CA92344-1753-01

FUJITSU Software
ServerView Infrastructure Manager V2.1
監視対象 OS、仮想化管理ソフトウェアに対する設定

2017 年 7 月

富士通株式会社

ServerView Infrastructure Manager V2.1(以下、"ISM2.1"と略す)で OS を管理するためには、OS 側に設定が必要です。本書は設定に必要な情報を提供します。

本書に記載の詳細や略語については、下記のマニュアルを参照してください。

・FUJITSU Software ServerView Infrastructure Manager V2.1 ユーザーズマニュアル

・FUJITSU Software ServerView Infrastructure Manager V2.1 用語集

1. 監視対象 OS・仮想化管理ソフトウェア毎の必要設定一覧

ISM2.1 から仮想マシン情報、装置情報表示(OS 情報、ディスクボリューム)、ログ管理機能(OS ログ収集)、ファームウェアアップデート(オンライン PCI カード)を使用するためには各 OS・仮想化管理ソフトウェアに設定が必要となります。以下の表に従い設定変更を実施してください。

(○：設定必要、×：設定不要、－：該当なし)

		サービス		セキュリティ			ドメイン	
		sshd	WinRM	Firewall	sslv3	PowerShell	SPN	ISM-VA 設定
Red Hat Enterprise Linux	6.x	○	-	×	-	-	-	○
	7.x	○	-	×	-	-	-	○
SUSE Linux Enterprise Server	11	○	-	○	-	-	-	○
	12	○	-	○	-	-	-	○
Windows Server	2008R2	-	○	○	-	○	○	○
	2012	-	○	○	-	○	○	○
	2012R2	-	○	○	-	○	○	○
	2016	-	○	○	-	○	○	○
VMware ESXi	5.x	-	-	-	○	-	-	○
	6.x	-	-	-	○	-	-	○

表 1 監視対象 OS 毎の必要設定一覧表

		各ホスト・仮想マシンへの設定	ドメイン		
		WinRM	SPