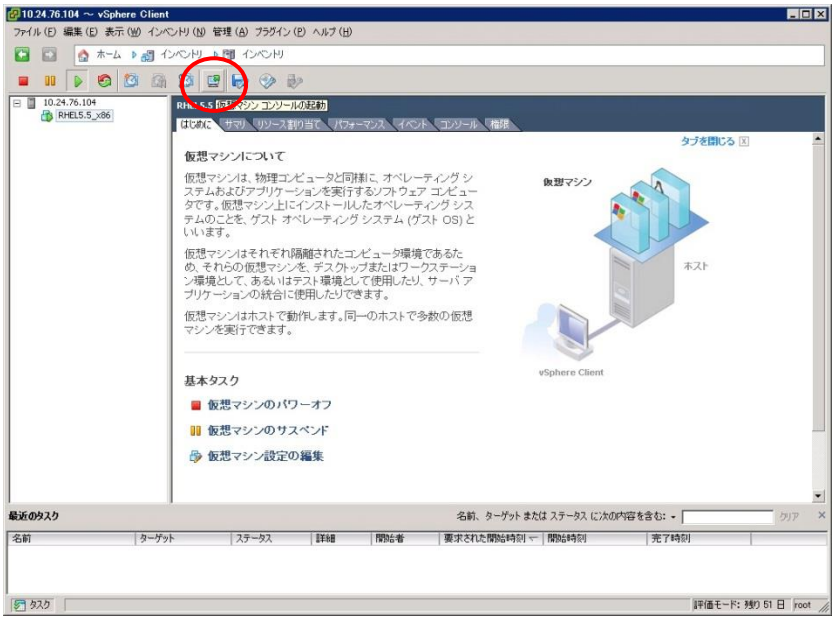


5. PSA-MMB-LAN のネットワークアダプタを選び、[MAC アドレス]を確認します。確認後、[OK]をクリックします。



ここでは、PSA-MMB 間通信 LAN の MAC アドレスは”**00：0C：29：c6：98：ea**”ということが確認できました。

6. 仮想マシンの上部にあるツールバーから[仮想マシンコンソールの起動]をクリックしてコンソールを立ち上げます。



7. 仮想マシンのコンソールを立ち上げます。

・ 仮想コンソール画面

8. ログインしたら、端末を立ち上げて、以下のコマンドを実行し、PSA-MMB 間通信 LAN が割り当たっているネットワークインターフェースを調べます。検索には MAC アドレスは 5 で確認した値を使います。

```
# ifconfig –a | grep –i <PSA-MMB 間通信 LAN の MAC アドレス>
```

【実行結果(例)】

```
# ifconfig –a | grep –i 00:0c:29:c6:98:ea
eth1 Link encap:Ethernet Hwaddr 00:0C:29:C6:98:EA
#
```

実行結果より、”eth1”が PSA-MMB 間通信 LAN ということが確認できました。

9. 以下のディレクトリに移動します。

```
# cd /etc/sysconfig/network-scripts
```

10. エディターなどで、対象のネットワークインターフェースの設定を開きます。ここでは、eth0 の設定ファイルを開いています。

```
# vi ifcfg-eth0
```

11. 以下のように設定ファイルを編集します。

・ 設定する IP アドレスはパーティション番号によって異なります。 以下の表の値を使用してください。

パーティション番号	IP アドレス	サブネットマスク
0	172.30.0.2	255.255.255.0
1	172.30.0.3	
2	172.30.0.4	
3	172.30.0.5	

<パーティション番号#1 の場合の例>

【編集前】

```
DEVICE = eth0
BOOTPROTO = dhcp
ONBOOT = yes
HWADDR = 00:0C:C6:98:EA
```

【編集後】

```
DEVICE = eth0
BOOTPROTO = static
ONBOOT = yes
HWADDR = 00:0C:C6:98:EA
IPADDR = 172.30.0.3
NETMASK = 255.255.255.0
```

注意：IP アドレスは同一筐体内で重複しない値を設定して下さい。

12. 設定反映のためにネットワークを再起動する。

```
# /sbin/service network restart
```

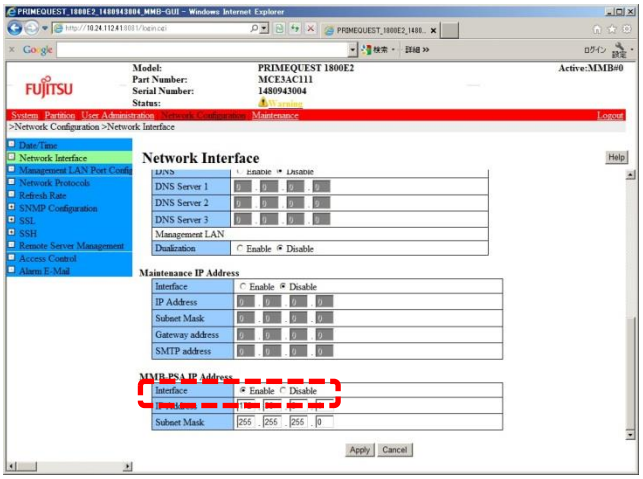
13. SVmcovm の設定ファイルを編集します。以下のファイルをエディターで開きます。

```
# vi /etc/fujitsu/SVmco/usr/mmblan.conf
```

14. 以下のパラメーターを設定します。

【設定値】

MMBIP：MMB Web-UI で設定した MMB-PSA IP Address の IP アドレス



ID：ESXi が稼働しているパーティション ID

【設定例】

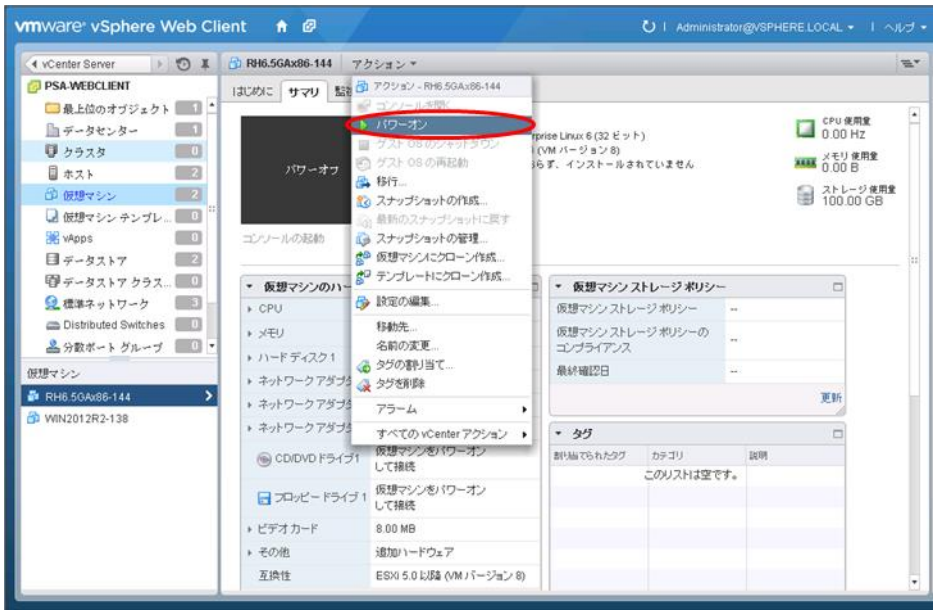
< MMB 側の PSA-MMB 間通信 LAN の IP アドレスが 172.30.0.1、パーティション番号が 1 の時>

```
[NETWORK]
MMBIP = 172.30.0.1

[PARTITION]
ID = 1
```

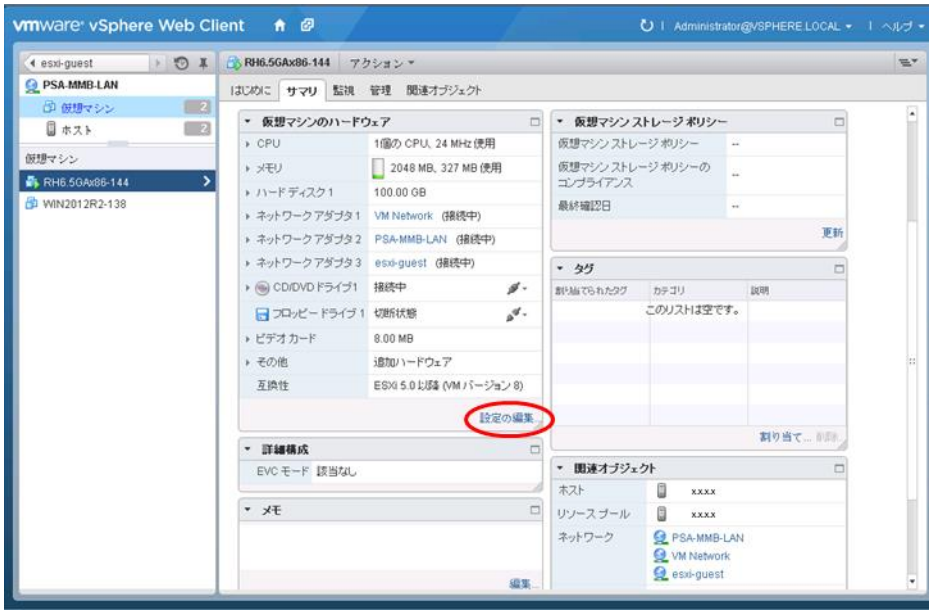
PSA-MMB 間通信 LAN の設定は以上です。

2.4.4.2.2. VMware vSphere Web Client の場合

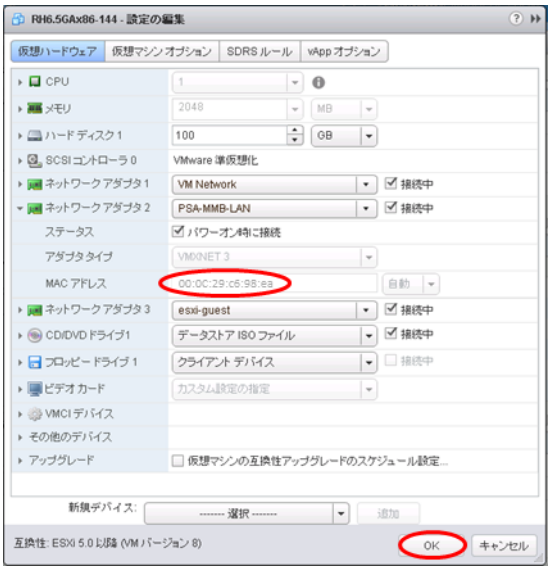
1. VMware vShpere Web Client を起動します。
2. 『2.4.2SVmcovm のインストール前の確認/設定』で PSA-MMB-LAN の仮想スイッチを割り当てた仮想マシンをクリックします。
3. [アクション]プルダウンより、 [パワーオン]をクリックします。



4. 仮想マシンが立ち上がったら、PSA-MMB 間通信 LAN の MAC アドレスを調べるために、対象仮想マシンの[仮想マシンのハードウェア]の[設定の編集]をクリックします。

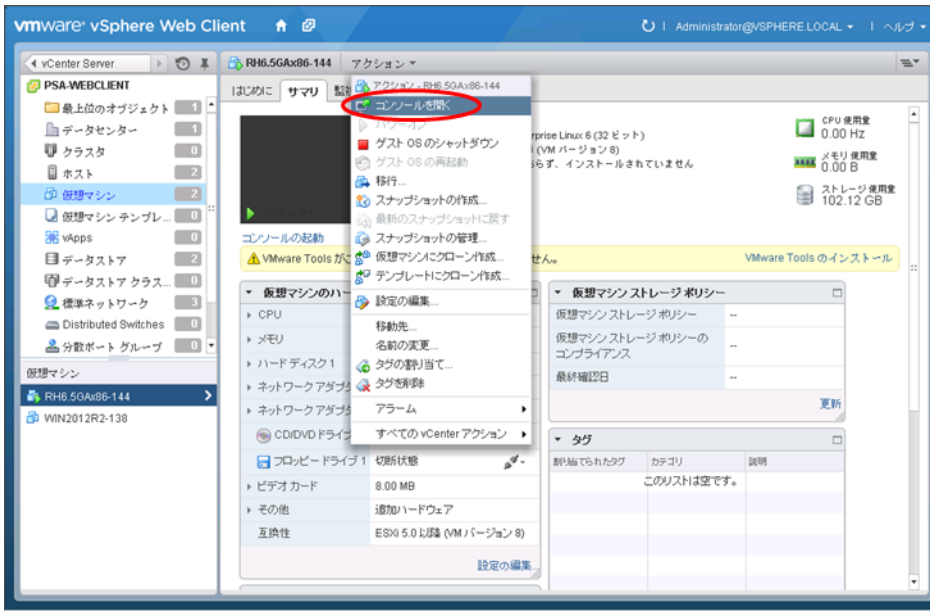


5. PSA-MMB-LAN のネットワークアダプタを選び、[MAC アドレス]を確認します。確認後、[OK]をクリックします。



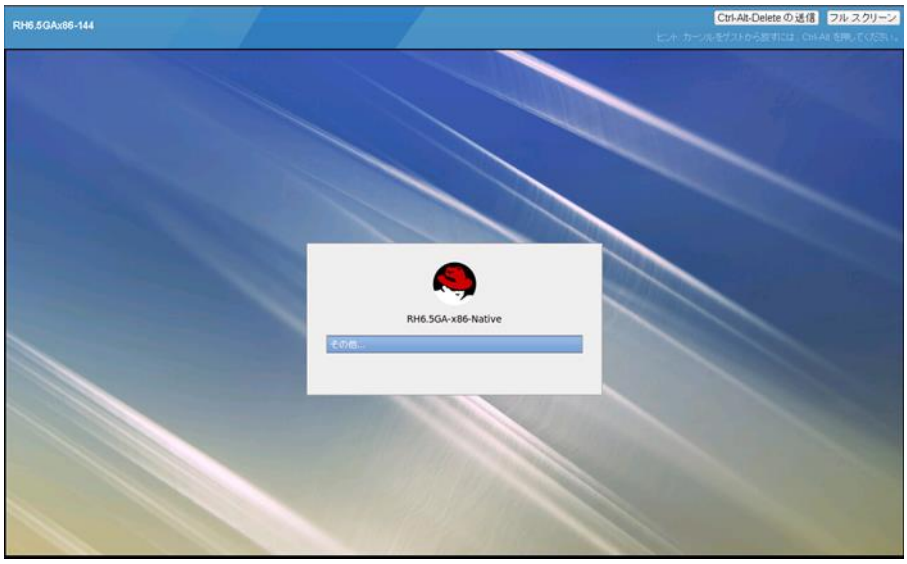
ここでは、PSA-MMB 間通信 LAN の MAC アドレスは” **00:0C:29:c6:98:ea**”ということが確認できました。

6. アクション]プルダウンより、[コンソールを開く]をクリックしてコンソールを立ち上げます。



7. 仮想マシンのコンソールを立ち上げます。

・ 仮想コンソール画面



8. ログインしたら、端末を立ち上げて、以下のコマンドを実行し、PSA-MMB 間通信 LAN が割り当たっているネットワークインターフェースを調べます。検索には MAC アドレスは 5 で確認した値を使います。

```
# ifconfig –a | grep –i <PSA-MMB 間通信 LAN の MAC アドレス>
```

【実行結果(例)】

```
# ifconfig –a | grep –i 00:0c:29:c6:98:ea
eth1 Link encap:Ethernet Hwaddr 00:0C:29:C6:98:EA
#
```

実行結果より、”eth1”が PSA-MMB 間通信 LAN ということが確認できました。

9. 以下のディレクトリに移動します。

```
# cd /etc/sysconfig/network-scripts
```

10. エディターなどで、対象のネットワークインターフェースの設定を開きます。ここでは、eth0 の設定ファイルを開いています。

```
# vi ifcfg-eth0
```

11. 以下のように設定ファイルを編集します。

- 設定する IP アドレスはパーティション番号によって異なります。 以下の表の値を使用してください。

パーティション番号	IP アドレス	サブネットマスク
0	172.30.0.2	255.255.255.0
1	172.30.0.3	
2	172.30.0.4	
3	172.30.0.5	

<パーティション番号#1 の場合の例>

【編集前】

```
DEVICE = eth0
BOOTPROTO = dhcp
ONBOOT = yes
HWADDR = 00:0C:C6:98:EA
```

【編集後】

```
DEVICE = eth0
BOOTPROTO = static
ONBOOT = yes
HWADDR = 00:0C:C6:98:EA
IPADDR = 172.30.0.3
NETMASK = 255.255.255.0
```

注意：IP アドレスは同一筐体内で重複しない値を設定して下さい。

12. 設定反映のためにネットワークを再起動する。

```
# /sbin/service network restart
```

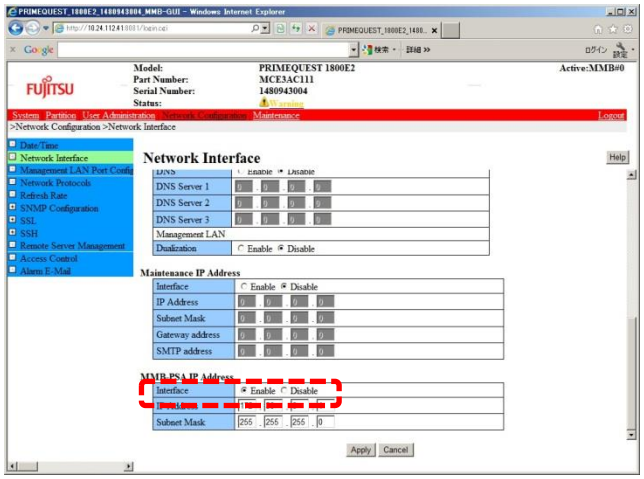
13. SVmcovm の設定ファイルを編集します。以下のファイルをエディターで開きます。

```
# vi /etc/fujitsu/SVmco/usr/mmblan.conf
```

14. 以下のパラメーターを設定します。

【設定値】

MMBIP：MMB Web-UI で設定した MMB-PSA IP Address の IP アドレス



ID：ESXi が稼働しているパーティション ID

【設定例】

< MMB 側の PSA-MMB 間通信 LAN の IP アドレスが 172.30.0.1、パーティション番号が 1 の時>

```
[NETWORK]
MMBIP = 172.30.0.1

[PARTITION]
ID = 1
```

PSA-MMB 間通信 LAN の設定は以上です。

2.4.4.3 ファイアーウォールの機能の確認

ここでは SVmcovm が運用上でのファイアーウォールの設定について説明します。

SVmcovm では、以下のポートを開放する必要があります。

№	ポート	ポート番号	説明
1	psa-mmb 通信ポート	tcp/MMB 側 5000	MMB-PSA 間ポート イベントの通知用

■ ファイアーウォール設定の実施例

1. 以下のディレクトリに移動する。

```
# /opt/fujitsu/SVmco/sh
```

2. ファイアーウォール設定シェルを実行します。

設定シェルの仕様は以下のようになります。

【仕様】

./setiptables.sh install <PSA-MMB 間通信 LAN の network interface 名>

※PSA-MMB 間通信 LAN の network interface 名は

『2.4.4.2 PSA-MMB 間通信 LAN の設定』で取得した値(eth0 など)です。

【実施例】

```
# ./setiptables.sh install eth1
```

3. iptables –L コマンドを実施し、設定チェイン”PSA-MMB_LAN”が存在することを確認します。

```
# iptables –L
Chain INPUT (policy DROP)
target     prot opt source               destination

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination

Chain PSA-MMB_LAN (0 references)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
ACCEPT     icmp --  anywhere             anywhere            icmp echo-request
ACCEPT     icmp --  anywhere             anywhere            icmp echo-reply
```

```
ACCEPT     tcp  --  anywhere             anywhere            tcp spt:commplex-main
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:commplex-main
```

4. PSA-MMB_LAN チェインへのジャンプ設定を INPUT と OUTPUT の適切な場所に追加します。この時、INPUT および、OUTPUT チェインにある既存の REJECT 設定や、ユーザー定義のチェインに遮断されないように注意して設定してください。

実施例：INPUT に REJECT 設定がある場合

```
# iptables –L
Chain INPUT (policy ACCEPT)
target    prot  opt source          destination
ACCEPT     all   --  0.0.0.0/0           0.0.0.0/0  state
RELATED,ESTABLISHED
ACCEPT     icmp  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     all   --  0.0.0.0/0           0.0.0.0/0
ACCEPT     tcp   --  0.0.0.0/0            0.0.0.0/0  state NEW tcp dpt:22
REJECT     all   --  0.0.0.0/0           0.0.0.0/0  reject-with icmp-host-
prohibited

Chain FORWARD (policy ACCEPT)
target   prot  opt source        destination
REJECT     all   --  0.0.0.0/0           0.0.0.0/0  reject-with icmp-host-
prohibited

Chain OUTPUT (policy ACCEPT)
target   prot  opt source        destination
```

次ページにつづく

前ページよりづづき

```
Chain PSA-MMB_LAN (0 references)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
ACCEPT     icmp --  anywhere             anywhere            icmp echo-request
ACCEPT     icmp --  anywhere             anywhere            icmp echo-reply
ACCEPT     tcp  --  anywhere             anywhere            tcp spt:commplex-
main
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:commplex-
main
```

5. 例では、PSA-MMB_LAN チェインを INPUT チェインの 5 番目(REJECT 設定の前)および、OUTPUT チェインに追加します。(iptables のオプションの詳細は man マニュアルを参照してください。)

```
# /sbin/iptables –I INPUT 5 –j PSA-MMB_LAN
# /sbin/iptables –A OUTPUT –j PSA-MMB_LAN
```

6. iptables –L　コマンドを実行し、INPUT チェインおよび、OUTPUT チェインについて、追加された PSA-MMB_LAN がその前の REJECT、DROP などにより遮断されていない事を確認します。

```
# iptables –L
Chain INPUT (policy ACCEPT)
target    prot  opt source          destination
ACCEPT    all   --  0.0.0.0/0       0.0.0.0/0  state
RELATED,ESTABLISHED
ACCEPT    icmp  --  0.0.0.0/0       0.0.0.0/0
ACCEPT    all   --  0.0.0.0/0       0.0.0.0/0
ACCEPT    tcp   --  0.0.0.0/0       0.0.0.0/0  state NEW tcp dpt:22
PSA-MMB_LAN    all   --  0.0.0.0/0       0.0.0.0/0
REJECT    all   --  0.0.0.0/0       0.0.0.0/0  reject-with icmp-host-
prohibited

Chain FORWARD (policy ACCEPT)
target   prot  opt source       destination
REJECT    all   --  0.0.0.0/0       0.0.0.0/0  reject-with icmp-host-
prohibited

Chain OUTPUT (policy ACCEPT)
target   prot  opt source       destination
PSA-MMB_LAN    all   --  0.0.0.0/0       0.0.0.0/0

次ページにつづく
```

```
前ページよりづづき


Chain PSA-MMB_LAN (0 references)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     all  --  anywhere             anywhere
ACCEPT     icmp --  anywhere             anywhere            icmp echo-request
ACCEPT     icmp --  anywhere             anywhere            icmp echo-reply
ACCEPT     tcp  --  anywhere             anywhere            tcp spt:commplex-main
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:commplex-main
```

7. ポート解放の確認のため、MMB 側の PSA-MMB 間通信 LAN の IP アドレス(ここでは 172.30.0.1 に設定してあると仮定)に対して Ping の応答があるか確認します。

```
# ping 172.30.0.1
```

8. ファイアーウォールの設定を保存します。

```
# /sbin/service iptables save
```

2.4.4.4 ESXi へのアクセス情報の設定

SVmcovm は起動時に ESXi への ssh 経由で PCI カード情報やログを取得しています。

ここでは、ESXi へのアクセスするための設定を行います。

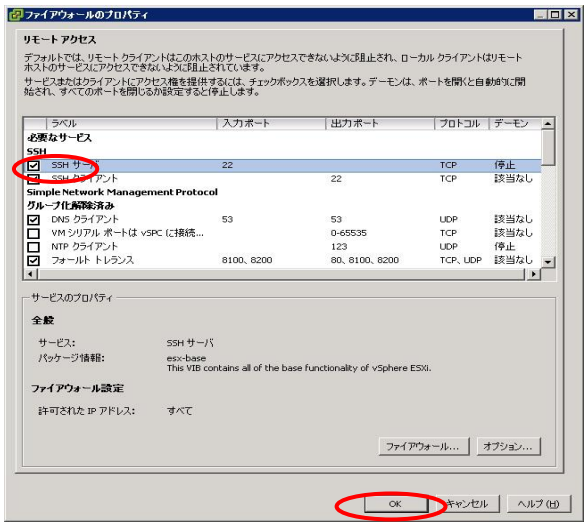
本設定により、SVmcovm 起動時に ESXi から自動的に PCI カード情報やログを取得することで PCI カードの故障検出が可能となります。

【注意】

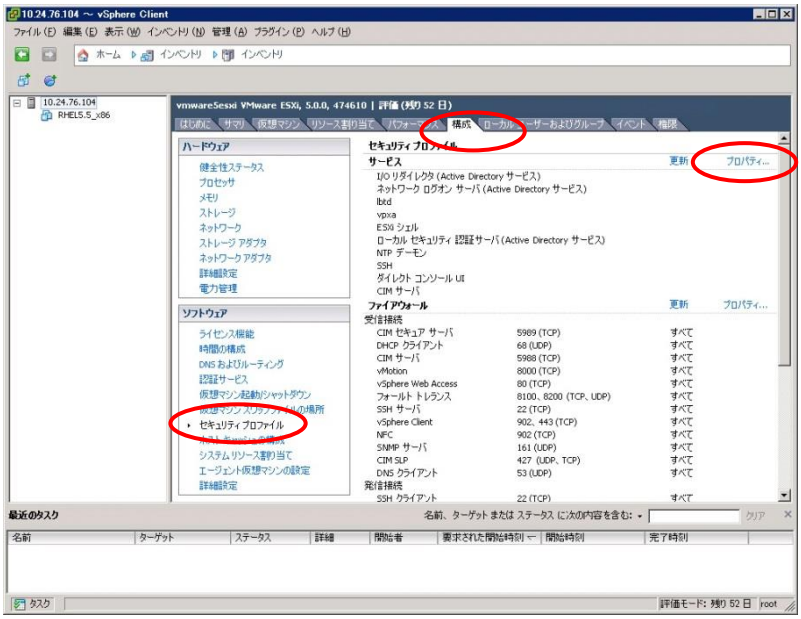
DNS サーバーを利用している場合には、ESXi と SVmcovm をインストールしている仮想マシンが名前解決が出来るように DNS サーバーにホスト情報を登録して下さい。

2.4.4.4.1. VMware vSphere Client の場合

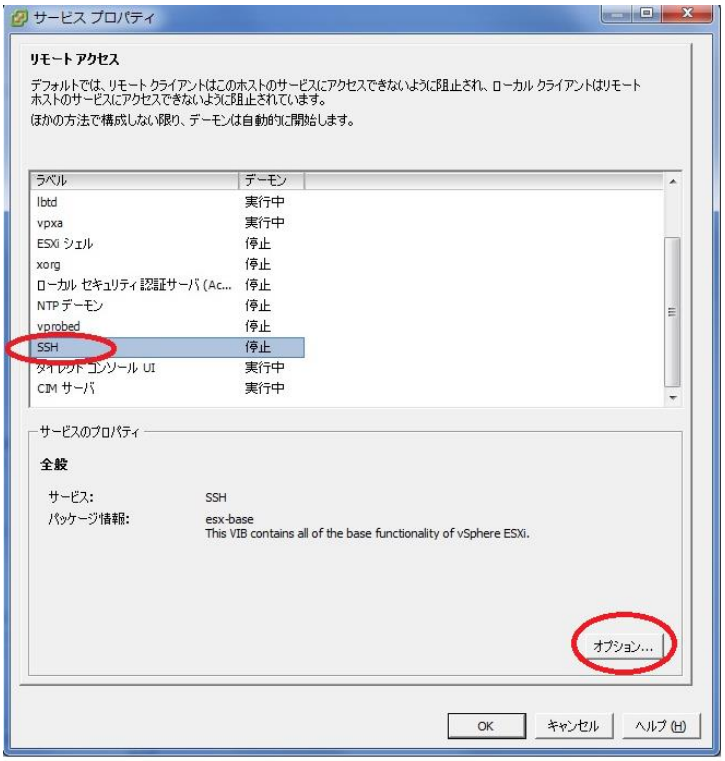
1. VMware vShpere Client を起動します。
2. [ホーム] → [インベントリ] → [インベントリ] から、[構成] タブをクリックします。
3. 左下にある [ソフトウェア] 内の [セキュリティプロファイル] をクリックします。
4. [セキュリティプロファイル] 情報が表示された画面のファイアウォールの[プロパティ] をクリックします。
5. [SSH サーバ]をチェックし、[OK]ボタンをクリックします。



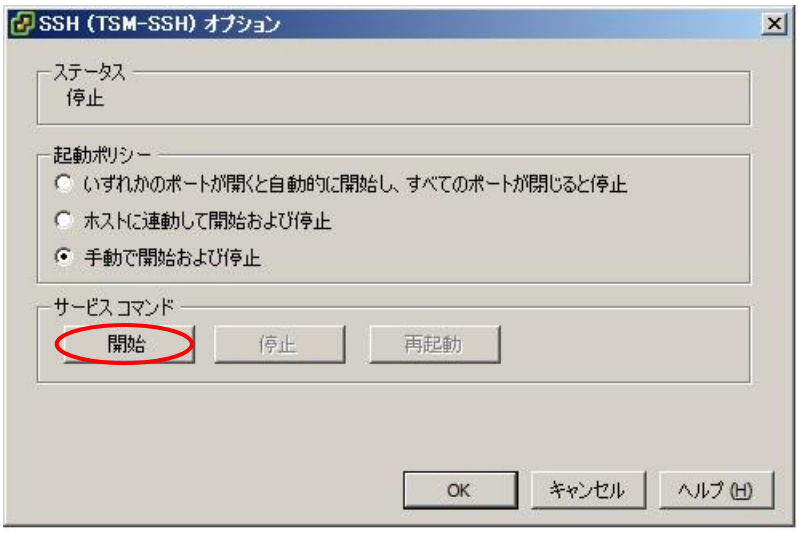
6. [セキュリティプロファイル] 情報が表示された画面の右上にある [プロパティ] をクリックします。



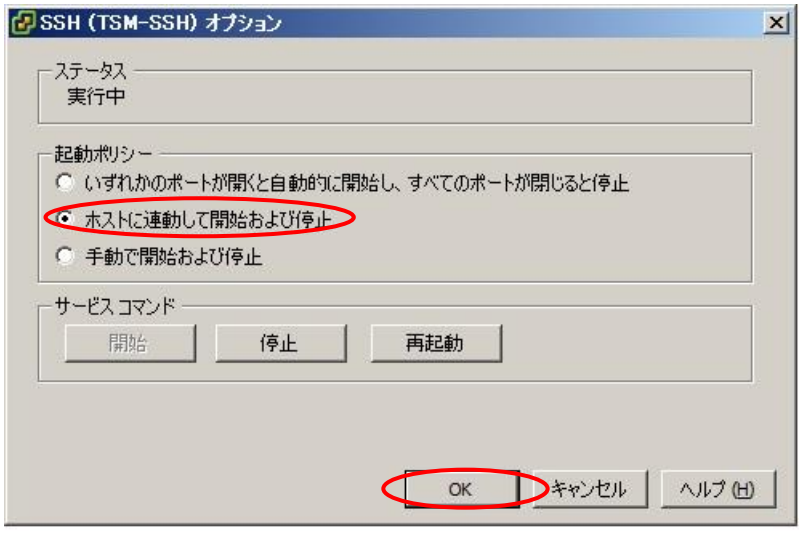
7. [SSH]をチェックし、[オプション]ボタンをクリックします。



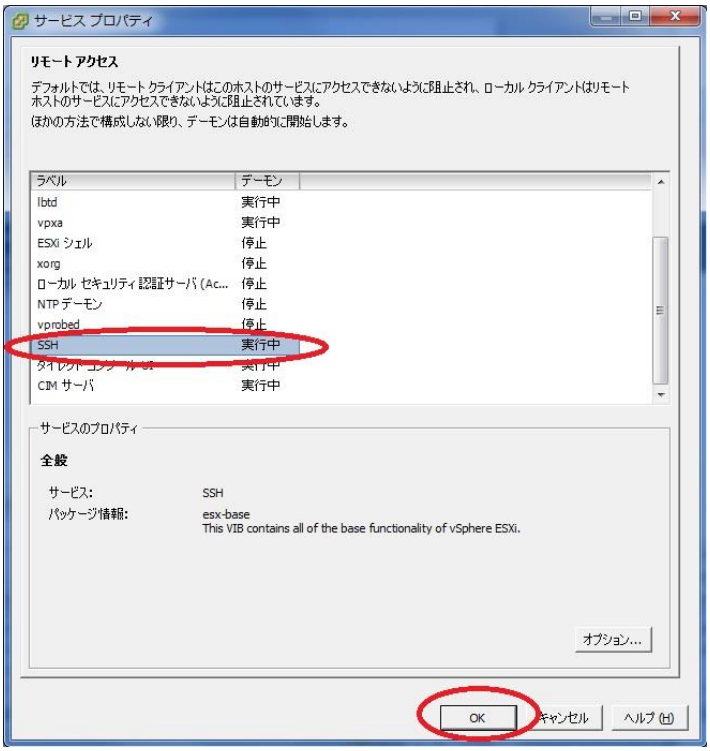
8. [サービスコマンド]で開始をクリックします。



9. 次に[起動ポリシー]の[ホストに連動して開始および停止]を選択し、[OK]をクリックします。



10. [SSH]の[デーモン]が実行中になっていることを確認して[OK]をクリックします。



11. 仮想マシンへログインし、以下のディレクトリへ移動します。

```
# cd /opt/fujitsu/SVmco/bin/
```

12. コマンドを以下のオプションを付けて実行します。

対話形式で ESXi の IP,ログイン ID,とパスワードを入力します。

```
# ./setuserinfo -i
```

設定する IP アドレスは、ESXi へアクセスするための IP アドレスです。
ネットワークの構成によって設定値が異なります。

1. ネットワーク構成例 1 の場合：

   2.4.2.5.1 章の手順 8 で設定した ESXi からの情報取得用 IP アドレスを設定します。

2. ネットワーク構成例 2 の場合：

   管理ネットワークの ESXi に割り当てた IP アドレスを設定します。

13. 実行後、以下のオプションを付けて実行し、2.で入力した値のチェックを行います。

```
# ./setuserinfo –c
Successful execution of the command.
```

上記のメッセージが出力されれば設定終了です。

ESXi のアクセスに失敗する場合は、以下のようなメッセージが表示されます。

```
# ./setuserinfo –c
Failed to execute the command.
```

原因としては、以下が考えられます。

1. ESXi へのログイン ID かパスワードが間違っている。

   対処：
   ESXi へアクセス出来る、正しいログイン ID or パスワードを再設定する（手順 12）。

2. ESXi と SVmcovm をインストールしている仮想マシンの名前解決が出来ない。

   対処：
   ESXi と SVmcovm をインストールしている仮想マシンが名前解決が出来るように DNS サーバーにホスト情報を登録する。

運用条件などにより、ssh 接続が出来ない場合は、手動にて ESXi から PCI カード情報を取得し、仮想マシンの指定の場所に配置後に SVmcovm の再起動が必要です。

また、SSH 接続を許可しない環境において PCI カードの追加/交換があった場合も、本手順の実施が必要です。

尚、SSH 接続設定を実施しない場合は、以下の監視上の制約が発生します。

1. SVmcovm 起動前の PCI カード/ディスクの故障検出が出来ない

   SVmcovm 起動後は監視可能
2. MMB の PCI レーン縮退監視が出来ない
3. システムステータスが OS Running/OS Shutdown に変更されない。

以下に手順を示します。

1. SSH で ESXi へログインし、以下のコマンドを実行します。

・PCI カード情報取得コマンド

```
# /sbin/esxcli hardware pci list > pcicardinfo
```

・NIC 情報取得コマンド

```
# /sbin/esxcfg-nics -l > nicinfo
```

■ 実行結果 (例)

・pcicardinfo

```
000:000:19.0
Address: 000:000:19.0
Segment: 0x0000
Bus: 0x00
Slot: 0x19
Function: 0x00
VMkernel Name: vmnic0
Vendor Name: Intel Corporation
Device Name: 82567LF-2 Gigabit Network Connection
Configured Owner: Unknown
Current Owner: VMkernel
Vendor ID: 0x8086
Device ID: 0x10cd
SubVendor ID: 0x10cf
SubDevice ID: 0x159b
Device Class: 0x0200
```

nicinfo

```
Name    PCI          Driver      Link Speed     Duplex MAC Address       MTU    Description

vmnic0  0000:00:19.00 e1000e      Up   100Mbps   Full   00:17:42:de:7c:4b 1500   Intel
Corporation 82567LF-2 Gigabit Network Connection

vmnic1  0000:05:00.00 igb         Up   100Mbps   Full   00:17:42:9b:dc:b4 1500   Intel
Corporation 82576 Gigabit Network Connection

vmnic2  0000:05:00.01 igb         Down 0Mbps     Half   00:17:42:9b:dc:b5 1500   Intel
Corporation 82576 Gigabit Network Connection

vmnic3  0000:06:00.00 igb         Down 0Mbps     Half   00:17:42:9b:dc:b6 1500   Intel
Corporation 82576 Gigabit Network Connection

vmnic4  0000:06:00.01 igb         Down 0Mbps     Half   00:17:42:9b:dc:b7 1500   Intel
Corporation 82576 Gigabit Network Connection

vmnic5  0000:0e:00.00 e1000e      Down 0Mbps     Half   00:15:17:7d:d4:e2 1500   Intel
Corporation 82571EB Gigabit Ethernet Controller

vmnic6  0000:0e:00.01 e1000e      Down 0Mbps     Half   00:15:17:7d:d4:e3 1500   Intel
Corporation 82571EB Gigabit Ethernet Controller
```

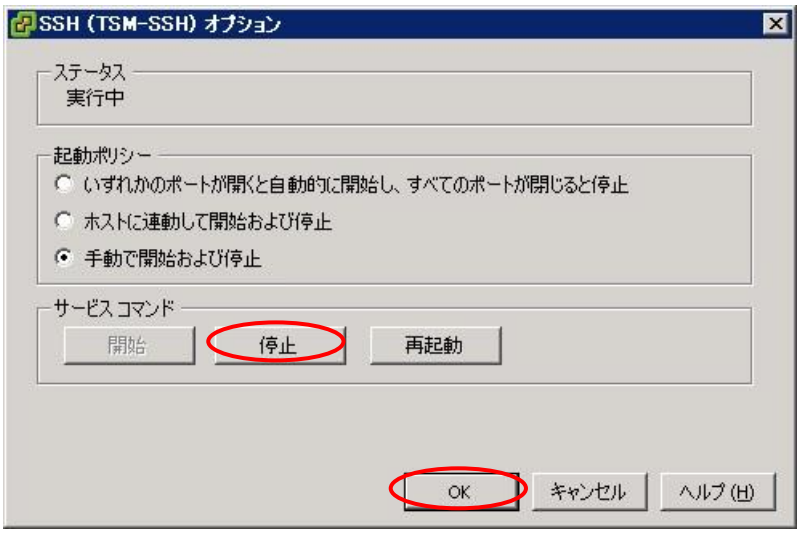
2. 作成した二つのファイル(pcicardinfo,nicinfo)を **SVmcovm をインストール予定の仮想マシンの以下のディレクトリにコピー**します。

```
/etc/fujitsu/SVmco/usr
```

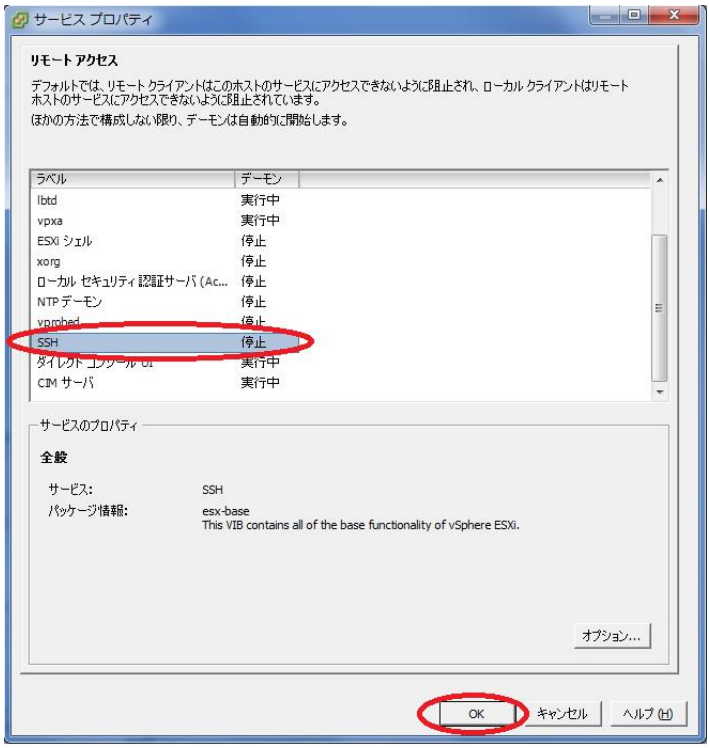
コピーが完了したら、以下の方法で ESXi への ssh 接続出来ないように設定を元に戻します。

3. 確認後、SSH のサービスを停止させます。SSH を起動させた時のように、VMware vSphere Client を起動させて、[ホーム]→[インベントリ]→[インベントリ]から[構成]タブをクリックし、左下の[ソフトウェア]内の[セキュリティプロファイル]からプロパティをクリックし、[サービスのプロパティ]画面で[ssh サービス]を選択し、[オプション]を開きます。

   以下のように[サービスコマンド]で[停止]をクリックした後、[OK]をクリックします。

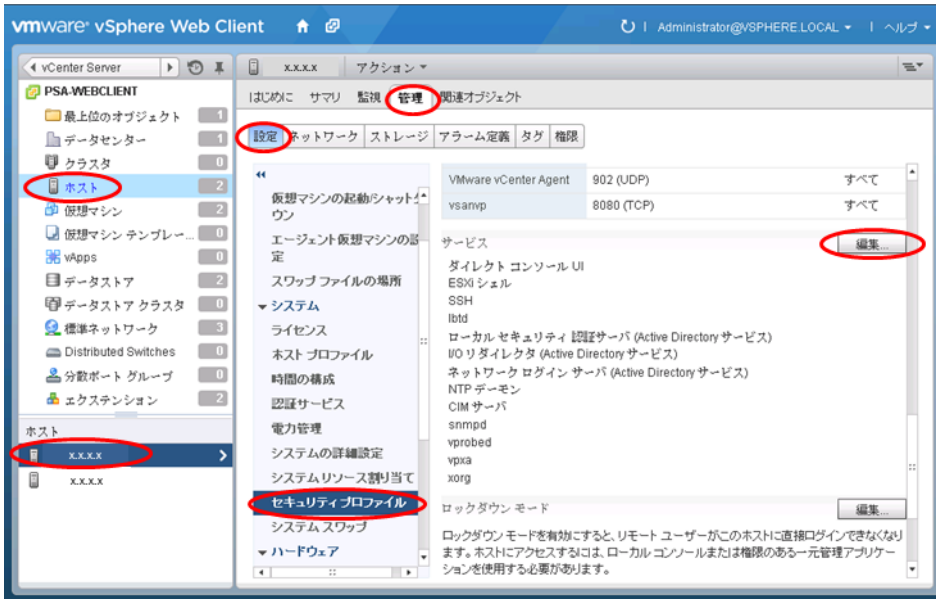


4. [SSH サーバ]のチェックが外れ、[デーモン]が停止になっていることを確認してください。



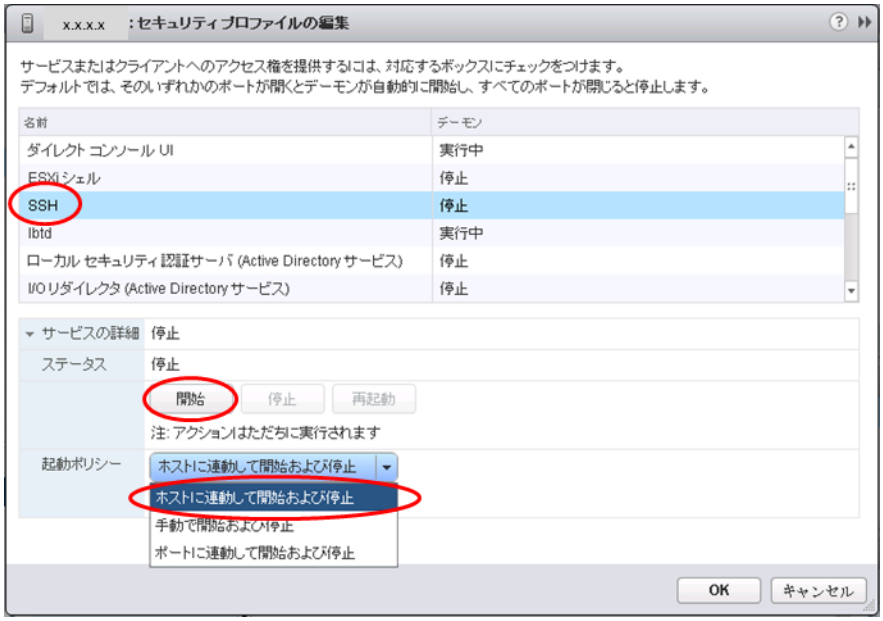
2.4.4.4.2. VMware vSphere Web Client の場合

1. VMware vShpere Web Client を起動します。
2. [ホスト] → [対象ホスト名] から、[管理] タブをクリックします。
3. 管理画面表示後、[設定]タブから [セキュリティプロファイル] をクリックします。
4. [セキュリティプロファイル] 情報が表示され、サービスの[編集] をクリックします。

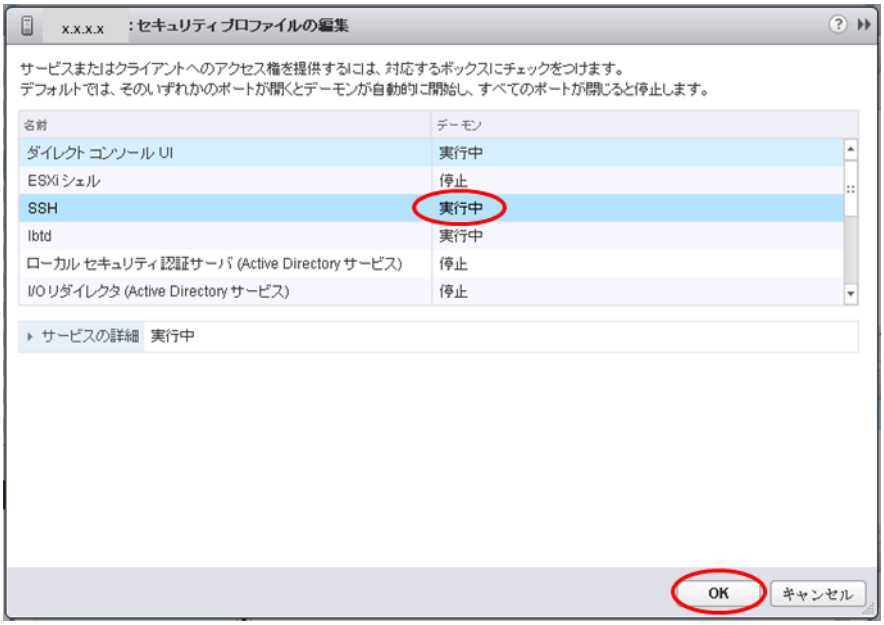


5. [SSH]を選択し、[開始]ボタンをクリックします。

6. 次に[起動ポリシー]の[ホストに連動して開始および停止]を選択します。



7. [SSH]の[デーモン]が実行中になっていることを確認して[OK]をクリックします。



8. コマンドを以下のオプションを付けて実行します。

仮想マシンへログインし、以下のディレクトリへ移動します。

```
# cd /opt/fujitsu/SVmco/bin/
```

9. コマンドを以下のオプションを付けて実行します。

対話形式で ESXi の IP,ログイン ID,とパスワードを入力します。

```
# ./setuserinfo -i
```

設定する IP アドレスは、ESXi へアクセスするための IP アドレスです。
ネットワークの構成によって設定値が異なります。

1. ネットワーク構成例 1 の場合：

   2.4.2.5.2 章の手順 10 で設定した ESXi からの情報取得用 IP アドレスを設定します。

2. ネットワーク構成例 2 の場合：

   管理ネットワークの ESXi に割り当てた IP アドレスを設定します。

10. 実行後、以下のオプションを付けて実行し、2.で入力した値のチェックを行います。

```
# ./setuserinfo –c
Successful execution of the command.
```

上記のメッセージが出力されれば設定終了です。

ESXi のアクセスに失敗する場合は、以下のようなメッセージが表示されます。

```
# ./setuserinfo –c
Failed to execute the command.
```

原因としては、以下が考えられます。

1. ESXi へのログイン ID かパスワードが間違っている。

   対処：
   ESXi へアクセス出来る、正しいログイン ID or パスワードを再設定する（手順 9）。

2. ESXi と SVmcovm をインストールしている仮想マシンの名前解決が出来ない。

   対処：
   ESXi と SVmcovm をインストールしている仮想マシンが名前解決が出来るように DNS サーバーにホスト情報を登録する。

運用条件などにより、ssh 接続が出来ない場合は、手動にて ESXi から PCI カード情報を取得し、仮想マシンの指定の場所に配置後に SVmcovm の再起動が必要です。

また、SSH 接続を許可しない環境において PCI カードの追加/交換があった場合も、本手順の実施が必要です。

尚、SSH 接続設定を実施しない場合は、以下の監視上の制約が発生します。

1. SVmcovm 起動前の PCI カード/ディスクの故障検出が出来ない

   SVmcovm 起動後は監視可能
2. MMB の PCI レーン縮退監視が出来ない
3. システムステータスが OS Running/OS Shutdown に変更されない。

以下に手順を示します。

1. SSH で ESXi へログインし、以下のコマンドを実行します。

・PCI カード情報取得コマンド

```
# /sbin/esxcli hardware pci list > pcicardinfo
```

・NIC 情報取得コマンド

```
# /sbin/esxcfg-nics -l > nicinfo
```

■ 実行結果 (例)

・pcicardinfo

```
000:000:19.0
Address: 000:000:19.0
Segment: 0x0000
Bus: 0x00
Slot: 0x19
Function: 0x00
VMkernel Name: vmnic0
Vendor Name: Intel Corporation
Device Name: 82567LF-2 Gigabit Network Connection
Configured Owner: Unknown
Current Owner: VMkernel
Vendor ID: 0x8086
Device ID: 0x10cd
SubVendor ID: 0x10cf
SubDevice ID: 0x159b
Device Class: 0x0200
```

nicinfo

```
Name    PCI          Driver      Link Speed     Duplex MAC Address       MTU    Description

vmnic0  0000:00:19.00 e1000e      Up   100Mbps   Full   00:17:42:de:7c:4b 1500   Intel
Corporation 82567LF-2 Gigabit Network Connection

vmnic1  0000:05:00.00 igb         Up   100Mbps   Full   00:17:42:9b:dc:b4 1500   Intel
Corporation 82576 Gigabit Network Connection

vmnic2  0000:05:00.01 igb         Down 0Mbps     Half   00:17:42:9b:dc:b5 1500   Intel
Corporation 82576 Gigabit Network Connection

vmnic3  0000:06:00.00 igb         Down 0Mbps     Half   00:17:42:9b:dc:b6 1500   Intel
Corporation 82576 Gigabit Network Connection

vmnic4  0000:06:00.01 igb         Down 0Mbps     Half   00:17:42:9b:dc:b7 1500   Intel
Corporation 82576 Gigabit Network Connection

vmnic5  0000:0e:00.00 e1000e      Down 0Mbps     Half   00:15:17:7d:d4:e2 1500   Intel
Corporation 82571EB Gigabit Ethernet Controller

vmnic6  0000:0e:00.01 e1000e      Down 0Mbps     Half   00:15:17:7d:d4:e3 1500   Intel
Corporation 82571EB Gigabit Ethernet Controller
```

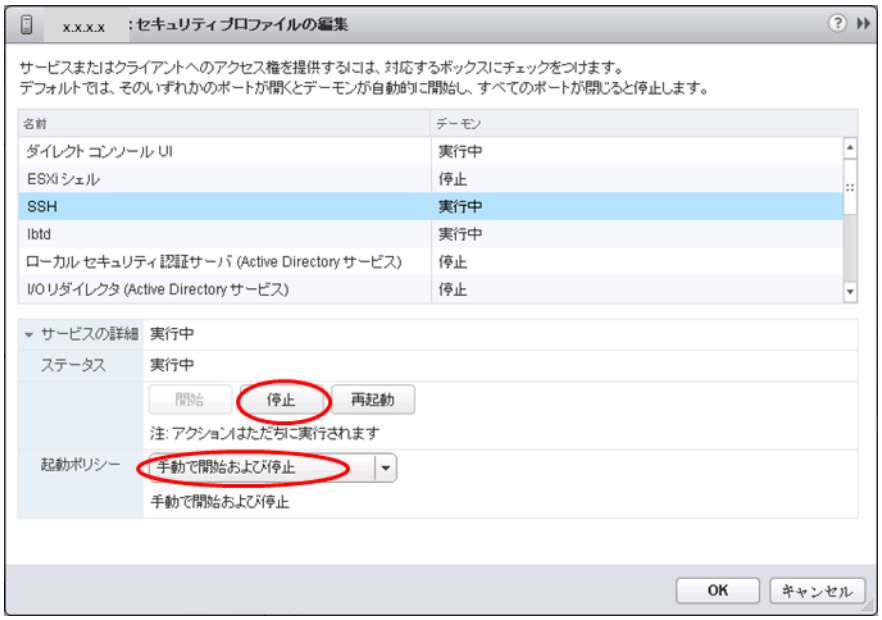
2. 作成した二つのファイル(pcicardinfo,nicinfo)を SVmcovm をインストール予定の仮想マシンの以下のディレクトリにコピーします。

```
/etc/fujitsu/SVmco/usr
```

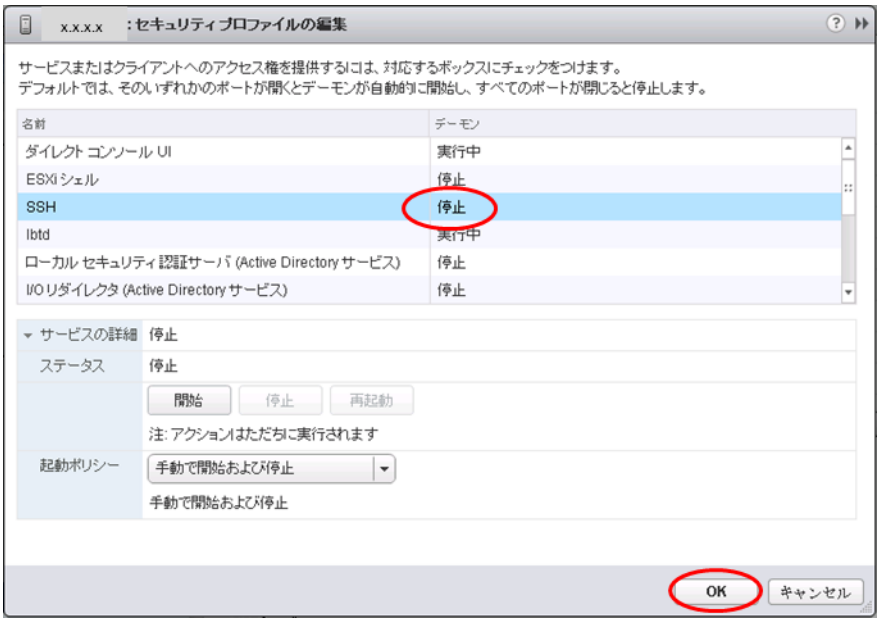
コピーが完了したら、以下の方法で ESXi への ssh 接続出来ないように設定を元に戻します。

3. 確認後、SSH のサービスを停止させます。SSH を起動させた時のように、VMware vSphere Web Client を起動させて、[ホスト] → [対象ホストの IP アドレス] から、[管理] タブをクリックし、管理画面表示後、[設定]タブから [セキュリティプロファイル] をクリックし、[セキュリティプロファイル] 情報が表示され、サービスの[編集] をクリックします。

4. [SSH]を選択し、[停止]をクリックします。



5. [SSH]の[デーモン]が停止になっていることを確認して[OK]をクリックします。



2.4.4.5 仮想 OS へのログ転送の設定(ログ受信側)

ログ転送への設定にはログデーモンの設定とファイアウォールの設定が必要です。

2.4.4.5.1. ログデーモンの設定

仮想 OS のログデーモンによって設定方法が異なります。

ここでは、RHEL5(syslog)と RHEL6(rsyslog)の設定方法について説明します。

syslog(RHEL5 環境の場合)

1. 以下のファイルをエディターで開く

```
# vi /etc/sysconfig/syslog
```

2. ファイルの“SYSLOGD_OPTION”変数を以下のように編集する。

・編集前

```
SYSLOGD_OPTIONS=”-m 0”
```

・編集後

```
SYSLOGD_OPTIONS=”-m 0 -r”
```

3. Syslog デーモンを再起動

```
# service syslog restart
```

4. 以下のコマンドを実行し、udp の 514 ポートが表示されることを確認します。

```
# netstat –an | grep –i udp | grep 514
udp    0      0   0.0.0.0:514     0.0.0.0:*
```

上記のように表示されれば、ログ受信可能な状態です。

rsyslog(RHEL6 環境の場合)

1. 以下のファイルをエディターで開く

```
# vi /etc/rsyslog.conf
```

2. 以下のパラメーターのコメントアウトを外して保存します。

・編集前

```
#$ModLoad imudp.so
#$UDPServerRun 514
```

・編集後

```
$ModLoad imudp.so
$UDPServerRun 514
```

3. rsyslog デーモンを再起動します。

```
# service rsyslog restart
```

4. 以下のコマンドを実行し、udp の 514 ポートが表示されることを確認します

```
# netstat –an | grep –i udp | grep 514
udp        0      0 0.0.0.0:514             0.0.0.0:*
udp        0      0 :::514                  :::*
```

上記のように表示されれば、ログ受信可能な状態です。

2.4.4.5.2. ログ転送用のファイアウォールの設定

■ **ログ受信側(仮想マシン)の設定**

1. ログ受信のため、udp の 514 ポートを以下のコマンドで開きます。

```
# iptables -I INPUT -p udp --dport 514 -j ACCEPT
```

2. ファイアウォールの設定を保存します。

```
## /sbin/service iptables save
```

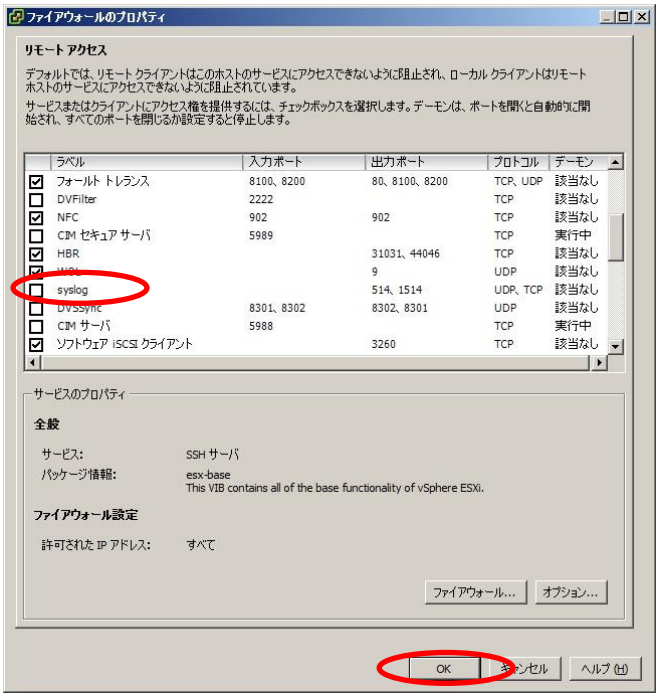
■ **ログ送信側(ESXi)の設定**

2.4.4.5.2.1. VMware vSphere Client の場合

1. vClient から対象の ESXi の[構成]画面を開き、ソフトウェアの[セキュリティプロファイル]を選ぶとサービスとファイアウォールの情報が表示されます。

ここでは、ファイアウォールの[プロパティ]を選択します。

2. ラベルから”syslog”を選び、[OK]を選択します。

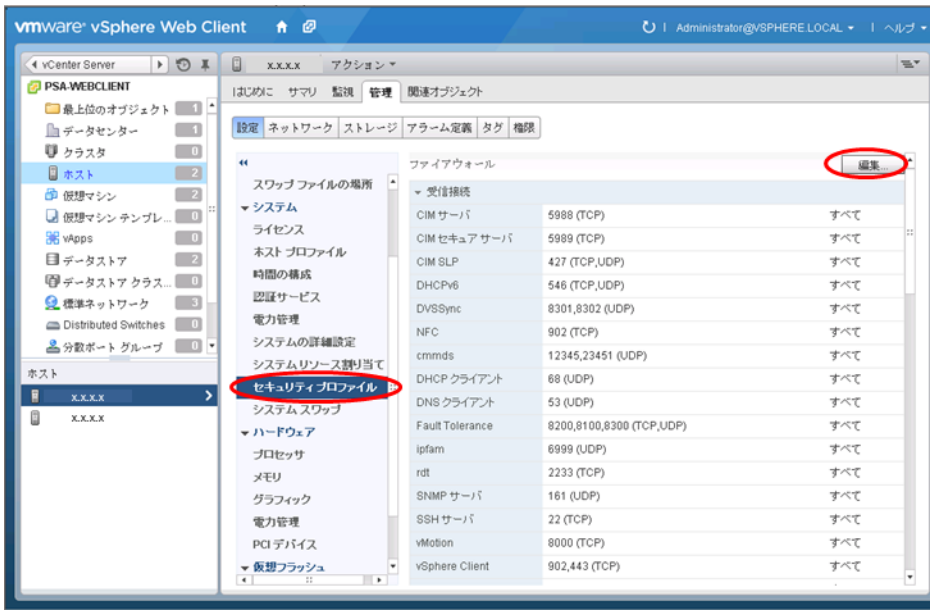


3. ファイアウォールの”発信接続”に”syslog”が存在することを確認して下さい。

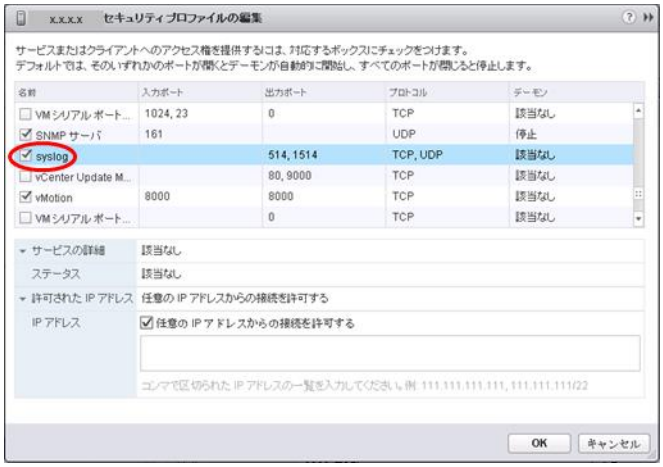
2.4.4.5.2.2. VMware vSphere Web Client の場合

1. 対象ホストの[管理]タブの[設定]画面を開き、 [セキュリティプロファイル]を選ぶとサービスとファイアウォールの情報が表示されます。

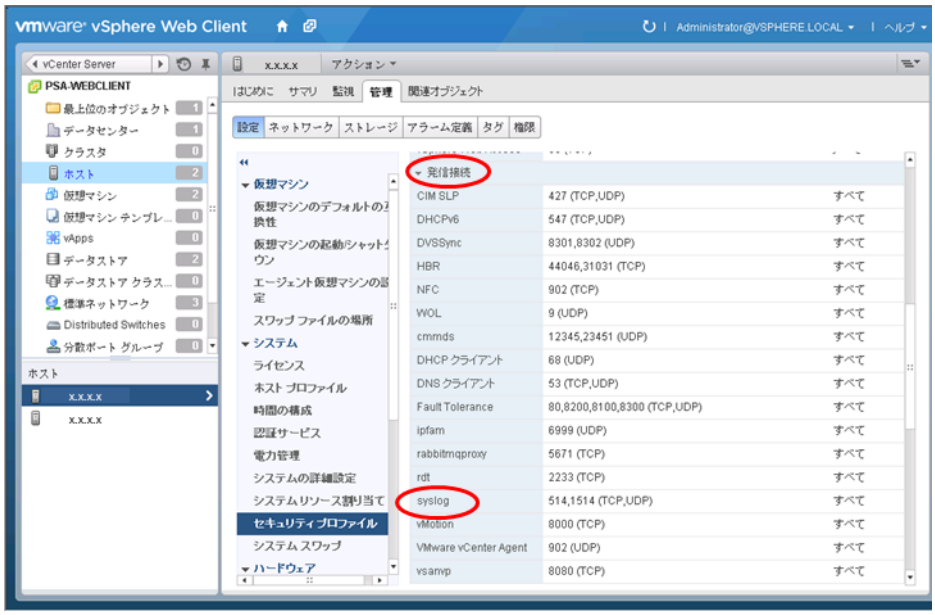
   ファイアウォールの[編集]を選択します。



2. 名前から”syslog”をチェックし、[OK]を選択します。



3. ファイアウォールの”発信接続”に”syslog”が存在することを確認して下さい。

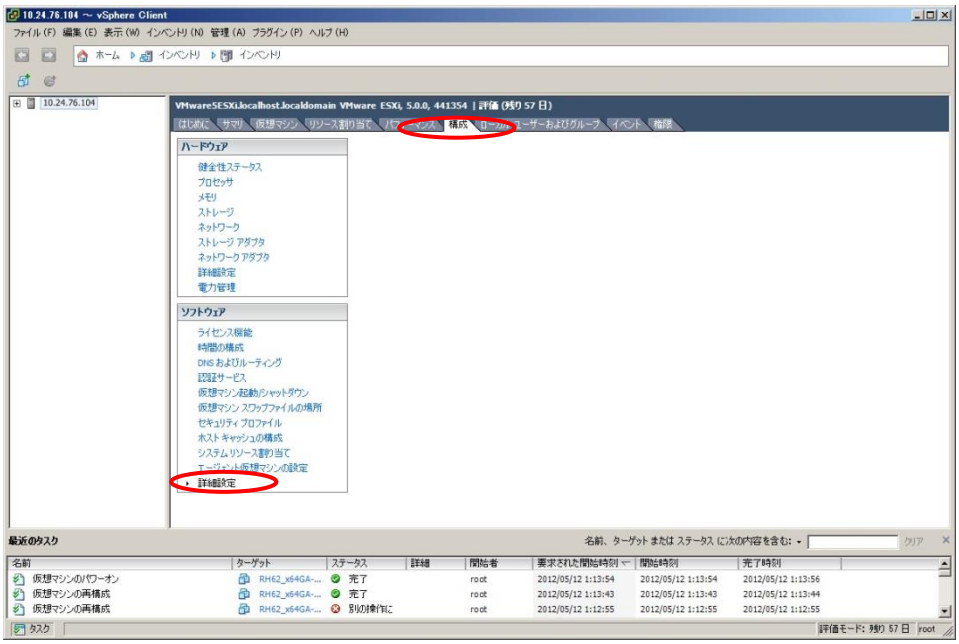


2.4.4.6 仮想 OS へのログ転送の設定(ログ送信側)

2.4.4.6.1. VMware vSphere Client の場合

■ **仮想 OS へのログ転送の設定**

1. VClient を立ち上げて、[構成]のタブのソフトウェアの項目の[詳細設定]を選択します。



[syslog]の項目の[global]を選択し、Syslog.global.logHost に転送先(管理用仮想 OS)の IP アドレスを入力して OK を押します。

設定する IP アドレスはネットワークの構成によって異なります。

1. ネットワーク構成例 1 の場合：

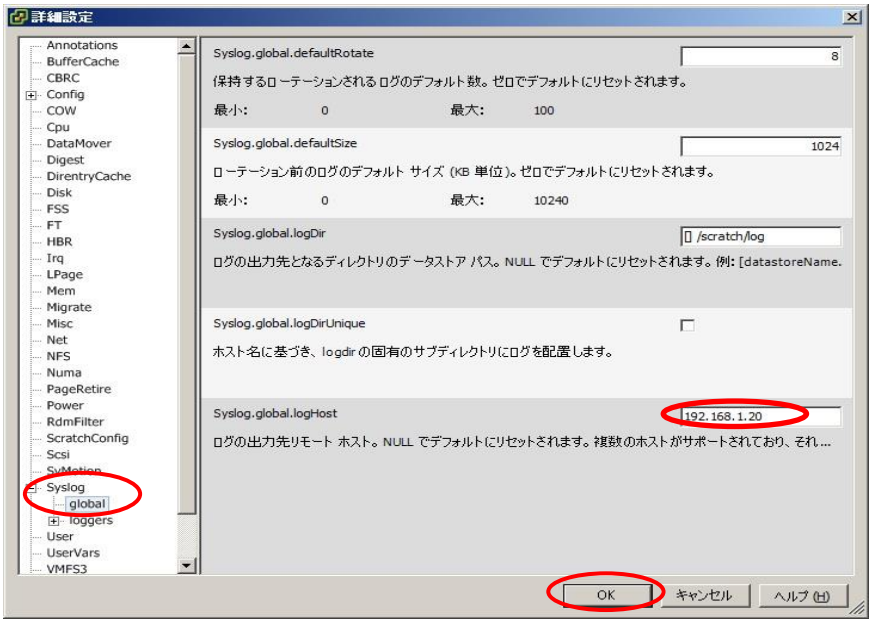
   2.4.2.5.3 章の手順 5 で仮想マシンに設定した ESXi 通信用 IP アドレスを設定します。

2. ネットワーク構成例 2 の場合：

   管理ネットワークの仮想マシンに割り当てた IP

   アドレスを設定します。

例)ネットワーク構成が 1 の場合



2. ログの転送確認

   仮想 OS にログインし、/var/log/messages に ESXi のログが転送されていることを確認して下さい。

   転送されない場合は、以下の手順を実施してからログが転送されているか確認します。

   1. SSH などで ESXi にログイン
   2. 以下のコマンドを実施

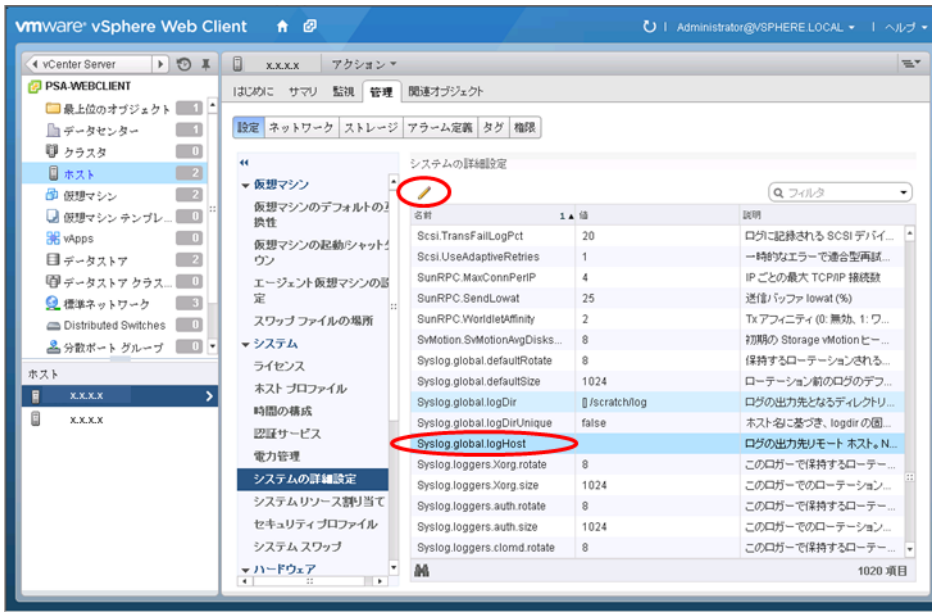
```
# esxcli system syslog reload
```

   ファイルが更新されない場合は、再度設定を見直して下さい。

2.4.4.6.2. VMware vSphere Web Client の場合

1. 対象ホストの[管理]タブの[設定]画面を開き、 [システムの詳細設定]をクリックします。

2. [Syslog.global.logHost]を選択し、[編集]アイコンをクリックします。



設定する IP アドレスはネットワークの構成によって異なります。

1. **ネットワーク構成例 1 の場合：**

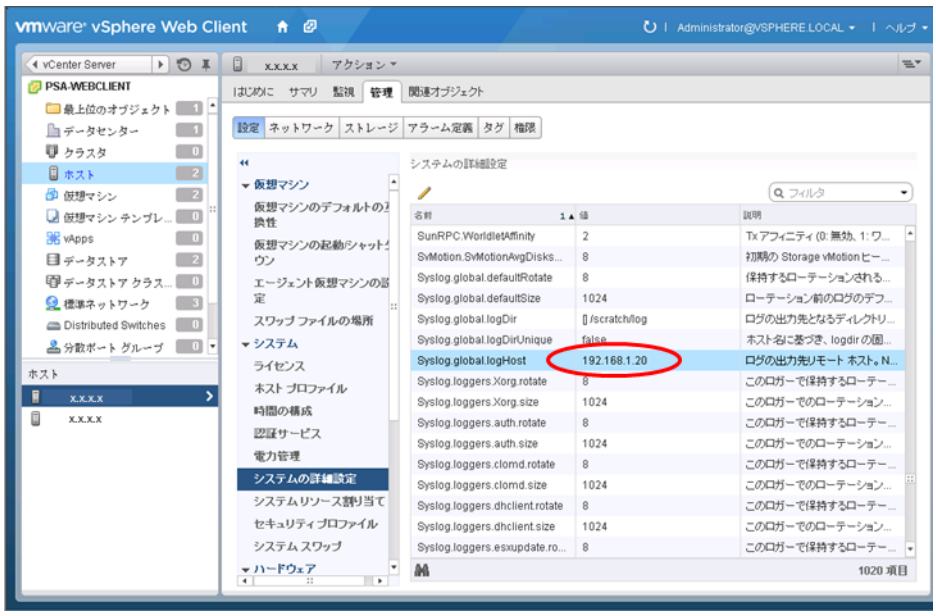
   2.4.2.5.3 章の手順 5 で仮想マシンに設定した ESXi 通信用 IP アドレスを設定します。

2. **ネットワーク構成例 2 の場合：**

   管理ネットワークの仮想マシンに割り当てた IP

   アドレスを設定します。

例)ネットワーク構成が 1 の場合



3. ログの転送確認

仮想マシンにログインし、/var/log/messages に ESXi のログが転送されていることを確認して下さい。

転送されない場合は、以下の手順を実施してからログが転送されているか確認します。

1. SSH などで ESXi にログイン
2. 以下のコマンドを実施

```
# esxcli system syslog reload
```

ファイルが更新されない場合は、再度設定を見直して下さい。

2.4.4.7 MMB 経由の Trap 送信の設定

MMB 経由で送信する Trap の設定を行います。

MMB 経由の Trap の送信先は MMB Web-UI で設定した宛先となります。

設定については、『PRIME QUEST1000 シリーズ 導入マニュアル』の”SNMP の設定”の章を参照して下さい。

Trap 通知には以下の情報を設定する必要があります。

・パーティションの名前

パーティションに割り振られた名前です。

詳細は、『PRIME QUEST1000 シリーズ 導入マニュアル』の”パーティション名の設定”の章を参照して下さい。

・MMB の仮想 IP アドレス

MMB Web-UI にアクセスするための仮想 IP アドレスです。

詳細は、『PRIME QUEST1000 シリーズ 導入マニュアル』の”MMB のネットワーク設定”の章を参照して下さい。

備考：

運用管理ソフトウェア(Systemwalker など)がパーティションを管理する場合には、本設定が必要です。

1. 仮想マシン上の以下の設定ファイルを開きます。

ファイル格納場所：

/etc/fujitsu/SVmco/usr/svmcovmtrap.conf

Trap 送信に必要な情報のパラメータは以下のようになります。

・TRAP_SET:

説明：MMB 経由の Trap 通報の有無

設定値：1:Trap 通報あり, 0:Trap 通報無し (デフォルト”1”)

・**Partition_Name**

説明：パーティション名を設定値

設定値：0～63 文字 (デフォルト 空)

・**MMB_V_IP**

説明：MMB の仮想 IP アドレスを設定値

設定値：0.0.0.0 ～255.255.255.255(デフォルト 255.255.255.255)

以下に例を示します。

MMB 経由の Trap 通報有りで、パーティション名が”Test Machine”で、MMB の仮想 IP アドレスが”192.168.40.1”の時

・　設定前

```
[TRAP]
TRAP_SET=1

Partition_Name =

MMB_V_IP=255.255.255.255
```

・　設定後(例)

```
[TRAP]
TRAP_SET=1

Partition_Name=Test Machine

MMB_V_IP=192.168.40.1
```

以上で設定は終了です。

2.4.5 仮想マシンの再起動

SVmcovm のインストール後の設定後、仮想マシンを再起動します。

【入力形式】

```
# /sbin/reboot
```

OS 起動後の確認事項

1. Syslog に以下のメッセージが出力され、その他に異常なメッセージが無い事の確認

```
I 00502 MMBA MMB connected
```

2. 仮想 OS にログインし、/var/log/messages に ESXi のログが転送されていることを確認して下さい。

転送されない場合は、以下の手順を実施してからログが転送されているか確認します。

1. SSH などで ESXi にログイン
2. 以下のコマンドを実施

```
# esxcli system syslog reload
```

ファイルが更新されない場合は、再度設定を見直して下さい。

2.4.6 SVmcovm のアップデートインストール

Red Hat Enterprise Linus での SVmcovm のアップデートインストール方法について説明します。アップデートの際にも、2.4.3.1　SVmcovm 動作に必要なパッケージをご確認ください。

以下の説明は、作業ディレクトリ (以下、$WORK_DIR と呼びます) 内に SVmcovm のパッケージ (SVmcovm-$VER.tar.gz) が展開されてディレクトリ "SVmcovm" が作成されていることを前提としています。 本作業は root 権限で行ってください。

1. DVD ドライブに『ServerView Suite DVD2』をセットし、以下のディレクトリから対象のモジュールを任意の場所にコピーします。

```
SVSLocalTools/Japanese/SVmcovm/SR_Linux/SVmcovm-XXX.tar.gz
```

2. SVmcovm サービスを停止します。

```
# /sbin/service y30SVmco stop
```

3. 作業ディレクトリ内のディレクトリ "SVmcovm" に移動します。

```
# cd $WORK_DIR/SVmcovm
```

4. 以下のコマンドを実行し、インストールを実施します。

```
# ./INSTALL.sh
```

5. SVmcovm サービスを起動します。

```
# /sbin/service y30SVmco start
```

6. /var/log/messages に ESXi のログが転送されていることを確認して下さい。

転送されない場合は、以下の手順を実施してからログが転送されているか確認します。

3. SSH などで ESXi にログイン
4. 以下のコマンドを実施

```
# esxcli system syslog reload
```

ファイルが更新されない場合は、再度設定を見直して下さい。

【注意】

SVmcovm アップデート時の注意事項

- SVmcovm アップデート時に以下のメッセージが出力されることがありますが、動作上問題はありません。

  /sbin/ldconfig: <ライブラリ名> is not a symbolic link

・SVmcovm1.1 版以前からのアップデートする場合、MMB 経由の Trap 送信の設定を実施して下さい。

2.4.7 SVmcovm のアンインストール

Red Hat Enterprise Linux での SVmcovm のアンインストール方法について説明します。

以下のコマンドの順番で、SVmcovm のサービスを停止してから、SVmcovm パッケージをアンインストールします。

【入力形式】

```
/sbin/service y30SVmco stop
/bin/rpm -e SVmcovm
```

2.4.8 VMware SVmcovm 保守情報取得

SVmcovm に関するトラブルが発生した場合、SVmcovm 調査資料収集コマンド (getosvmco) を実行し、さらに ESXi 上に ssh などでログインし、vm-support コマンドを実行します。

1. getosvmco コマンド

```
# /opt/fujitsu/SVmco/sh/getosvmco <ファイル名>
```

コマンド実行後、ファイル名に指定したファイルを収集して下さい。

2. vm-support コマンド

<実施例>

```
# vm-support
```

vm-support コマンド実行後、以下のようなメッセージが出力されますので、対象のファイルを収集して下さい。

```
To see the files collected, run: tar -tzf '/var/tmp/esx-vmware5esxi-xxxx-xx-xx--xx.xx.tgz'
```

備考

VMware ではコアファイルは /var/core 配下に出力され、自動では削除されません。
vm-support コマンド実行後、適宜コアファイルを削除することをお勧めします。

2.4.9 インストール(Windows Server 2008/2012)

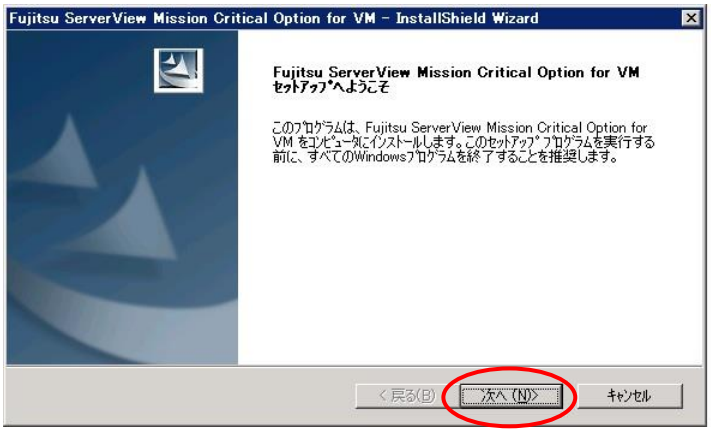
以下は、作業ディレクトリに SVmcovm パッケージファイルが格納されていることを前提に説明します。

本作業は Administrator 権限で行って下さい。

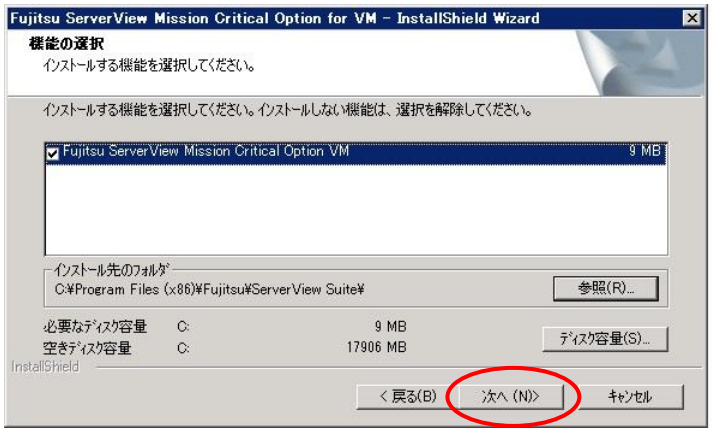
1. DVD ドライブに『ServerView Suite DVD2』をセットし、以下のディレクトリから対象のモジュールを任意の場所にコピーします。

   <ドライブ名>:\SVSLocalTools\Japanese\SVmcovm\SR_Windows\ ServerViewMissionCriticalOptionVM_Win.exe

2. エクスプローラから作業ディレクトリを開きます。
3. ServerViewMissionCriticalOptionVM_Win.exe を選択し、ダブルクリックまたはマウスの右クリックメニューから「開く」で起動します。
4. 「セットアップへようこそ画面」が表示されますので、「次へ(N)」をクリックします。



5. 「インストール先の選択画面」が表示されますので、インストール先を変更しない場合は「次へ(N)」ボタンをクリックします。



6. インストールが完了すると、「InstallShield Wizard の完了画面」が表示されます。インストール後の設定のため、「いいえ、後でコンピュータを再起動します。」を選択し、「完了」ボタンをクリックします。

以上でインストールは完了です。

2.4.10 インストール後の設定(Windows Server 2008/2012)

SVmcovm インストール後の設定は以下の手順で行ってください。

1. PSA-MMB 間通信 LAN の設定
2. PSA-MMB 間通信用ファイアーウォール機能の確認
3. ESXi へのアクセス情報の設定
4. 仮想マシンへのログ転送の設定(ログ受信側)
5. 仮想マシンへのログ転送の設定(ログ送信側)
6. MMB 経由の Trap 送信の設定

2.4.10.1 PSA-MMB 間通信 LAN の設定

ここでは SVmcovm が MMB と通信するための PSA-MMB 間通信 LAN の設定について説明します。

【注意】:

・SVmcovm が MMB と通信するためには、仮想マシンに PSA-MMB 間通信 LAN の物理アダプタが割り当たっている必要があります。

割り当てる方法については、2.4.2 SVmcovm のインストール前の確認/設定を参照してください。

・設定する IP アドレスは、MMB 側の PSA-MMB 間通信 LAN の IP アドレスと同一のサブネットの IP である必要があります。MMB 側の IP アドレスは、MMB Web-UI から設定してください。

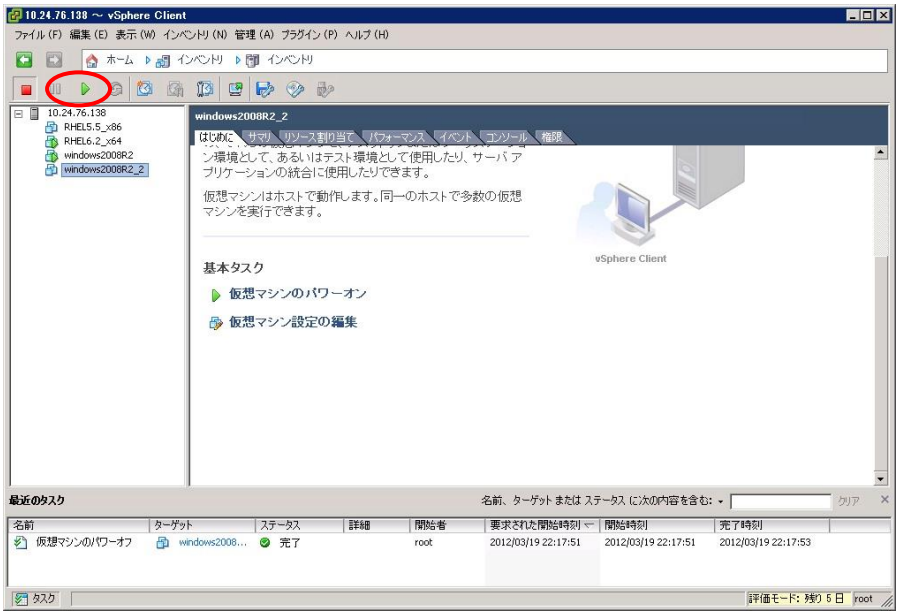
・MMB Web-UI の[Network Configuration]-[Network Interface]画面にて、[MMB-PSA IP Address]の[Interface]が Disable の場合、イベント通報機能が使用出来ません。尚、Disable から Enable に変更した場合、変更後に OS の再起動が必要です。

3. PSA-MMB 間通信 LAN の設定

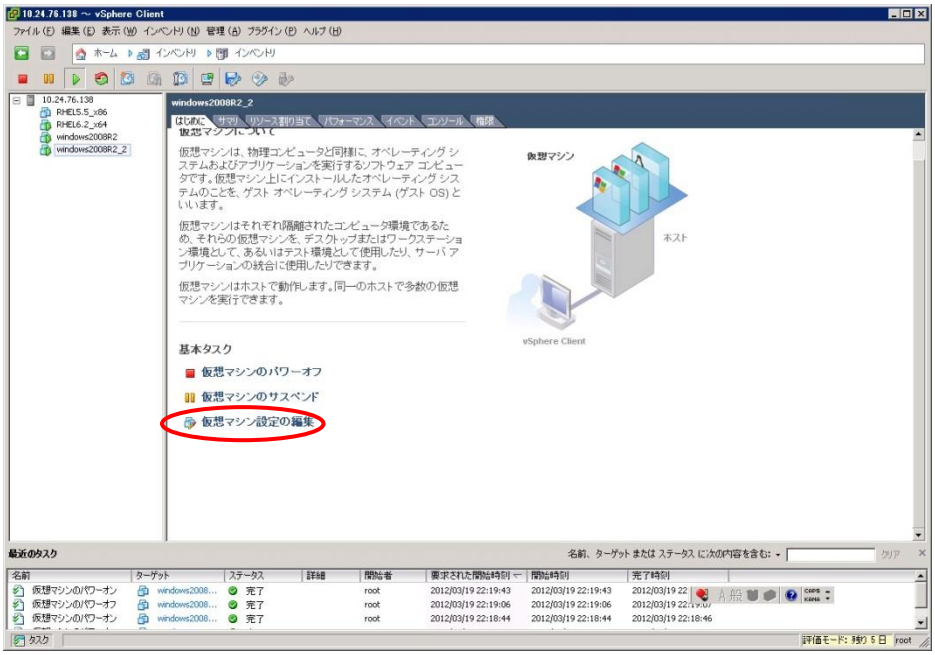
以下の手順で、PSA-MMB 間通信 LAN の設定を行います。

2.4.10.1.1. VMware vSphere Client の場合

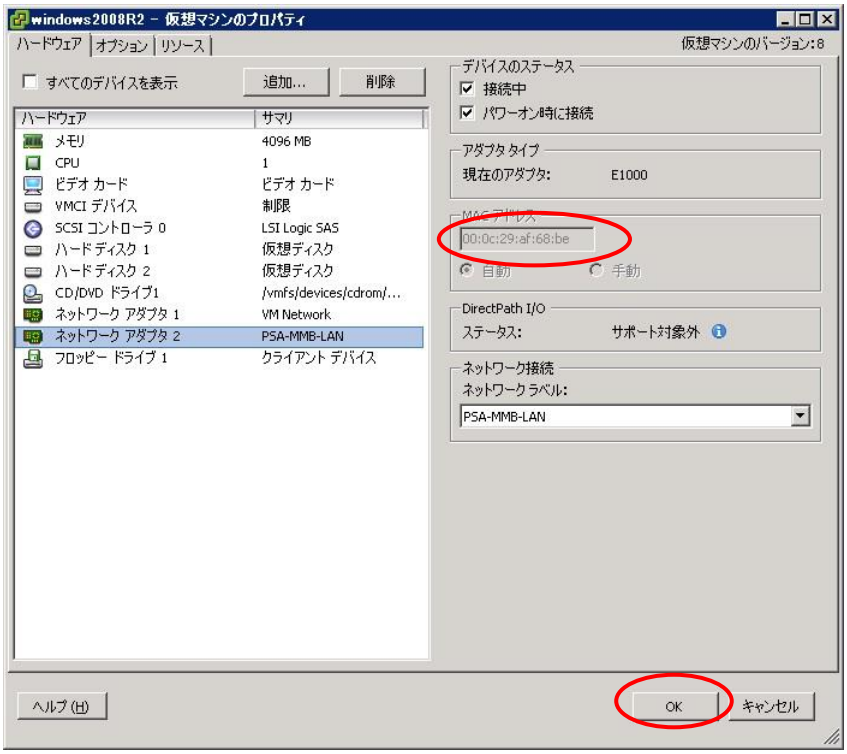
1. VMware vShpere Client を起動します。
2. 左上から『2.4.2 SVmcovm のインストール前の確認/設定』で PSA-MMB-LAN の仮想スイッチを割り当てた仮想マシンをクリックします。
3. 上部にあるツールバーから[パワーオン]をクリックします。



4. 仮想マシンが立ち上がったら、PSA-MMB 間通信 LAN の MAC アドレスを調べるために、[はじめに]タブの[仮想マシン設定の編集]をクリックします。

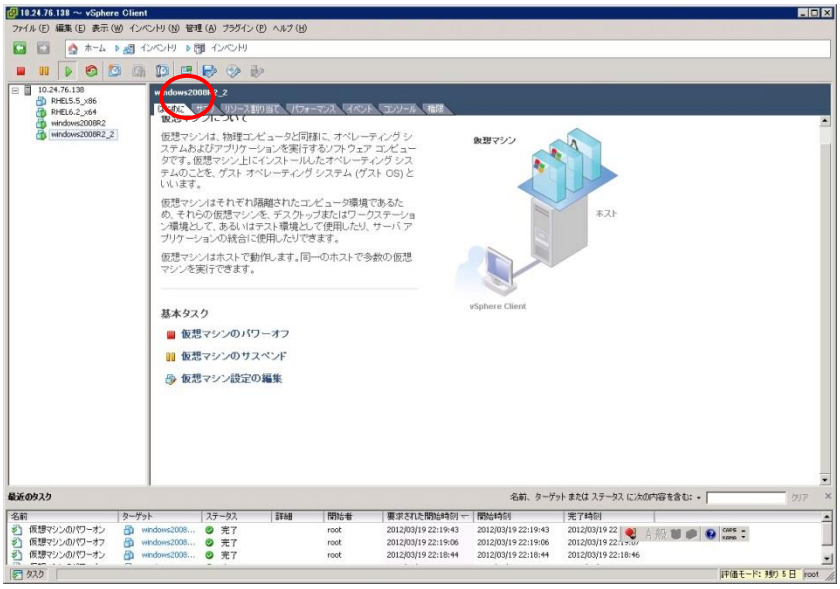


5. PSA-MMB-LAN のネットワークアダプタを選び、[MAC アドレス]を確認します。確認後、[OK]をクリックします。

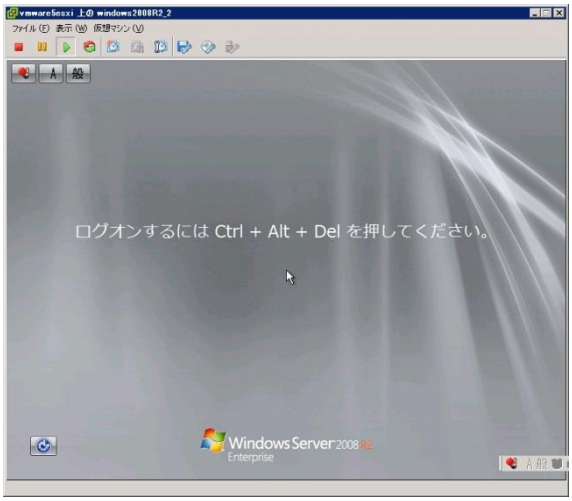


ここでは、PSA-MMB 間通信 LAN の MAC アドレスは”**00：0C：29：af：68：be**”ということが確認できました。

6. 仮想マシンの上部にあるツールバーから[仮想マシンコンソールの起動]をクリックしてコンソールを立ち上げます。



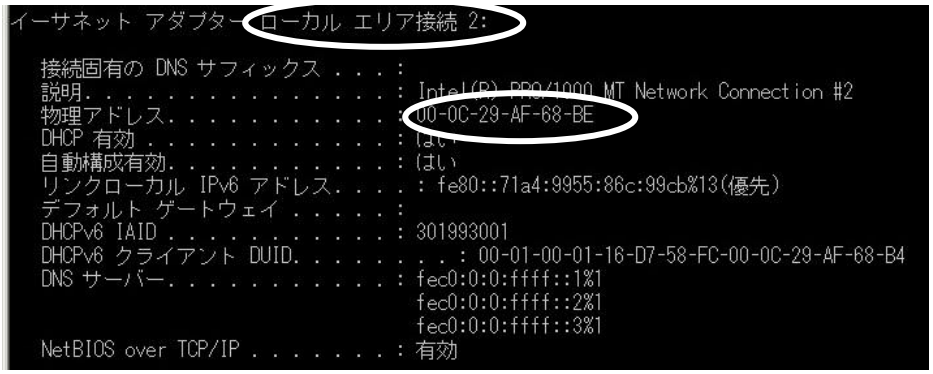
・仮想コンソール画面



7. ログインしたら、コマンドプロンプトを立ち上げて、以下のコマンドを実行し、PSA-MMB 間通信 LAN が割り当たっているネットワークインターフェースを調べます。検索には MAC アドレスは 5 で確認した値を使います。

```
> ipconfig /all
```

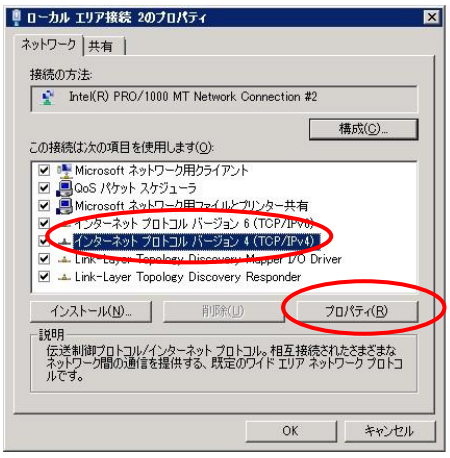
【実行結果(例)】



実行結果より、”ローカルエリア接続 2”が PSA-MMB 間通信 LAN ということが確認できました。

8. [コントロールパネル] -> [ネットワークとインターネット] -> [ネットワークの共有センター]を開き、手順 7 で確認した LAN(ここでは、ローカルエリア接続 2)を選びます。

9. ローカルエリア接続 2 の[プロパティ]から[インターネットプロトコルバージョン 4(TCP/IPv4)]を選んだ状態で、[プロパティ]をクリックします。

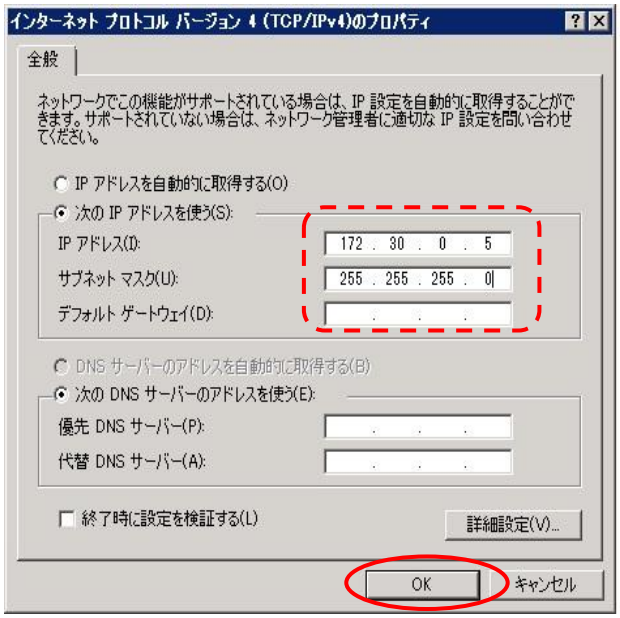


10. 以下のように IP アドレスを設定します。

- 設定する IP アドレスはパーティション番号によって異なります。 以下の表の値を使用して[OK]をクリックします。

パーティション番号	IP アドレス	サブネットマスク
0	172.30.0.2	255.255.255.0
1	172.30.0.3	
2	172.30.0.4	
3	172.30.0.5	

<パーティション番号#3 の場合の例>



注意：IP アドレスは同一筐体内で重複しない値を設定して下さい。

11. MMB に対して、Ping 応答があることを確認します。(MMB Web-UI での MMB-PSA IP Address の設定値が”172.30.0.1”の場合)

```
# ping 172.30.0.1
```

12. SVmcovm の設定ファイルを編集します。以下のファイルをエディターで開きます。

```
[SVmco インストール先フォルダ] ¥etc¥fujitsu¥SVmco¥usr¥mmblan.conf

(例. C:¥Program Files (x86)¥Fujitsu¥ServerView
Suite¥SVmco¥etc¥fujitsu¥SVmco¥usr¥mmblan.conf)
```

13. 以下のパラメーターを設定します。

【設定値】

MMBIP：MMB Web-UI で設定した MMB-PSA IP Address の IP アドレス

ID：ESXi が稼働しているパーティション ID

【設定例】

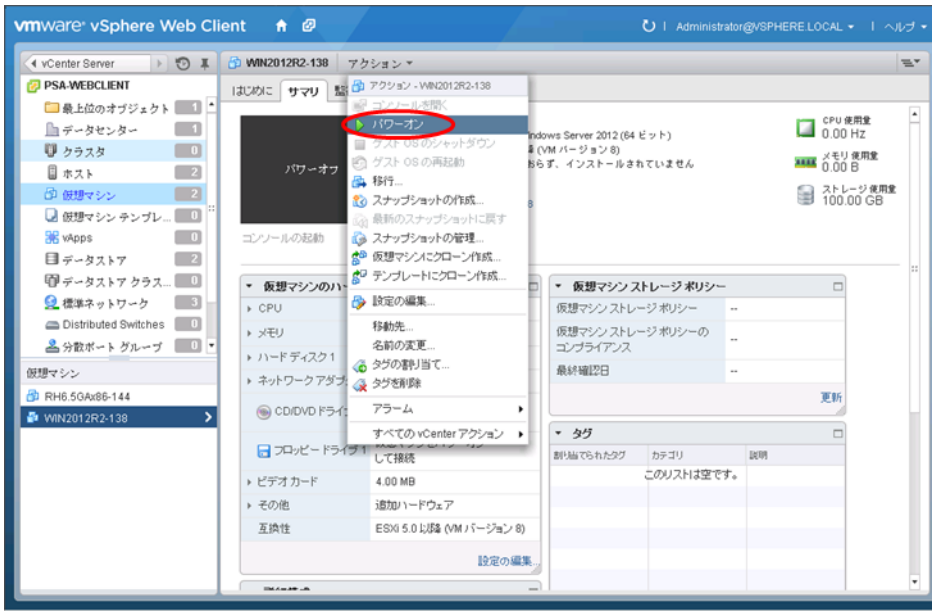
< MMB 側の PSA-MMB 間通信 LAN の IP アドレスが 172.30.0.1、パーティション番号が 3 の時>

```
[NETWORK]
MMBIP = 172.30.0.1


[PARTITION]
ID = 3
```

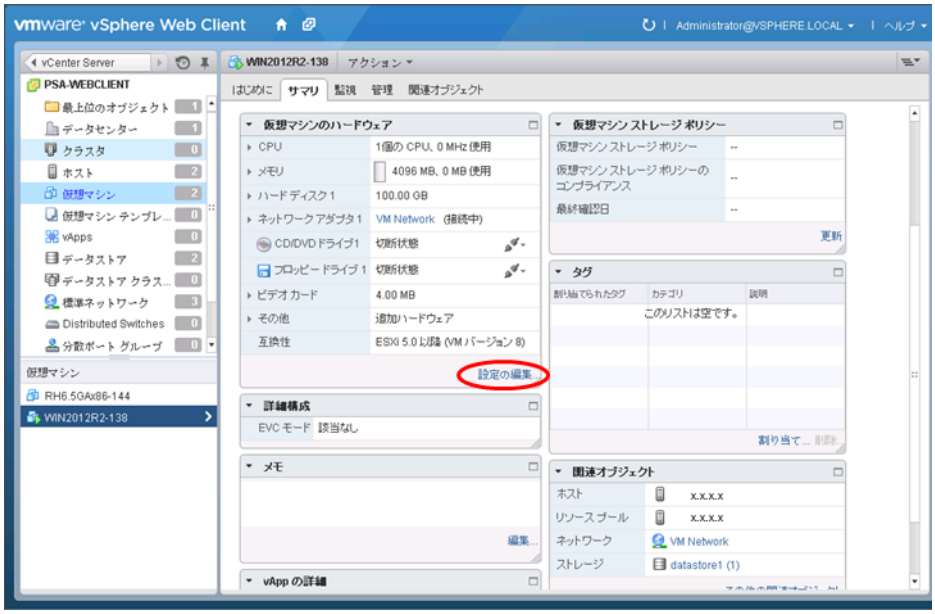
PSA-MMB 間通信 LAN の設定は以上です。

2.4.10.1.2. VMware vSphere Web Client の場合

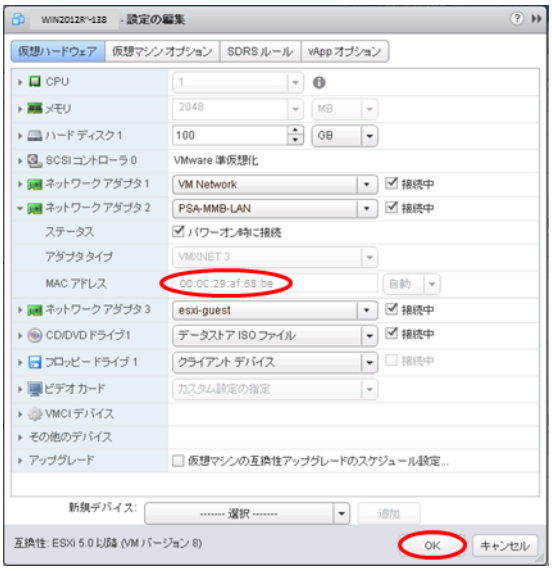
1. VMware vShpere Web Client を起動します。
2. 『2.4.2SVmcovm のインストール前の確認/設定』で PSA-MMB-LAN の仮想スイッチを割り当てた仮想マシンをクリックします。
3. [アクション]プルダウンより、 [パワーオン]をクリックします。



4. 仮想マシンが立ち上がったら、PSA-MMB 間通信 LAN の MAC アドレスを調べるために、対象仮想マシンの[仮想マシンのハードウェア]の[設定の編集]をクリックします。

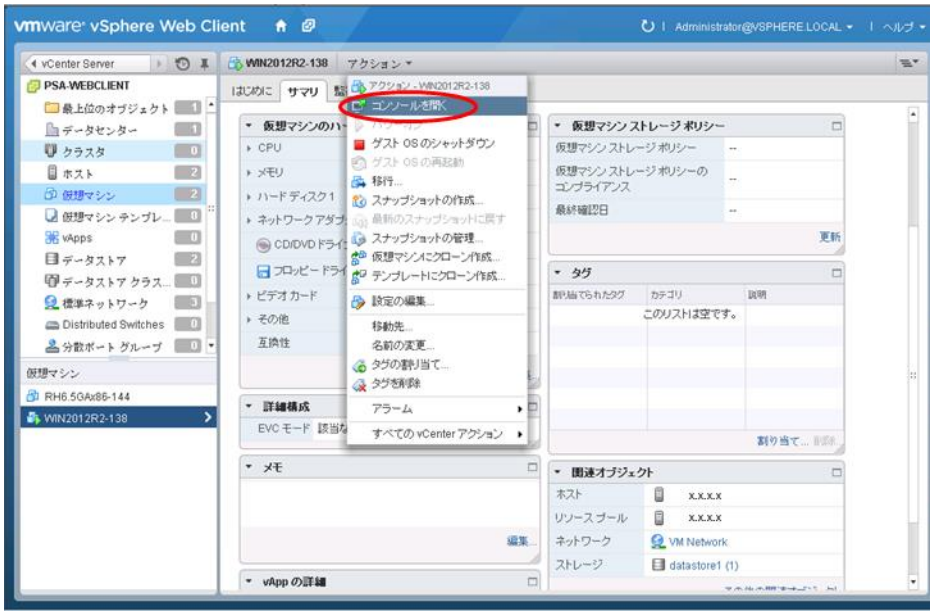


5. PSA-MMB-LAN のネットワークアダプタを選び、[MAC アドレス]を確認します。確認後、[OK]をクリックします。



ここでは、PSA-MMB 間通信 LAN の MAC アドレスは” **00:0C:29:af:68:be**”ということが確認できました。

6. [アクション]プルダウンより、[コンソールを開く]をクリックしてコンソールを立ち上げます。



・仮想コンソール画面

WIN2012R2-138
Ctrl-Alt-Delete の送信
フル スクリーン
サインインするには Ctrl + Alt + Del キーを押してください。
14:53
1月8日 水曜日

7. ログインしたら、コマンドプロンプトを立ち上げて、以下のコマンドを実行し、PSA-MMB 間通信 LAN が割り当たっているネットワークインターフェースを調べます。検索には MAC アドレスは 5 で確認した値を使います。

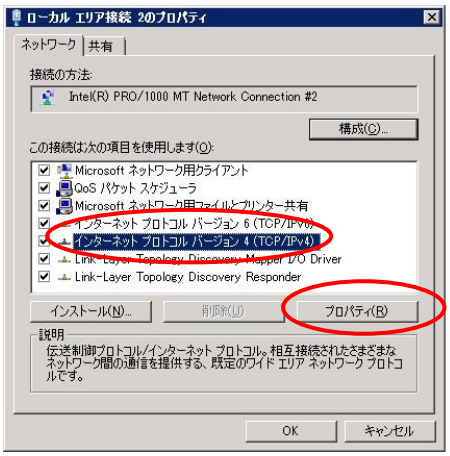
```
> ipconfig /all
```

【実行結果(例)】

実行結果より、”ローカルエリア接続 2”が PSA-MMB 間通信 LAN ということが確認できました。

8. [コントロールパネル] -> [ネットワークとインターネット] -> [ネットワークの共有センター]を開き、手順 7 で確認した LAN(ここでは、ローカルエリア接続 2)を選びます。

9. ローカルエリア接続 2 の[プロパティ]から[インターネットプロトコルバージョン 4(TCP/IPv4)]を選んだ状態で、[プロパティ]をクリックします。

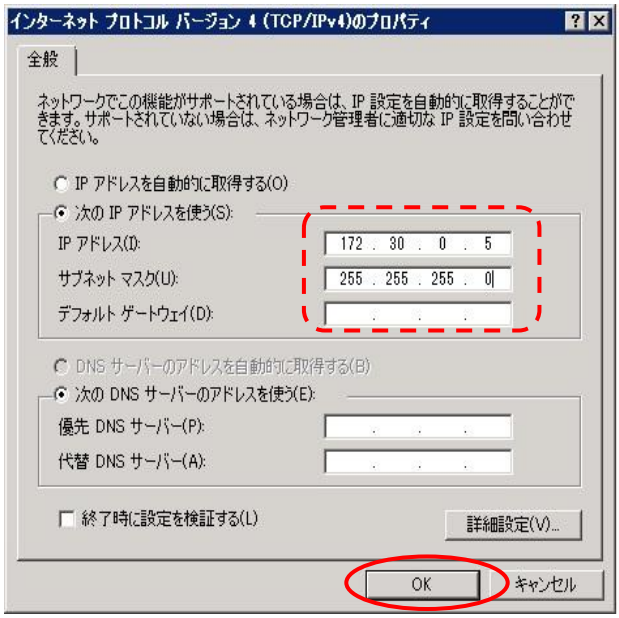


10. 以下のように IP アドレスを設定します。

- 設定する IP アドレスはパーティション番号によって異なります。 以下の表の値を使用して[OK]をクリックします。

パーティション番号	IP アドレス	サブネットマスク
0	172.30.0.2	255.255.255.0
1	172.30.0.3	
2	172.30.0.4	
3	172.30.0.5	

<パーティション番号#3 の場合の例>



注意：IP アドレスは同一筐体内で重複しない値を設定して下さい。

11. MMB に対して、Ping 応答があることを確認します。(MMB Web-UI での MMB-PSA IP Address の設定値が”172.30.0.1”の場合)

```
# ping 172.30.0.1
```

12. SVmcovm の設定ファイルを編集します。以下のファイルをエディターで開きます。

```
[SVmco インストール先フォルダ] ¥etc¥fujitsu¥SVmco¥usr¥mmblan.conf

(例. C:¥Program Files (x86)¥Fujitsu¥ServerView
Suite¥SVmco¥etc¥fujitsu¥SVmco¥usr¥mmblan.conf)
```

13. 以下のパラメーターを設定します。

【設定値】

MMBIP：MMB Web-UI で設定した MMB-PSA IP Address の IP アドレス

ID：ESXi が稼働しているパーティション ID

【設定例】

< MMB 側の PSA-MMB 間通信 LAN の IP アドレスが 172.30.0.1、パーティション番号が 3 の時>

```
[NETWORK]
MMBIP = 172.30.0.1


[PARTITION]
ID = 3
```

PSA-MMB 間通信 LAN の設定は以上です。

2.4.10.2 ファイアーウォールの機能の確認

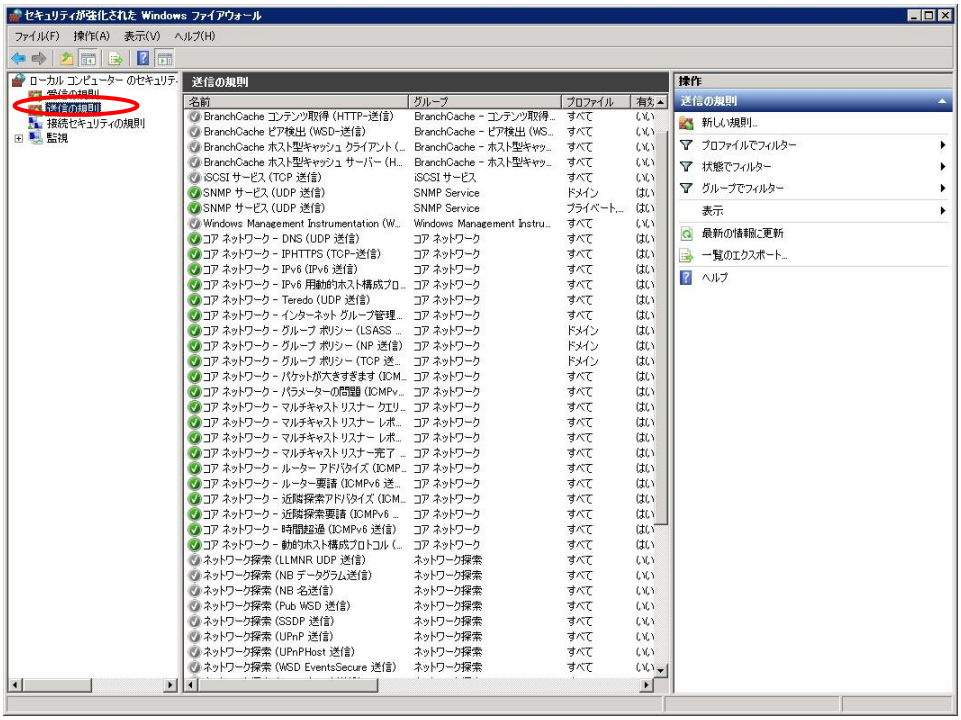
Windows ファイアーウォールを有効にして運用する場合、以下のポートは MMB とのデータ送受信に使用されるため、開放する必要があります。

- svmcommbs.exe が使用する MMB への送信ポート (MMP 側 TCP:5000 ポート用)
- svmcommbs.exe が使用する MMB への ICMP プロトコル

・ 操作手順

1. [スタート] - [管理ツール] - [セキュリティが強化された Windows ファイアウォール] の順に選択します
2. [セキュリティが強化された Windows ファイアウォール] 画面の左ペインから [送信の規則] をクリックします。

中央ペインに [送信の規則] 一覧が表示されます。



3. [セキュリティが強化された Windows ファイアウォール] 画面の右ペインから [新しい規則] または [新規の規則] をクリックします。[新規の送信の規則のウィザード] 画面が開き、左上に [規則の種類] と表示されます。[カスタム] を選択し、[次へ] ボタンをクリックします。

4. 左上に [プログラム] と表示されます。[このプログラムのパス] を選択し、[参照] ボタンをクリックします。" svmcommbs.exe" を選択し、[次へ] ボタンをクリックします。

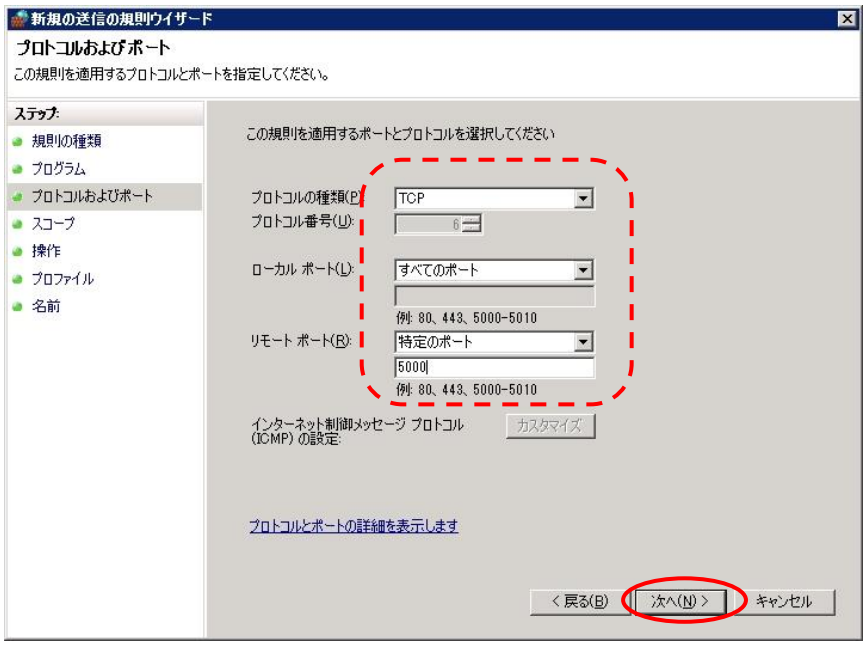
備考

svmcommbs.exe は SVmco のインストールパス配下の opt¥fujitsu¥SVmco¥bin¥にあります。SVmco のインストールパスは初期値で Program Files¥fujitsu¥ServerView Suite¥SVmco¥です。

5. 左上に [プロトコルおよびポート] と表示されます。以下の項目を選択または入力して、[次へ] ボタンをクリックします。

プロトコルおよびポート] の設定項目

画面項目	選択または入力する値
[プロトコルの種類]	[TCP]
[ローカルポート]	[すべてのポート]
[リモートポート]	[特定のポート]を選択し、下のテキストボックスに「5000」と入力する。



6. 左上に [スコープ] と表示されます。以下の項目を選択または入力して、[次へ] ボタンをクリックします。

   [スコープ] の設定項目

画面項目		選択または入力する値
Windows2008	Windows2008R2 Windows2012	
[この規則はどのローカル IP アドレスに一致しますか?]	**この規則を適用するローカル IP アドレスを選択してください。**	[任意の IP アドレス]
[この規則はどのリモート IP アドレスに一致しますか?]	この規則を適用するリモート IP アドレスを選択してください。	[これらの IP アドレス] を選択し、[追加] ボタンをクリックする。 MMB の PSA-MMB 通信 LAN 用 IP アドレスを入力する。

7. 左上に [操作] と表示されます。[接続を許可する] を選択し、[次へ] ボタンをクリックします。
8. 左上に [プロファイル] と表示されます。[ドメイン] 、[プライベート]、[パブリック] すべてのチェックボックスをオンにして、[次へ] ボタンをクリックします。
9. 左上に [名前] と表示されます。[名前[N]:] に「MCOMMBS」と入力し、[完了] ボタンをクリックします。

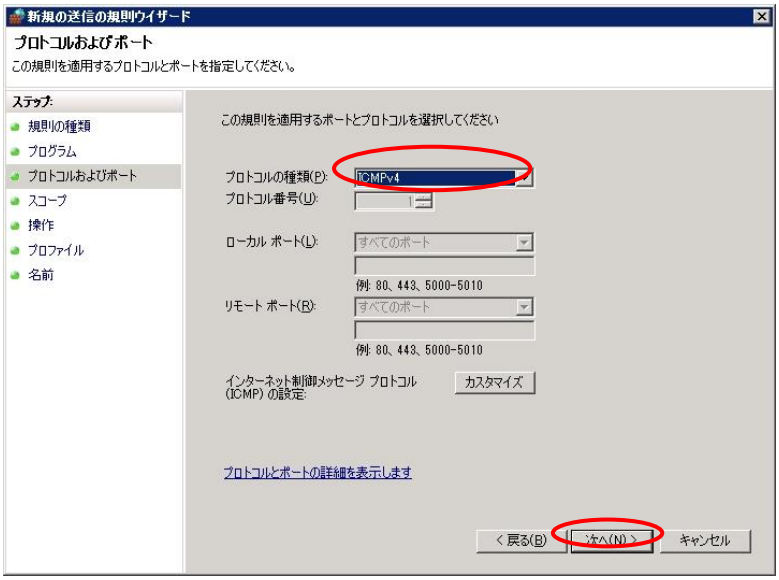
続けて [セキュリティが強化された Windows ファイアウォール] 画面の右ペインから [新しい規則] または [新規の規則] をクリックします。[新規の送信の規則のウィザード] が開き、左上に [規則の種類] と表示されます。[カスタム] を選択し、[次へ] ボタンをクリックします。

10. 左上に [プログラム] と表示されます。[このプログラムのパス] を選択し、[参照] ボタンをクリックします。[svmcommbs.exe] を選択し、[次へ] ボタンクリックします。

備考

svmcommbs.exe は SVmco のインストールパス配下の opt¥fujitsu¥SVmco¥bin¥にあります。SVmco のインストールパスは初期値で Program Files¥fujitsu¥ServerView Suite¥SVmco¥です。

11. 左上に [プロトコルおよびポート] と表示されます。[プロトコルの種類] で [ICMPv4] を選択し、[次へ] ボタンをクリックします。



12. 左上に [スコープ] と表示されます。以下の項目を選択または入力して、[次へ] ボタンをクリックします。

    [スコープ] の設定項目

画面項目		選択または入力する値
Windows2008	Windows2008R2 Windows2012	
[この規則はどのローカル IP アドレスに一致しますか?]	この規則を適用するローカル IP アドレスを選択してください。	[任意の IP アドレス]
[この規則はどのリモート IP アドレスに一致しますか?]	この規則を適用するリモート IP アドレスを選択してください。	[これらの IP アドレス] を選択し、[追加] ボタンをクリックする。 MMB の PSA-MMB 通信 LAN 用 IP アドレスを入力する。

13. 左上に [操作] と表示されます。[接続を許可する[A]] を選択し、[次へ] ボタンをクリックします。

14. 左上に [プロファイル] と表示されます。[ドメイン]、[プライベート]、[パブリック] すべてのチェックボックスをオンにして、[次へ] ボタンをクリックします。

15. 左上に [名前] と表示されます。[名前[N]:] に「MCOICMP」と入力し、[完了] ボタンをクリックします。

以上でファイアーウォールの設定は終了です。

2.4.10.3 ESXi へのアクセス情報の設定

SVmcovm は起動時に ESXi への ssh 経由で PCI カード情報やログを取得しています。

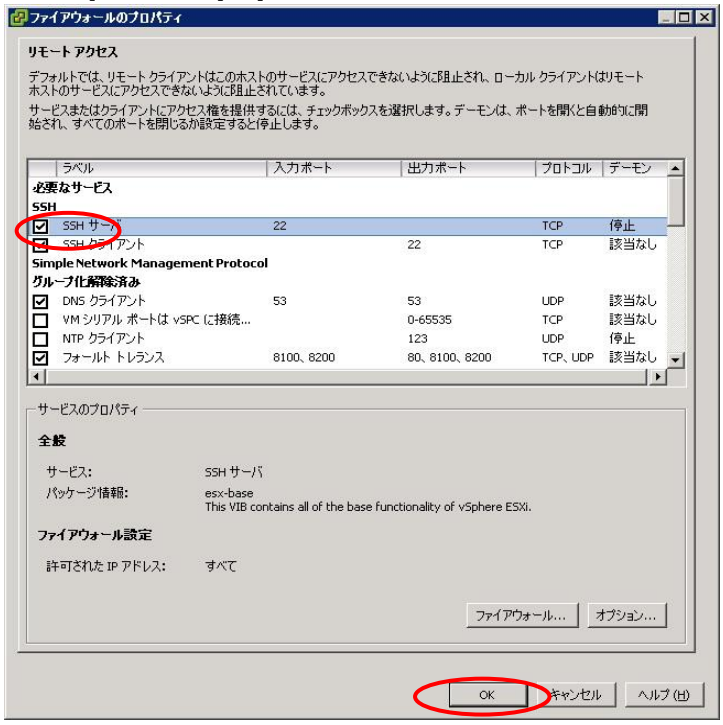
ここでは、ESXi へのアクセスするための設定を行います。

本設定により、SVmcovm 起動時に ESXi から自動的に PCI カード情報やログを取得することで PCI カードの故障検出が可能となります。

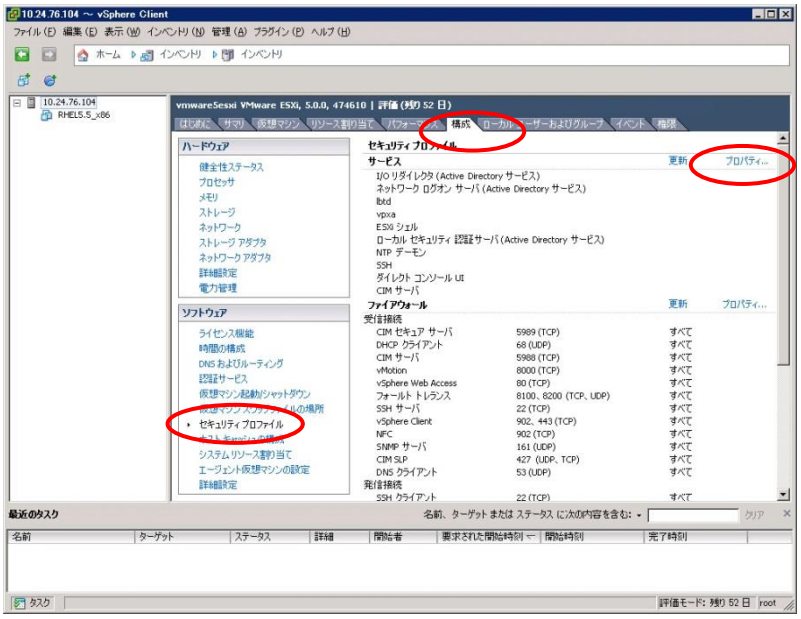
2.4.10.3.1. VMware vSphere Client の場合

1. VMware vShpere Client を起動します。
2. [ホーム] → [インベントリ] → [インベントリ] から、[構成] タブをクリックします。
3. 左下にある [ソフトウェア] 内の [セキュリティプロファイル] をクリックします。
4. [セキュリティプロファイル]情報が表示された画面のファイアウォールの[プロパティ]をクリックします。

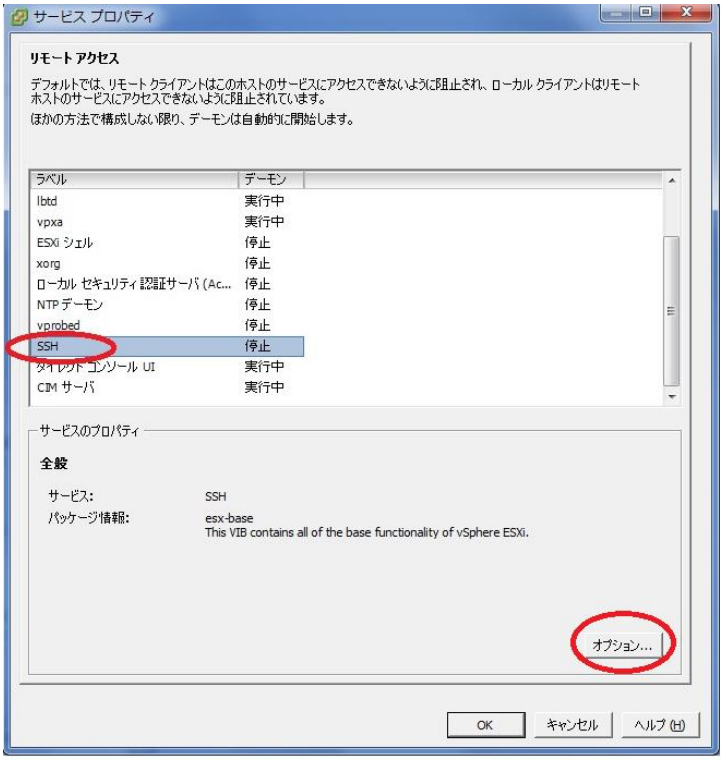
5. [SSH サーバ]を選択し、[OK]ボタンをクリックします。



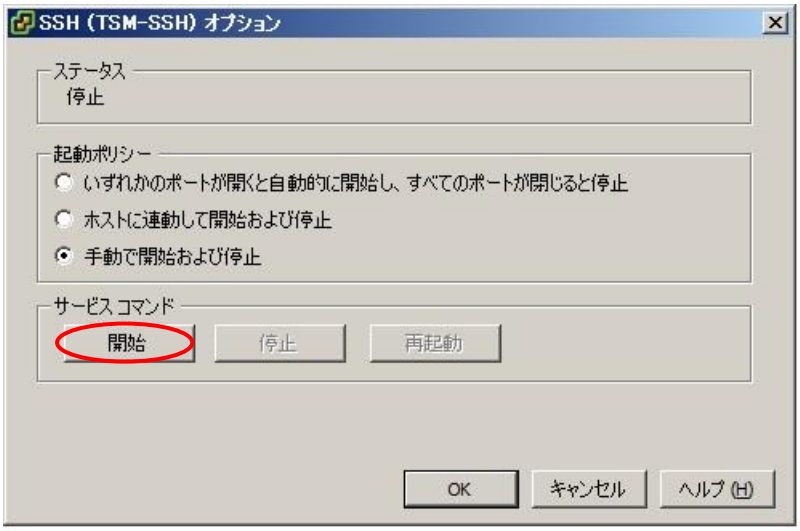
6. [セキュリティプロファイル] 情報が表示された画面の右上にある [プロパティ] をクリックします。



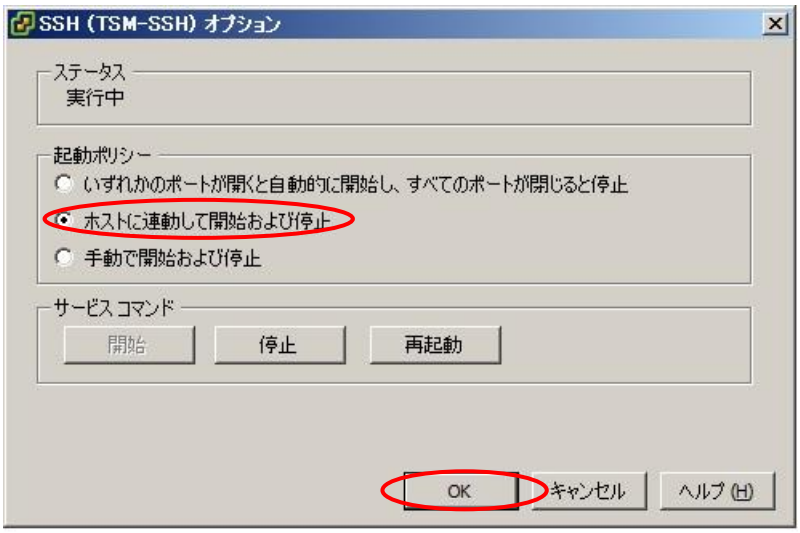
7. [SSH]を選択し、[オプション]ボタンをクリックします。



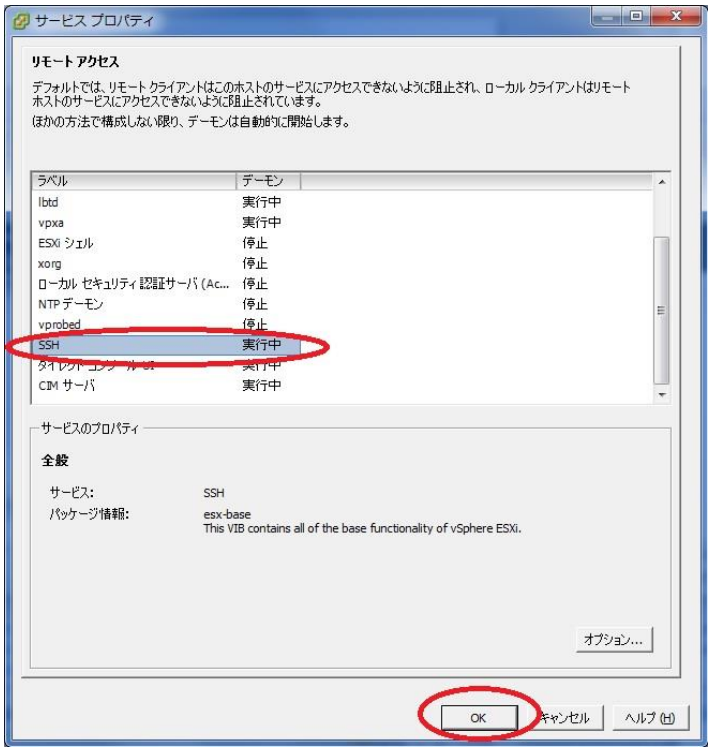
8. [サービスコマンド]で開始をクリックします。



9. 次に[起動ポリシー]の[ホストに連動して開始および停止]を選択し、[OK]をクリックします。



10. [SSH サーバ]の[デーモン]が実行中になっていることを確認して[OK]をクリックします。



11. 仮想マシンへログインし、コマンドプロンプトで以下のディレクトリへ移動します。

```
# cd <SVmcovm のインストールパス>opt¥fujitsu¥SVmco¥bin
```

12. コマンドプロンプトを管理者権限で起動させ、コマンドを以下のオプションを付けて実行します。

対話形式で ESXi の IP,ログイン ID,とパスワードを入力します。

```
# setuserinfo.exe  -i
```

設定する IP アドレスは、ESXi へアクセスするための IP アドレスです。

ネットワークの構成によって設定値が異なります。

1. ネットワーク構成例 1 の場合：

   2.4.2.5.1 章の手順 8 で設定した ESXi からの情報取得用 IP アドレスを設定します。

2. ネットワーク構成例 2 の場合：

   管理ネットワークの ESXi に割り当てた IP アドレスを設定します。

13. 実行後、以下のオプションを付けて実行し、2.で入力した値のチェックを行います。

```
# setuserinfo.exe  –c
Successful execution of the command.
```

上記のメッセージが出力されれば設定終了です。

運用条件などにより、ssh 接続が出来ない場合は、手動にて ESXi から PCI カード情報を取得し、仮想マシンの指定の場所に配置後に SVmcovm の再起動が必要です。

また、SSH 接続を許可しない環境において PCI カードの追加/交換があった場合も、本手順の実施が必要です。

尚、SSH 接続設定を実施しない場合は、以下の監視上の制約が発生します。

1. SVmcovm 起動前の PCI カード/ディスクの故障検出が出来ない

   ※SVmcovm 起動後は監視可能
2. MMB の PCI レーン縮退監視が出来ない
3. システムステータスが OS Running/OS Shutdown に変更されない。

以下に手順を示します。

1. SSH で ESXi へログインし、以下のコマンドを実行します。

・ PCI カード情報取得コマンド

```
# /sbin/esxcli hardware pci list > pcicardinfo
```

・ NIC 情報取得コマンド

```
# /sbin/esxcfg-nics -l > nicinfo
```

4. 実行結果 (例)

・ pcicardinfo

```
000:000:19.0
   Address: 000:000:19.0
   Segment: 0x0000
   Bus: 0x00
   Slot: 0x19
   Function: 0x00
   VMkernel Name: vmnic0
   Vendor Name: Intel Corporation
   Device Name: 82567LF-2 Gigabit Network Connection
   Configured Owner: Unknown
   Current Owner: VMkernel
   Vendor ID: 0x8086
   Device ID: 0x10cd
   SubVendor ID: 0x10cf
   SubDevice ID: 0x159b
   Device Class: 0x0200
 .
 .
```

・ nicinfo

```
Name    PCI          Driver      Link Speed     Duplex MAC Address       MTU    Description

vmnic0  0000:00:19.00 e1000e     Up   100Mbps   Full   00:17:42:de:7c:4b 1500   Intel Corporation 82567LF-2
Gigabit Network Connection

vmnic1  0000:05:00.00 igb        Up   100Mbps   Full   00:17:42:9b:dc:b4 1500   Intel Corporation 82576 Gigabit
Network Connection

vmnic2  0000:05:00.01 igb        Down 0Mbps     Half   00:17:42:9b:dc:b5 1500   Intel Corporation 82576
Gigabit Network Connection

vmnic3  0000:06:00.00 igb        Down 0Mbps     Half   00:17:42:9b:dc:b6 1500   Intel Corporation 82576
Gigabit Network Connection

vmnic4  0000:06:00.01 igb        Down 0Mbps     Half   00:17:42:9b:dc:b7 1500   Intel Corporation 82576
Gigabit Network Connection

vmnic5  0000:0e:00.00 e1000e     Down 0Mbps     Half   00:15:17:7d:d4:e2 1500   Intel Corporation 82571EB
Gigabit Ethernet Controller

vmnic6  0000:0e:00.01 e1000e     Down 0Mbps     Half   00:15:17:7d:d4:e3 1500   Intel Corporation 82571EB
Gigabit Ethernet Controller
```

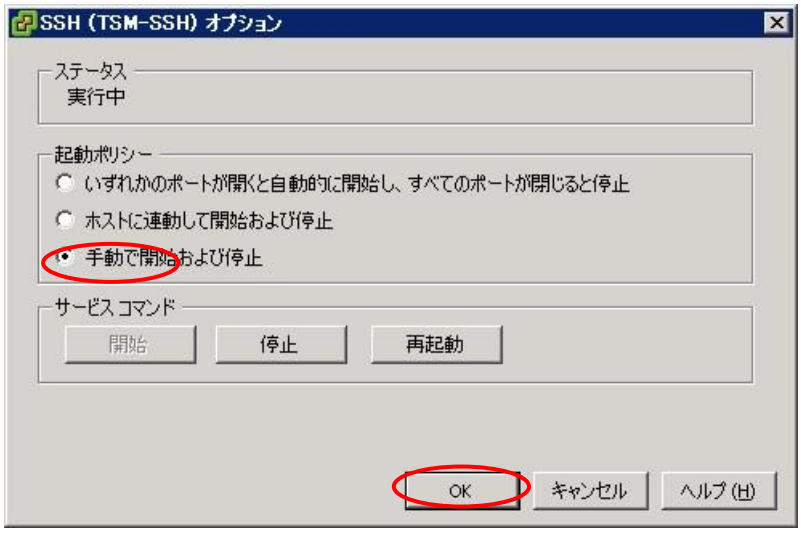
2. 作成した二つのファイル(pcicardinfo,nicinfo)を **SVmcovm をインストール予定の仮想マシンの以下のディレクトリにコピー**します。

```
<SVmcovm のインストールパス>¥etc¥fujitsu¥SVmco¥usr
```

コピーが完了したら、以下の方法で ESXi への ssh 接続出来ないように設定を元に戻します。

3. 確認後、SSH のサービスを停止させます。SSH を起動させた時のように、VMware vSphere Client を起動させて、[ホーム]→[インベントリ]→[インベントリ]から[構成]タブをクリックし、左下の[ソフトウェア]内の[セキュリティプロファイル]からプロパティをクリックし、[ファイアウォールのプロパティ]画面で[ssh サービス]を選択し、[オプション]を開きます。

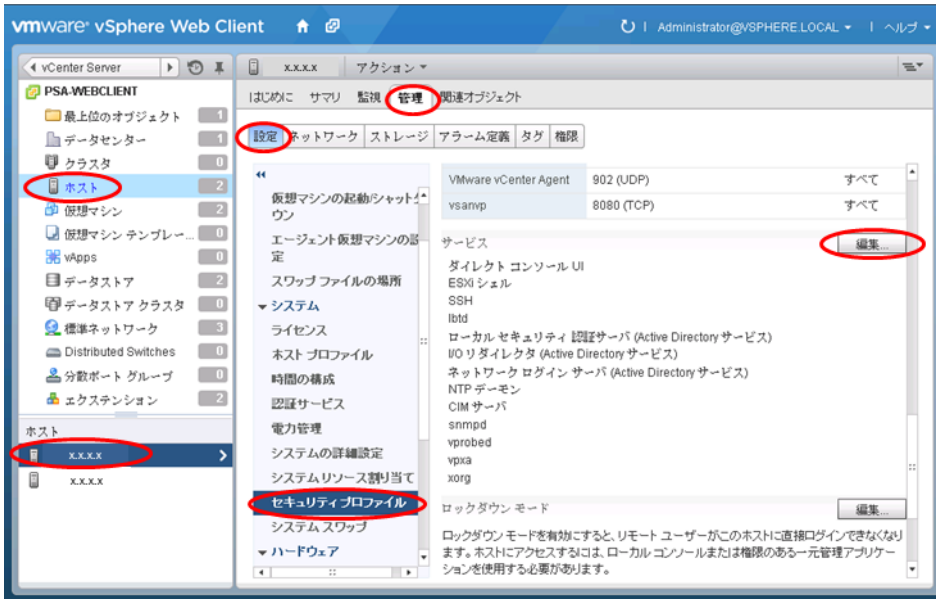
   以下のように[サービスコマンド]で[停止]をクリックした後、[OK]をクリックします。



4. [SSH サーバ]のチェックが外れ、[デーモン]が停止になっていることを確認してください。

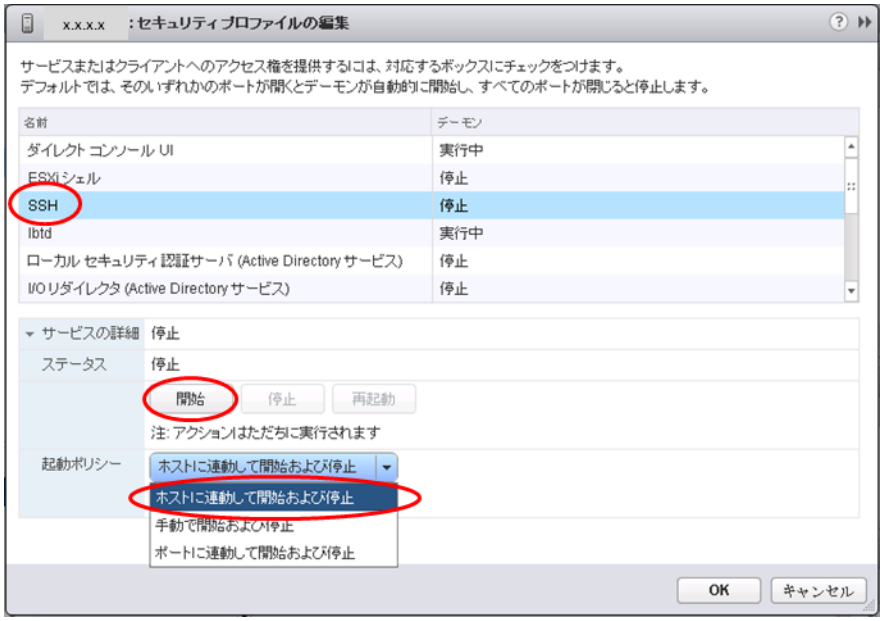
2.4.10.3.2. VMware vSphere Web Client の場合

1. VMware vShpere Web Client を起動します。
2. [ホスト] → [対象ホスト名] から、[管理] タブをクリックします。
3. 管理画面表示後、[設定]タブから [セキュリティプロファイル] をクリックします。
4. [セキュリティプロファイル] 情報が表示され、サービスの[編集] をクリックします。

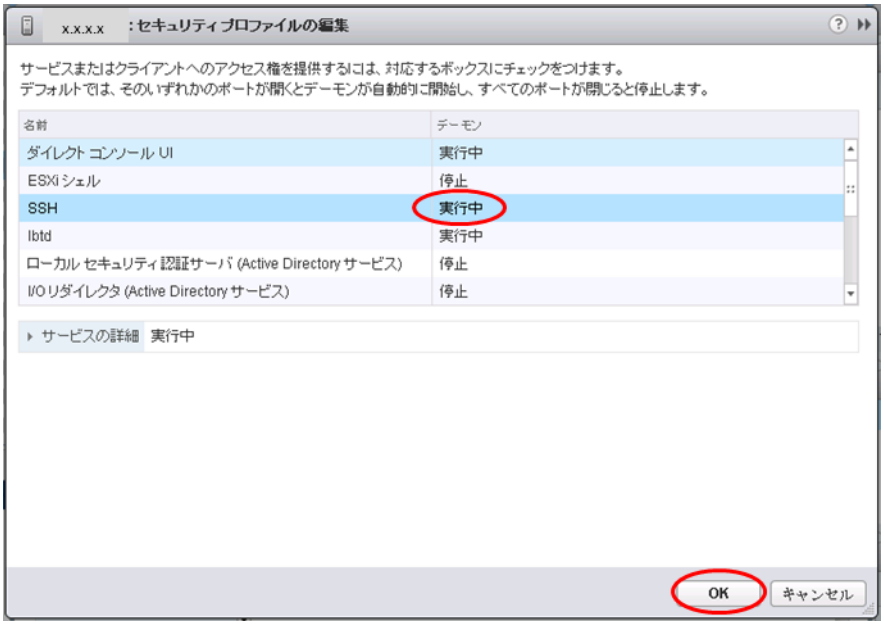


5. [SSH]を選択し、[開始]ボタンをクリックします。

6. 次に[起動ポリシー]の[ホストに連動して開始および停止]を選択します。



7. [SSH]の[デーモン]が実行中になっていることを確認して[OK]をクリックします。



8. 仮想マシンへログインし、コマンドプロンプトで以下のディレクトリへ移動します

```
# cd <SVmcovm のインストールパス>opt¥fujitsu¥SVmco¥bin
```

9. コマンドプロンプトを管理者権限で起動させ、コマンドを以下のオプションを付けて実行します。

対話形式で ESXi の IP,ログイン ID,とパスワードを入力します。

```
# setuserinfo.exe  -i
```

設定する IP アドレスは、ESXi へアクセスするための IP アドレスです。

ネットワークの構成によって設定値が異なります。

1. ネットワーク構成例 1 の場合：

   2.4.2.5.2 章の手順 10 で設定した ESXi からの情報取得用 IP アドレスを設定します。

2. ネットワーク構成例 2 の場合：

   管理ネットワークの ESXi に割り当てた IP アドレスを設定します。

10. 実行後、以下のオプションを付けて実行し、2.で入力した値のチェックを行います。

```
# setuserinfo.exe  –c
Successful execution of the command.
```

上記のメッセージが出力されれば設定終了です。

運用条件などにより、ssh 接続が出来ない場合は、手動にて ESXi から PCI カード情報を取得し、仮想マシンの指定の場所に配置後に SVmcovm の再起動が必要です。

また、SSH 接続を許可しない環境において PCI カードの追加/交換があった場合も、本手順の実施が必要です。

尚、SSH 接続設定を実施しない場合は、以下の監視上の制約が発生します。

1. SVmcovm 起動前の PCI カード/ディスクの故障検出が出来ない

   ※SVmcovm 起動後は監視可能
2. MMB の PCI レーン縮退監視が出来ない
3. システムステータスが OS Running/OS Shutdown に変更されない。

以下に手順を示します。

1. SSH で ESXi へログインし、以下のコマンドを実行します。

・ PCI カード情報取得コマンド

```
# /sbin/esxcli hardware pci list > pcicardinfo
```

・ NIC 情報取得コマンド

```
# /sbin/esxcfg-nics -l > nicinfo
```

5. 実行結果 (例)

・ pcicardinfo

```
000:000:19.0
   Address: 000:000:19.0
   Segment: 0x0000
   Bus: 0x00
   Slot: 0x19
   Function: 0x00
   VMkernel Name: vmnic0
   Vendor Name: Intel Corporation
   Device Name: 82567LF-2 Gigabit Network Connection
   Configured Owner: Unknown
   Current Owner: VMkernel
   Vendor ID: 0x8086
   Device ID: 0x10cd
   SubVendor ID: 0x10cf
   SubDevice ID: 0x159b
   Device Class: 0x0200
 .
 .
```

・ nicinfo

```
Name    PCI          Driver      Link Speed     Duplex MAC Address       MTU    Description
vmnic0  0000:00:19.00 e1000e     Up   100Mbps   Full   00:17:42:de:7c:4b 1500   Intel Corporation 82567LF-2 Gigabit Network Connection
vmnic1  0000:05:00.00 igb        Up   100Mbps   Full   00:17:42:9b:dc:b4 1500   Intel Corporation 82576 Gigabit Network Connection
vmnic2  0000:05:00.01 igb        Down 0Mbps     Half   00:17:42:9b:dc:b5 1500   Intel Corporation 82576 Gigabit Network Connection
vmnic3  0000:06:00.00 igb        Down 0Mbps     Half   00:17:42:9b:dc:b6 1500   Intel Corporation 82576 Gigabit Network Connection
vmnic4  0000:06:00.01 igb        Down 0Mbps     Half   00:17:42:9b:dc:b7 1500   Intel Corporation 82576 Gigabit Network Connection
vmnic5  0000:0e:00.00 e1000e     Down 0Mbps     Half   00:15:17:7d:d4:e2 1500   Intel Corporation 82571EB Gigabit Ethernet Controller
vmnic6  0000:0e:00.01 e1000e     Down 0Mbps     Half   00:15:17:7d:d4:e3 1500   Intel Corporation 82571EB Gigabit Ethernet Controller
```

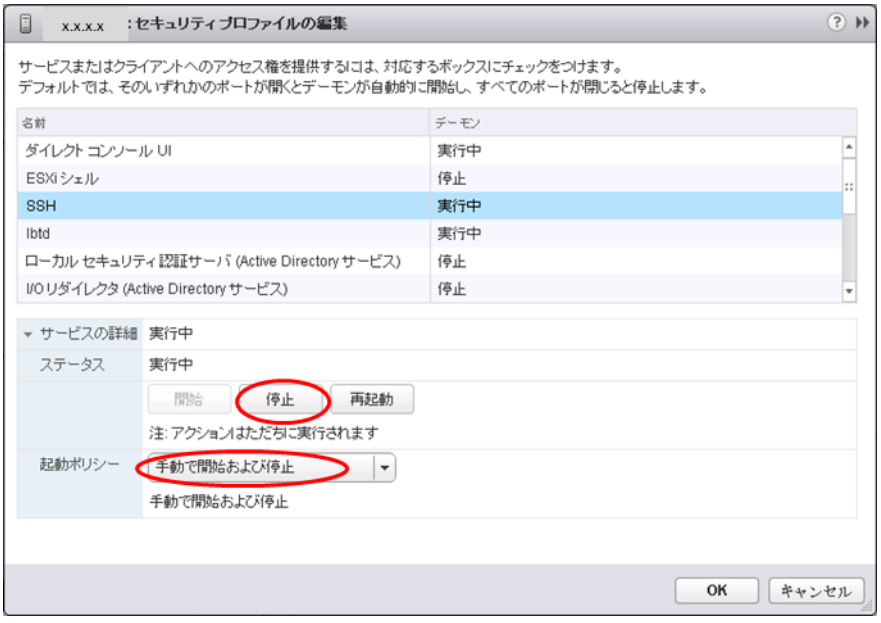
2. 作成した二つのファイル(pcicardinfo,nicinfo)を **SVmcovm をインストール予定の仮想マシンの以下のディレクトリにコピー**します。

```
<SVmcovm のインストールパス>¥etc¥fujitsu¥SVmco¥usr
```

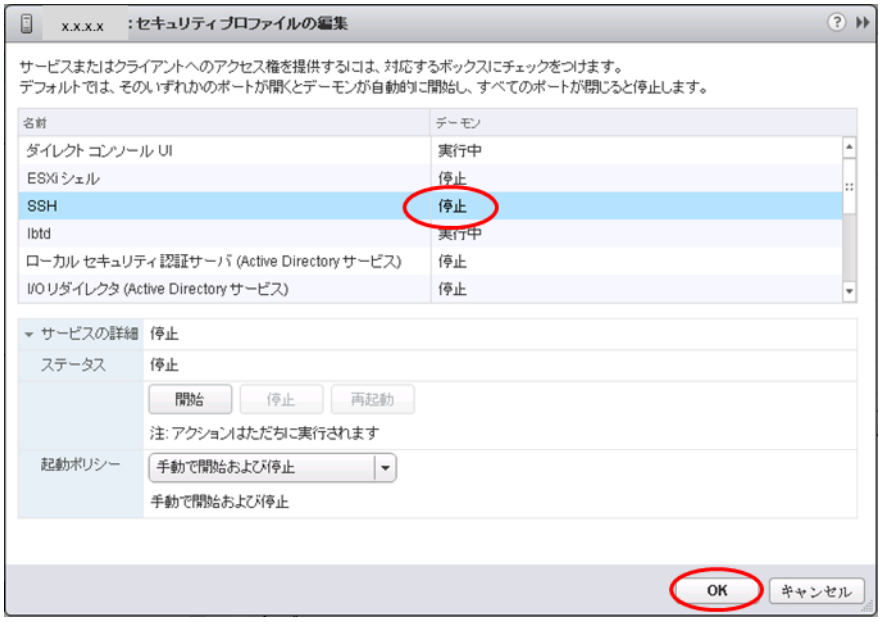
コピーが完了したら、以下の方法で ESXi への ssh 接続出来ないように設定を元に戻します。

3. 確認後、SSH のサービスを停止させます。SSH を起動させた時のように、VMware vSphere Web Client を起動させて、[ホスト] → [対象ホストの IP アドレス] から、[管理] タブをクリックし、管理画面表示後、[設定]タブから [セキュリティプロファイル] をクリックし、[セキュリティプロファイル] 情報が表示され、サービスの[編集] をクリックします。

4. [SSH]を選択し、[停止]をクリックします。



5. [SSH]の[デーモン]が停止になっていることを確認して[OK]をクリックします。



2.4.10.4　仮想マシンへのログ転送の設定(ログ受信側)

Windows には二つのログ転送方式があり、設定により選択可能です。

- VMware 提供の”Syslog Collector”使用 (vCenter ライセンス購入が必要)
- SSH 経由のファイル転送 (SVmcovm が実施)

■ **VMware vCenter Server 5.x の場合：**

以下の条件を満たしている場合は、Syslog Collector の使用を推奨します。

1. vCenter のライセンスを購入していること。

2. システムが vCenter Server のハードウェアおよびソフトウェア要件を満たしていること。

※要件に関しては、vSphere Installation and Setup Guide のシステム要件を参照して下さい。

上記の 1,2 を満たしている場合は、

2.4.10.4.1 ログ転送設定 1(Syslog Collector が使用出来る場合)へ

vCenter のライセンスが無い、または要件を満たしていない場合、

2.4.10.4.2 ログ転送設定 2(syslog collector を使わない場合)の設定を行って下さい。

■ **VMware vCenter Server 6.x の場合：**

vCenter Server がインストールされている環境の場合は 2.4.10.4.1 ログ転送設定 1(Syslog Collector が使用出来る場合) の設定を行って下さい。

vCenter Server がインストールされていない環境では 2.4.10.4.2 ログ転送設定 2(syslog collector を使わない場合)の設定を行って下さい。

※VMware vCenter Server6.x の場合、vCenter Server がインストールされていない環境に Syslog Collector を単独でインストールすることができない為。

2.4.10.4.1　ログ転送設定 1(Syslog Collector が使用出来る場合)

ログ転送に Syslog Collector を使用する場合の設定方法を示します。

Syslog Collector は vCenter とは別に単独でインストールが可能です。

2.4.10.4.1.1.　Syslog Collector のインストール

Syslog Collector のインストール方法は、VMware vCenter Server 5.x と VMware vCenter Server 6.x で異なります。

VMware vCenter Server 5.x の場合は、「VMware vCenter Server 5.x の場合」に従い、VMware vCenter インストーラから Syslog Collector をインストールしてください。

VMware vCenter Server 6.x の場合は、「VMware vCenter Server 6.x の場合」を行ってください。VMware vCenter Server6.x をインストールすると、Syslog Collector もインストールされます。Syslog Collector のみのインストールはできません。インストール手順については、VMware 社のサイトを確認してください。

【注意】

VMware vCenter Server5.x から VMware vCenter Server6.x へアップデートを行う場合の注意事項です。

・VMware vCenter Server5.x から VMware vCenter Server6.x へアップデートを行う場合は Syslog Collector をアンインストールしてから実施してください。

・vCenter Server がインストールされていないかつ ESXi6.x 環境でログ転送に Syslog Collector を使用している場合、Syslog Collector をアンインストールしてから 2.4.10.4.2 ログ転送設定 2(syslog collector を使わない場合)を実施してください。

2.4.10.4.1.1.1. VMware vCenter Server 5.x の場合

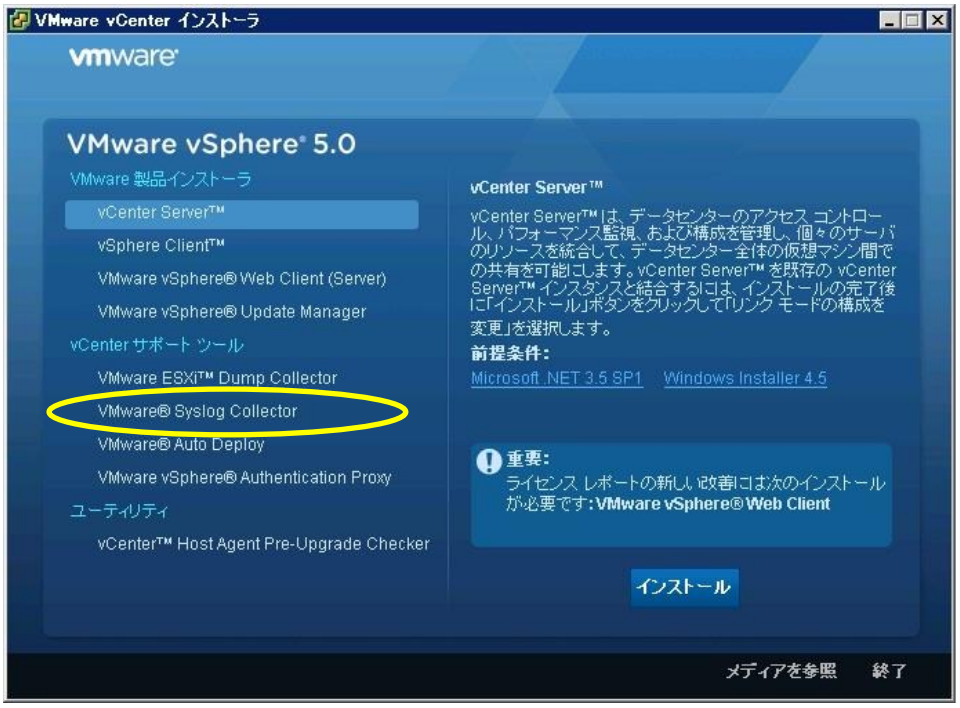
1. Syslog Collector は、vCenter のインストーラに含まれています。

   vCenter インストーラを VMware 社のサイトからダウンロードして下さい。

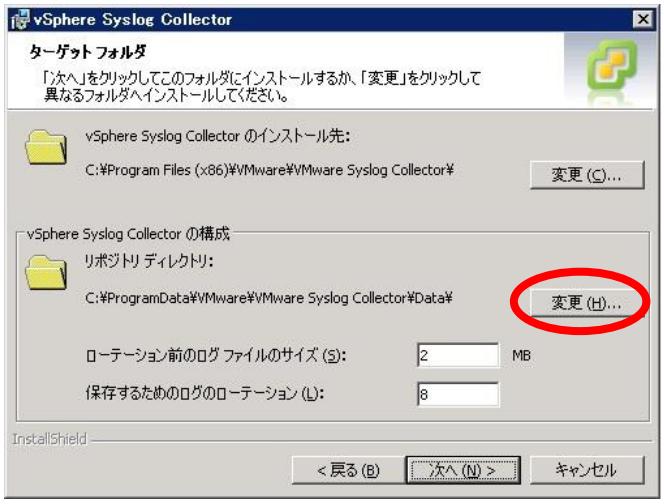
   ※ダウンロードには、vCenter のライセンス購入が必要です。

2. 仮想マシン上で、vCenter のインストーラの展開し、インストーラを実行します。

3. 以下の画面から、”VMware Syslog Collector”を選択します。



4. ターゲットフォルダの vSphere Syslog Collector の構成を編集します。
まず、リポジトリディレクトリを変更します。

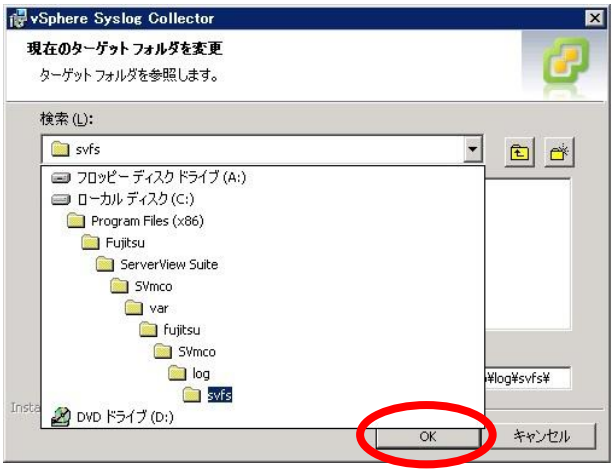


5.　ターゲットディレクトリのパスを以下のように設定して[OK]を押します。

パス：<SVmcovm のインストールディレクトリ>¥var¥fujitsu¥SVmco¥log¥svfs

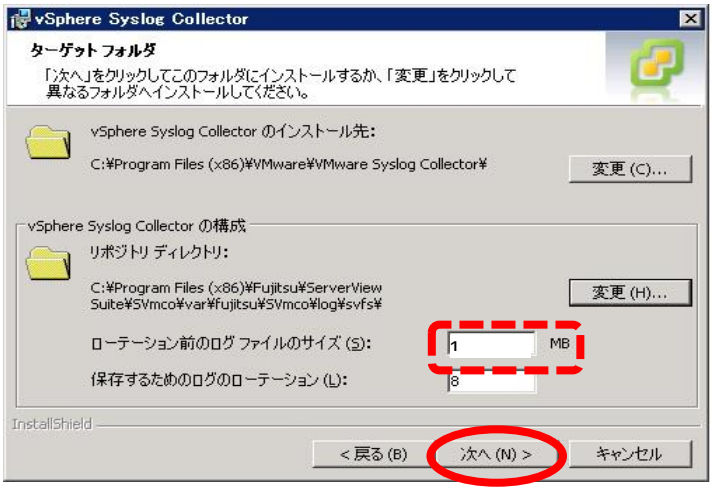
※ターゲットディレクトリのパスはデフォルト値のまま使うことも可能です。

例 SVmcovm が windows2008 x64 環境の C ドライブにインストールされている場合

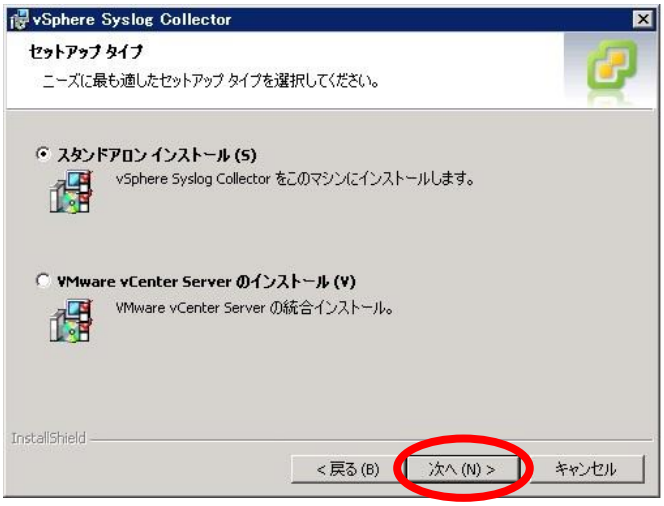


6. 次にローテーション前のログサイズを以下のように設定して[OK]をクリックします。

ローテーション前のログファイルのサイズ： 1MB



7. セットアップタイプは”スタンドアロンインストール”を選択し[次へ]を選択します。



8. ポートの設定はデフォルトのままで、[次へ]を選択します。

9. ID 設定する IP アドレスは、**ネットワークの構成**によって設定値が異なります。

1. **ネットワーク構成例 1 の場合：**

   2.4.2.5.4 章の手順 5 で設定した IP アドレスを設定します。

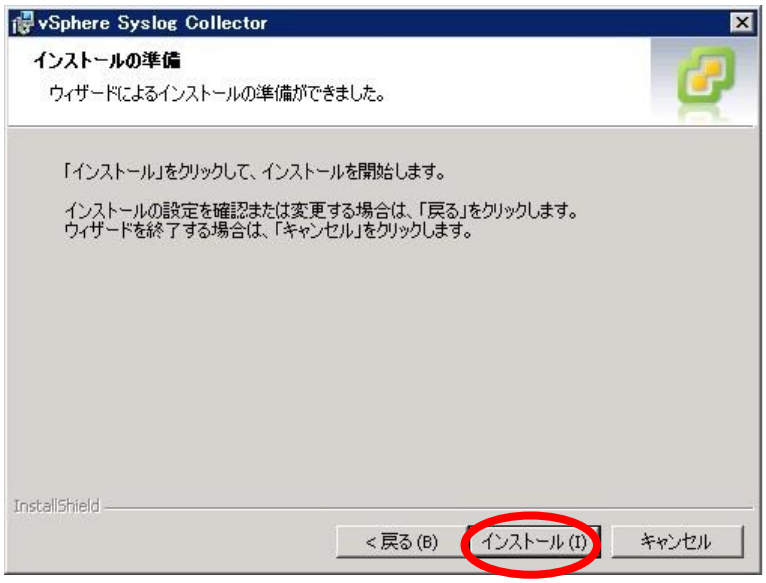
2. **ネットワーク構成例 2 の場合：**

   管理ネットワークの仮想マシンに割り当てた IP

   アドレスを設定します。

画面は、ネットワーク構成例 1 の場合です。

10. [インストール]を選択してインストールは完了です。



Syslog Collector の詳細については、VMware 社が公開している vCenter のインストールガイドを参照して下さい。

11. インストールが完了したら、仮想マシンコンソールなどから仮想 OS にログインし、以下の SVmcovm の設定ファイルを編集します。

パス：

<SVmcovm のインストールディレクトリ>¥etc¥fujitsu¥SVmco¥usr¥getlog.conf

ファイルの NAME パラメータを編集します。フォーマットは以下のようになります。

NAME = **<SVmcovm のインストールパス>**¥var¥fujitsu¥SVmco¥log¥svfs¥**<ログ転送元の ESXi の IP アドレス>**¥syslog.log

※ログ転送元の ESXi の IP アドレス

設定する IP アドレスは、ネットワークの構成によって設定値が異なります。

1. ネットワーク構成例 1 の場合：

   2.4.2.5.1 章の手順 8 または 2.4.2.5.2 章の手順 10 で設定した IP アドレスを設定します。

2. ネットワーク構成例 2 の場合：

   管理ネットワークの ESXi に割り当てた IP

   アドレスを設定します。

※手順 5 でリポジトリディレクトリを推奨の (/var/fujitsu/SVmco/log/svfs)以外に設定した場合は、フォーマットは以下のようになります。

NAME = <リポジトリディレクトリのパス> <ログ転送元の ESXi の IP アドレス>\syslog.log

例)リポジトリディレクトリが”C:ProgramData\VMware\VMware Syslog Collector\Data\”(デフォルト設定)でログ転送元の IP が 192.168.1.10 の場合

NAME = C:ProgramData¥VMware¥VMware Syslog Collector¥Data¥ 192.168.1.10¥syslog.log

例)　ESXI の IP が 192.168.1.10 で、SVmcovm が C:¥Program Files (x86)¥Fujitsu¥ServerView Suite¥SVmco にインストールされている場合。

※TIME パラメータは 60 秒が推奨値です。

◆設定前

```
[SYSLOG]
OPTION=0

[INTERVAL]
TIME=60

[FILE]
NAME= C:¥Program Files (x86)¥Fujitsu¥ServerView Suite¥SVmco¥var¥fujitsu¥SVmco¥log¥svfs¥255.255.255.255¥syslog.log
```

設定後

```
[SYSLOG]
OPTION=0

[INTERVAL]
TIME=60

[FILE]
NAME=C:¥Program Files (x86)¥Fujitsu¥ServerView Suite¥SVmco¥var¥fujitsu¥SVmco¥log¥svfs¥192.168.1.10¥syslog.log
```

2.4.10.4.1.1.2. VMware vCenter Server 6.x の場合

1. VMware vCenter Server6.x をインストールします。

   インストール手順については、VMware 社のサイトを確認してください。

2. [サービス] で [VMware vSphere Syslog Collector]サービス（*）を停止します。

   *: ESXi の版数により、[VMware Syslog コレクター] など、サービスの名前表記が異なる場合があります。

3. 以下のファイルで、Syslog Collector の設定の確認または修正を行います。

   %PROGRAMDATA%\VMware\vCenterServer\cfg\vmsyslogcollector\config.xml

   ※リポジトリディレクトリ以外は修正必須項目です。

   修正の詳細については、以下の URL を参照してください。

   http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2021652

No.	項目	意味
1	<defaultDataPath>xxxxx</defaultDataPath>	リポジトリディレクトリ（ログ保存先のパス）
2	<serviceAddress>x.x.x.x</serviceAddress>	vSphere Syslog Collector の識別名（IP アドレス）
3	<maxSize>2</maxSize>	ローテーション前のログファイルのサイズ
4	<hostnamePosition>1</hostnamePosition>	ホストの識別

1. <defaultDataPath>xxxxx</defaultDataPath>を以下のように設定します。

```
<defaultDataPath><SVmcovm のインストールディレクトリ
>\var\fujitsu\SVmco\log\svfs\ </defaultDataPath>
```

デフォルトの SVmcovm のインストールディレクトリ

C:\Program Files (x86)\Fujitsu\ServerView Suite\SVmco

※ターゲットディレクトリのパスはデフォルト値のまま使うことも可能です。

2. <serviceAddress>x.x.x.x</serviceAddress>を以下のように設定します。

IP アドレスは、**ネットワークの構成**によって設定値が異なります。

1. **ネットワーク構成例 1 の場合：**
   2.4.2.5.4 章の手順 5 で設定した IP アドレスを設定します。
2. **ネットワーク構成例 2 の場合：**
   管理ネットワークの仮想マシンに割り当てた IP
   アドレスを設定します。

下記は、ネットワーク構成例 1 の場合です。

```
<serviceAddress>192.168.1.20</serviceAddress>
```

3. <maxSize>2</maxSize>を以下のように設定します。

ローテーション前のログファイルのサイズ： 1MB

```
<maxSize>1</maxSize>
```

4. <hostnamePosition>1</hostnamePosition>を以下のように設定します。

IP アドレスで識別する： 0

```
<hostnamePosition>0</hostnamePosition>
```

4. [サービス] で [VMware vSphere Syslog Collector]サービス（*）を開始します。

   *: ESXi の版数により、[VMware Syslog コレクター] など、サービスの名前表記が異なる場合があります。

5. 仮想マシンコンソールなどから仮想 OS にログインし、以下の SVmcovm の設定ファイルを編集します。

パス：

<SVmcovm のインストールディレクトリ>¥etc¥fujitsu¥SVmco¥usr¥getlog.conf

ファイルの NAME パラメータを編集します。フォーマットは以下のようになります。

NAME = **<SVmcovm のインストールパス>**¥var¥fujitsu¥SVmco¥log¥svfs¥**<ログ転送元の ESXi の IP アドレス>**¥syslog.log

※ログ転送元の ESXi の IP アドレス

設定する IP アドレスは、ネットワークの構成によって設定値が異なります。

1. ネットワーク構成例 1 の場合：

   2.4.2.5.1 章の手順 8 または 2.4.2.5.2 章の手順 10 で設定した IP アドレスを設定します。

2. ネットワーク構成例 2 の場合：

   管理ネットワークの ESXi に割り当てた IP

   アドレスを設定します。

※手順 3 でリポジトリディレクトリを推奨の (/var/fujitsu/SVmco/log/svfs)以外に設定した場合は、フォーマットは以下のようになります。

```
NAME = <リポジトリディレクトリのパス> <ログ転送元の ESXi の IP アドレス>\syslog.log
```

例)リポジトリディレクトリが”C:\ProgramData\VMware\vCenterServer\data\vmsyslogcollector\”(デフォルト設定)でログ転送元の IP が 192.168.1.10 の場合

```
NAME = C:¥ProgramData¥VMware¥vCenterServer¥data¥vmsyslogcollector¥192.168.1.10¥syslog.log
```

例)　ESXI の IP が 192.168.1.10 で、SVmcovm が C:¥Program Files (x86)¥Fujitsu¥ServerView Suite¥SVmco にインストールされている場合。

※TIME パラメータは 60 秒が推奨値です。

◆設定前

```
[SYSLOG]
OPTION=0

[INTERVAL]
TIME=60

[FILE]
NAME= C:¥Program Files (x86)¥Fujitsu¥ServerView
Suite¥SVmco¥var¥fujitsu¥SVmco¥log¥svfs¥255.255.255.255¥syslog.log
```

◆設定後

```
[SYSLOG]
OPTION=0

[INTERVAL]
TIME=60

[FILE]
NAME=C:¥Program Files (x86)¥Fujitsu¥ServerView
Suite¥SVmco¥var¥fujitsu¥SVmco¥log¥svfs¥192.168.1.10¥syslog.log
```

2.4.10.4.1.2. ログ転送のためのファイアウォールの設定

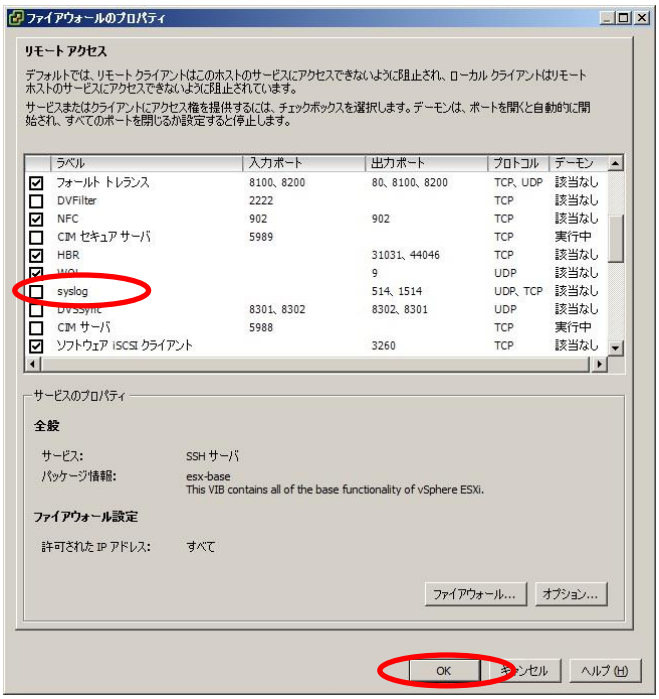
ログ転送のためにファイアウォールの設定を行います。

2.4.10.4.1.2.1. VMware vSphere Client の場合

1. vClient から対象の ESXi の[構成]画面を開き、ソフトウェアの[セキュリティプロファイル]を選ぶとサービスとファイアウォールの情報が表示されます。

   ここでは、ファイアウォールの[プロパティ]を選択します。

2. ラベルから”syslog”を選び、[OK]を選択します。

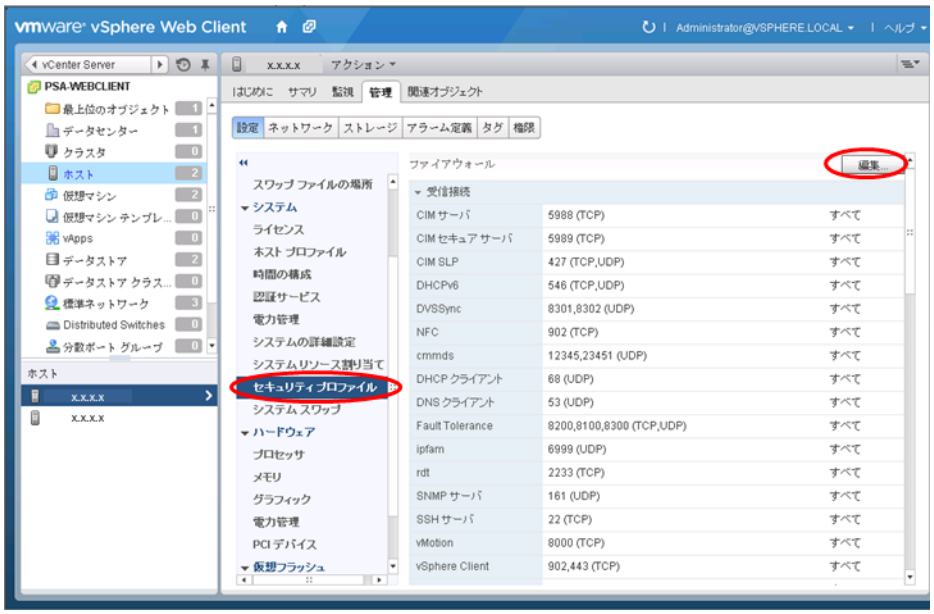


3. ファイアウォールの”発信接続”に”syslog”が存在することを確認して下さい。

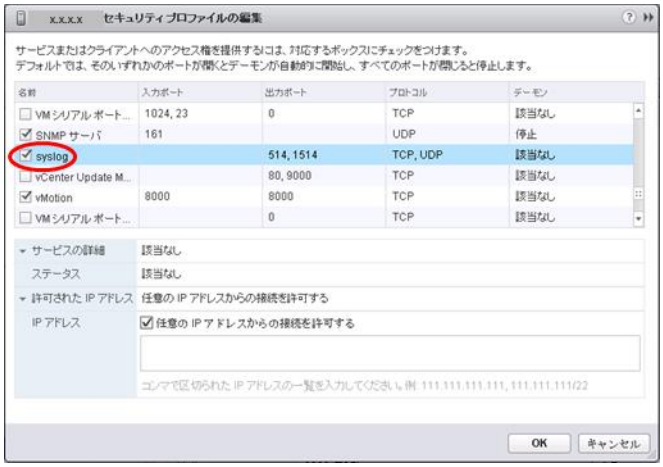
2.4.10.4.1.2.2. VMware vSphere Web Client の場合

1. 対象ホストの[管理]タブの[設定]画面を開き、 [セキュリティプロファイル]を選ぶとサービスとファイアウォールの情報が表示されます。

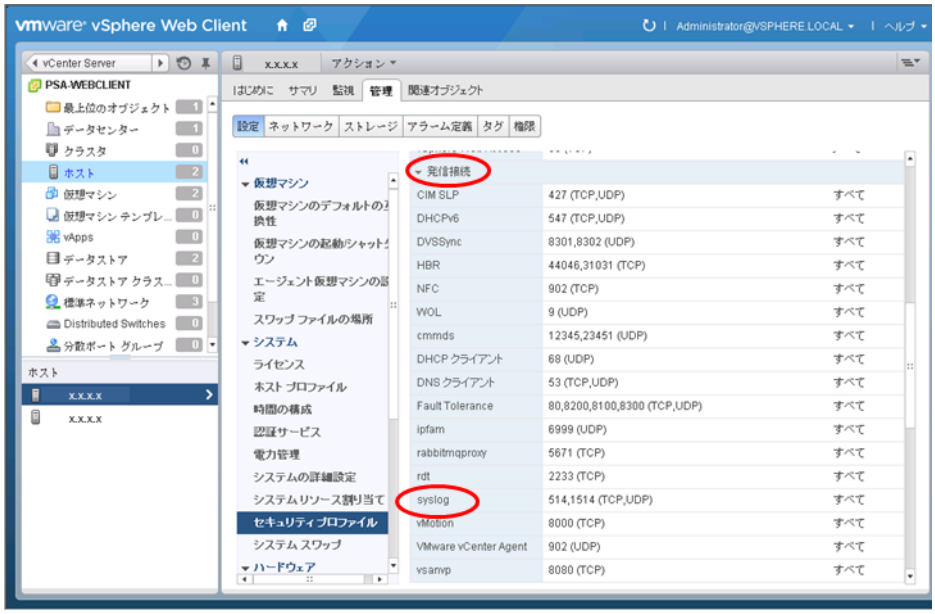
   ファイアウォールの[編集]を選択します。



2. 名前から”syslog”をチェックし、[OK]を選択します。



3. ファイアウォールの”発信接続”に”syslog”が存在することを確認して下さい。



2.4.10.4.2　ログ転送設定 2(Syslog Collector を使わない場合)

ログ転送に Syslog Collector を使用しない場合の設定を示します。

1. 仮想マシンコンソールなどから仮想 OS にログインし、以下の SVmcovm の設定ファイルを編集します。

パス：

<SVmcovm のインストールディレクトリ>/etc/fujitsu/SVmco/usr/getlog.conf

ファイルの OPTION パラメータを編集します。

例)　ESXI の IP が 192.168.1.10 で、SVmcovm が C:\Program Files (x86)\Fujitsu\ServerView Suite\SVmco にインストールされている場合。

◆設定前

```
[SYSLOG]
OPTION=0
```

◆設定後

```
[SYSLOG]
OPTION=1
```

以上で仮想マシンへのログ転送設定は終了です。

2.4.10.5 仮想マシンへのログ転送の設定(ログ送信側)

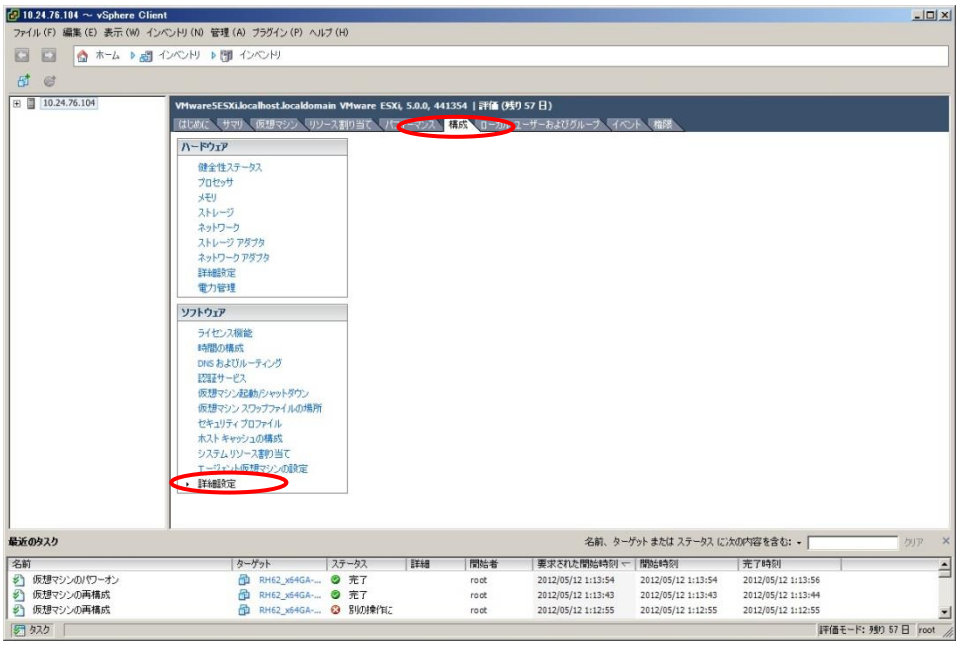
ログ送信側の仮想マシンへのログ転送の設定をおこないます。

仮想マシンへのログ転送の設定(ログ受信側)で設定した内容によって手順が異なります。

2.4.10.5.1　Syslog Collector を使用している場合

2.4.10.5.1.1.　VMware vSphere Client の場合

1. VClient を立ち上げて、[構成]のタブのソフトウェアの項目の[詳細設定]を選択します。



2. [syslog]の項目の[global]を選択し、Syslog.global.logHost に転送先(管理用仮想OS)の IP アドレスを入力して OK を押します。

   設定する IP アドレスはネットワークの構成によって異なります。

1. ネットワーク構成例 1 の場合：

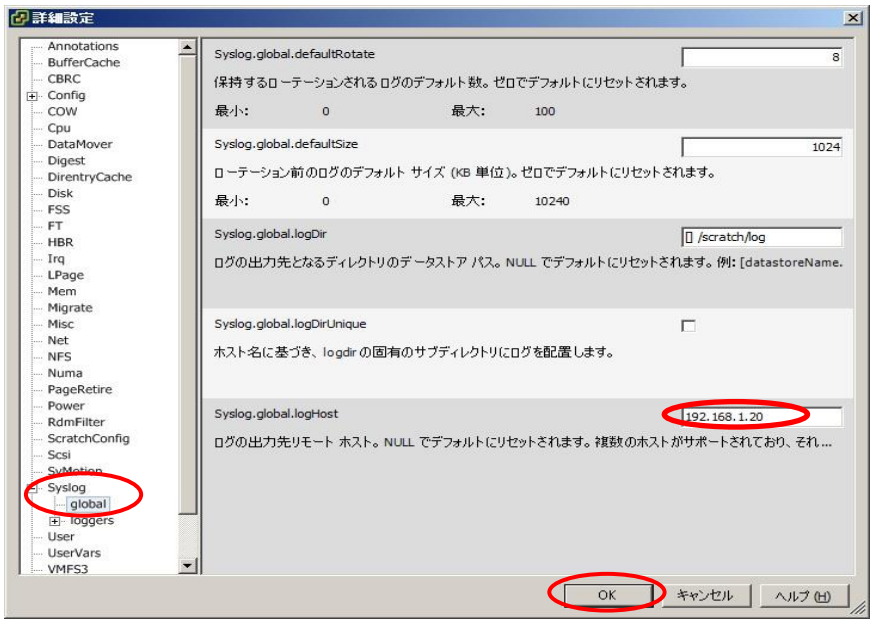
   2.4.2.5.4 章の手順 5 で仮想マシンに設定した ESXi 通信用 IP アドレスを設定します。

2. ネットワーク構成例 2 の場合：

   管理ネットワークの仮想マシンに割り当てた IP

   アドレスを設定します。

例)ネットワーク構成が 1 の場合



3. 仮想 OS にログインし、数分後、Syslog Collector のインストールの手順 6 で設定したリポジトリディレクトリにログが転送されている(syslog.log が存在し、ファイルの更新日時が更新されている)ことを確認して下さい。

※転送されない場合は、以下の手順を実施してからログが転送されているか確認します。

1. SSH などで ESXi にログイン
2. 以下のコマンドを実施

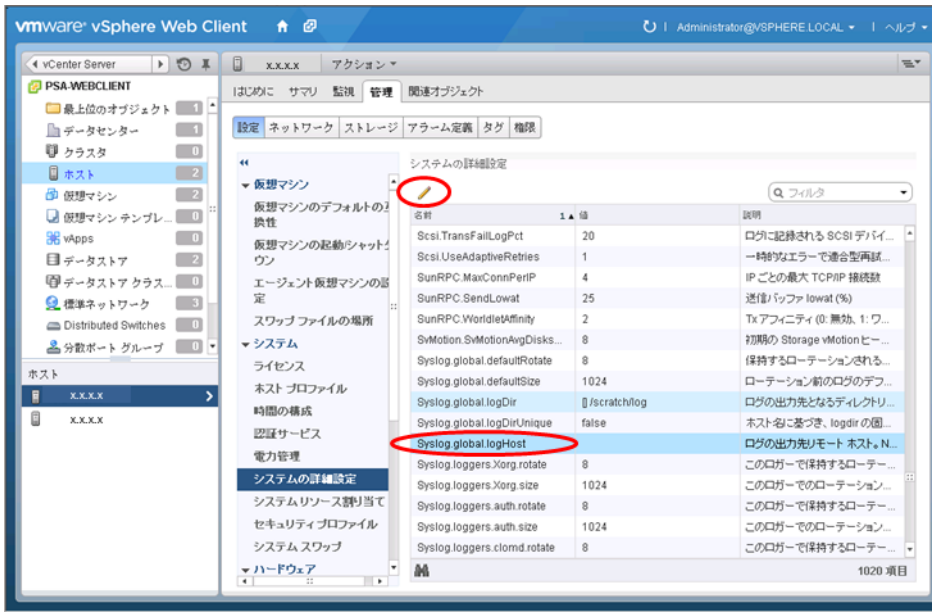
```
# esxcli system syslog reload
```

ファイルが更新されない場合は、再度設定を見直して下さい。

2.4.10.5.1.2. VMware vSphere Web Client の場合

■ 対象ホストの[管理]タブの[設定]画面を開き、 [システムの詳細設定]クリックします。

■ [Syslog.global.logHost]を選択し、[編集]アイコンをクリックします。



設定する IP アドレスはネットワークの構成によって異なります。

1. ネットワーク構成例 1 の場合：

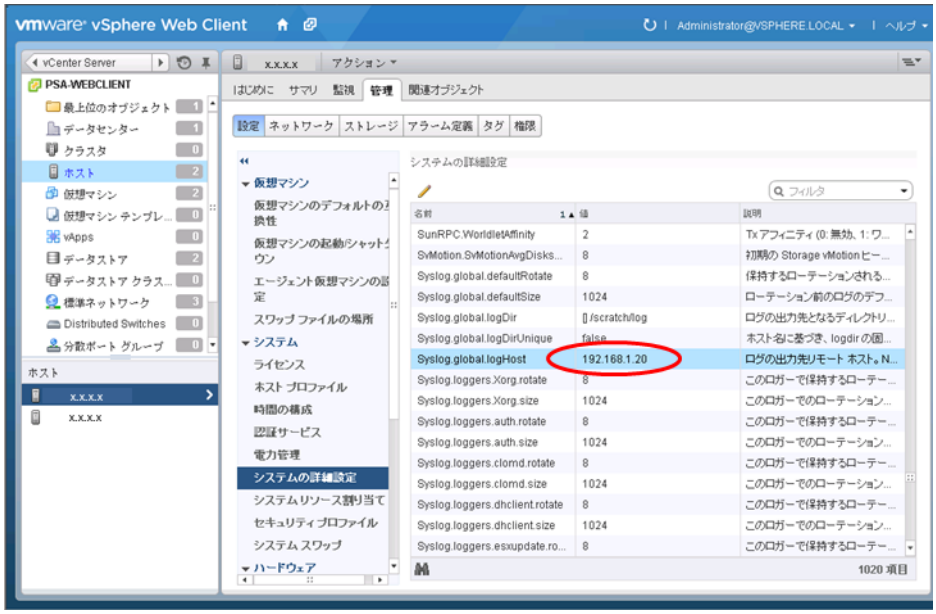
   2.4.2.5.4 章の手順 5 で仮想マシンに設定した ESXi 通信用 IP アドレスを設定します。

2. ネットワーク構成例 2 の場合：

   管理ネットワークの仮想マシンに割り当てた IP

   アドレスを設定します。

例）ネットワーク構成が 1 の場合



3. 仮想 OS にログインし、数分後、Syslog Collector のインストールの手順 6 で設定したリポジトリディレクトリにログが転送されている(syslog.log が存在し、ファイルの更新日時が更新されている)ことを確認して下さい。

※転送されない場合は、以下の手順を実施してからログが転送されているか確認します。

1. SSH などで ESXi にログイン
2. 以下のコマンドを実施

```
# esxcli system syslog reload
```

ファイルが更新されない場合は、再度設定を見直して下さい。

2.4.10.5.2　Syslog Collector を使用しない場合

ログが転送されているか確認するためには、SVmcovm を起動しなければ確認出来ません。

残りのインストール後の設定が完了した上で、仮想マシンの再起動後に確認します。

2.4.10.6 MMB 経由の Trap 送信の設定

MMB 経由で送信する Trap の設定を行います。

MMB 経由の Trap の送信先は MMB Web-UI で設定した宛先となります。

設定については、『PRIME QUEST1000 シリーズ 導入マニュアル』の”SNMP の設定”の章を参照して下さい。

Trap 通知には以下の情報を設定する必要があります。

・パーティションの名前

パーティションに割り振られた名前です。

詳細は、『PRIME QUEST1000 シリーズ 導入マニュアル』の”パーティション名の設定”の章を参照して下さい。

・MMB の仮想 IP アドレス

MMB Web-UI にアクセスするための仮想 IP アドレスです。

詳細は、『PRIME QUEST1000 シリーズ 導入マニュアル』の”MMB のネットワーク設定”の章を参照して下さい。

備考：

運用管理ソフトウェア(Systemwalker など)がパーティションを管理する場合には、本設定が必要です。

2. 仮想マシン上の以下の設定ファイルを開きます。

ファイル格納場所：

[SVmcovm インストール先フォルダ]

¥etc¥fujitsu¥SVmco¥usr¥svmcovmtrap.conf

Trap 送信に必要な情報のパラメータは以下のようになります。

- **TRAP_SET:**

説明：MMB 経由の Trap 通報の有無

設定値：1:Trap 通報あり, 0:Trap 通報無し (デフォルト”1”)

- **Partition_Name**

説明：パーティション名を設定値

設定値：0～63 文字 (デフォルト 空)

- **MMB_V_IP**

説明：MMB の仮想 IP アドレスを設定値

設定値：0.0.0.0 ～255.255.255.255(デフォルト 255.255.255.255)

以下に例を示します。

Trap 通報有りで、パーティション名が”Test Machine”で、MMB の仮想 IP アドレスが”192.168.40.1”の時

・設定前

```
[TRAP]
TRAP_SET=1

Partition_Name =

MMB_V_IP=255.255.255.255
```

・設定後(例)

```
[TRAP]
TRAP_SET=1

Partition_Name=Test Machine

MMB_V_IP=192.168.40.1
```

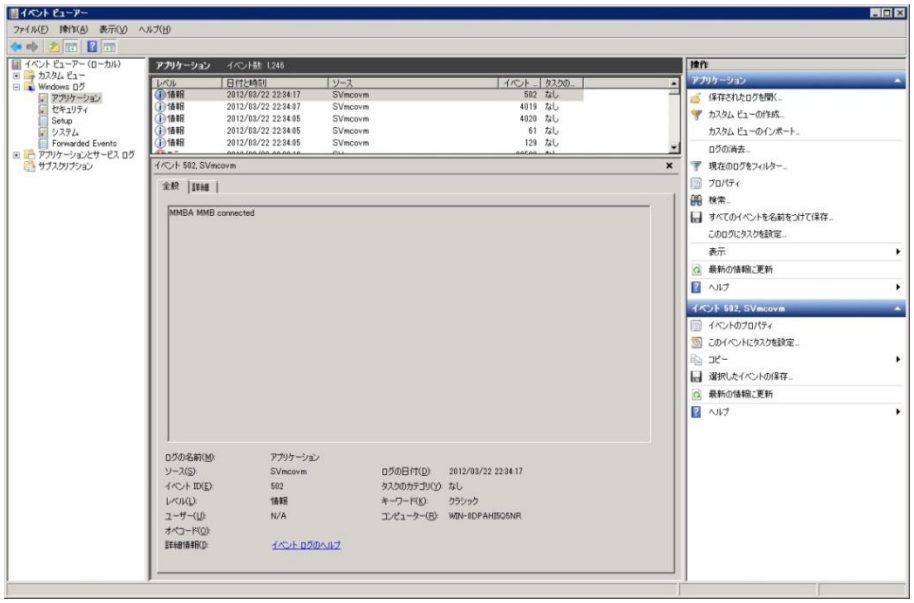
以上で設定は終了です。

2.4.11 仮想マシンの再起動

SVmcovm のインストール後の設定後、仮想マシンを再起動します。

・OS 起動後の確認

1. イベントビュアーに以下のメッセージが出力され、SVmcovm のソース名でその他に異常なメッセージが無い事を確認します。



2. 仮想 OS にログが転送されいるか確認します。

   確認方法は、仮想マシンへのログ転送の設定(ログ受信側)で設定した内容によって異なります。

◆ Syslog Collector を使用している場合

仮想 OS にログインし、数分後、[2.4.10.4.1.1 Syslog Collector のインストールの手順 5]で設定したリポジトリディレクトリにログが転送されている(syslog.log が存在し、ファイルの更新日時が更新されている)ことを確認して下さい。

転送されない場合は、以下の手順を実施してからログが転送されているか確認します。

1. SSH などで ESXi にログイン
2. 以下のコマンドを実施

```
# esxcli system syslog reload
```

   ファイルが更新されない場合は、再度設定を見直して下さい。

◆ Syslog Collector を使用していない場合

仮想 OS にログインし、数分後、ログが以下のディレクトリに転送されていることを確認してください。（ログファイル(vmkernel.log)のファイルの更新日時が更新されていること)

パス：

<SVmcovm のインストールディレクトリ>/var/fujitsu/SVmco/log/svfs/vmkernel.log

※転送されない/ファイルが更新されない場合は、再度設定(ESXi へのアクセス情報の設定やログ転送設定 2(Syslog Collector を使わない場合)など)を見直して下さい。

2.4.12 SVmcovm のアップデートインストール

SVmcovm のアップデートインストール手順を説明します。

備考

- インストールされている SVmcovm のバージョンと同じバージョンの修正プログラムの場合、確認メッセージ画面で [OK] ボタンをクリックすると、SVmcovm が一度アンインストールされ、その後再度インストールされます。アンインストールしない場合は、[プログラムの削除] 画面で [キャンセル] ボタンをクリックしてください。

- 修正プログラムの入手については、製品を購入されたさいの販売会社、または担当営業員に問い合わせてください。

- ログ転送に Syslog Collector を使用している場合は、アップデート前に必ず Syslog Collector サービスを停止させて下さい。

  SVmcovm アップデート後に、Syslog Collector を起動させる必要があります。

■ **操作手順**

作業ディレクトリに SVmco vm のアップデートパッケージファイル

（ServerViewMissionCriticalOptionVM_Win.exe）が格納されていることを前提に説明します。

本作業は Administrator 権限で作業を行ってください。

ログ転送に Syslog Collector を使用している場合は、SVmcovm のアップデート前に Syslog Collctor サービスを停止させてください。

1. DVD ドライブに『ServerView Suite DVD2』をセットし、以下のディレクトリから対象のモジュールを任意の場所にコピーします。

   <ドライブ名
   >:\SVSLocalTools\Japanese\SVmcovm\SR_Windows\ ServerViewMissionCriticalOptionVM_Win.exe

2. エクスプローラから作業ディレクトリを開きます。

3. [ServerViewMissionCriticalOptionVM_Win.exe]を選択し、ダブルクリックまたはマウスの右クリックメニューから[開く]で起動します。

4. [アップデート画面]が表示されますので、[次へ(N)]をクリックします。

5. インストールが完了すると[InstallShield Wizard の完了画面]が表示されますので、[完了]ボタンをクリックします。

尚、SVmcovm のアップデート後に、OS の再起動が必要な場合があります。

※SVmcovm1.1 版以前からのアップデートする場合、MMB 経由の Trap 送信の設定を実施して下さい。

OS を再起動する必要がなかった場合、SVmcovm サービスを手動で起動させてください。

また、ログ転送に Syslog Collector を使用している場合は、以下の手順で仮想マシンの Syslog Collector を起動させる必要があります。

1. 仮想マシンの Syslog Collector サービスを起動させます。

2. 仮想 OS にログインし、数分後、Syslog Collector のインストールの手順 6 で設定したリポジトリディレクトリにログが転送されている(syslog.log が存在し、ファイルの更新日時が更新されている)ことを確認して下さい。

   転送されない場合は、以下の手順を実施してからログが転送されているか確認します。

1. SSH などで ESXi にログイン
2. 以下のコマンドを実施

```
# esxcli system syslog reload
```

ファイルが更新されない場合は、再度設定を見直して下さい。

以上で、アップデートの処理は終了です。

2.4.13 SVmcovm のアンインストール

SVmcovm のアンインストール手順を説明します。

備考

SVmcovm をアンインストールすると、[SVmcovm インストール先フォルダ] 配下のファイルはすべて削除されます。必要なファイルはアンインストールする前に退避しておいてください。[SVmcovm インストール先フォルダ] については、環境変数 (SVmco_INSTALLPATH) で確認できます。

■ 操作手順
※ログ転送に Syslog Collector を使用している場合は、Syslog Collector サービスを停止させて下さい。

1. [コントロールパネル] - [プログラムと機能] の順に選択します。

[プログラムと機能] 画面が表示されます。

2. 現在インストールされているプログラムの一覧から [ServerView Mission Critical Option VM] を選択し、[アンインストール] をクリックします。

[インストールの準備] 画面が表示され、削除の確認メッセージが表示されます。

3. [OK] ボタンをクリックします。

→アンインストールが開始されます。

アンインストールが完了すると、アンインストール完了画面が表示されます。

4. [完了] ボタンをクリックします。

2.4.14 VMware SVmcovm 保守情報取得

SVmcovm に関するトラブルが発生した場合、SVmcovm 調査資料収集コマンド (getosvmco) を実行し、さらに ESXi 上に ssh などでログインし、vm-support コマンドを実行します。

1. getosvmco コマンド

```
>[SVmcovm のインストール先フォルダ] /opt/fujitsu/SVmco/sh/getosvmco <ファイル名>
```

コマンド実行後、ファイル名に指定したファイルを収集して下さい。

2. vm-support コマンド

<実施例>

```
# vm-support
```

vm-support コマンド実行後、以下のようなメッセージが出力されますので、対象のファイルを収集して下さい。

```
To see the files collected, run: tar -tzf '/var/tmp/esx-vmware5esxi-xxxx-xx-xx--xx.xx.tgz'
```

備考

VMware ではコアファイルは /var/core 配下に出力され、自動では削除されません。
vm-support コマンド実行後、適宜コアファイルを削除することをお勧めします。

3　SVmco/SVmcovm の CLI

本章では、CLI (Command Line Interface) を使って SVmco/SVMcovm を操作する場合のコマンドについて説明します。

CLI は OS にログインして使用します。

ユーザー権限により使用できないコマンドもあります。SVmco は「3.1. 1　CLI コマンド一覧」を、SVmcovm は「」を参照してください。

3.1　SVmco/SVmcovm の CLI

3.1.1　CLI コマンド一覧

SVmco の CLI コマンドの一覧を示します。

コマンド一覧

No	コマンド名	権限	備考	コマンド		
				Linux	Windows	VMware
1	ディスク操作コマンド	root (Linux) 権限または Admin (Windows) 権限が必要 (*3)	HDD の操作	あり	あり (*1)	なし
2	SVmco 調査資料収集コマンド	root (Linux) 権限または Admin (Windows) 権限が必要 (*3)	SVmco 調査資料の収集	あり	あり	あり

No	コマンド名	権限	備考	コマンド		
				Linux	Windows	VMware
3	SNMP セキュリティ設定コマンド	root (Linux) 権限または Admin (Windows) 権限が必要 (*3)	SNMP パケットを受け付けるホストの設定	なし	あり	なし
4	PCI カード操作コマンド	Admin (Windows) 権限が必要 (*3)	PCI ホットプラグを行う	なし	あり	なし
5	管理 LAN 用インターフェース向けファイアーウォール設定コマンド	root (Linux) 権限	PRIMECLUSTER/PRIMESOFT 連携を行うさいに、管理 LAN 用インターフェースに対するファイアーウォール設定をサポートするコマンド	あり	なし	なし
6	PSA-MMB 通信 LAN 設定コマンド	Admin (Windows) 権限が必要 (*3)	PSA-MMB 通信 LAN のネットワーク設定	なし	あり	なし
7	Iptables 設定ツール	root (Linux) 権限または Admin	SVmco 用 iptables の設定ツール	あり	なし	なし

1： Linux と Windows でサポートするオプションが異なります。

*2：起動：[コントロールパネル] - [管理ツール] - [サービス]の順にクリックし、「PRIMEQUEST Environment Control Service」を起動します。「ServerView Mission Critical Option」と「PRIMEQUEST PEMCommand Service」が順次起動されます。

停止：[コントロールパネル] - [管理ツール] - [サービス]の順にクリックし、「PRIMEQUEST Environment Control Service」、「ServerView Mission Critical Option」、「PRIMEQUEST PEM Command Service」を選択して停止します。

*3：Windows の場合、OS 機能 (アクセス制御機能) により、Admin 権限以外で実行すると終了ステータスが不定になります。

3.1.2 ディスク操作コマンド (diskctrl)

diskctrl コマンドは、指定されたオプションに従って、HDD の一覧表示、HDD のディスク回転停止、HDD 搭載位置を示すロケーション LED を点灯／消灯します。

備考

- 本コマンドは、Linux と Windows でサポートするオプションが異なります。
- 本コマンドの実行には、root (Linux) 権限または Admin (Windows) 権限が必要です。Windows の場合、OS 機能 (アクセス制御機能) により、Admin 権限以外で実行すると終了ステータスが不定になります。
- 予防交換などにより HDD の電源を切断する場合、以下の操作をする必要があります。
  - GDS でミラーリングをしている場合は、先に切り離してください。
  - GDS でミラーリングをしていない場合は、アンマウントしてください。

注意

- 本コマンドの操作手順について詳しくは「4. ハードディスクの活性交換」を参照してください。
- RAID 装置は操作対象外です。
- VMware ではハードディスクの活性交換をサポートしていません。
- 本コマンドでハードディスクを交換する場合、ディスク実装操作のとき、以下のメッセージが表示されることがあります。このメッセージが表示されても、動作上の問題はありません。

```
kernel: mptscsih: ioc0: >>  Attempting bus reset! \
(sc=e000004082adc480)
kernel: mptbase: ioc0: IOCStatus(0x0048):  SCSI \
```

```
Task Terminated
```

¥：改行しないことを表す。

- ハードディスクを挿入後、誤って挿入したためにディスクを回転停止させる場合は、ディスク挿入後 60 秒程度の時間を空けてからディスクの回転停止操作をしてください。ディスク挿入操作により OS の HotPlug 処理が動作するため、挿入後すぐにディスクの停止操作をすると、以下のようなエラーメッセージが表示される場合があります。

```
kernel: Device sdb not ready.
kernel: end_request: I/O error, dev sdb,  sector 204706
kernel: Buffer I/O error on device sdb1,  logical block 6396
```

- ディスク操作コマンドを同時に複数実行すると、異常終了する場合があります。実行中のディスク操作コマンドがないことを確認してから実行してください。

(1)入力形式

- Linux の場合

```
/opt/fujitsu/SVmco/bin/diskctrl {-l|-e|-i|-o|-c} {Devicename| iocx/slotno}
```

- Windows の場合

```
diskctrl {-l|-i|-o} {diskno| ¥¥device¥scsiportno¥slotno}
```

(2)オプション

{-l|-e|-i|-o|-c}

- l：状態表示
  OS で認識されている HDD の一覧を画面に表示する。
- e：ディスク回転停止指示

[Devicename]で指定された HDD、または [iocx/slotno]で指定されたディスクの回転を停止し、Fault LED を点灯する。

- i：ロケーション表示

  [Devicename]で指定された HDD、または [iocx/slotno]で指定された SGPIO コントローラーのスロット位置の Fault LED を点滅する。

- o：ロケーション消灯

  [Devicename]で指定された HDD、または [iocx/slotno]で指定された SGPIO コントローラーのスロット位置の Fault LED を消灯する。

- c：Fault LED 消灯指示

  [iocx/slotno]で指定された SGPIO コントローラーのスロット位置の Fault LED を消灯する。

備考

- Linux の指定方法

  操作する HDD を論理装置名または SGPIO コントローラーのスロット番号で指定します。また、論理装置名を指定する場合は、状態表示(-l)で OS 上に存在するかを確認してください。

  - Devicename：OS の論理装置名を指定する。

    例．/dev/sda

  - iocx/slotno: SGPIO コントローラーの IOC 番号、およびディスクのスロット番号を指定する。
    例．ioc0 のスロット 1 の場合、ioc0/1

- Windows の指定方法

操作する HDD を論理装置名または SGPIO コントローラーのスロット番号で指定します。また、指定する前に、状態表示(-l)で対象のデバイスが存在するかを確認してください。

  - diskno：ディスク番号を指定する。(ディスクアドミニストレーターで表示されるディスク番号)

    例：Disk0 の場合、0

  - ¥¥device¥scsiportno¥slotno: SGPIO コントローラーの SCSI 番号、およびディスクのスロット番号を指定する。

例：SCSI 番号 1 のスロット 2 の場合、¥¥device¥scsiport1¥2

(3)使用例

- Linux の場合

  OS に存在するすべての SGPIO コントローラーとそのスロットの状態一覧を表示する場合の例を、以下に示します。

```
# /opt/fujitsu/SVmco/bin/diskctrl -l
```

SGPIO コントローラーとスロットの状態 (Linux)

表示例	状態説明
ioc0 0 /dev/sda Fault LED-Off 1 /dev/sdb Fault LED-Off 2 --mount Fault LED-Off 3 --mount Fault LED-On	 ←正常動作中 ←回転停止
ioc1 0 /dev/sdd Fault LED-Identify 1 none 2 none 3 none	 ←ロケーション表示中 ←空きスロット

- **備考**

  ioc の下に表示される数字は、スロット番号です。

  - HDD の交換、取外しのためにディスクの回転を停止する

    ```
    # /opt/fujitsu/SVmco/bin/diskctrl -e ioc0/3
    ```

  - HDD を増設するために搭載位置を確認する

    ```
    # /opt/fujitsu/SVmco/bin/diskctrl -i ioc0/3
    ```

  - HDD の交換/増設のために点滅させていたロケーション表示の Fault LED を消灯する

```
# /opt/fujitsu/SVmco/bin/diskctrl -o ioc0/3
```

○ ディスク回転停止操作後、Fault LED を消灯する

```
# /opt/fujitsu/SVmco/bin/diskctrl -c ioc0/3
```

- Windows の場合

OS に存在するすべての SGPIO コントローラーとそのスロットの状態一覧を表示する場合の例を、以下に示します。

```
diskctrl -l
```

SGPIO コントローラーとスロットの状態 (Windows)

表示例	状態説明
\¥device¥scsiport0	
0 Disk0 Fault LED-Off	←正常動作中
1 Disk1 Fault LED-Identify	←ロケーション表示中
2 none	←空きスロット
3 --mount Fault LED-On	←回転停止

備考

¥¥device¥scsiportx の下に表示される数字は、スロット番号です。

○ HDD の搭載位置を確認する

```
diskctrl -i 1
```

○ 点滅させていたロケーション表示の Fault LED を消灯する

diskctrl -o 1

(4)出力メッセージ一覧

この CLI で表示されるメッセージを、以下に示します。

- Linux の場合

SVmco : W 02152 diskctrl no memory available
SVmco : W 02158 diskctrl Cannot blinking location-LED
SVmco : W 02159 diskctrl Cannot clear loation-LED
SVmco : W 02165 diskctrl Operation not permitted
SVmco : W 02167 diskctrl Invalid option

- Windows の場合

SVmco : W 02152 diskctrl no memory available
SVmco : W 02158 diskctrl Cannot blinking location-LED
SVmco : W 02159 diskctrl Cannot clear location-LED
SVmco : W 02165 diskctrl Operation not permitted
SVmco : W 02167 diskctrl Invalid option
SVmco : W 02169 diskctrl too few or more option
SVmco : W 02170 diskctrl Cannot stop HDD
SVmco : W 02171 diskctrl Cannot get device information(SCSI)

SVmco : W 02172 diskctrl Cannot get device information(Registry)
SVmco : W 02173 diskctrl Cannot get device
SVmco : W 02174 diskctrl Device not found
SVmco : W 02181 diskctrl Cannot get device information(Snmp)
SVmco : W 02182 diskctrl Cannot get device information(WMI)
Svmco : W 02187 diskctrl internal error
SVmco : W 02189 diskctrl Target Device is not connected

(5)出力メッセージ詳細

この CLI で表示されるメッセージに関して詳細を、以下に示します。

- Linux の場合

  SVmco : W 02152 diskctrl no memory available

  意味：

  メモリ不足が発生しました

  対処：

  システムのメモリの空き状況を確認し、不要なプログラムを終了してから再度実行してください。

  SVmco : W 02158 diskctrl Cannot blinking location-LED

  意味：

  LED の点滅処理に失敗しました。

  対処：

  ハードウェア環境の確認を行い、再度コマンドを実行してください。

再度実行しても異常が解消されない場合は、必要な保守情報を採取して、修理相談窓口または担当営業員に連絡してください。

SVmco : W 02159 diskctrl Cannot clear loation-LED

意味：

LED の消灯処理に失敗しました。

対処：

ハードウェア環境の確認を行い、再度コマンドを実行してください。

再度実行しても異常が解消されない場合は、必要な保守情報を採取して、修理相談窓口または担当営業員に連絡してください。

SVmco : W 02165 diskctrl Operation not permitted

意味：

実行権限がありません。

対処：

スーパーユーザーでログインして、実行してください。

SVmco : W 02167 diskctrl Invalid option

意味：

無効なオプションが指定されました。

対処：

オプションまたはディスクの内容が正しく入力されているかを確認し、再度実行してください。

- Windows の場合

  SVmco : W 02152 diskctrl no memory available

  意味：

メモリ不足が発生しました。

対処：

システムのメモリの空き状況を確認し、不要なプログラムを終了してから再度実行してください。

SVmco : W 02158 diskctrl Cannot blinking location-LED

意味：

LED の点滅処理に失敗しました。

対処：

ハードウェア環境の確認を行い、再度コマンドを実行してください。

再度実行しても異常が解消されない場合は、必要な保守情報を採取して、修理相談窓口または担当営業員に連絡してください。

SVmco : W 02159 diskctrl Cannot clear location-LED

意味：

LED の消灯処理に失敗しました。

対処：

ハードウェア環境の確認を行い、再度コマンドを実行してください。

再度実行しても異常が解消されない場合は、必要な保守情報を採取して、修理相談窓口または担当営業員に連絡してください。

SVmco : W 02165 diskctrl Operation not permitted

意味：

実行権限がありません。

対処：

Administrator 権限のある ID でログインして、実行してください。

SVmco : W 02167 diskctrl Invalid option

意味：

無効なオプションが指定されました。

対処：

オプションまたはディスクの指定内容が正しく入力されているかを確認し、再度実行してください。

SVmco : W 02169 diskctrl too few or more option

意味：

コマンドオプション数に誤りがあります。

対処：

指定したオプションを確認し、正しいオプションを指定して再度実行してください。

SVmco : W 02170 diskctrl Cannot stop HDD

意味：

HDD の回転を停止できませんでした。

対処：

ハードウェア環境の確認を行い、再度コマンドを実行してください。

再度実行しても異常が解消されない場合は、必要な保守情報を採取して、修理相談窓口または担当営業員に連絡してください。

SVmco : W 02171 diskctrl Cannot get device information(SCSI)

意味：

SCSI から装置情報が取得できませんでした。

対処：

ハードウェア環境の確認を行い、再度コマンドを実行してください。原因として次のことが考えられます。

- RAID のみでディスクが構成されている (RAID 配下のディスクは diskctrl 操作対象外です) 。

SVmco : W 02172 diskctrl Cannot get device information(Registry)

意味：

Registry から装置情報が取得できませんでした。

対処：

ハードウェア環境の確認を行い、再度コマンドを実行してください。

再度実行しても異常が解消されない場合は、必要な保守情報を採取して、修理相談窓口または担当営業員に連絡してください。

SVmco :W 02173 diskctrl Cannot get device

意味：

装置の獲得 (open) に失敗した。

対処：

ハードウェア環境の確認を行い、再度コマンドを実行してください。

再度実行しても異常が解消されない場合は、必要な保守情報を採取して、修理相談窓口または担当営業員に連絡してください。

SVmco : W 02174 diskctrl Device not found

意味：

指定された装置が存在しません。

対処：

装置の存在の有無を確認し、再度コマンドを実行してください。

SVmco : W 02181 diskctrl Cannot get device information(Snmp)

意味：

snmp から装置情報が取得できません。

対処：

ハードウェア環境の確認を行い、再度コマンドを実行してください。

再度実行しても異常が解消されない場合は、必要な保守情報を採取して、修理相談窓口または担当営業員に連絡してください。

SVmco : W 02182 diskctrl Cannot get device information(WMI)

意味：

WMI から装置情報が取得できません。

対処：

ハードウェア環境の確認を行い、再度コマンドを実行してください。

再度実行しても異常が解消されない場合は、必要な保守情報を採取して、修理相談窓口または担当営業員に連絡してください。

SVmco : W 02187 diskctrl internal error

意味：

内部エラーが発生しました。

対処：

本コマンドまたは、システム障害の可能性があります。

必要な保守情報を採取して、修理相談窓口または担当営業員に連絡してください。

SVmco : W 02189 diskctrl Target Device is not connected

意味：

装置が接続されていません。

対処：

snmpd または SVmco が停止している可能性があります。

snmp または SVmco が停止している場合は、起動してから再度コマンドを実行してください。

3.1.3 SVmco 起動／停止コマンド (y30SVmco)

y30SVmco コマンドは、SVmco の起動または停止をします。

備考

- 本コマンドは、Linux のみ使用可能です。
- 本コマンドの実行には root 権限が必要です。
- SVmco はデーモンプログラムであるため、通常はブート時に自動起動されています。

(1)入力形式

```
/sbin/service y30SVmco {start | stop | status}
```

(2)オプション

start | stop | status

- start：SVmco を起動する。
- stop：SVmco を停止する。
- status：SVmco の起動状態を確認する。

(3)使用例

a.SVmco を起動する場合の例

```
# /sbin/service y30SVmco start
```

b.SVmco を停止する場合の例

```
# /sbin/service y30SVmco stop
```

c.SVmco の起動状態を確認する場合の例

```
# /sbin/service y30SVmco status
```

SVmco がすでに起動している場合、以下のメッセージが出力されます。

```
SVmco is already running
```

SVmco が停止している場合、以下のメッセージが出力されます。

```
SVmco is stopped(xxxx)
```

SVmco 起動時に、PSA-MMB LAN の IP 設定に異常がある場合、SVmco の起動が失敗すると共に、以下のメッセージが出力されます。

```
Please check the setting of PSA-MMB LAN and tommbipsetup.conf
```

その場合、PSA-MMB LAN のネットワークインターフェースファイル(ifcfg-ethX)や/etc/fujitsu/SVmco/usr/tommbipsetup.conf ファイルの IP 設定を見直して下さい。

備考

(xxxx) には詳細情報が入ります。

(4)終了ステータス

0：正常終了

>0：異常終了

(5)注意事項

y30SVmco コマンドによって SVmco を起動したときに、以下のメッセージが表示されることがあります。このメッセージが表示されても、動作上問題はありません。

```
/bin/mknod: `/dev/watchdog': ファイルが存在します。
```

3.1.4 SVmco 調査資料収集コマンド (getosvmco)

getosvmco コマンドは、SVmco の障害発生時の調査資料として、以下の情報を一括して 1 つの圧縮ファイルにまとめて出力します。

- アプリケーションパッケージのインストール状況
- ファイル／モジュール一覧情報
- 設定ファイル
- 内部ログ
- トレースファイルなど

備考

本コマンドの実行には、root (Linux) 権限または Admin (Windows) 権限が必要です。Windows の場合、OS 機能 (アクセス制御機能) により、Admin 権限以外で実行すると終了ステータスが不定になります。

(1)入力形式

output_filename には、圧縮した調査資料の出力先ファイルをフルパスで指定します。

- Linux または VMware の場合

```
/opt/fujitsu/SVmco/sh/getosvmco {output_filename}
```

- Windows の場合

```
getosvmco output_filename
```

(2)オプション

なし

(3)使用例

- Linux の場合

調査資料が、/tmp/dump/mco_dump のパスのファイルに出力されます。

```
# /opt/fujitsu/SVmco/sh/getosvmco  /tmp/dump/mco_dump
```

- Windows の場合

調査資料が、C:¥temp¥dump¥mco_dump のパスのファイルに出力されます。

```
> getosvmco C:¥temp¥dump¥mco_dump
```

(4)終了ステータス

0：正常終了

>0：異常終了

3.1.5 SNMP セキュリティ設定コマンド (setsnmpsec)

setsnmpsec コマンドは、SNMP サービスのセキュリティ設定 (SNMP パケットを受け付けるホストの設定) をします。SNMP サービスのセキュリティ設定が「すべてのホストから SNMP パケットを受け付ける」の場合には実行する必要はありません。

SNMP サービスのセキュリティ設定を「これらのホストから SNMP パケットを受け付ける」で運用中で、SVmco インストール後に PSA-MMB 間通信 LAN の MMB の IP アドレスを変更した場合、SNMP サービスのセキュリティ設定を「すべてのホストから SNMP パケットを受け付ける」から「これらのホストから SNMP パケットを受け付ける」に変更した場合に実行します。

備考

- 本コマンドは、Windows のみ使用可能です。
- 本コマンドの実行には、Admin 権限が必要です。OS 機能 (アクセス制御機能) により、Admin 権限以外で実行すると終了ステータスが不定になります。

(1)入力形式

```
setsnmpsec
```

(2)オプション

なし

(3)使用例

```
> setsnmpsec
```

(4)出力メッセージ

- 正常終了時:

  SVmco : I 04200 Security setting for SNMP Service was completed.

- **異常終了時**:

  SVmco : E 04201 An error occurred at the time of security setting for SNMP Service.

(5)注意事項

本コマンドを実行した場合、SNMP Service の再起動が必要です。

3.1.6 PCI カード操作コマンド(fjpciswap)

fjpciswap コマンドは、PCI カードの物理位置情報（UnitName：識別名）の表示、DeviceName の表示を行います。これにより、交換を行いたい PCI カードの情報を確認できます。

注意

- 二重化ソフトなどを使用している場合は、そのソフトからの切り離しを行った上で本コマンドを使用してください。切り離しを行わない場合、OS が停止する可能性があります。

- コマンドを途中で停止しないでください。以下の現象が発生する可能性があります。

fjpciswap コマンド中断時の現象

現象	対処
OS 上の資源が解放されずに残ってしまい、システム負荷が上がる	OS のリブートを行う

- SAN ブート接続用の FC カードは、このコマンドの対象外です。
- カードの先に存在するディスク上に Pagefile や Dump の出力先がある FC カードは、このコマンドの対象外です。
- 交換対象の PCI カードに、接続されているデバイスがある場合は、PCI カードを交換できません。

備考

- 本コマンドは Windows Server 2008/2012 のみ使用可能です。
- 本コマンドの実行には、Admin 権限が必要です。OS 機能 (アクセス制御機能) により、Admin 権限以外で実行すると終了ステータスが不定になります。
- 本コマンドを実行するには SVagent,SVmco、SNMP サービスが正常に動作していることが条件となります。
- システム上で使用している PCI カードを交換する場合は、システム上での使用を停止し、デバイスマネージャー上で無効化した上で本コマンドを使用してください。

  デバイスマネージャー上での無効化の方法は、以下のとおりです。

  1. デバイスマネージャーを開きます。
  2. 該当のデバイスを右クリックし、無効化を選択します。

(1)入力形式

```
>fjpciswap [-l|-r|-a] [UnitIdetificationName]
```

UnitIdentificationName (識別名スロット位置の指定)

指定する名前は大文字、小文字も区別されます。

例：IOB-PCIC#0、PCI_Box-PCIC#1、IOB#0-PCIC#1、PCI_Box#0-PCIC#1

(2)オプション

[-l|-r|-a]

-l ：表示

コマンドで交換可能な PCI カードの一覧を表示します。下記の項目を表示します。

UnitName ：

UnitName（識別名）を表示します。[PCI Devices] 画面の[Unit] に相当する情報

Func ：

Function 番号

Device Name：

Device Name を表示します。[PCI Devices] 画面の[Device Name] に相当する情報

-r ：交換

[UnitIdetificationName]で指定した PCI カードの交換操作を行います。電源オフ操作、交換指示、交換後のデバイスの認識処理がすべて完了した時点でコマンドは終了します。

-a ：追加

[UnitIdetificationName]で指定した PCI カードの追加操作を行います。デバイスの追加処理がすべて完了した時点でコマンドは終了します。

(3)使用例

[表示機能]を使用して一覧表示したときの例を示します。

【例 1】

```
C:¥>fjpciswap -l


Replaceable PCI cards are displayed
```

```
UnitName     Func   DeviceName
IOB#1-PCIC#5 FUNC#0 Intel(R) PRO/1000 PT Dual Port Server Adapter
IOB#1-PCIC#5 FUNC#1 Intel(R) PRO/1000 PT Dual Port Server Adapter #2

C:¥>
```

[交換機能] を使用して交換可のカードを指定した場合の例を示します。

【例 2】

```
C:¥>fjpciswap -r IOB#1-PCIC#5
Selected card name is
                Intel(R) PRO/1000 PT Dual Port Server Adapter
                Intel(R) PRO/1000 PT Dual Port Server Adapter #2

Please delete all settings about this card
Do you want to remove this card?(y/n)
y ←ユーザー入力
```

```
Removing the card....
The card has removed.

Please replace the card, and input "y" key.
```

上記のメッセージが表示されたら、PCI カードの交換作業を行います。

```
Please replace the card, and input "y" key.
```

y

Adding the card.....

The card has added.

C:￥>

(4)出力メッセージ 一覧

この CLI で表示されるメッセージを、以下に示します。

SVmco : E 08740 this command can not execute doubly :%s
SVmco : E 08741 this command needs Administrators privilege :%s
SVmco : E 08742 invalid option :%s
SVmco : E 08743 option num is invalid :%s
SVmco : E 08744 no unit id :%s
SVmco : E 08745 internal error :%s
SVmco : E 08746 can not make event file :%s
SVmco : E 08748 no resource :%s
SVmco : E 08751 command timeout(WMI) :%s
SVmco : E 08752 configuration file error :%s
SVmco : E 08753 This card cannot be removed :%s
SVmco : E 08754 can not get snmp information :%s
SVmco : E 08755 no card :%s
SVmco : E 08756 internal error(ipmi) :%s
SVmco : E 08757 this command can not execute during refresh :%s

SVmco : E 08758 this unit is occupied :%s
SVmco : E 08759 command timeout(SNMP) :%s

(5)出力メッセージ 詳細

この CLI で表示されるメッセージの詳細について、以下に示します。

SVmco : E 08740 this command can not execute doubly :%s

意味：

本コマンドは二重起動できません。

対処：

他で本コマンドが実行されていないか確認してください。本コマンドは二重起動できないので、コマンドが終了してから再度実行してください。

SVmco : E 08741 this command needs Administrators privilege :%s

意味：

本コマンドの実行には Admin 権限が必要です。

対処：

Admin 権限のコンソールで実行してください。

SVmco : E 08742 invalid option :%s

意味：

不正なオプションが指定されました。

対処：

正しいオプションを指定して実行してください。指定するオプションは、大文字、小文字も区別されます。

PCI カード操作コマンド (fjpciswap) のオプションについては詳しくは、「3.6 PCI カード操作コマンド (fjpciswap)」を参照してください。

SVmco : E 08743 option num is invalid :%s

意味：

オプションの数が異常です。

対処：

正しいオプションを指定して実行してください。

PCI カード操作コマンド (fjpciswap) のオプションについて詳しくは、「3.6 PCI カード操作コマンド (fjpciswap)」を参照してください。

SVmco : E 08744 no unit id :%s

意味：

パーティションに存在しないユニット名を指定しています。

対処：

パーティションに存在するユニット名を指定してください。

SVmco : E 08745 internal error :%s

意味：

内部エラーが発生しました。

対処：

PCI カード状態のリカバリーを実行します。PCI カード状態のリカバリーについては詳しくは、「■ PCI カード状態のリカバリー」を参照してください。

再度実行して同様のメッセージが表示される場合は、修理相談窓口または担当営業員に連絡してください。

SVmco : E 08746 can not make event file :%s

意味：

イベント通知用ファイルの作成に失敗しました。

対処：

ディスク容量を確保します。

再度実行して同様のメッセージが表示される場合は、修理相談窓口または担当営業員に連絡してください。

SVmco : E 08748 no resource :%s

意味：

メモリなど資源の獲得に失敗しました。

対処：

OS の資源が十分にあるか確認してください。OS の資源に問題がない場合は、修理相談窓口または担当営業員に連絡してください。

SVmco : E 08751 command timeout(WMI) :%s

意味：

WMI の原因によるコマンドのタイムアウトが発生しました。

対処：

1. "Windows Management Instrumentation"(WMI)サービスの動作を確認します。起動されていない場合は起動します。
2. PCI カード状態のリカバリーを実行します。

   PCI カード状態のリカバリーについては詳しくは、「■　PCI カード状態のリカバリー」を参照してください。
3. PCI カードの状態が想定どおりにならない場合には修理相談窓口または担当営業員に連絡してください。

SVmco : E 08752 configuration file error :%s

意味：

設定ファイルの異常が発生しました。

対処：

修理相談窓口または担当営業員に連絡してください。

SVmco : E 08753 This card cannot be removed :%s

意味：

交換をサポートしていないカードを交換対象として選択しました。

対処：

交換をサポートしているカードを交換対象として選択してください。

SVmco : E 08754 can not get snmp information :%s

意味：

ユニット ID が SNMP から取得できません。

対処：

1. SNMP Service の動作を確認します。起動されていない場合は起動します。
2. 再度実行して同様のメッセージが表示される場合は、SVmco の再起動を行ってください。SVmco の起動方法は、「3.1 CLI コマンド一覧」の*2 を参照してください。
3. 再度実行して同様のメッセージが表示される場合は、修理相談窓口または担当営業員に連絡してください。

SVmco : E 08755 no card :%s

意味：

指定したスロットにカードが挿入されていません。

対処：

カードを挿入したスロット位置を確認してから、追加操作をしてください。

SVmco : E 08756 internal error(ipmi) :%s

意味：

内部エラーが発生しました。

対処：

PCI カード状態のリカバリーを実行します。PCI カード状態のリカバリーについては詳しくは、「■　PCI カード状態のリカバリー」を参照してください。

再度実行して同様のメッセージが表示される場合は、修理相談窓口または担当営業員に連絡してください。

SVmco : E 08757 this command can not execute during refresh :%s

意味：

SVmco 情報更新中のため、カードの更新ができません。

対処：

OS 起動から 30 分経過していない場合、30 分経過してから再度実行してください。

OS 起動から 30 分以上経過している場合は、1 分以上待ってから再度実行してください。

SVmco : E 08758 this unit is occupied :%s

意味：

すでにカードが実装されているスロットに追加しようとしました。

対処：

カードを追加したスロット位置を確認してから追加操作をしてください。

SVmco : E 08759 command timeout(SNMP) :%s

意味：

SVmco もしくは SNMP が原因のコマンドタイムアウトが発生しました。

対処：

SVmco および SNMP Service の動作を確認し、起動されていない場合は起動してください。

再度実行して同様のメッセージが表示される場合は、PCI カード状態のリカバリーを実行します。PCI カード状態のリカバリーについては詳しくは、「■　PCI カード状態のリカバリー」を参照してください。

再度実行して同様のメッセージが表示される場合は、修理相談窓口または担当営業員に連絡してください。

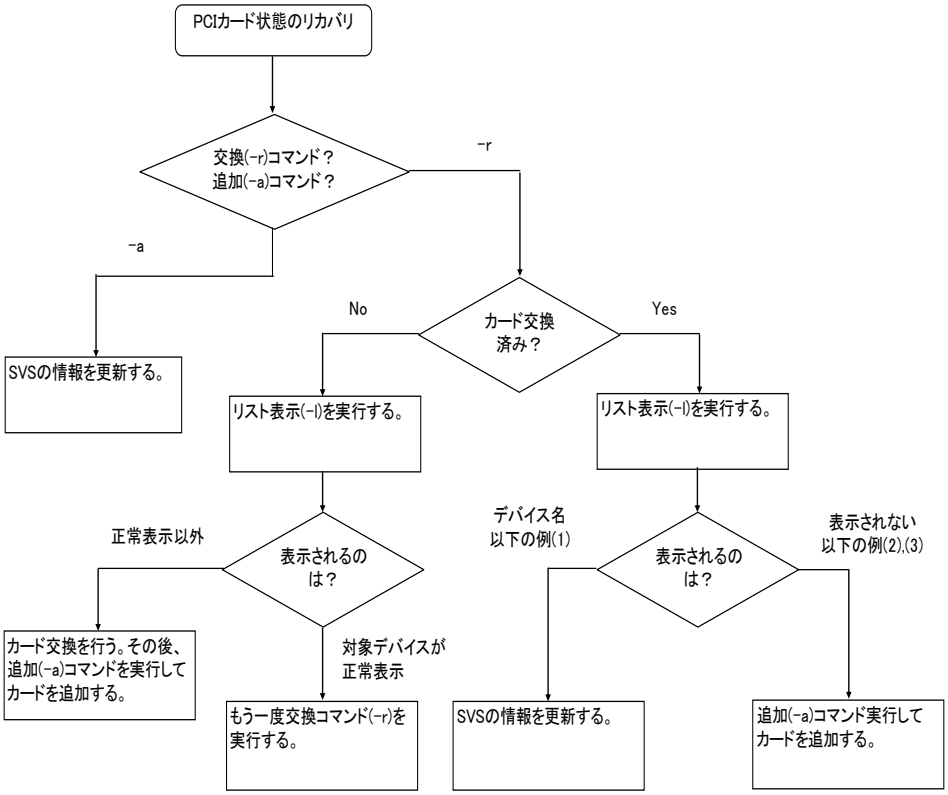
■　PCI カード状態のリカバリー

エラーメッセージにより PCI Hot Plug 手順の途中でコマンドが終了した場合や、PCI カード交換後に正常な状態にならない場合に、以下の手順を実行します。

注意

この手順はエラーメッセージの対処実行後に行ってください。ただし、対処実行できない場合でもリカバリーは可能です。この手順で復旧できない場合は、当社保守員へ連絡してください。

PCI カード状態のリカバリー



(1)リスト表示で識別名が表示されない場合の例

```
C:¥>fjpciswap -l


Replaceable PCI cards are displayed
UnitName Func DeviceName
- Emulex LightPulse LPe1250-F8, PCI Slot 4, Storport
Miniport Driver
- Intel(R) PRO/1000 PT Dual Port Server Adapter #1
- Intel(R) PRO/1000 PT Dual Port Server Adapter #2
- Intel(R) PRO/1000 PT Dual Port Server Adapter #3
- Intel(R) PRO/1000 PT Dual Port Server Adapter #4


C:¥>
```

(2)リスト表示で PCI カードの情報がまったく表示されない場合の例

ただし、操作対象の PCI カードのみが表示されない場合もあります。また、PCI カードが交換されていない場合にはカード交換後、追加コマンドを実行してください。

```
C:¥>fjpciswap -l


Replaceable PCI cards are displayed
Unit Name          Func      Device Name
there are no removable pci card


C:¥>
```

(3)リスト表示で該当の PCI カード (IOB#1-PCIC#4-FUNC#0) の情報が表示されない場合の例

```
C:¥>fjpciswap -l

Replaceable PCI cards are displayed
UnitName        Func     DeviceName
IOB#1-PCIC#5    FUNC#0   Intel(R) PRO/1000 PT Dual Port Server Adapter #1
IOB#1-PCIC#5    FUNC#1   Intel(R) PRO/1000 PT Dual Port Server Adapter #2
IOB#1-PCIC#7    FUNC#0   Intel(R) PRO/1000 PT Dual Port Server Adapter #3
IOB#1-PCIC#7    FUNC#1   Intel(R) PRO/1000 PT Dual Port Server Adapter #4

C:¥>
```

3.1.7 管理 LAN 用インターフェース向けファイアーウォール設定コマンド (setmlanfw.sh)

setmlanfw.sh コマンドは、管理 LAN 用インターフェースに対しファイアーウォールが設定され、かつ管理 LAN ネットワークを通じて PRIMECLUSTER と連携を行う場合に、必要なポートの開放をサポートするツールです。

このコマンドにより、指定した IP アドレスに対して以下のポートを開放します。

- snmptrap ポート：udp/162
- rmcp+ポート：udp/7000～7100

注意

管理 LAN 用インターフェースの IP アドレスが変更されるなど、ファイアーウォール設定の変更が必要となった場合は、削除手順に従っていったん設定を削除した上で再度設定手順を実行してください。

備考

- 本コマンドは Linux のみ使用可能です。
- 本コマンドの実行には root 権限が必要です。
- 本コマンドの実行は、以下の手順どおりに行ってください。

(1)入力形式

config_file で、ポートを開放する相手先 IP アドレスを記載した設定ファイルを指定します。

/opt/fujitsu/SVmco/sh/setmlanfw.sh {config_file}

(2)使用例

config_file で、ポートを開放する相手先 IP アドレスを/tmp/config.txt に記載しておきます。

/opt/fujitsu/SVmco/shsetmlanfw.sh /tmp/config.txt

(4)出力メッセージ 一覧

この CLI で表示されるメッセージを以下に示します。

Too few argument
Too more argument
Cannot read the file : %s
No IP setting or illegal IP format in /etc/fujitsu/SVmco/usr/ipsetup.conf
No IP setting in %s
Already set iptables
The setting was completed

備考

上記のほか、設定の内容を確認するメッセージも表示されます。

(5)出力メッセージ 詳細

この CLI で表示されるメッセージの詳細を以下に示します。

Too few argument

意味：

オプションの数が不正です。

対処：

実行には設定ファイルの指定が必要です。設定ファイルを指定したうえで再度実行してください。

Too more argument

意味：

オプションの数が不正です。

対処：

実行には設定ファイルの指定が必要です。設定ファイルを指定したうえで再度実行してください。

Cannot read the file : %s

意味：

実行に必要なファイルが見つかりません。

対処：

メッセージに表示されているファイルが見つかりません。ファイルの存在を確認したうえで再度実行してください。

No IP setting or illegal IP format in /etc/fujitsu/SVmco/usr/ipsetup.conf

意味：

SVmco 動作ファイル"/etc/fujitsu/SVmco/usr/ipsetup.conf" に管理 LAN の IP アドレスが設定されていません。または IP アドレスのフォーマットが不正です。

対処：

「2.1.5 管理 LAN IP アドレスの設定」を参照し、管理 LAN の IP アドレスを設定したうえで、再度実行してください。

No IP setting in %s

意味：

メッセージに表示されているファイルに設定が見つかりません。

対処：

%s:/etc/fujitsu/SVmco/usr/ipsetup.conf の場合

「2.1.5 管理 LAN IP アドレスの設定」を参照し、管理 LAN の IP アドレスを設定したうえで、再度実行してください。

%s:上記以外

メッセージに表示されているファイルに IP アドレスを設定したうえで、再度実行してください。

Already set iptables

意味：

すでに設定が行われています。

対処：

iptables -L –n を確認し、設定に問題がない場合は対処は不要です。

設定内容に変更・不備がある場合、いったん設定を削除したうえで再度実行してください。

The setting was completed

意味：

設定が完了しました。

対処：

不要です。

(6)終了ステータス

0 : 正常終了

>0: 異常終了

(7)設定手順

本コマンドを実行する場合、事前に管理 LAN インターフェースの設定が必要です。

設定内容は管理 LAN で使用している通信プロトコルによって異なります。

■ **IPv4 で使用している場合**

1. SVmco の動作設定ファイル(/etc/fujitsu/SVmco/usr/ipsetup.conf)に、管理 LAN 用インターフェースの IP アドレスを設定します。

   管理 LAN 用インターフェースの IP アドレスの設定について詳しくは、「2.1.5 管理 LAN IP アドレスの設定」を参照してください。

   [設定例] /etc/fujitsu/SVmco/usr/ipsetup.conf

   ```
   [NETWORK]
   ManagementIP=192.168.0.1
   ```

2. ポートを開放する相手先 IP アドレスを記載した設定ファイルを準備します。

   設定ファイルには以下のように "[PCL]" とだけ記載した行に続き、PRIMECLUSTER で定義された全クラスタノードに属する MMB の物理 IP (MMB Physical IP Address <MMB#0/MMB#1>)または上記 MMB の物理 IP を含むネットワーク IP を、1 行 1 項目単位で記載してください。

【設定例】/tmp/config.txt

```
[PCL]
192.168.0.0/24
192.168.1.5
```

備考

設定ファイルのサンプルは以下に配置してあります。

/opt/fujitsu/SVmco/sh/sample_conf_setmlanfw.txt

3. setmlanfw.sh に手順 2 で準備した設定ファイルを付与して実行します。

   実行すると、手順 1 および手順 2 で設定した内容について確認を求めるメッセージが出力されます。設定内容がなければ ″Y″、再設定したい場合は ″N″ と入力し、 処理を進めてください。

   [実行例] 手順 2 で準備した設定ファイルを指定します。

```
# /opt/fujitsu/SVmco/sh/setmlanfw.sh /tmp/config.txt
Management LAN IP address:
192.168.0.1

Source IPs for PRIMECLUSTER Service:
192.168.0.0/24
192.168.1.5

Press "Y" to confirm above settings, "N" to cancel all settings
> Y
The setting was completed
```

4. 作成された設定チェイン "MMLAN" を INPUT および OUTPUT チェインに追加します。このとき、INPUT および OUTPUT チェインにある既存の REJECT 設定や、ユーザー定義のチェインに遮断されないように、注意して設定してください。 (設定の詳細は 2.1.4 ファイアーウォール機能の確認を参照して下さい。)

[設定例]

```
# iptables -L -n
Chain INPUT (policy DROP)
target  prot opt source     destination
MMLAN   all  -- 0.0.0.0/0    0.0.0.0/0

Chain FORWARD (policy DROP)
target   prot opt source    destination

Chain OUTPUT (policy DROP)
target   prot opt source    destination
MMLAN   all -- 0.0.0.0/0   0.0.0.0/0

Chain MMLAN (2 references)
target  prot opt source     destination
ACCEPT  udp  -- 192.168.0.0/24  192.168.0.1   udp dpts:7000:7100
ACCEPT  udp  -- 192.168.0.1   192.168.0.0/24 udp spts:7000:7100
ACCEPT  udp  -- 192.168.0.0/24 192.168.0.1   udp dpt:162
ACCEPT  udp  -- 192.168.0.1   192.168.0.0/24 udp spt:162
ACCEPT  udp  -- 192.168.1.5   192.168.0.1   udp dpts:7000:7100
ACCEPT  udp  -- 192.168.0.1   192.168.1.5   udp spts:7000:7100
ACCEPT  udp  -- 192.168.1.5   192.168.0.1   udp dpt:162
ACCEPT  udp  -- 192.168.0.1   192.168.1.5   udp spt:162
```

(8)設定削除手順

管理 LAN 用インターフェースの IP アドレスが変更となるなど、ファイアーウォール設定の変更が必要となった場合は、設定をいったん削除する必要があります。

削除した後、再度設定してください。

削除方法は管理 LAN で使用している通信プロトコルによって異なります。

■ **IPv4 で使用している場合**

1. iptables -L -n を実行し、設定チェーン "MMLAN"が存在することを確認します。
   存在しない場合は、以下の手順は不要です。

2. INPUT/OUTPUT チェーンから MMLAN への参照を削除します。

   [実行例]

```
# iptables -D INPUT -j MMLAN
# iptables -D OUTPUT -j MMLAN
```

3. 設定チェーン"MMLAN"内の設定を削除します。

   [実行例]

```
# iptables -F MMLAN
```

4. 設定チェーン "MMLAN" を削除します。

   [実行例]

```
# iptables -X MMLAN
```

3.1.8 PSA-MMB 通信 LAN 設定コマンド(setpsalan)

setpsalan コマンドは、PSA-MMB 通信 LAN のネットワーク設定を行います。

SVmco のインストール後、本コマンドの実行が必要です。OS を再起動してから本コマンドを実行してください。

本コマンドを実行すると、以下のとおりに PSA-MMB 通信 LAN のネットワークが設定されます。

- IP アドレス

  172.30.0.<パーティション ID + 2>/24

  例) パーティション ID が 2 の場合

  172.30.0.4/24
- 通信設定

  Auto Negotiation：off

  Speed：100Mbps

  Duplex：full

備考

- 本コマンドは、Windows のみ使用可能です。
- 本コマンドの実行には、Admin 権限が必要です。OS 機能 (アクセス制御機能) により、Admin 権限以外で実行すると終了ステータスが不定になります。

(1)入力形式

```
setpsalan
```

(2)オプション

なし

(3)使用例

```
> setpsalan
```

(4)終了ステータス

0：正常終了

>0：異常終了

(5)注意事項

SVmco インストール後、OS を再起動してから本コマンドを実行してください。

3.1.9 iptables 設定ツール

setiptable.sh シェルは、SVmco 用の iptables の設定ツールです。

- 本シェルは、Linux のみ使用可能です。
- 本シェルの実行には root 権限が必要です。
- 本シェルは、SVmco 用の iptables のチェイン(PSA-MMB_LAN)を作成のみを行います。INPUT や OUTPUT への設定は手動での設定が必要です。

  設定の詳細は『ファイアーウォールの機能の確認』を参照して下さい。

(1)入力形式

```
# ./setiptables.sh <オプション>
```

(2)オプション

manual :

iptables に SVmcovm 用の iptables のチェイン(PSA-MMB_LAN)を作成する。

(3)使用例

```
# ./setiptables.sh manual
```

⑷終了ステータス

0：正常終了

>0：異常終了

3.2 SVMcovm の CLI

3.2.1 CLI コマンド一覧

SVmcovm の CLI コマンドの一覧を示します。

コマンド一覧

No	コマンド名	権限	備考	コマンド	
				Linux	Windows
1	SVmcovm 起動/停止コマンド	root (Linux) 権限または Admin (Windows) 権限が必要 (*2)	SVmcovm の起動/終了	あり	(*1)
2	SVmcovm 調査資料収集コマンド	root (Linux) 権限または Admin (Windows) 権限が必要 (*2)	SVmcovm 調査資料の収集	あり	あり
3	SVmcovm 用 iptables 設定ツール	root (Linux) 権限が必要	SVmcovm 用 iptables の設定ツール	あり	なし
4	ESXi へのアクセス情報の設定コマンド	root(Linux)権限または Admin (Windows) 権限が必要(*2)	ログイン情報は暗号化して保存する。	あり	あり

*1:

起動：[コントロールパネル] - [管理ツール] - [サービス]の順にクリックし、「ServerView Mission Critical Option VM」を起動します。

停止：[コントロールパネル] - [管理ツール] - [サービス]の順にクリックし、「ServerView Mission Critical Option VM」を選択して停止します。

*2：Windows の場合、OS 機能 (アクセス制御機能) により、Admin 権限以外で実行すると終了ステータスが不定になります。

3.2.2 SVmcovm 起動／停止コマンド (y30SVmco)

y30SVmco コマンドは、SVmcovm の起動または停止をします。

備考

- 本コマンドは、Linux のみ使用可能です。
- 本コマンドの実行には root 権限が必要です。
- SVmcovm はデーモンプログラムであるため、通常はブート時に自動起動されています。

(1)入力形式

```
/sbin/service y30SVmco {start | stop | status}
```

(2)オプション

start | stop | status

- start：SVmcovm を起動する。
- stop：SVmcovm を停止する。
- status：SVmcovm の起動状態を確認する。

(3)使用例

a.SVmcovm を起動する場合の例

```
# /sbin/service y30SVmco start
```

b.SVmcovm を停止する場合の例

```
# /sbin/service y30SVmco stop
```

c.SVmcovm の起動状態を確認する場合の例

```
# /sbin/service y30SVmco status
```

SVmcovm がすでに起動している場合、以下のメッセージが出力されます。

```
SVmco is already running
```

SVmcovm が停止している場合、以下のメッセージが出力されます。

```
SVmco is stopped(xxxx)
```

備考

(xxxx) には詳細情報が入ります。

⑷終了ステータス

0：正常終了

>0：異常終了

3.2.3 SVmcovm 調査資料収集コマンド (getosvmco)

getosvmco コマンドは、SVmcovm の障害発生時の調査資料として、以下の情報を一括して 1 つの圧縮ファイルにまとめて出力します。

- アプリケーションパッケージのインストール状況
- ファイル／モジュール一覧情報
- 設定ファイル
- 内部ログ
- トレースファイルなど

備考

本コマンドの実行には、root (Linux) 権限または Admin (Windows) 権限が必要です。Windows の場合、OS 機能 (アクセス制御機能) により、Admin 権限以外で実行すると終了ステータスが不定になります。

(1)入力形式

output_filename には、圧縮した調査資料の出力先ファイルをフルパスで指定します。

- Linux の場合

```
/opt/fujitsu/SVmco/sh/getosvmco {output_filename}
```

- Windows の場合

```
getosvmco output_filename
```

(2)オプション

なし

(3)使用例

- Linux の場合

  調査資料が、/tmp/dump/mco_dump のパスのファイルに出力されます。

```
# /opt/fujitsu/SVmco/sh/getosvmco  /tmp/dump/mco_dump
```

- Windows の場合

  調査資料が、C:¥temp¥dump¥mco_dump のパスのファイルに出力されます。

```
> getosvmco C:¥temp¥dump¥mco_dump
```

(4)終了ステータス

0：正常終了

>0：異常終了

3.2.4 SVmcovm 用 iptables 設定ツール

Setiptable.sh シェルは、SVmcovm 用の iptables の設定ツールです。

- 本シェルは、Linux のみ使用可能です。
- 本シェルの実行には root 権限が必要です。
- 本シェルは、SVmcovm 用の iptables のチェイン(PSA-MMB_LAN)を作成のみを行います。INPUT や OUTPUT への設定は手動での設定が必要です。

設定の詳細は『ファイアーウォールの機能の確認』を参照して下さい。

(1)入力形式

```
# ./setiptable.sh install <PSA-MMB 間通信 LAN の割り当たっているネットワークインターフェース名>
```

(2)オプション

Install

- **install**： iptables に SVmcovm 用の iptables のチェイン(PSA-MMB_LAN)を作成する。

(3)使用例

PSA-MMB 間通信 LAN が eth0 の割り当たっている場合：

```
# ./setiptable.sh install eth0
```

(4)終了ステータス

0：正常終了

>0：異常終了

3.2.5 ESXi へのアクセス情報設定コマンド (setuserinfo)

Setuserinfo コマンドは SVmcovm が PCI カード情報やログ情報を ESXi から取得する時に必要な情報を対話形式で設定するコマンドです。設定内容は以下のようになっています。

- ESXi の IP※ 1
- ESXi へのログイン ID
- ESXi へのログインパスワード※2

※1 IPv4 のみサポート

※2 設定した情報は暗号化して保存します。

備考

本コマンドの実行には、root (Linux) 権限または Admin (Windows) 権限が必要です。Windows の場合、OS 機能 (アクセス制御機能) により、Admin 権限以外で実行すると終了ステータスが不定になります。

(1)入力形式

- Linux

```
# /opt/fujitsu/SVmco/bin/setuserinfo <オプション>
```

- Windows

```
#<SVmcovm のインストールパス>¥opt¥fujitsu¥SVmco¥bin¥setuserinfo <オプション>
```

(2)オプション

-i : 対話形式で、ESXi の IP アドレス、ログイン ID,パスワードを暗号化し、ファイルへ出力する。

-c: 設定した情報が正しいか確認する。

⑶使用例

例として linux の場合を示します。

1. ESXi へのログイン情報を設定する。

   情報を暗号化したファイルが、/etc/fujitsu/SVmco/local/userinfo ファイルに出力されます。

```
# /opt/fujitsu/SVmco/bin/setuserinfo –i

Input  ESXi Host IPv4 address: x.x.x.x

Input Login ID: xxxxx

Input Login PASSWORD:
```

2. 設定した情報が正しいかチェックを行う。

```
# /opt/fujitsu/SVmco/bin/setuserinfo –c
```

コマンド成功：Successful execution of the command.

コマンド失敗：Failed to execute the command

⑷終了ステータス

0：正常終了

1,2：異常終了

4　ハードディスクの活性交換

本章では、ハードディスクの活性交換について説明します。この操作は Red Hat でのみサポートされています。

4.1　ハードディスクの活性交換の概要

SVmco には、パーティション上のハードディスクの活性交換を支援する機能があります。システム保守契約を結んでいる場合は、ハードディスクは当社技術員が交換します。

SVmco は、ハードウェアの故障検出時、ディスク交換時、およびディスク増設時などに、ディスク LED 制御およびディスクの状態表示をするための機能を提供しています。

注意

- VMware ではハードディスクの活性交換をサポートしていません。
- ハードディスク実装時に、以下のようなメッセージが出力されることがありますが、動作上の問題はありません。

  ```
  kernel: mptscsih: ioc0: >> Attempting bus reset! (sc=e000004082adc480)
  kernel: mptbase: ioc0: IOCStatus(0x0048): SCSI Task Terminated
  ```

- ハードディスクを挿入した後、誤った位置に挿入したなどの理由でディスクの回転を停止させて、正しい位置に挿入しなおす場合、ディスク実装後 60 秒程度の時間をおいてから、ディスクの回転を停止させてください。ディスク実装操作により OS の Hot Plug 処理が動作するため、すぐにディスクの回転を停止させると以下に示すようなエラーが出力される場合があります。

```
kernel: Device sdb not ready.
kernel: end_request: I/O error, dev sdb, sector 204706
kernel: Buffer I/O error on device sdb1, logical block 6396
```

- ディスク操作コマンドを同時に複数実行すると、異常終了する場合があります。実行中のディスク操作コマンドがないことを確認してから実行してください。
- ディスク操作コマンドでは以下の操作が可能です。「3.2 ディスク操作コマンド (diskctrl)」を参照してください。
  - SGPIO、SES コントローラーの一覧、およびそのコントローラーで管理されているハードディスクの一覧表示
  - ハードディスクのロケーション LED 点滅・消灯
- ファイルシステムの構成情報キャッシュファイルの削除(Red Hat Enterprise Linux 5)

  ディスクの活性交換、活性増設、活性削除の後、および静的な交換、増設、削除の前に、以下のコマンドを実施して、ファイルシステム構成のキャッシュファイルを削除してください。

  ```
  # rm /etc/blkid/blkid.tab
  ```

  Red Hat Enterprise Linux では、fsck コマンドによりファイルシステムを点検するさい、ファイルシステムの構成をキャッシュファイルとして保持している /etc/blkid/blkid.tab ファイルが存在する場合はその情報が使われます。

  ディスクの活性交換、活性増設、または活性削除が行われた場合、システムの状態と/etc/blkid/blkid.tab の内容が一致しません。このため、次回 fsck コマンドを実行した場合に正しく点検されず、ファイルシステムが破壊されることがあります。

  このファイルは、いったん作成されると更新されません。このため、ディスクの活性交換、活性増設、活性削除の後、さらに静的な交換、増設、削除の前は、キャッシュファイルを削除する必要があります。

  キャッシュファイルは必要に応じて再作成されますので、削除しても問題ありません。
- smartd サービスの停止について (Red Hat Enterprise Linux 5)

  ハードディスクの活性保守 (活性交換・活性増設・活性削除) の実施中は、smartd サービスを停止してください。

smartd サービスは、ハードディスクの自己診断機能 S.M.A.R.T. (Self-Monitoring、Analysis and Reporting Technology System) を使用してハードディスクを監視するサービスです。

smartd サービスはハードディスクの活性保守に対応していないため、smartd サービスが起動時に取得したハードディスクの情報が、活性保守後のハードディスクの情報と一致しなくなり、以下のメッセージが 30 分毎に出力され続けます。

```
smartd[XXXXX]: Device: /dev/YYY, No such device, open() failed
```

XXXXX および YYY：環境により出力が異なる部分

このため、smartd サービスを利用している場合はハードディスクの活性保守前に smartd サービスを停止し、活性保守後に最新のハードディスクの状態で smartd サービスを再開させる必要があります。

対処方法を以下に示します。

1. ハードディスクの活性保守前に、smartd サービスを停止します。

   smartd サービスの稼動状況を、以下の操作の出力結果で確認します。

   [例：smartd サービスが稼動している場合の出力結果]

   ```
   # /sbin/service smartd status
   smartd (pid XXXXX) is running...
   ```

   XXXXX：環境により出力が異なる部分

   smartd サービスが開始されている場合、以下の操作でサービスを停止します。

   ```
   # /sbin/service smartd stop
   ```

2. ハードディスクの活性保守を実施し、完了させてください。
3. smartd サービスを開始します。

   手順 1 で稼動中の smartd サービスを停止した場合、ハードディスクの活性保守が完了したのち、再開させる必要があります。

   以下の操作で smartd サービスを開始します。

```
# /sbin/service smartd start
```

- SAS ディスクユニットを搭載し、Red Hat Enterprise Linux 5 で標準提供される SAS カード用ドライバ (Fusion MPT SAS Driver) で稼動しているシステムの場合、SAS ディスクの活性交換・活性削除はできません。

  SAS アレイディスクユニットを搭載したシステムでは、本問題は発生しません。

  本問題の修正時期は未定です。

  なお、有償サポート・サービス (SupportDesk Standard) を契約されているお客様は、サービスで提供される「富士通 Linux サポートパッケージ(FJ-LSP)」内の「富士通拡張ドライバ」を導入することにより、本問題が回避されます。

4.2 ディスクの追加・削除・交換

ディスク操作コマンドを使用した、ハードディスクの追加・削除・交換の手順を以下に示します。ここでは、SASU の内蔵ハードディスクの操作を例としています。ディスク操作コマンドで表示される装置名は、iocx が SGPIO コントローラーで、/dev/sdx がハードディスクです。

4.2.1 追加の手順

ハードディスクを追加する作業手順を以下に示します。

1. SASU の空きスロットにハードディスクを挿入します。
2. ディスク操作コマンドの状態表示でハードディスクが挿入された位置を確認します。

```
# //opt/fujitsu/SVmco/bin/diskctrl -l
```

```
ioc0
0 /dev/sda    Fault LED-Off
1 /dev/sdb    Fault LED-Off
3 /dev/sdc    Fault LED-Off
4 /dev/sdd    Fault LED-Off
```

3. ハードディスクが挿入されると、しばらくしてディスクがアクセスできる状態になります。以下の手順で挿入したスロットを特定してください。

4. ディスク操作コマンドのロケーション表示機能で、Fault LED を点滅させます。

```
# //opt/fujitsu/SVmco/bin/diskctrl -i ioc0/1
```

5. ハードディスクを挿入したスロットの Fault LED が点滅しているか確認します。

スロットの位置が正しい場合は、ディスク操作コマンドの状態表示機能で、"Fault LED-Identify" と表示されるスロットを確認します。

```
# //opt/fujitsu/SVmco/bin/diskctrl -l
ioc0
0 none
1 none  Fault LED-Identify
```

備考

手順 4.でスロットの位置が違っている場合：

ディスク操作コマンドのロケーション消灯機能で、Fault LED の点滅をオフにします。

```
# //opt/fujitsu/SVmco/bin/diskctrl -o ioc0/1
```

別のスロットを指定して、正しいスロット位置が確認できるまで手順 3.～手順 4.を繰り返します。

4.2.2 削除の手順

ハードディスクを取り外す手順を以下に示します。

1. 削除対象のハードディスクが raw、swap の各デバイスに指定されているパーティションを含んでいる場合、以下の操作をします。

   - raw デバイスを含んでいる場合：

     削除対象のハードディスクに raw デバイスで運用しているパーティションが含まれている場合、このパーティションに raw アクセスする可能性があるアプリケーションをすべて終了してからハードディスクを削除してください。

   - swap デバイスを含んでいる場合：

     削除対象のハードディスクに swap デバイスに指定されているパーティションが含まれている場合、システムを停止してからハードディスクを削除してください。

2. 以下の操作をします。削除対象のハードディスクが PRIMECLUSTER GDS で Mirror 構成を組んでいるかいないかによって、操作が異なります。

   - PRIMECLUSTER GDS で Mirror 構成を組んでいる場合：

     PRIMECLUSTER GDS から切り離すディスクを選択し、切り離します。切り離し手順については、PRIMECLUSTER GDS のマニュアルを参照してください。

   - PRIMECLUSTER GDS で Mirror 構成を組んでいない場合：

     削除対象ディスクでマウントしているすべてのディスクパーティションをアンマウントします。

     ```
     # umount /dev/sdc1
     ```

```
# umount /dev/sdc2
        .
        .
        .
```

備考

raw、swap の各デバイスとして運用していたパーティションはアンマウントする必要はありません。ただし、削除したデバイスに対する raw デバイスの設定変更、swap デバイスの設定変更は必要です。

3. ディスク操作コマンドでディスクの回転を停止させます。

   ディスク操作コマンドを実行するとは、以下の処理をします。

   - ハードディスクの回転停止、および Fault LED (Amber) の点灯
   - OS に対する対象ディスクの削除指示

```
# //opt/fujitsu/SVmco/bin/diskctrl -e /dev/sdc
```

4. Fault LED (Amber) が点灯している位置のハードディスクを取り外します。内蔵ハードディスクを取り外した場合は、スロットの奥にある Fault LED が点灯します。Fault LED は、パーティションを電源オフまたはリブートするか、ディスク操作コマンドでオフにしない限り、点灯または点滅します。

   注意

   SSD の場合、SSD を取り出した時に、SVagent を出力元とした「W 13139」のメッセージがシステムイベントログに出力されることがあります。

   ディスク操作コマンドで Fault LED を消灯させる場合は、以下の操作をします。

   1) ディスク操作コマンドで状態を表示し、Fault LED が点灯している位置を確認します。

```
# //opt/fujitsu/SVmco/bin/diskctrl -l
```

```
ioc0
0 /dev/sda    Fault LED-Off
1 /dev/sdb    Fault LED-Off
2 none        Fault LED-On
3 /dev/sdd    Fault LED-Off
```

例に示す内容では、ioc0 のスロット 2 の Fault LED が点灯しており、sdc が踏査されていた位置であることが確認できます。

2) 以下のディスク操作コマンドで Fault LED を消灯します。

```
# //opt/fujitsu/SVmco/bin/diskctrl -o ioc0/2
```

Fault LED が消灯します。

ディスク操作コマンドで状態を表示します。

ioc0 のスロット 2 の装置名に none が表示され、そのスロットが空きであることが確認できます。

```
# //opt/fujitsu/SVmco/bin/diskctrl -l
ioc0
0 /dev/sda    Fault LED-Off
1 /dev/sdb    Fault LED-Off
2 none
3 /dev/sdd    Fault LED-Off
```

4.2.3 交換の手順 (ハードディスクが無応答となる故障以外の場合)

ハードディスクの故障や、S.M.A.R.T.による予兆検出によって、ハードディスクを交換する手順を以下に示します。

1. 交換対象のハードディスクが raw、swap の各デバイスに指定されているパーティションを含んでいる場合、以下の操作をします。

   - raw デバイスを含んでいる場合：

     交換対象のハードディスクに raw デバイスで運用しているパーティションが含まれている場合、このパーティションに raw アクセスする可能性があるアプリケーションをすべて終了してからハードディスクを交換してください。

   - swap デバイスを含んでいる場合：

     交換対象のハードディスクに swap デバイスに指定されているパーティションが含まれている場合、システムを停止してからハードディスクを交換してください。

2. 以下の操作をします。交換対象のハードディスクが PRIMECLUSTER GDS で Mirror 構成を組んでいるかいないかによって、操作が異なります。

   - GDS で Mirror 構成を組んでいる場合：
     PRIMECLUSTER GDS から切り離すディスクを選択し、切り離します。
     切り離し手順については、PRIMECLUSTER GDS のマニュアルを参照してください。

   - GDS で Mirror 構成を組んでいない場合：
     交換対象ディスクでマウントしているすべてのディスクパーティションをアンマウントします。

```
# umount /dev/sdc1
# umount /dev/sdc2
        ・
        ・
        ・
```

備考

raw、swap の各デバイスとして運用していたパーティションは、アンマウントする必要はありません。

3. ディスク操作コマンドでディスクの回転を停止させます。

   ディスク操作コマンドを実行すると、以下の処理をします。

   - ハードディスクの回転停止、および Fault LED (Amber) の点灯
   - OS に対する対象ディスクの削除指示

```
# //opt/fujitsu/SVmco/bin/diskctrl -e /dev/sdc
```

   Fault LED (Amber) が点灯している位置のハードディスクを取り外します。

4. ディスク操作コマンドで状態を表示し、Fault LED が点灯している位置を確認します。

```
# //opt/fujitsu/SVmco/bin/diskctrl -l
ioc0
0 /dev/sda    Fault LED-Off
1 /dev/sdb    Fault LED-Off
2 --mount     Fault LED-On
3 /dev/sdd    Fault LED-Off
```

5. ディスクを交換します。

ioc0 のスロット 2 に Fault LED が点灯しており、ハードディスクが挿入された位置であることが確認できます。

以下のディスク操作コマンドで Fault LED を消灯させます。

```
# //opt/fujitsu/SVmco/bin/diskctrl -c ioc0/2
```

注意

SSD の場合、SSD を取り出した時に、SVagent を出力元とした「W 13139」のメッセージがシステムイベントログに出力されることがあります。

ディスク操作コマンドの状態表示でハードディスクが挿入された位置を確認します。

```
# //opt/fujitsu/SVmco/bin/diskctrl -l
ioc0
0 /dev/sda    Fault LED-Off
1 /dev/sdb    Fault LED-Off
2 /dev/sdc    Fault LED-Off
3 /dev/sdd    Fault LED-Off
```

6. ディスク操作コマンド完了後、ディスクパーティションのマウント、または PRIMECLUSTER GDS で Mirror 構成を組んでいた場合は、PRIMECLUSTER GDS に組み込みます。

7. raw の各デバイスを復旧させる場合は、以下の操作をします。

   ○ raw デバイスを含んでいた場合：

   交換後のハードディスクに raw アクセスするアプリケーションのマニュアルを参照して、raw デバイスを設定してください。設定完了後、交換前に終了したアプリケーションを起動してください。

備考

sadump のダンプデバイスを含んでいた場合、ダンプデバイスの再設定を行うために以下のコマンドを実行してください。

```
#service sadump searchdisk
```

4.2.4 交換の手順 (ハードディスクが無応答となる故障の場合)

ハードディスクの故障で無応答となり、ドライバによるリカバリーが不可能な場合に、ハードディスクを交換する手順を以下に示します。

1. ハードディスクが無応答となる故障の場合、SVagent が検出した以下のメッセージが出力され、ハードディスクの Fault LED が点灯します。

RHEL5 の場合：

```
SVagent: E 14134 IOB#n-HDD#n scsi:%h:%c:%i:%l ¥
Device error (offlined) vendor=xxxxxxxx ¥
model=xxxxxxxx serial-no=xxxxxxxxxx ¥
SCSI 番号： %h=host 番号、%c=channel 番号、¥
%i=id 番号、%l=lun 番号
```

行末の¥は、改行しないことを表す。

2. ディスク操作コマンドで状態を確認します。このとき、Fault LED が On になっているものがオフラインエラーが発生したディスク (*) です。

○ RHEL5：

SASU 内蔵ディスクの場合

```
# //opt/fujitsu/SVmco/bin/diskctrl -l
ioc0
0 /dev/sda Fault LED-Off
1 /dev/sdb Fault LED-Off
2 --mount  Fault LED-On  ←(*)
3 /dev/sdd Fault LED-Off
```

3. 交換対象のハードディスクが raw、swap の各デバイスに指定されているパーティションを含んでいる場合、以下の操作をします。

○ **raw デバイスを含んでいる場合**:

交換対象のハードディスクに raw デバイスで運用しているパーティションが含まれている場合、このパーティションに raw アクセスする可能性

があるアプリケーションをすべて終了してからハードディスクを交換してください。

- swap デバイスを含んでいる場合：

  交換対象のハードディスクに swap デバイスに指定されているパーティションが含まれている場合、システムを停止してからハードディスクを交換してください。

4. 以下の操作をします。交換対象のハードディスクが PRIMECLUSTER GDS で Mirror 構成を組んでいるかいないかによって、操作が異なります。

   - GDS で Mirror 構成を組んでいる場合：

     PRIMECLUSTER GDS から切り離すディスクを選択し、切り離します。切り離し手順については、PRIMECLUSTER GDS のマニュアルを参照してください。

   - GDS で Mirror 構成を組んでいない場合：

     交換対象ディスクでマウントしているすべてのディスクパーティションをアンマウントします。

```
# umount /dev/sdc1
# umount /dev/sdc2
        .
        .
        .
```

備考

raw、swap の各デバイスとして運用していたパーティションは、アンマウントする必要はありません。

5. ディスク操作コマンドでディスクの回転を停止させます。手順 3.で確認したスロットを指定してディスクの回転を停止させます。

```
# /opt/Svmco/bin/diskctrl -e ioc0/2
```

6. Fault LED (アンバー) が点灯している位置のハードディスクを交換します。

7. 例に示す内容では、ioc0 のスロット 2 の Fault LED が点灯しており、ハードディスクが挿入された位置であることが 確認できます。

   以下のディスク操作コマンドで Fault LED を消灯させます。

```
# //opt/fujitsu/SVmco/bin/diskctrl -c ioc0/2
```

8. ディスク操作コマンドの状態表示でハードディスクが挿入された位置を確認します。

```
# //opt/fujitsu/SVmco/bin/diskctrl -l
ioc0
0/dev/sda  Fault LED-Off
1/dev/sdb  Fault LED-Off
2/dev/sdc  Fault LED-Off
3/dev/sdd  Fault LED-Off
```

9. ディスク操作コマンド完了後、ディスクパーティションのマウント、または PRIMECLUSTER GDS で Mirror 構成を組んでいた場合は、PRIMECLUSTER GDS に組み込みます。

10. raw の各デバイスを復旧させる場合は、以下の操作をします。

    - **raw デバイスを含んでいた場合**:

      交換後のハードディスクに raw アクセスするアプリケーションのマニュアルを参照して、raw デバイスを設定してください。設定完了後、交換前に終了したアプリケーションを起動してください。

5 Windows における PCI カードの活性保守

本章では、Windows における PCI カードのホットプラグ手順について説明します。なお、ホットプラグは Windows Server 2008/2012 のみでサポートしています。

5.1 活性保守の概要

ホットプラグの手順には、すべてのカードに共通な部分と、そのカードの機能や使用するドライバによって手順が追加される部分があります。ここでは、すべてのカードに必要な操作と、特定の種類のカードを特定のソフトウェアと組み合わせた場合の両方について説明します。

■ ホットプラグの概要

Windows Server 2008/2012 でサポートするホットプラグはカードの追加・交換です。カードの交換のさいに必要となる OS 上のコマンドと、実際のハードウェアの操作を示します。全体の流れについては、「5.1.1 全体の流れ」を参照してください。

■ ホットプラグの共通手順

すべての PCI カードについて、共通に必要な交換の手順を具体的に示します。PCI カードのホットプラグの共通手順については、「5.2 PCI カードのホットプラグの共通手順」を参照してください。

■ 個別のカードのホットプラグの手順

追加の手順が必要なカードに関する手順を示します。ここでは、ネットワークカード (以降、NIC と表記) と、ファイバチャネルカード (以降 FC カードと表記) の手順を記述しています。NIC のホットプラグについては、「5.3 NIC のホットプラグ」を参照してください。FC カードのホットプラグについては、「5.4 FC カードのホットプラグ」を参照してください。

上記以外のカードで個別の手順を必要とする場合には、関連するハードウェア、ソフトウェアのマニュアル、ならびに本章を参考にして作業してください。また、通常、これらのカード (NIC、FC カード) は、二重化ソフトウェア (Intel PROSET/ETERNUS マルチパスドライバ) と組み合わせて使用します。本章では、これらの二重化ソフトウェアと組み合わせた場合と単独で運用する場合の両方の手順を説明します。

注意

手順には、関連ソフトウェアに対する操作を記述しています。構成によっては手順が異なったり、追加の操作が必要になったりする場合があります。実際に作業をする場合には、必ず関連製品のマニュアルを参照してください。

5.1.1 全体の流れ

ホットプラグの全体の流れを示します。

以下の手順は現在の Windows Server 2008 の PCI ホットプラグサポートにおける、すべての種類のカードにおいて必要な手順です。特定の種類の PCI カードで必要となる操作があるときは、手順の中で説明します。操作の内容は、カードの種類と組み合わせるソフトウェアによって異なります。

なお、fjpciswap コマンドの詳細については、「3.6 PCI カード操作コマンド (fjpciswap) 」を参照してください。

■ 交換の手順

1. fjpciswap コマンド表示機能を利用して、物理位置を確認します。
2. fjpciswap コマンド交換機能を利用して、PCI カードを交換します。
3. fjpciswap コマンド表示機能を利用して、交換したカードを確認します。

■ 追加の手順

1. fjpciswap コマンド追加機能を利用して、PCI カードを追加します。
2. fjpciswap コマンド表示機能を利用して、追加したカードを確認します。

5.2 PCI カードのホットプラグの共通手順

付加手順がない場合 (二重化アプリケーションを使用していないなど) の PCI カードの交換手順は、以下のとおりです。

注意

PCI カードを挿入するさいは、確実に挿入してください。

5.2.1 交換の手順

1. fjpciswap コマンド表示機能を利用して、物理位置を確認します。

```
C:¥>fjpciswap -l


Replaceable PCI cards are displayed
UnitName        Func      DeviceName
IOB#1-PCIC#5    FUNC#0    Intel(R) PRO/1000 PT Dual Port Server
Adapter #15
IOB#1-PCIC#5    FUNC#1    Intel(R) PRO/1000 PT Dual Port Server
Adapter #16
```

```
C:¥>
```

2. fjpciswap コマンド交換機能を利用して、PCI カードを交換します。

```
C:¥>fjpciswap -r IOB#1-PCIC#5
Selected card name is
         Intel(R) PRO/1000 PT Dual Port Server Adapter #15
         Intel(R) PRO/1000 PT Dual Port Server Adapter #16

Please delete all settings about this card
Do you want to remove this card?(y/n)
y ←ユーザー入力
```

"Do you want to remove this card? (y/n) " と表示されたら、[y] キーを押します。

```
Removing the card....
The card has removed.


Please replace the card, and input "y" key.
```

"Please replace the card" と表示されたら、PCI カードを交換します。

```
Please replace the card, and input "y" key.
y
Adding the card.....
The card has added.
```

```
C:￥>
```

PCI カードの交換終了後、 [y] キーを押します。

3. fjpciswap コマンド表示機能を利用して、交換したカードを確認します。

```
C:¥>fjpciswap -l


Replaceable PCI cards are displayed
UnitName        Func      DeviceName
IOB#1-PCIC#5    FUNC#0    Intel(R) PRO/1000 PT Dual Port Server
Adapter #15
IOB#1-PCIC#5    FUNC#1    Intel(R) PRO/1000 PT Dual Port Server
Adapter #16


C:¥>
```

5.2.2 追加の手順

1. fjpciswap コマンド追加機能を利用して、PCI カードを追加します。

   PCI カードを実装するカードスロットに実装した後、該当の PCI カードスロットを指定し追加コマンド (-a) を実行します。

```
C:￥>fjpciswap -a IOB#1-PCIC#5
Adding the card.....................
```

2. OS に認識され、コマンドが完了します。

```
C:￥>fjpciswap -a IOB#1-PCIC#5
Adding the card.....
The card has added.

C:￥>
```

3. fjpciswap コマンド表示機能を利用して、追加したカードを確認します。

```
C:￥>fjpciswap -l

Replaceable PCI cards are displayed
UnitName        Func      DeviceName
IOB#1-PCIC#5    FUNC#0    Intel(R) PRO/1000 PT Dual Port Server Adapter #15
IOB#1-PCIC#5    FUNC#1    Intel(R) PRO/1000 PT Dual Port Server Adapter #16

C:￥>
```

5.2.3 削除について

注意

Windows では PCI カードの削除をサポートしていません。

5.3 NIC のホットプラグ

NIC のホットプラグ (交換) をする場合、「5.2 PCI カードのホットプラグの共通手順」で記述した手順に加えて、さらに特別に考慮する点があります。

以下、チーミングと組み合わせる場合について説明します。

なお、fjpciswap コマンドの詳細については「3.6　PCI カード操作コマンド (fjpciswap) 」を参照してください。

5.3.1 チーミングに組み込まれている NIC のホットプラグ

ここでは、NIC がチーミングに組み込まれている場合のホットプラグの手順を説明します。

注意

- 必ず切離し操作後にホットプラグを実行してください。切り離しをしない場合、OS が停止することがあります。
- Intel PROSet (R) を使用したチーミングに関して、留意事項があります。留意事項については、『PQ1000 シリーズ　運用管理マニュアル』（C122-E108）の「G.10 NIC (ネットワークインターフェースカード)」を参照してください。

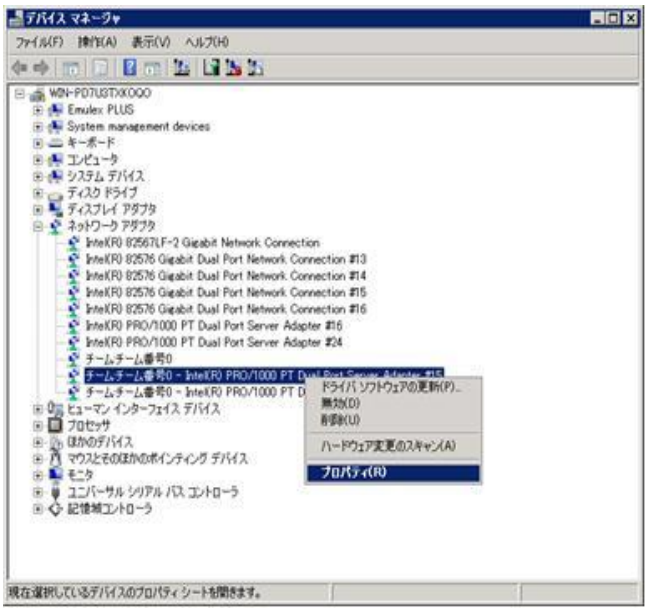
1. fjpciswap コマンド表示機能を利用して物理位置の確認をします。ここでは IOB-PCIC#5 を交換の対象とします。

```
C:¥>fjpciswap -l


Replaceable PCI cards are displayed
```

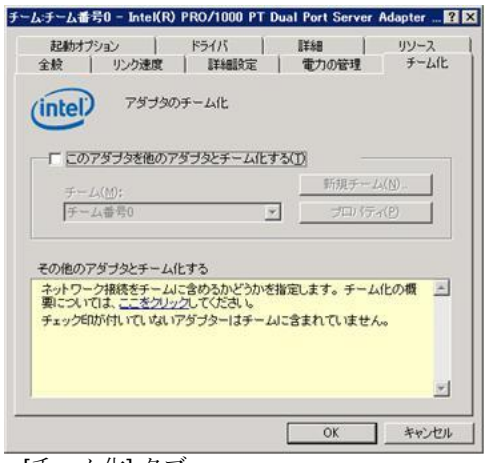
```
UnitName        Func      DeviceName
IOB#1-PCIC#4    FUNC#0    Emulex LightPulse LPe1250-F8, PCI Slot 4, ¥
Storport Miniport Driver
IOB#1-PCIC#5    FUNC#0    チーム:チーム番号 0 - Intel(R) PRO/1000 PT ¥
Dual Port Server Adapter #15
IOB#1-PCIC#5    FUNC#1    Intel(R) PRO/1000 PT Dual Port Server ¥
Adapter #16
IOB#1-PCIC#7    FUNC#0    チーム:チーム番号 0 - Intel(R) PRO/1000 PT ¥
Dual Port Server Adapter #23
IOB#1-PCIC#7    FUNC#1    Intel(R) PRO/1000 PT Dual Port Server Adapter #24


C:¥>
```

行末の¥は、改行しないことを表す。

2. デバイスマネージャから削除するインターフェースを選択し、プロパティを参照します。



3. "チーム化" タブを選択し、"このアダプタを他のアダプタとチーム化する" チェックボックスを外し、[OK] ボタンをクリックします。



[チーム化] タブ

4. 下記のメッセージが表示されるので、[はい] ボタンをクリックします。

[アダプタのチーム化] のプロパティ

5. fjpciswap コマンド表示機能を利用して Device Name を確認します。チーミングに組み込まれていないことを確認してください。

```
C:¥>fjpciswap -l

Replaceable PCI cards are displayed
UnitName        Func      DeviceName
IOB#1-PCIC#4    FUNC#0    Emulex LightPulse LPe1250-F8, PCI Slot 4, ¥
Storport Miniport Driver
IOB#1-PCIC#5    FUNC#0    Intel(R) PRO/1000 PT Dual Port Server Adapter #15
IOB#1-PCIC#5    FUNC#1    Intel(R) PRO/1000 PT Dual Port Server Adapter #16
IOB#1-PCIC#7    FUNC#0    チーム:チーム番号 0 - Intel(R) PRO/1000 PT ¥
Dual Port Server Adapter #23
IOB#1-PCIC#7    FUNC#1    Intel(R) PRO/1000 PT Dual Port Server Adapter #24

C:¥>
```

行末の¥は、改行しないことを表す。

6. fjpciwap コマンドで該当 NIC を交換します。

```
C:¥>fjpciswap -r IOB#1-PCIC#5
Selected card name is
```

```
              Intel(R) PRO/1000 PT Dual Port Server Adapter #15
              Intel(R) PRO/1000 PT Dual Port Server Adapter #16

Please delete all settings about this card
Do you want to remove this card?(y/n)
y
Removing the card......
The card has removed.

Please replace the card, and input "y" key.
y
Adding the card..............
The card has added.



C:¥>
```

"Please replace the card" と表示されたら、NIC を交換し、ケーブルを挿します。
NIC の交換終了後、 [y] キーを押します。

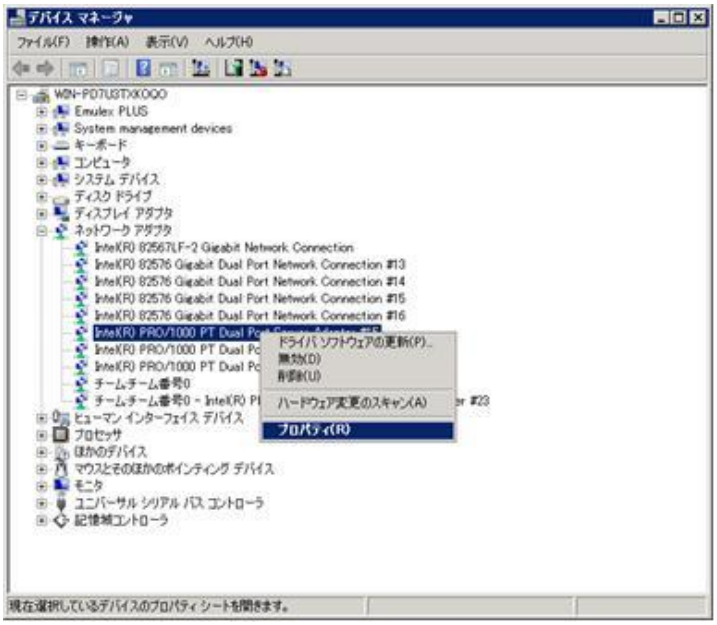
7. fjpciswap コマンド表示機能を利用して、正常に交換されていることを確認します。

```
C:¥>fjpciswap -l

Replaceable PCI cards are displayed
UnitName        Func      DeviceName
IOB#1-PCIC#4    FUNC#0    Emulex LightPulse LPe1250-F8, PCI Slot 4, ¥
Storport Miniport Driver
IOB#1-PCIC#5    FUNC#0    Intel(R) PRO/1000 PT Dual Port Server
```

```
Adapter #15

IOB#1-PCIC#5    FUNC#1    Intel(R) PRO/1000 PT Dual Port Server
Adapter #16

IOB#1-PCIC#7    FUNC#0    チーム:チーム番号 0 - Intel(R) PRO/1000 PT ¥

Dual Port Server Adapter #23

IOB#1-PCIC#7    FUNC#1    Intel(R) PRO/1000 PT Dual Port Server
Adapter #24


C:¥>
```

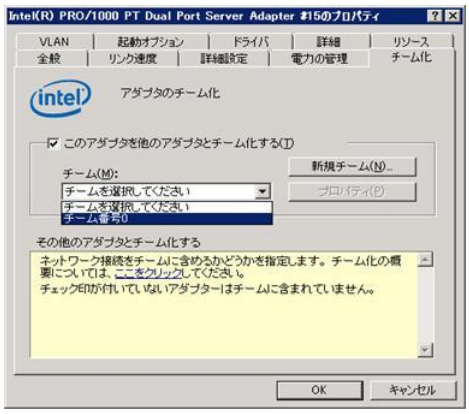
行末の¥は、改行しないことを表す。

8. 交換完了後、デバイスマネージャを開き、チーミングに組み込む NIC のプロパティを開きます。



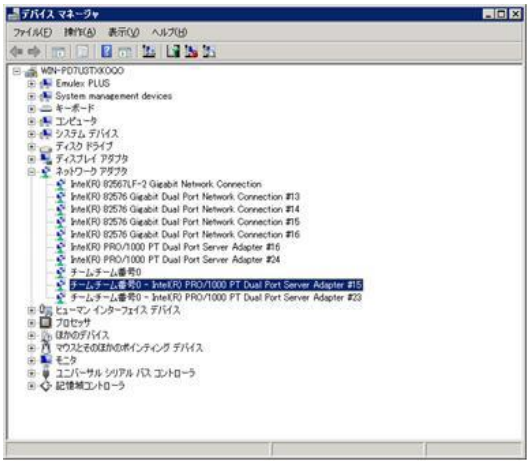
[デバイスマネージャ] 画面

9. "チーム化" タブで "このアダプタを他のアダプタとチーム化する" を選択し、交換前に組み込まれていたチームを選択して [OK] ボタンをクリックします。



[チーム化] タブ

10. デバイスマネージャ上でチームに組み込まれていることを確認します。



[デバイスマネージャ] 画面

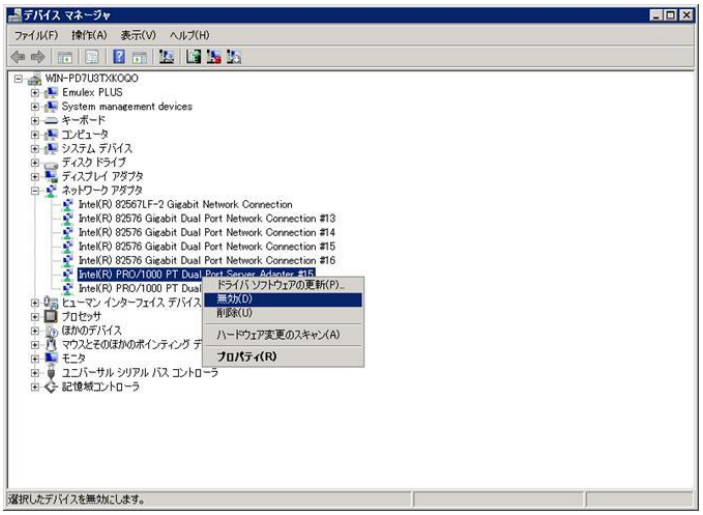
5.3.2 冗長化されていない NIC のホットプラグ

ここでは、ネットワークが冗長化されていない (NIC がチーミングに組み込まれていない) 場合の、ホットプラグの手順を説明します。

1. fjpciswap コマンド表示機能を利用して、物理位置の確認をします。ここでは IOB#1-PCIC#5 を交換の対象とします。

```
C:¥>fjpciswap -l

Replaceable PCI cards are displayed

UnitName        Func       DeviceName

IOB#1-PCIC#5    FUNC#0     Intel(R) PRO/1000 PT Dual Port Server Adapter
#15

IOB#1-PCIC#5    FUNC#1     Intel(R) PRO/1000 PT Dual Port Server Adapter
#16


:¥>
```

2. デバイスマネージャを使用し、該当のデバイスを無効にします。



3. fjpciwap コマンドで該当 NIC を交換します。

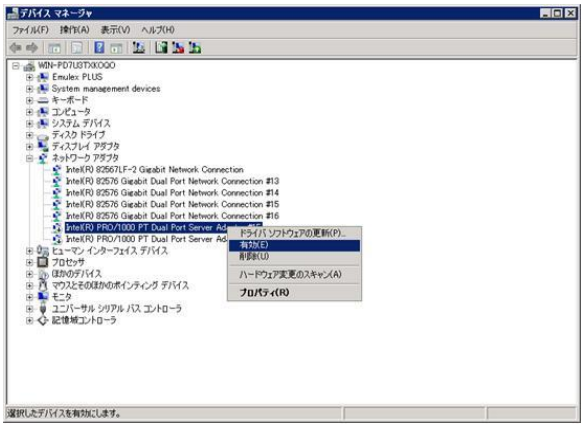
```
C:¥>fjpciswap -r IOB#1-PCIC#5
Selected card name is
              Intel(R) PRO/1000 PT Dual Port Server Adapter #15
              Intel(R) PRO/1000 PT Dual Port Server Adapter #16

Please delete all settings about this card
Do you want to remove this card?(y/n)
y
Removing the card....
The card has removed.

Please replace the card, and input "y" key.
y
Adding the card..............
The card has added.



C:¥>
```

"Please replace the card" と表示されたら、NIC を交換し、ケーブルを挿します。
NIC の交換終了後、[y] キーを押します。

4. コマンドプロンプトを起動します。fjpciaswap コマンドを使用し、PCI カード活性交換可能 PCI カードのリストを表示します。追加したカードが正しく表示されていることを確認します。

```
C:¥>fjpciswap -l

Replaceable PCI cards are displayed
UnitName        Func      DeviceName
IOB#1-PCIC#5    FUNC#0    Intel(R) PRO/1000 PT Dual Port Server Adapter #15
IOB#1-PCIC#5    FUNC#1    Intel(R) PRO/1000 PT Dual Port Server Adapter #16

C:¥>
```

5. 下図のように、デバイスマネージャで該当のデバイスを右クリックし、表示されるメニューに [有効] がある場合は有効にします ([無効] の場合は本作業は不要です)。



5.3.3 NIC の追加手順

「5.2　PCI カードのホットプラグの共通手順」を参照して、NIC を追加します。

5.4 FC カードのホットプラグ

FC カードのホットプラグ (交換) をする場合「5.2 PCI カードのホットプラグの共通手順」で記述した手順に加えて、さらに特別に考慮する点があります。

FC カードの WWN を FC スイッチや RAID 装置 (ETERNUS) に設定している場合、ホットプラグをすることにより FC カードの WWN が変わります。新しいカードの WWN の再設定の方法は、各装置のマニュアルを参照ください。

以下、ETERNUS マルチパスドライバ (MultiPath Driver: MPD) と組み合わせる場合について説明します。

なお、fjpciswap コマンドの詳細については、「3.6 PCI カード操作コマンド (fjpciswap) 」を参照してください。

注意

- SAN ブートのパスは対象外です。
- LTO ライブラリ装置はサポート対象外です。
- Windows の仕様により、PageFile などが FC カードの接続先に存在する場合は対象外です。
- 交換手順の途中で、イベントログに、ソース：SVagent、ID：25004 のエラーメッセージが出力されることがありますが、問題ありません。

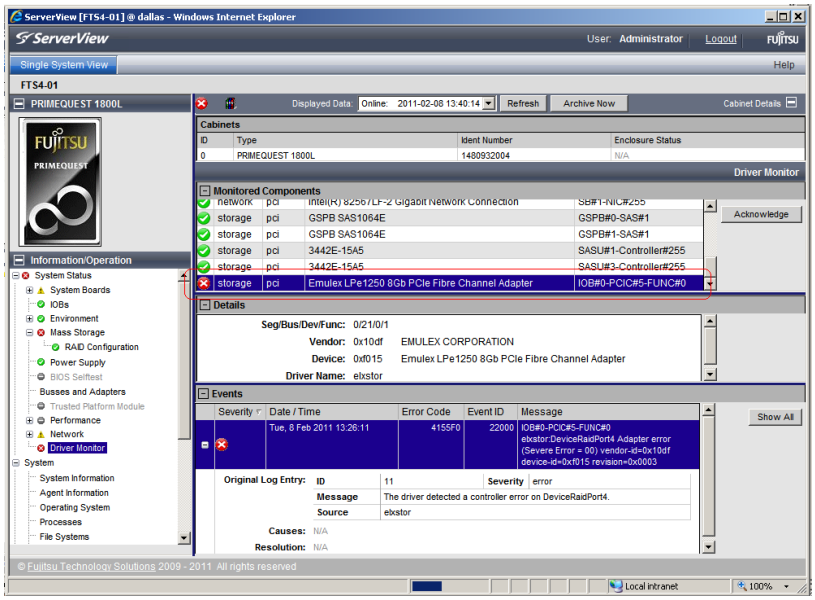
5.4.1 ETERNUS マルチパスドライバに組み込まれている FC カードのホットプラグ

ここでは、FC カードが ETERNUS マルチパスドライバに組み込まれている場合の、ホットプラグ手順を説明します。

1. SVOM の Web-UI から、[System Status] - [Driver Monitor] 画面を参照して、交換対象の FC カードを探します。

交換対象 FC カードは、Unit 名または BUS 番号で検索できます。

IOB#0-PCIC#5 を交換したい場合、対象デバイスは赤枠で囲んだ部分となります。



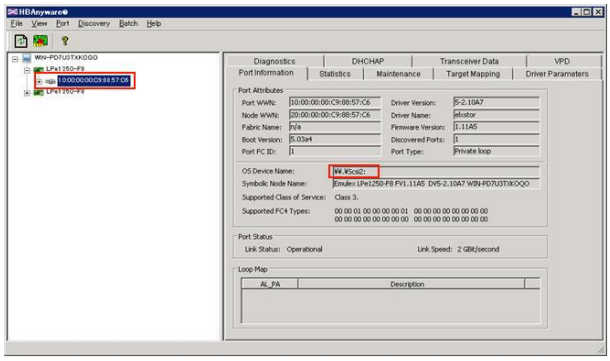
備考

マルチファンクションカードの場合、Unit 名で FUNC 以下のみが異なるものや、"Seg/Bus/Dev/Func" 項で Func 番号のみが異なるものが複数存在します。この場合は、それぞれについて、以降の手順 2.と 3.を実施します。

2. 交換対象 FC カードの UNIT 名を選択し、[Driver Monitor] 画面の Detail を開き、交換デバイスの "WWN (hex)" を記録します。

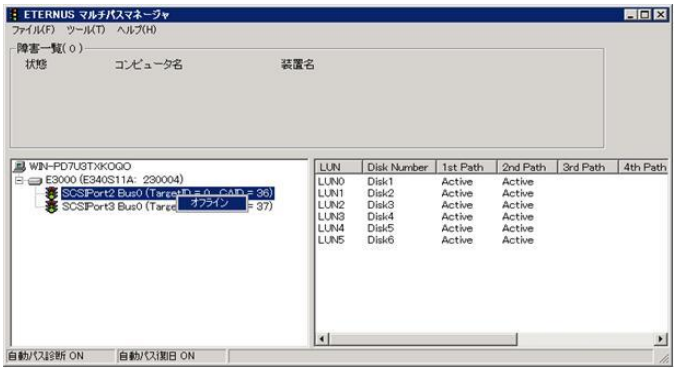
3. HBAnywhere を起動し、手順 2.で求めた WWN をもとにして、交換デバイスのポート番号を求めます。

左ペインから該当する WWN を選択し、右ペインで [Port Information] タブを選択します。OS Device Name に記載されている情報がポート番号です (下記例の場合 ¥¥. ¥Scsi2) 。



HBAnyware

4. ETERNUS マルチパスマネージャを起動し、交換するすべてのデバイスをオフラインにします。



ETERNUS マルチパスマネージャ

5. コマンドを実行して FC カードを交換します。

   ETERNUS マルチパスマネージャと HBAnyware を終了します。fjpciswap コマンド交換機能を使用して、該当カードの replace 操作を行います。

```
C:¥>fjpciswap -r IOB#0-PCIC#5
Selected card name is
Emulex LightPulse LPe1250-F8, PCI Slot 4, Storport Miniport Driver

Please delete all settings about this card
Do you want to remove this card?(y/n)
y
Removing the card.....
The card has removed.

Please replace the card, and input "y" key.
y
Adding the card..............
The card has added.



C:¥>
```

"Please replace the card" と表示されたら、FC カードを交換し、ケーブルを挿します。FC カードの交換終了後、[y] キーを押します。

備考

下記のメッセージで終了することがあります。このメッセージは該当の FC カードを参照しているアプリケーションがある場合やオフラインにしてから replace 操作するまでの時間が短い場合に出力されます。

参照しているアプリケーションがないことを確認し、ない場合は 10 分程度おいてから再度実行してください。なお、構成によりさらに時間がかかる場合があります。

```
C:¥>fjpciswap -r IOB#0-PCIC#5

Selected card name is

              Emulex LightPulse LPe1250-F8, PCI Slot 4, Storport Miniport
              Driver


Please delete all settings about this card

Do you want to remove this card?(y/n)

y

Removing the card...

SVmco : E 08745 internal error :Device_Eject
failed:PCI¥VEN_10DF&DEV_F015& ¥

SUBSYS_F01510DF&REV_03¥8&39e14fc5&0&00000008

0048:23:679


C:¥>
```

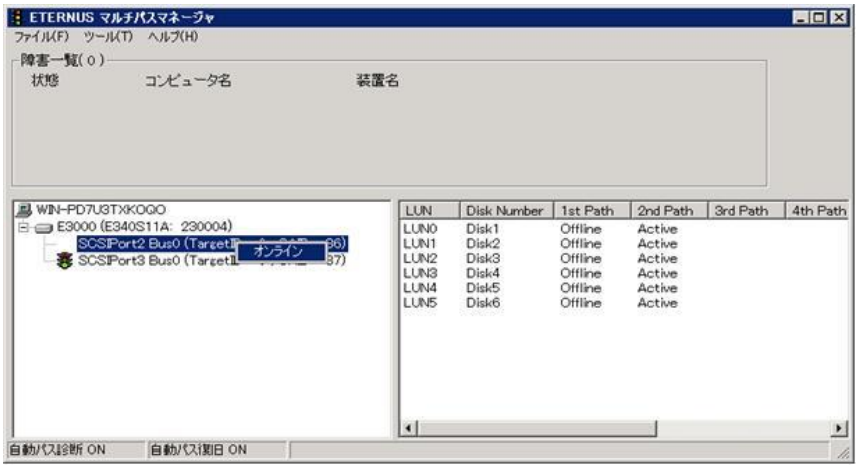
行末の¥は、改行しないことを表す。

6. fjpciswap コマンドで FC カードの導入を確認します。

```
C:¥>fjpciswap -l


Replaceable PCI cards are displayed

UnitName        Func      DeviceName

IOB#0-PCIC#5    FUNC#0    Emulex LightPulse LPe1250-F8, PCI Slot 4, ¥

Storport Miniport Driver

IOB#1-PCIC#6    FUNC#0    Emulex LightPulse LPe1250-F8, PCI Slot 6, ¥

Storport Miniport Driver


C:¥>
```

行末の¥は、改行しないことを表す。

7. ETERNUS マルチパスマネージャを起動し、交換したすべてのデバイスをオンラインにします。デバイスが正常にマルチパスドライバに組み込まれていることを確認します。



ETERNUS マルチパスマネージャ

5.4.2 FC カードの追加手順

「5.2 PCI カードのホットプラグの共通手順」を参照して、FC カードを追加します。

5.5 Windows の iSCSI (NIC) の活性交換

iSCSI (NIC) の活性交換をする場合、以下が前提条件となります。

- Windows Server 2008 以降が対象
- 作業の実施には Administrator 権限が必要
- ETERNUS マルチパスドライバ (MPD) を適用していること
- 複数のカードを交換する場合、1 枚ずつ作業を実施すること

fjpciswap コマンド詳細については「3.6 PCI カード操作コマンド (fjpciswap)」を参照してください。

5.5.1 MPD の組込み確認

ここでは、MPD の組込みを確認する手順を説明します。

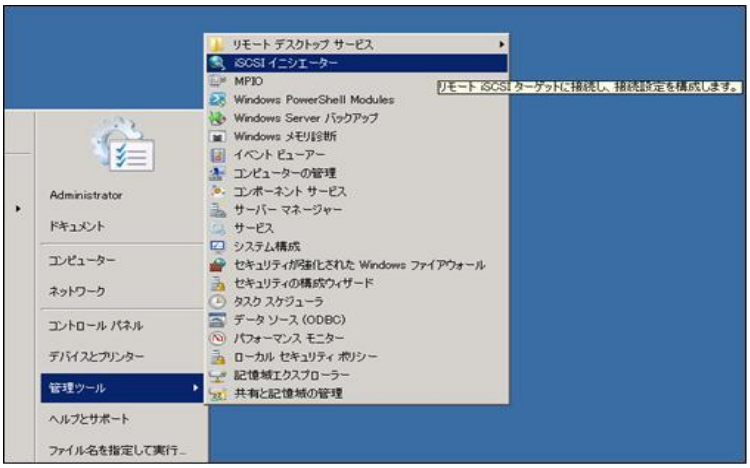
■ Windows Server 2008/2012 の場合

1. MMB の Web-UI から、[System Status] - [Driver Monitor] 画面を参照して、交換対象の NIC を探します。交換対象 NIC は、Unit 名または BUS 番号で検索できます。

   マルチファンクションカードの場合、Unit 名で FUNC 以下のみが異なるものや、[Seg/Bus/Dev/Func] 項で Func 番号のみが異なるものが複数存在します。この場合は、それぞれについて、以降の手順 2～9 を実施します。

2. 交換対象 NIC の UNIT 名を選択し、[Driver Monitor] 画面を開き、MAC アドレスを記録します。また、[System Status] - [Network] - [Network Interface]から記録した MAC アドレスから交換デバイスの検索、および交換後の再設定のために [IP Address (IP v4 Interfaces)] と [IP Subnet Mask] を記録しておきます。

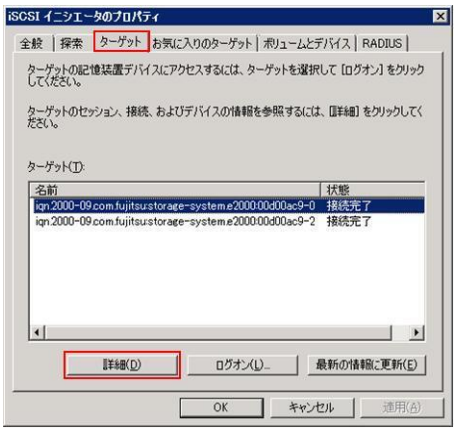
3. iSCSI イニシエーターを起動します。



4. [iSCSI イニシエーターのプロパティ] ウィンドウの [ターゲット] タブをクリックします。

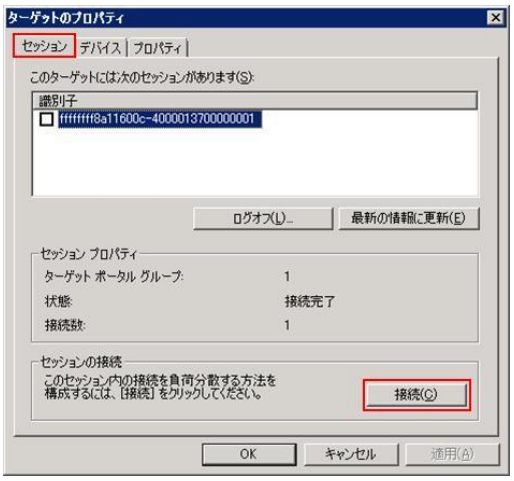
   [ターゲット(T)] に表示されているターゲットのうち、交換対象の NIC と接続しているターゲットがわかっている場合はそのターゲットを選択し、[詳細(D)] ボタンをクリックして手順 8 へ進みます。

   交換対象の NIC と接続しているターゲットがわからない場合は任意のターゲットを選択し、[詳細(D)] ボタンをクリックして手順 5 へ進みます。



[iSCSI イニシエータのプロパティ] 画面 (Windows Server 2008 の場合)

5. [ターゲットのプロパティ] ウィンドウの [セッション] タブをクリックし、[接続(C)] ボタンをクリックします。



6. [セッションの接続] ウィンドウの [ソース ポータル] 欄に表示されている IP アドレスが、手順 2 で記録しておいた IP アドレスと一致するか確認します。

   一致した場合は、このターゲットに結び付けられているデバイスが交換対象であることがわかります (例では、192.168.3.150)。

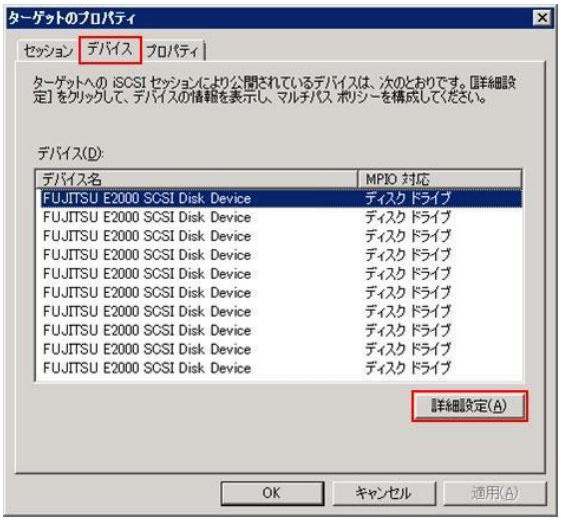
[セッションの接続] 画面

7. 手順 6 で IP アドレスが一致しなかった場合は、以下の作業を繰り返します。

    1. [キャンセル] ボタンをクリックして手順 5 の [ターゲットのプロパティ] ウィンドウに戻ります。
    2. さらに [キャンセル] ボタンをクリックして手順 4 の [iSCSI イニシエーターのプロパティ] ウィンドウに戻ります。
    3. 次のターゲットを選択して手順 4 以降の作業を繰り返します。

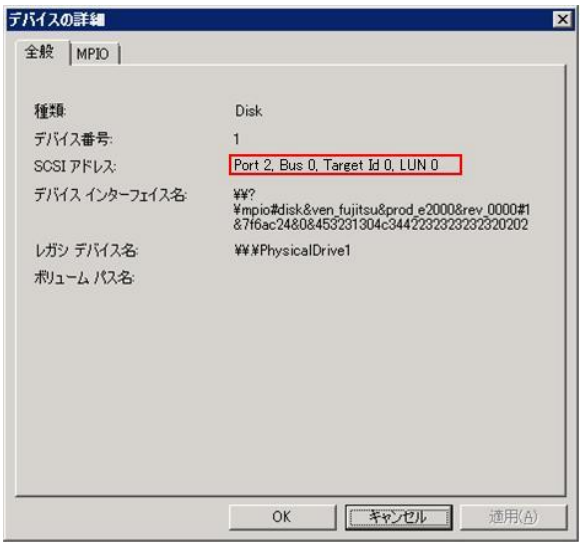
    IP アドレスが一致した場合は、[キャンセル] ボタンをクリックして手順 5 の [ターゲットのプロパティ] ウィンドウへ戻り、手順 8 へ進みます。

8. [ターゲットのプロパティ] ウィンドウの [デバイス] タブをクリックし、[詳細設定(A)] ボタンをクリックします。



[ターゲットのプロパティ] 画面

9. [デバイスの詳細] ウィンドウの [SCSI アドレス] 欄に表示されている値 (例では Port 2: Bus 0: Target 0: LUN 0)を記録しておきます。



[デバイスの詳細] 画面

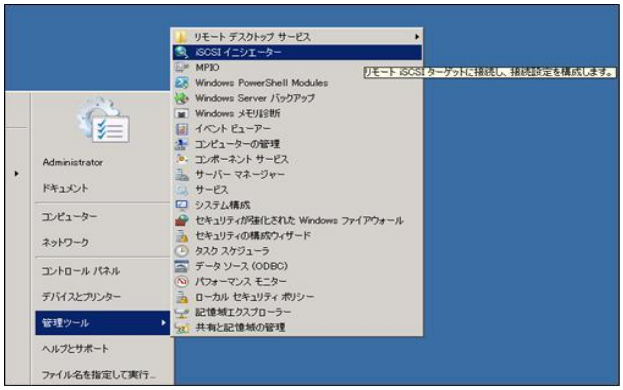
■ Windows Server 2008 R2 以降の場合

1. MMB の Web-UI から、[System Status] - [Driver Monitor] 画面を参照して、交換対象の NIC を探します。交換対象 NIC は、Unit 名または BUS 番号で検索できます。

   マルチファンクションカードの場合、Unit 名で FUNC 以下のみが異なるものや、[Seg/Bus/Dev/Func] 項で Func 番号のみが異なるものが複数存在します。この場合は、それぞれについて、以降の手順 2～9 を実施します。

2. 交換対象 NIC の UNIT 名を選択し、[Driver Monitor] 画面を開き、MAC アドレスを記録します。また、[System Status] - [Network] - [Network Interface]から記録した MAC アドレスから交換デバイスの検索、および交換後の再設定のために [IP Address (IP v4 Interfaces)] と [IP Subnet Mask] を記録しておきます。

3. iSCSI イニシエーターを起動します。



[iSCSI イニシエーター] の起動

4. [iSCSI イニシエーターのプロパティ] ウィンドウの [ターゲット] タブをクリックします。

   [検出されたターゲット(G)] に表示されているターゲットのうち、交換対象の NIC と接続しているターゲットがあらかじめわかっている場合はそのターゲットを選択し、[デバイス(V)] ボタンをクリックして手順 9 へ進みます。

   交換対象の NIC と接続しているターゲットがわからない場合は任意のターゲットを選択し、[プロパティ(P)] ボタンをクリックして手順 5 へ進みます。

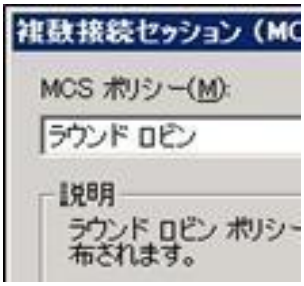
[iSCSI イニシエーターのプロパティ] 画面 (Windows Server 2008 R2 以降の場合)

5. [プロパティ] ウィンドウの [セッション] タブをクリックし、[MCS(M)] ボタンをクリックします。

[プロパティ] 画面

6. [複数接続セッション(MCS)] ウィンドウの [ソース ポータル] に表示されている IP アドレスが、手順 2 で記録しておいた IP アドレスと一致するか確認します。

   一致した場合は、このターゲットに結び付けられているデバイスが交換対象であることがわかります(例では、192.168.3.150)。



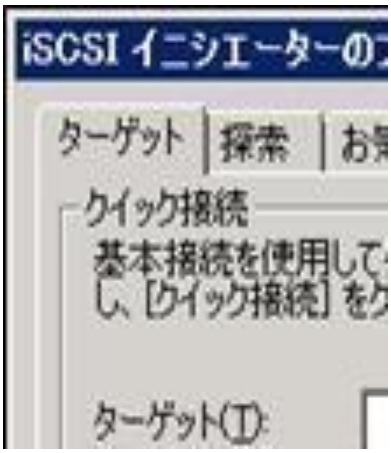
[複数接続セッション (MCS)] 画面

7. [キャンセル(C)] ボタンをクリックして手順 5 の [プロパティ] ウィンドウへ戻ります。

   さらに [キャンセル] ボタンをクリックして手順 4 の [iSCSI イニシエーターのプロパティ] ウィンドウに戻ります。

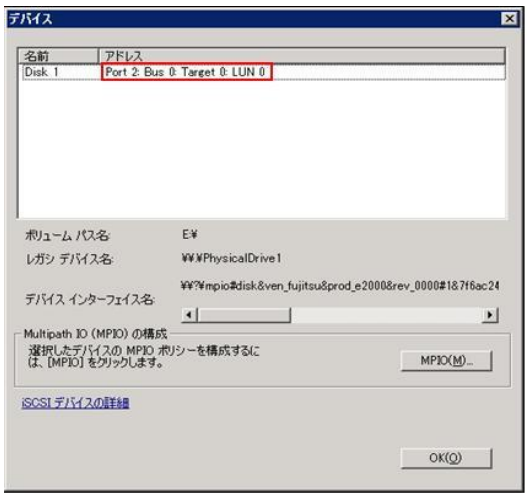
8. 手順 6 で IP アドレスが一致しなかった場合は、次のターゲットを選択して手順 4 以降の作業を繰り返します。

   一致した場合は、[デバイス(V)] ボタンをクリックします。



[iSCSI イニシエーターのプロパティ] 画面 (Windows Server 2008 R2 以降の場合)

9. [デバイス] ウィンドウの [アドレス] 欄に表示されている値 (例では Port 2: Bus 0: Target 0: LUN 0) を記録しておきます。



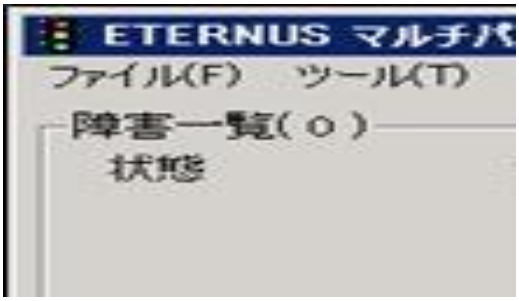
[デバイス] 画面

5.5.2 MPD の切離し作業

ここでは、MPD の切離し作業の手順を説明します。

1. ETERNUS マルチパスマネージャを起動します。

2. 「5.5.1 MPD の組込み確認」の手順 9 で記録しておいたアドレス値を確認して、交換対象のデバイスをオフラインにします。マルチファンクションの場合には複数のデバイスをオフラインにする必要があります。



[ETERNUS マルチパスマネージャ] 画面

3. 「5.3 NIC のホットプラグ」を参照して、NIC を交換します。

備考

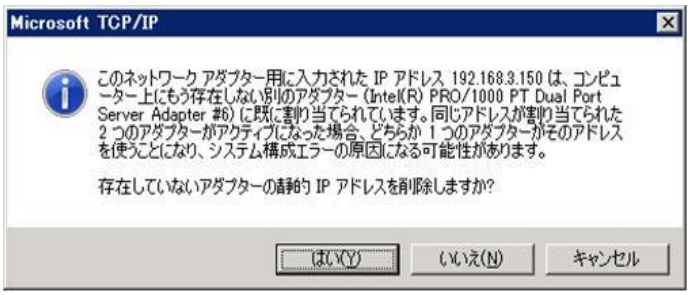
NIC の交換手順の途中で、イベントログに、ソース：SVagent、ID：25004 のエラーメッセージが出力されることがありますが、問題ありません。

4. 交換したデバイスに、IP を設定しなおします。

手順 2 で記録しておいた IP アドレスおよびサブネットマスクを設定しなおします。

備考

IP を設定しなおすさいに、以下のメッセージが表示される場合は、[はい(Y)] ボタンをクリックしてください。

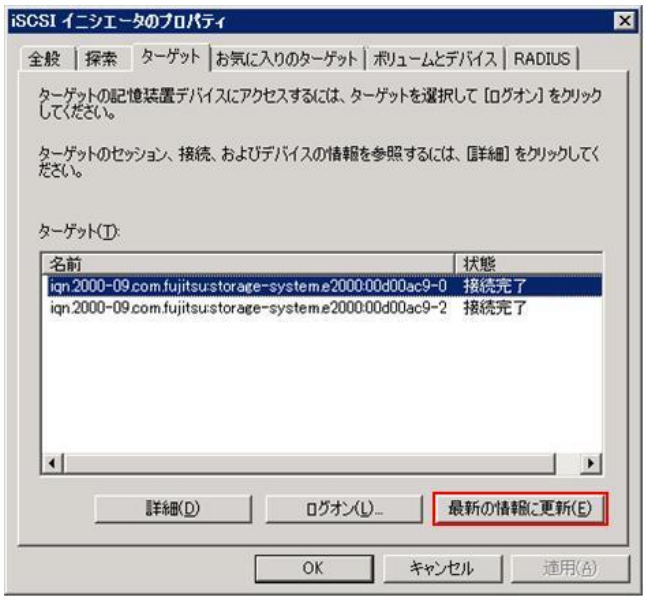


TCP/IP 削除メッセージ

5. [iSCSI イニシエーターのプロパティ] ウィンドウの [ターゲット] タブの、[最新の情報に更新] ボタンをクリックします。

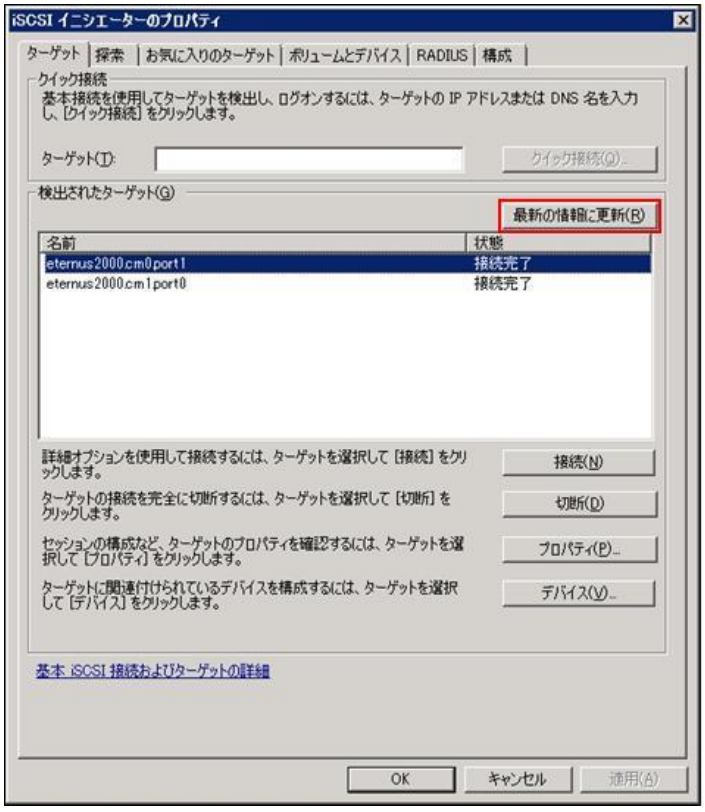
   ターゲットの状態が [接続完了] になることを確認します。

■Windows Server 2008 の場合



[iSCSI イニシエータのプロパティ] 画面 (Windows Server 2008)

■ Windows Server 2008 R2 以降の場合



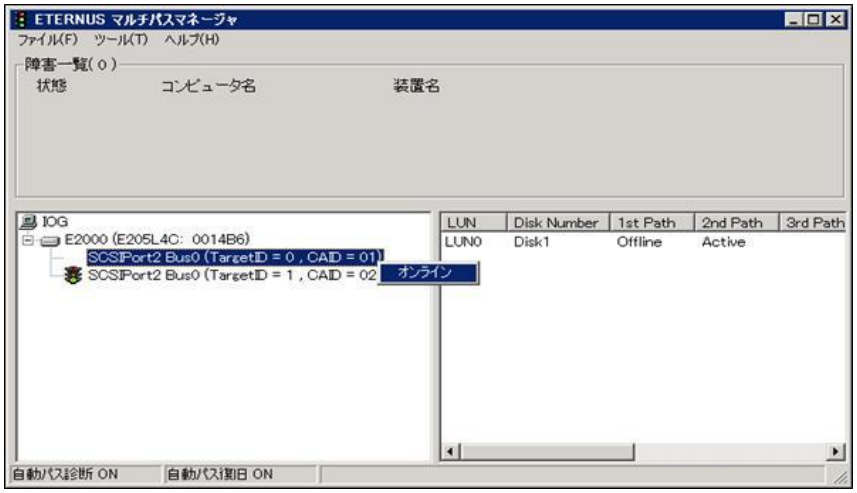
[iSCSI イニシエーターのプロパティ] 画面 (Windows Server 2008 R2 以降の場合)

5.5.3 MPD 組込み作業

ここでは、MPD の組込み作業の手順を説明します。

1. ETERNUS マルチパスマネージャを起動します。

2. 交換したデバイスをオンラインにします。マルチファンクションデバイスの場合はすべてのデバイスをオンラインにします。



ETERNUS マルチパスマネージャ

6 SVmco の手動インストール・アンインストール

本付録では、SVmco の手動インストール・アンインストールについて、OS ごとに説明します。

なお、SVIM を使用して OS をインストールする場合、SVmco の手動インストールは不要です。

6.1 SVmco の手動インストール (Linux: Red Hat Enterprise Linux)

SVmco の Linux OS (Red Hat Enterprise Linux) への手動インストールについて説明します。本設定は root 権限で作業を行ってください。

備考

PRIMEQUEST 1000x2 シリーズ以降の運用時は、必ず SVmco をインストールしてください。SVmco をアンインストールすると、以下の制限があります。

- REMCS 契約時にパーティション上の異常が通知されない。
- ハードディスクの活性保守ができない。必ずパーティション停止保守となる。
- PRIMECLUSTER 連携が使用できない。

6.1.1 インストールの流れ

SVmco のインストールについて詳しくは『ＰＲＩＭＥＱＵＥＳＴ　1000 シリーズ導入マニュアル』「第 4 章 OS および添付ソフトのインストール」を参照してくだ

さい。SVmco の設定については、「2.1 SVmco の設定 (Linux：RedHat Enterprise Linux)」を参照してください。

備考

- MMB の IP アドレスおよびパーティション側の管理 LAN の IP アドレスを変更した場合：
  必ず SVmco を再起動してください。再起動しないと、SVmco で検出するエラーが通知できません。
- SVIM を使用して OS をインストールする場合、SVmco、SIRMS の手動インストールは不要です。ただし、SVIM によるインストール後に、「6.1.2 SVmco インストール前の確認」および「6.1.7　SVmco インストール後の設定」にある各項目の確認および設定を実施する必要があります。

6.1.2 SVmco インストール前の確認

SVmco をインストールする前に確認する項目について説明します。

- PSA-MMB 間通信 LAN の設定確認
- SVmco 動作のための必須機能の確認

6.1.2.1 PSA-MMB 間通信 LAN の設定確認

PSA-MMB 間通信 LAN の設定確認について詳しくは、「2.1.1　PSA-MMB 間通信 LAN の設定」および「2.1.5　管理 LAN IP アドレスの設定」を参照してください。

6.1.2.2 iptables の状態確認

iptables の状態を確認します。

iptables が無効の場合、SVmco インストール時に iptables の設定がされません。必要な場合は iptables を有効にしてください。

6.1.3 SVmco のインストール

6.1.3.1 SVmco 動作に必要なパッケージ

SVmco の動作のためには、以下のパッケージが必要です。

SVmco インストール前に各パッケージがインストールされていることを rpm コマンドで確認してください。

注意：

RHEL5,RHEL6 共通して、X64 環境にインストールする時は、openssl の 32bit パッケージ(openssl-x.x.x-x.x.i686)を必ずインストールしてください。

また、RHEL6 の x64 環境のみ glibc の 32bit パッケージ(glibc-x.x-x.x.i686)をインストールが必要です。

インストールされていない場合は、SVmco が正常に起動出来ません。

パッケージ(RHEL5)

X86	X64
gdb-x.x.x-x.x.i386	gdb-x.x.x-x.x.x86_64
net-snmp-libs-x.x.x.x-x.x.i386	net-snmp-libs-x.x.x.x-x.x.i386
net-snmp-x.x.x.x-x.x.i386	net-snmp-x.x.x.x-x.x.x86_64
net-snmp-utils-x.x.x.x-x.x.i386	net-snmp-utils-x.x.x.x-x.x.x86_64
	openssl-x.x.x-x.x.i686

パッケージ(RHEL6)

X86	X64
gdb-x.x-x.x.i686	gdb-x.x-x.x.x86_64
net-snmp-libs-x.x-x.x.i686	glibc-x.x-x.x.x.i686
net-snmp-x.x-x.x.i686	openssl-x.x.x-x.x_x.x.i686
net-snmp-utils-x.x-x.x.i686	net-snmp-libs-x.x-x.x.i686
	net-snmp-x.x-x.x.x86_64
	net-snmp-utils-x.x-x.x.x86_64

6.1.3.2 SVmco のインストール

以下のコマンドで SVmco パッケージをインストールします。

以下の説明は、作業ディレクトリ (以下、$WORK_DIR と呼びます) 内に SVmco のパッケージ (SVmco-$VER-$REL.tar.gz) が展開された状態を前提としています。

【入力形式】

```
cd $WORK_DIR/SVmco
./INSTALL.sh
```

6.1.4 SVmco インストール時の自動設定

SVmco インストール時に、SVmco 動作のための設定が以下のように自動的に追記または変更されます。

SVmco インストール時に自動追記／変更される設定

対象	動作	備考
syslog.conf ファイル	設定追記	
snmpd.conf ファイル	設定追記	
snmptrapd.conf ファイル	設定追記	
snmptrapd の起動オプション	変更	
snmpd の起動オプション	変更	
PSA-MMB 間専用 LAN インターフェース	IP アドレス設定	「2.1.1　PSA-MMB 間通信 LAN の設定」を参照し、必要に応じて変更す

対象	動作	備考
		る。
iptables 設定	設定追加	手動で SVmco をインストールした場合は、PSA-MMB 間通信用チェインのみ作成される。 「6.1.7　SVmco インストール後の設定」の「ファイアーウォール機能の確認 (ポートの開放)」を参照し、手動で INPUT、OUTPUT チェインに、PSA-MMB 間通信用チェインへのジャンプ設定を追加する。
SELinux 設定ファイル (/etc/selinux/conf)	変更	RHEL5 の場合のみ、SELinux が無効化される。ただし、すでに無効化されている場合は変更しない
SELinux 設定	ポリシー適用	RHEL６．０以降の場合のみ、ポリシーモジュールが追加される。ただし、SELinux が Disable 設定時は本ポリシーモジュールは動作しない。なお、PRIMEQUEST としては、SELinux 有効化での運用はＲＨＥＬ６．２以降となっている。

6.1.5 SIRMS のインストール

以下のコマンドで、SIRMS 関連のパッケージをインストールします。

【入力形式】

```
/bin/rpm -ivh sirms-X.X.X-X.i386.rpm (*)
```

*：X.X.X-X は SIRMS の版数です。

6.1.6 パーティション再起動

SVmco、SIRMS インストール後、リブートによりパーティションを再起動します。

【入力形式】

```
/sbin/reboot
```

6.1.7 SVmco インストール後の設定

ここでは、SVmco をインストールしたあとに設定する項目について説明します。

- SELinux 機能の設定確認
- ファイアーウォール機能の確認 (ポートの開放)
- パーティションからのトラップ送信先の設定
- 複製ディスク使用時の SNMP 設定
- 管理 LAN の設定確認

6.1.7.1 SELinux 機能の設定確認

SELinux 機能の設定確認について詳しくは、「2.1.3 SELinux 機能の設定確認」を参照してください。

6.1.7.2 ファイアーウォール機能の確認 (ポートの開放)

iptables が有効である場合のみ、PSA-MMB 間通信 LAN、管理 LAN に必要な iptables のチェインを自動設定します。iptables が無効の場合は、iptables のチェインが設定されません。その場合は、「2.1.4 ファイアーウォール機能の確認(ポートの開放)」の「PSA-MMB 間通信 LAN 用インターフェースで開放するポート」を参考に、手動で設定する必要があります。

iptables 有効時にインストールすると、PSA-MMB 間通信用のチェイン(以下、PSA-MMB_LAN チェイン)が作成されます。

手動で iptables の INPUT および OUTPUT チェインに、PSA-MMB_LAN チェインへのジャンプ設定を追加してください。設定方法については「■PSA-MMB 間通信 LAN 用インターフェース」を参照してください。

PSA-MMB 間通信 LAN 用のインターフェースに関する設定は必ず設定してください。

6.1.7.3 PSA-MMB 間通信 LAN 用インターフェース

ファイアーウォールの設定は、環境により設定内容が異なるため、ここでは、以下の設定の場合について、PSA-MMB 間通信の設定例を示します。

実施例：INPUT および FORWARD に REJECT 設定がある場合

```
# iptables -L -n
Chain INPUT (policy ACCEPT)
target prot opt source destination
ACCEPT all -- 0.0.0.0/0 0.0.0.0/0 state
RELATED,ESTABLISHED
ACCEPT icmp -- 0.0.0.0/0 0.0.0.0/0
ACCEPT all -- 0.0.0.0/0 0.0.0.0/0
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 state NEW tcp dpt:22
REJECT all -- 0.0.0.0/0 0.0.0.0/0 reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
target prot opt source destination
REJECT all -- 0.0.0.0/0 0.0.0.0/0 reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
target prot opt source destination
```

```
Chain PSA-MMB_LAN (2 references)
target prot opt source destination
ACCEPT all -- 0.0.0.0/0 0.0.0.0/0
ACCEPT all -- 0.0.0.0/0 0.0.0.0/0
ACCEPT icmp -- 0.0.0.0/0 0.0.0.0/0 icmp type 8
ACCEPT icmp -- 0.0.0.0/0 0.0.0.0/0 icmp type 0
ACCEPT udp -- 0.0.0.0/0 0.0.0.0/0 udp dpt:161
ACCEPT udp -- 0.0.0.0/0 0.0.0.0/0 udp spt:161
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp spt:5000
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:5000
```

1. PSA-MMB_LAN チェインが作成されていることを確認します。

```
# /sbin/iptables -L
```

```
# iptables -L 実行結果
Chain INPUT (policy ACCEPT)
target prot opt source destination
ACCEPT all -- 0.0.0.0/0 0.0.0.0/0 state
RELATED,ESTABLISHED
ACCEPT icmp -- 0.0.0.0/0 0.0.0.0/0
ACCEPT all -- 0.0.0.0/0 0.0.0.0/0
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 state NEW tcp dpt:22
REJECT all -- 0.0.0.0/0 0.0.0.0/0 rejectwith icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
target prot opt source destination
REJECT all -- 0.0.0.0/0 0.0.0.0/0 rejectwith
icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
target prot opt source destination
Chain PSA-MMB_LAN (2 references)
target prot opt source destination
ACCEPT all -- 0.0.0.0/0 0.0.0.0/0
ACCEPT all -- 0.0.0.0/0 0.0.0.0/0
ACCEPT icmp -- 0.0.0.0/0 0.0.0.0/0 icmp type 8
ACCEPT icmp -- 0.0.0.0/0 0.0.0.0/0 icmp type 0
ACCEPT udp -- 0.0.0.0/0 0.0.0.0/0 udp dpt: 161
ACCEPT udp -- 0.0.0.0/0 0.0.0.0/0 udp spt: 161
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp spt: 5000
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt: 5000
```

2. INPUT および OUTPUT チェインに PSA-MMB_LAN チェインへのジャンプ設定を追加します。INPUT および OUTPUT チェインにある既存の REJECT 設定や、ユーザー定義のチェインなどに遮断されないように、設定してください。

ここでは、以下のコマンドを使って、INPUT チェインの 5 番目 (REJECT 設定の前)、OUTPUT チェインに追加します。(iptables のオプションの詳細は man マニュアルを参照してください。)

```
# /sbin/iptables –I INPUT 5 –j PSA-MMB_LAN
# /sbin/iptables –A OUTPUT –j PSA-MMB_LAN
```

3. iptables -L コマンドを実行し、INPUT チェインおよび OUTPUT チェインについて、追加した PSAMMB_LAN チェインが、その前の REJECT や DROP などにより遮断されていないことを確認します

設定例:

```
# iptables .L
Chain INPUT (policy ACCEPT)
target prot opt source destination
ACCEPT all -- 0.0.0.0/0 0.0.0.0/0 state
RELATED,ESTABLISHED
ACCEPT icmp -- 0.0.0.0/0 0.0.0.0/0
ACCEPT all -- 0.0.0.0/0 0.0.0.0/0
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 state NEW tcp dpt:22
PSA-MMB_LAN all -- 0.0.0.0/0 0.0.0.0/0
REJECT all -- 0.0.0.0/0 0.0.0.0/0 reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)
target prot opt source destination
REJECT all -- 0.0.0.0/0 0.0.0.0/0 reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)
target prot opt source destination
PSA-MMB_LAN all -- 0.0.0.0/0 0.0.0.0/0
```

```
Chain PSA-MMB_LAN (2 references)
target prot opt source destination
ACCEPT all -- 0.0.0.0/0 0.0.0.0/0
ACCEPT all -- 0.0.0.0/0 0.0.0.0/0
ACCEPT icmp -- 0.0.0.0/0 0.0.0.0/0 icmp type 8
ACCEPT icmp -- 0.0.0.0/0 0.0.0.0/0 icmp type 0
ACCEPT udp -- 0.0.0.0/0 0.0.0.0/0 udp dpt:161
ACCEPT udp -- 0.0.0.0/0 0.0.0.0/0 udp spt:161
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp spt:5000
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 tcp dpt:5000
```

4. 以下の手順で、ファイアーウォールの設定を確認します。

① PSA-MMB 間 LAN の IP アドレスを調べます。

```
# grep TOMMBIP=  /etc/fujitsu/SVmco/usr/tommbipsetup.conf
```

② 以下のコマンドを外部のターミナルから実行し、①で確認した IP アドレスが取得出来る事を確認します。

※外部ターミナルから snmp アクセスするには、事前に MMB に snmp のコミュニティの設定が必要です。詳細は「運用管理ツールリファレンス」の「SNMP Configuration」を参照して下さい。

```
# snmpwalk -v 1 -c public <MMB の仮想 IP アドレス>
1.3.6.1.4.1.211.1.31.1.2.<Partition の番号>.2.5.14| grep <PSA-MMB 間 LAN の IP アドレス>
```

以下のように、PSA-MMB 間 LAN の IP アドレスが取得できれば正しく iptables が設定されています。

実行例： (MMB の仮想 IP アドレスが 10.24.76.39、PSA-MMB 間 LAN の IP アドレスが 172.30.0.4、Partition の番号が 2 の場合)

```
# snmpwalk -v 1 -c public 10.24.76.39 1.3.6.1.4.1.211.1.31.1.2.2.2.5.14 | grep 172.30.0.4

SNMPv2-SMI::enterprises.211.1.31.1.2.2.2.5.14.1.1.4.0.0 = IpAddress: "172.30.0.4"
```

5. ファイアーウォールの設定を保存します。

```
# /sbin/service iptables save
```

6.1.7.4 パーティションからのトラップ送信先の設定

パーティションからのトラップ送信先の設定について詳しくは、「2.1.6 パーティションからのトラップ送信先の設定」を参照してください。

6.1.7.5 複製ディスク使用時の SNMP 設定

複製ディスク使用時の SNMP 設定について詳しくは、「2.1.7 複製ディスク使用時の SNMP 設定」を参照してください。

6.1.7.6 管理 LAN の設定確認

管理 LAN の設定確認について詳しくは、「2.1.2 管理 LAN の設定確認」を参照してください。

6.1.8 SVmco のアップデートインストール

SVmco のアップデートインストールについて詳しくは、「2.1.8 SVmco のアップデートインストール」を参照してください。

6.1.9 SIRMS のアップデートインストール

SIRMS のアップデートインストールについて詳しくは、「2.1.9 SIRMS のアップデートインストール」を参照してください。

6.1.10 SVmco のアンインストール

SVmco のアンインストールについて詳しくは、「2.1.10 SVmco のアンインストール」を参照してください。

6.1.11 SIRMS のアンインストール

SIRMS のアンインストールについて詳しくは、「2.1.11 SIRMS のアンインストール」を参照してください。

6.2 SVmco の手動インストール (Windows Server 2008/2012)

Windows Server 2008/2012 に SVmco をインストールする手順について説明します。インストールする場合は、必ず Administrator 権限でログインしてください。なお、Administrator 以外の Administrator 権限のユーザーで、SVmco のインストールを行

う場合、ファイルを右クリックして表示されるメニューの [管理者として実行] を選択してから、SVmco をインストールしてください。

備考

PRIMEQUEST 1000x2 シリーズ運用時は、必ず SVmco をインストールしてください。SVmco をアンインストールすると、以下の制限があります。

REMCS 契約時にパーティション上の異常が通知されません。

PCI カードの活性保守ができない。必ずパーティション停止保守となる。

6.2.1 インストールの流れ

SVmco のインストールの流れについて、『PRIMEQUEST 1000 シリーズ導入マニュアル』(C122-E107)の「第 4 章 OS および添付ソフトウェアのインストール 」を参照してください。SVmco の設定については、「2.2　SVmco の設定（Windows Server 2008/2012）を参照してください。

備考

- SVIM を使用して OS をインストールする場合、SVmco、SIRMS のインストールは不要です。ただし、SVIM によるインストール後に、「6.2.2 SVmco インストール前の確認」および「6.2.6 SVmco インストール後の設定」の各項目の確認および設定を実施する必要があります。
- SVmco インストール後に、以下のいずれかを実行する場合は、SNMP セキュリティ設定コマンド (setsnmpsec) を実行します。コマンドの詳細については「3.5　SNMP セキュリティ設定コマンド (setsnmpsec)」を参照してください。
- SNMP Service のセキュリティ設定を [すべてのホストから SNMP パケットを受け付ける] から [これらのホストから SNMP パケットを受け付ける] に変更する場合
- MMB の IP アドレスを変更する場合

  MMB の IP アドレスおよびパーティション側の管理 LAN の IP アドレスを変更した場合は、必ず SVmco を再起動してください。再起動しない場合、SVmco で検出するエラーの通知ができません。

- Windows Server 2008/2012 設定時の注意

- 以下のレジストリの値を 20000 (20 秒) 未満に設定すると、OS のシャットダウン時にハングアップする可能性があります。このためレジストリの値は、必ず 20000 (20 秒) 以上に設定してください。

HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Control

" WaitToKillServiceTimeout" (種類: REG_DWORD / default;20000)

- 上記のレジストリで、シャットダウン時にサービスを終了させるまでの待ち時間 (ms) を指定できます。

6.2.2 インストール前の確認

SVmco をインストールする前に確認する項目について説明します。

- PSA-MMB 間通信 LAN の設定確認
- SVmco 動作のための必須サービスの確認

6.2.2.1 PSA-MMB 間通信 LAN の設定確認

PSA-MMB 間通信 LAN の設定について詳しくは、「2.2.1 PSA-MMB 間通信 LAN の設定」を参照してください。

6.2.2.2 SVmco 動作のための必須サービスの確認

SVmco の動作のためには SNMP サービスが必要です。SNMP サービスを以下の手順で追加します。

- 操作手順

1. [スタート] メニュー - [管理ツール] - [サーバーマネージャー] をクリックします。

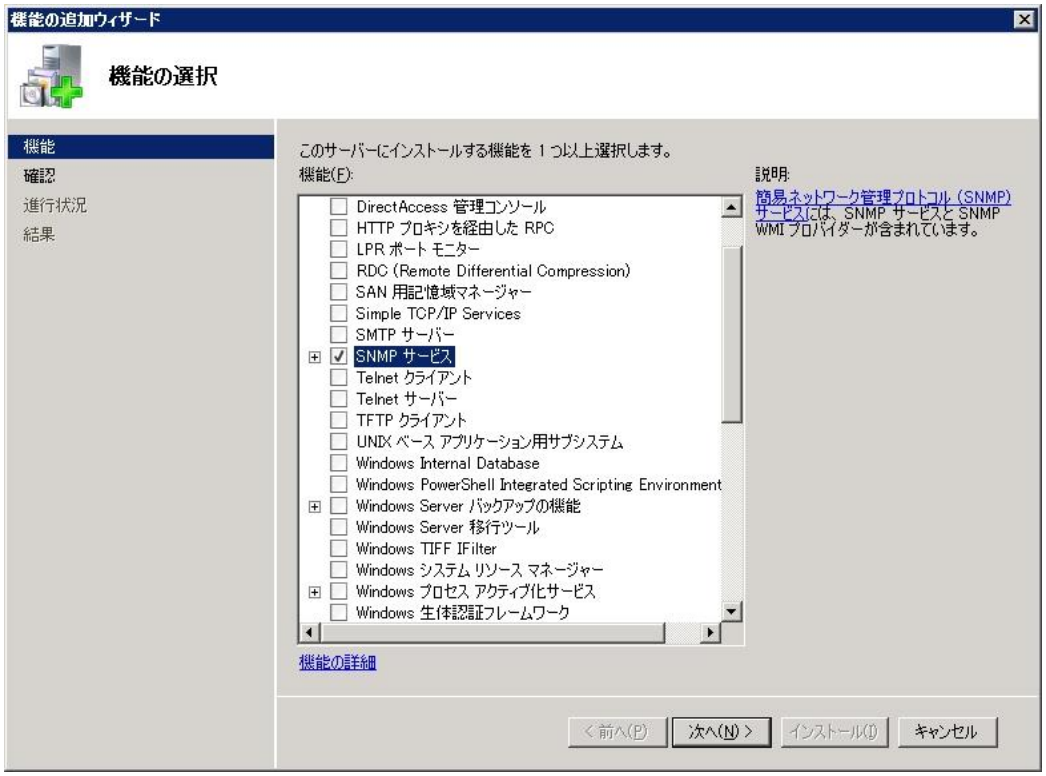
2. [サーバー マネージャー] 画面の [機能] - [機能の追加] - [SNMP サービス] を選択します。

3. [SNMP サービス] のチェックボックスがオンになっているか確認し、[OK] ボタンをクリックします。Windows コンポーネントウィザードに戻ります。

備考

チェックボックスがオンになっていない場合は、SNMP サービスがインストールされていません。チェックボックスをオンにして、SNMP サービスをインストールしてください。

Windows コンポーネントウィザード画面で [次へ] ボタンをクリックし、ウィザードの指示に従ってインストールします。


機能の追加ウィザード
機能の選択
機能
確認
進行状況
結果
このサーバーにインストールする機能を 1 つ以上選択します。
機能(F):
DirectAccess 管理コンソール
HTTP プロキシを経由した RPC
LPR ポート モニター
RDC (Remote Differential Compression)
SAN 用記憶域マネージャー
Simple TCP/IP Services
SMTP サーバー
SNMP サービス
Telnet クライアント
Telnet サーバー
TFTP クライアント
UNIX ベース アプリケーション用サブシステム
Windows Internal Database
Windows PowerShell Integrated Scripting Environment
Windows Server バックアップの機能
Windows Server 移行ツール
Windows TIFF IFilter
Windows システム リソース マネージャー
Windows プロセス アクティブ化サービス
Windows 生体認証フレームワーク
説明:
簡易ネットワーク管理プロトコル (SNMP) サービスには、SNMP サービスと SNMP WMI プロバイダーが含まれています。
機能の詳細
< 前へ(P)
次へ(N) >
インストール(I)
キャンセル

[機能の選択] 画面

6.2.3 SVmco のインストール

SVmco のパッケージをインストールします。

本体処理装置に添付されている『ServerView Suite』の DVD を用意します。

■ 操作手順

1. Tools¥Japanese¥SVmco¥ SR_Windows\ ServerViewMissionCriticalOption_Win.exe を実行します。

   「インストールの準備」画面が表示されます。

2. インストールの準備が整い以下の画面が表示されたら、実行する場合は [次へ] ボタンをクリックします。

3. インストール先を指定し、[次へ] ボタンをクリックします。

   SVmco はデフォルトで Program Files¥Fujitsu ¥ServerView Suite 配下または Program Files(x86)¥Fujitsu ¥ServerView Suite 配下にインストールされます。インストール先を変更する場合は [参照] ボタンをクリックしてインストール先を指定します。

4. インストールが完了すると、[セットアップ完了] 画面が表示されます。[完了] ボタンをクリックします。
5. 再起動が必要な場合は、すぐにコンピュータを再起動するかしないかを確認する画面が表示されます。

その場合は、再起動が可能かどうか確認してください。可能であれば、再起動のオプションを選択し、[完了] ボタンをクリックします。

6.2.4 SVmco インストール時の自動設定

SVmco のインストール時には、以下の SVmco 動作のための設定が自動的に行われます。

■ **サービスの設定**

- ServerView Mission Critical Option
- PRIMEQUEST PEM Command Service
- PRIMEQUEST Environment Control Service

■ **環境変数の設定**

- PATH 変数
  既存の PATH 変数に SVmco が使用する値を追加します。
- SVmco_INSTALLPATH 変数
  新規に変数が追加されます。

■ **SNMP のセキュリティ設定**

SVmco が MMB からの SNMP パケットを受け付ける必要があるため、SNMP Service のセキュリティを設定します。

SVmco インストール時に、[SNMP Service] の [プロパティ] 画面のセキュリティタブで選択されている項目により処理が異なります。

- 「すべてのホストから SNMP パケットを受け付ける」が選択されている場合
  SNMP のセキュリティ設定は実行されません。
- 「これらのホストから SNMP パケットを受け付ける」が選択されている場合
  MMB の IP アドレスと、localhost が設定されていない場合に localhost を、SNMP のセキュリティに設定します。

6.2.5 SIRMS のインストール

SIRMS のパッケージをインストールします。

本体処理装置に添付されている『ServerView Suite』の DVD を用意します。

■ 操作手順

1. Tools¥Japanese¥SIRMS¥SIRMS¥setup.exe を実行します。

インストールの準備のため、以下の画面が表示されます。

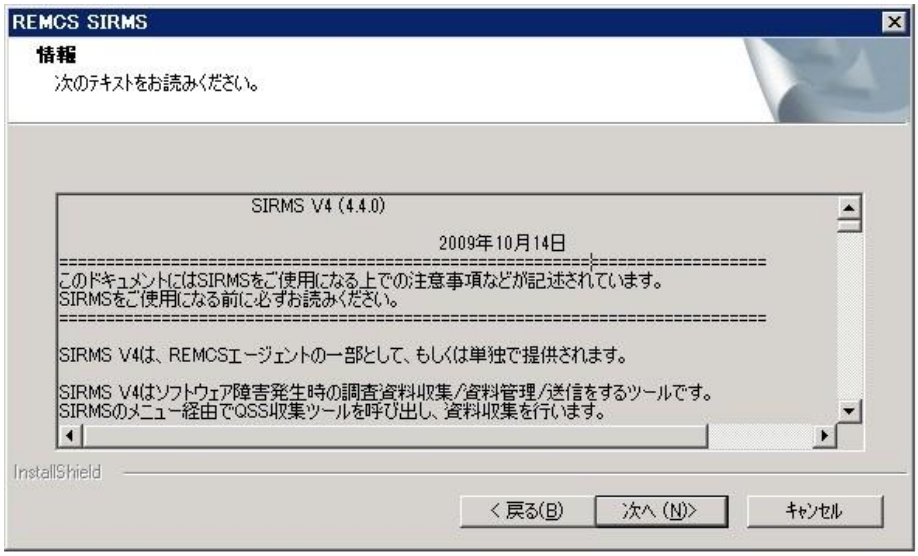
[セットアップの準備] 画面

2. インストールの準備が整うと以下の画面が表示されます。実行する場合は [次へ] ボタンをクリックします。

[SIRMS セットアップ] 画面

3. [情報一覧] 画面が表示されます。

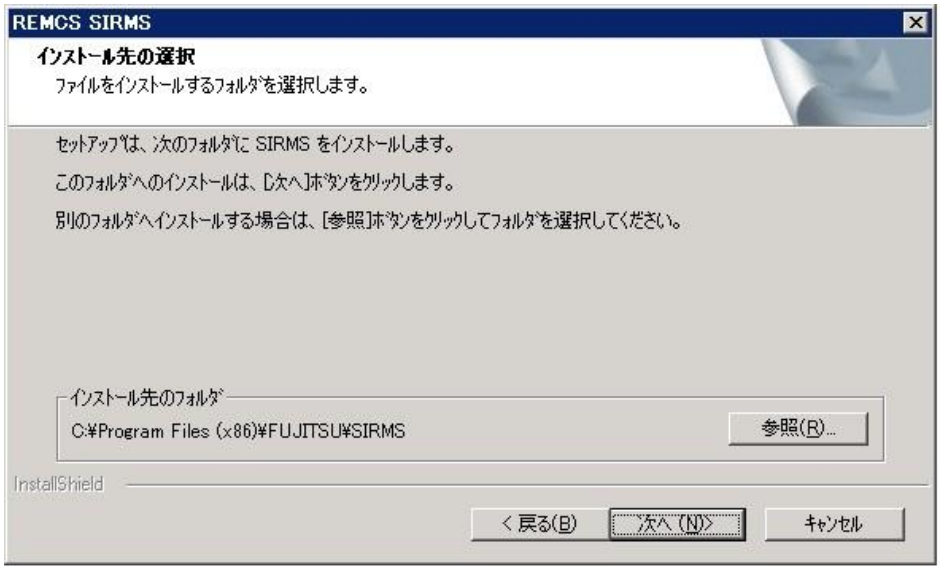
内容を確認し [次へ] ボタンをクリックします。



[情報一覧] 画面

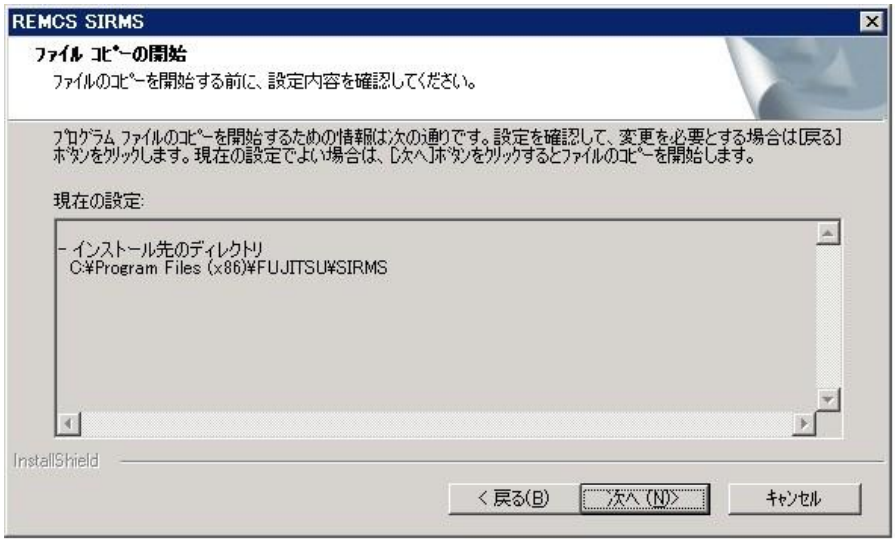
4. インストール先を指定し、[次へ] ボタンをクリックします。

SIRMS はデフォルトで Program Files¥Fujitsu 配下または Program Files(x86)¥Fujitsu にインストールされます。変更する場合は [参照] ボタンをクリックして、インストール先を指定します。



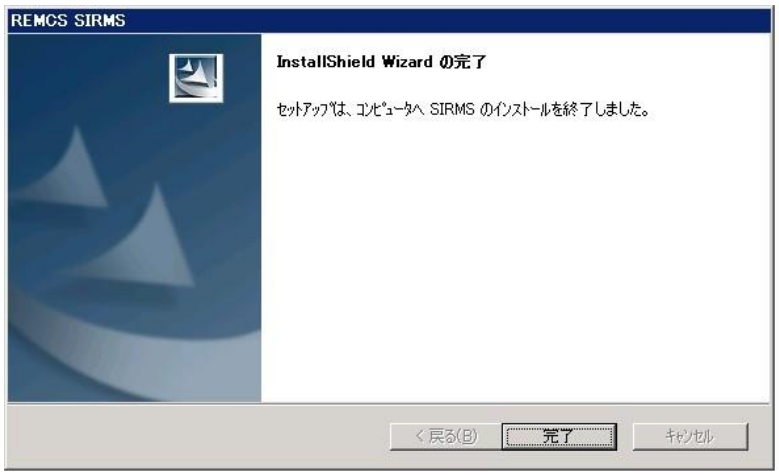
[インストール先の選択] 画面

5. 指定されたインストール先を確認し、[次へ] ボタンをクリックします。
   プログラムの転送が開始されます。



[ファイルコピーの開始] 画面

6. [完了] 画面が表示されたら [完了] ボタンをクリックして終了します。



[セットアップの完了] 画面

6.2.6 SVmco インストール後の設定

SVmco をインストールしたあとに設定する項目について説明します。

- パーティションからのトラップ送信先の設定
- Windows ファイアーウォールの設定
- STOP エラー(致命的なシステムエラー)発生後の Watchdog 監視設定
- PSHED Plugin ドライバのインストール
- 管理 LAN の設定確認

注意

イベントビューアのシステムログ、アプリケーションログのプロパティで [ログ サイズが最大値に達した時の操作] で [イベントを上書きしない] に変更しないでください。ログサイズが最大値に達した場合、それ以降にエラーが発生してもログに出力されないため、SVagent が検出できません。

6.2.6.1 パーティションからのトラップ送信先の設定

パーティションからのトラップ送信先の設定について詳しくは、「2.2.5 パーティションからのトラップ送信先の設定」を参照してください。

6.2.6.2 Windows ファイアーウォールの設定

Windows ファイアーウォールの設定について詳しくは、「2.2.4 Windows ファイアーウォールの設定」を参照してください。

6.2.6.3 STOP エラー(致命的なシステムエラー)発生後の Watchdog 監視設定

STOP エラー(致命的なシステムエラー)発生後の Watchdog 監視設定について詳しくは、「2.2.6 STOP エラー (致命的なシステムエラー) 発生後の Watchdog Timer 監視設定」を参照してください。

6.2.6.4 PSHED Plugin ドライバのインストール

PSHED Plugin ドライバのインストールについて詳しくは、「2.2.2 PSHED Plugin ドライバのインストール」を参照してください。

6.2.6.5 管理 LAN の設定確認

管理 LAN の設定確認については、「2.2.2 管理 LAN 設定確認」を参照して下さい。

6.2.7 SVmco のアップデートインストール

SVmco のアップデートインストールについて詳しくは、「2.2.8 SVmco のアップデートインストール」を参照してください。

6.2.8 SIRMS のアップデートインストール

SIRMS のアップデートインストールについて詳しくは、「2.2.9 SIRMS のアップデートインストール」を参照してください。

6.2.9 SVmco のアンインストール

SVmco のアンインストールについて詳しくは、「2.2.10 SVmco のアンインストール」を参照してください。

6.2.10 SIRMS のアンインストール

SIRMS のアンインストールについて詳しくは、「2.2.11 SIRMS のアンインストール」を参照してください。

7 SVmcovm の手動インストール

各 OS での SVmcovm のインストール方法は下記を参照して下さい。

2.4 SVmcovm のインストール/アンインストール

8 VMware5/6 における PCI カード故障箇所の特定手順

本章では、VMware5/6 の場合の PCI カード故障箇所の特定手順について説明します。

VMware5/6 の場合、通報されるメッセージの中に Unit 名が出力されず、Unit 名の欄に BUS 番号が出力されます。MMB-WebUI の[Partition Event Log]画面も同様で、Unit 名の欄に BUS 番号[例：0:0:25.0（すべて１０進数表記）]が表示されます。

このため、BUS 番号からアダプタを特定する必要があります。

下記は、MMB-WebUI の[Partition Event Log]画面例です。

は、Unit が BUS 番号で通報されています。

Partition Event Log

Severity	Date/Time	Partition No	Unit	Event ID	Description
Warning	2012/06/11 18:50:58	Partition#3	Software	11803	ixgbe:(null) Adapter or Software error (request_irq failed for MSIX interrupt Error)
Warning	2012/06/11 18:50:58	Partition#3	0:0:25.0	12005	lpfc:0000:00:19.0 Device or FC-Network error (Nodev timeout) vendor-id=8086 device-id=10cd revision=0
Warning	2012/06/11 18:50:58	Partition#3	Software	11704	igb:(null) Adapter or Software error (Invalid MAC Address)
Warning	2012/06/11 18:48:47	Partition#3	0:0:25.0	11802	ixgbe:vmnic0 Adapter error (Fan has stopped) vendor-id=8086 device-id=10cd revision=0
Warning	2012/06/11 09:09:11	Partition#0	SASU#1-HDD#0	14001	sd:sda Device error (Not ready) vendor=FUJITSU model=MBD2300RC serial-no=D017PB4002H1
Warning	2012/06/11 09:09:01	Partition#0	IOB#0-PCIC#7-FUNC#0	12005	lpfc:0000:16:00.0 Device or FC-Network error (Nodev timeout) vendor-id=8086 device-id=105E revision=6
Warning	2012/06/11 09:08:51	Partition#0	SASU#1-HDD#0	14001	sd:sda Device error (Not ready) vendor=FUJITSU model=MBD2300RC serial-no=D017PB4002H1
			IOB#0-		lpfc:0000:16:00.0 Device or FC-

Filter Clear

まず、イベント ID からカードの種類を特定してください。

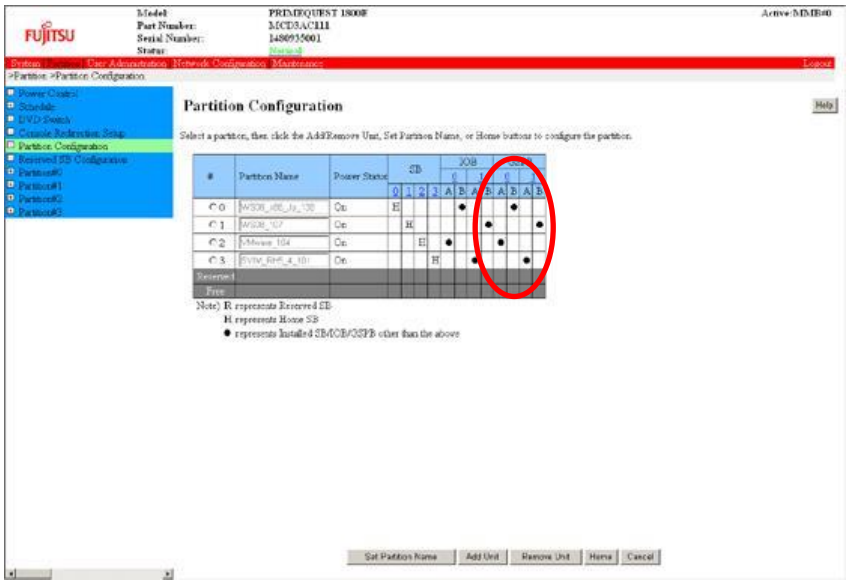
イベント ID	カードの種類
11000 番台	LAN カード
12000 番台	FC カード
13000 番台	SAS 配下のテープ装置
18500-18899 28500-28899	RAID カード

各カードごとにアダプタの特定手順について説明します。

8.1　LAN カードの特定手順

■　操作手順

1.　BUS 番号が 0:0:19.0 の場合は、Home SB の内蔵 NIC が該当します。MMB-WebUI の「Partition > Partition Configuration」画面で、Home　SB を確認してください。



2. BUS 番号が 0:0:19.0 以外の場合

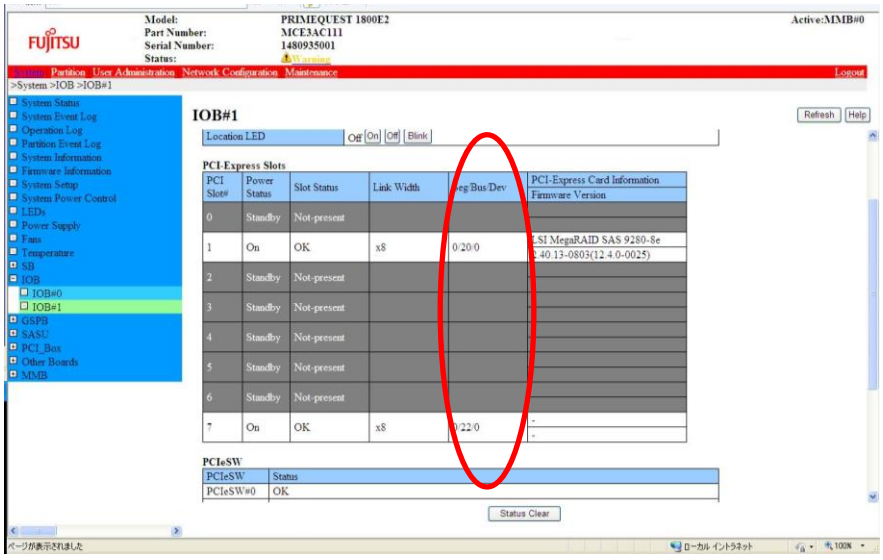
以下の MMB-WebUI を参照し、PCI-Express Slots 一覧に該当する Seg/Bus/Dev のカードが存在するか確認します。

>System>IOB>IOB#0

>System>IOB>IOB#1

>System>PCI_Box>PCI_Box#0

>System>PCI_Box>PCI_Box#1



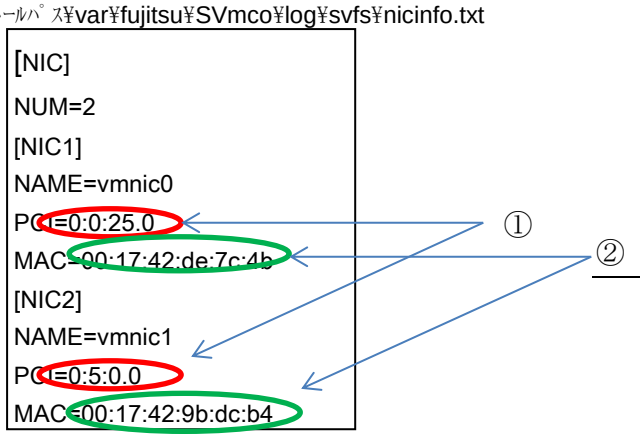
該当する IOB#または PCI_Box#と PCI Slot からアダプタの場所（Unit 名）が特定できます。

3.　1 と 2.でアダプタが特定できなかった場合には下記の手順を行ってください。

nicinfo.txt ファイルを確認します。ファイルの場所は、SVmcovm がインストールされているゲスト OS 上になりますが、OS により異なります

- Linux の場合：/var/fujitsu/SVmco/log/svfs/nicinfo.txt
- Windows の場合：

SVmcovm ｲﾝｽﾄｰﾙﾊﾟｽ¥var¥fujitsu¥SVmco¥log¥svfs¥nicinfo.txt



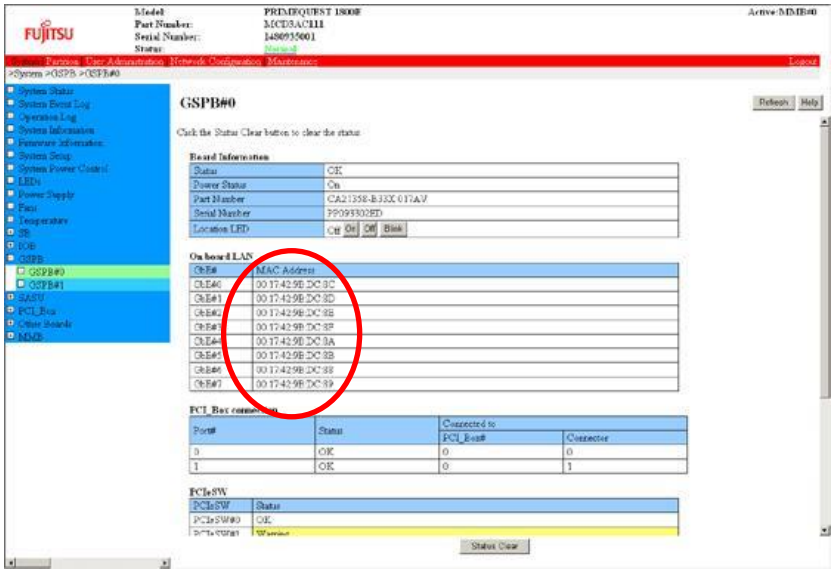
nicinfo.txt ファイル(例)

①　ファイル内に該当する BUS 番号（Seg/Bus/Dev/Func と同義）がないか検索します。

②　あった場合は、一致した番号の下の MAC を控えてください。

③　以下の MMB-WebUI を参照し、On board LAN に該当する MAC Address がないか確認してください。

```
>System>GSPB>GSPB#0
>System>GSPB>GSPB#1
```



④　一致した画面の GSPB#と On board LAN の Gb#からアダプタの場所（UNIT 名）を特定することができます。

8.2　FC カードの特定手順

■　操作手順

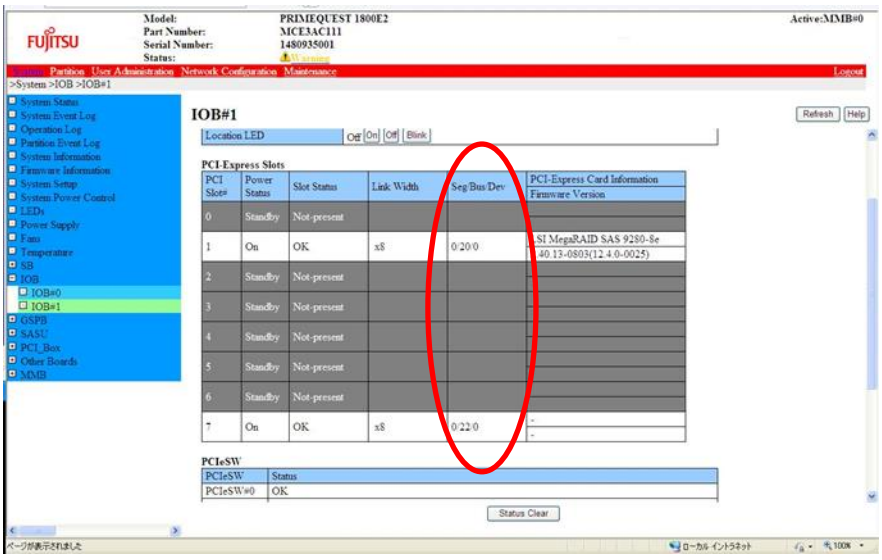
1.　以下の MMB-WebUI を参照し、PCI-Express Slots 一覧に該当する Seg/Bus/Dev のカードが存在するか確認してください。

>System>IOB>IOB#0

>System>IOB>IOB#1

>System>PCI_Box>PCI_Box#0

>System>PCI_Box>PCI_Box#1



該当する IOB#または PCI_Box#と PCI Slot からアダプタの場所（Unit 名）が特定できます。

8.3 RAID カードの特定手順

■ 操作手順

1. 以下の MMB-WebUI を参照し、PCI-Express Slots 一覧に該当する Seg/Bus/Dev のカードが存在するか確認してください。

>System>IOB>IOB#0

>System>IOB>IOB#1

>System>PCI_Box>PCI_Box#0

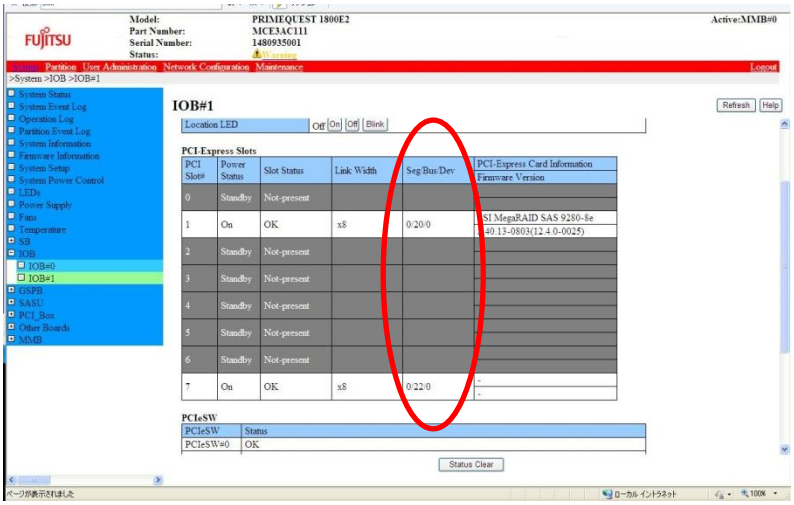
>System>PCI_Box>PCI_Box#1

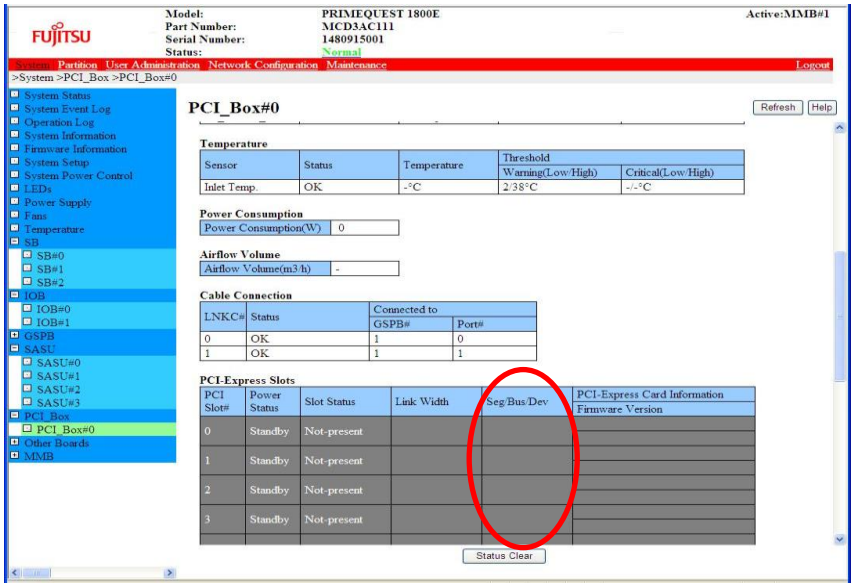
>System>SASU>SASU#0

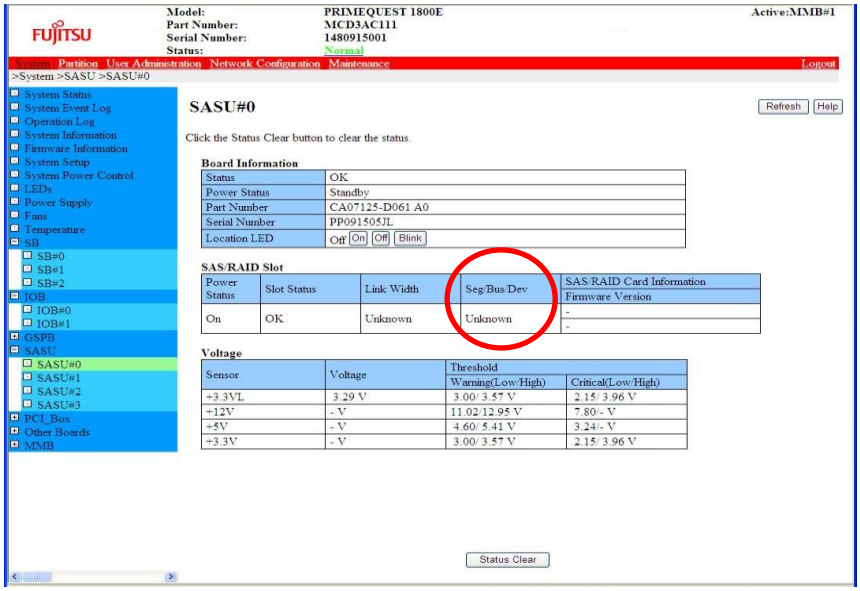
>System>SASU>SASU#1

>System>SASU>SASU#2

>System>SASU>SASU#3







一致した画面の IOB# / PCI_Box# と PCI Slot# または SASU# からアダプタの場所（Unit 名）が特定できます。

8.4 SAS 配下のテープ装置の特定手順

SAS 配下のテープ装置の場合は、アダプタの場所（Unit 名）は、

GSPB#n-SAS#m (ｎと m は数が入ります) のみとなります。

アダプタ異常の場合は、実際にテープ装置の接続されている IOB が交換対象となります。

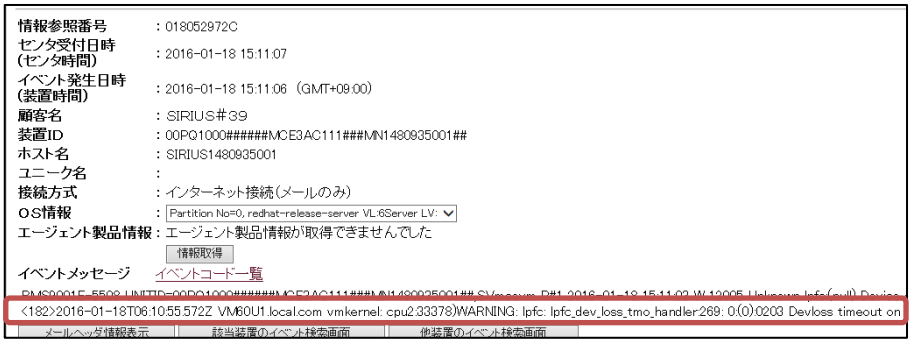
8.5 VMware6.x で FC カードの故障箇所が Unknown または誤った箇所で通報された場合の故障箇所特定方法について

VMware6.x 環境にて FC カードの故障箇所が Unknown または誤った箇所で通報された場合は、以下の方法で故障箇所を特定してください。

■ 操作手順

1. REMCS に通報されたメッセージを確認します。

例.イベント ID12005 の場合



イベントメッセージの 2 行目のドライバメッセージを確認します。

```
<182>2016-01-
18T06:10:55.572Z xxxx vmkernel: cpu2:33378)WARNING: lpfc: lpfc_dev_loss
_tmo_handler:269 0:(0):0203 Devloss timeout on WWPN 27:00:00:e0:00:a8:
04:81 NPort x0000ef Data: x8 x8 x0
```

ドライバメッセージより、Board Number を確認します。

:(n)の直前の番号、上記では 0 が Board Number になります。

2. バス番号(Bus/Dev)を確認します。

ESXi に ssh でログインし、下記コマンドを実行します。

```
/usr/lib/vmware/vmkmgmt_keyval/vmkmgmt_keyval -a
```

コマンド結果より、先ほど確認した Board Number でバス番号(Bus/Dev)を特定します。

```
Key Value Instance:  vmhba4/Emulex
Listing keys:
Name:   adapter
Type:   string
value:
lpfc Adapter Page

Emulex LightPulse FC SCSI 10.6.126.0
Emulex LPe1250-F8 8Gb PCIe Fibre Channel Adapter on PCI bus 0000:13 device 00
fn 0 Link Speed: 0 Gb

BoardNum:       0
FW Version:     2.01A12
HW Version:     31004549
ROM Version:    6.30a9
SerialNum:      VM91635054
Vendor Id:      f01510df
```

上記より、Board Number 0 のバス番号(Bus/Dev)が 13/0 と特定できます。

MMB 画面の表示と合わせるため、16 進数から 10 進数に変換します。

また、seg 番号は 0 固定です。

変換後の Seg/Bus/Dev 番号

0/19/0

変換後の Seg/Bus/Dev 番号より、マニュアル「8.2 FC カードの特定手順」に従い、故障カードの交換を実施してください。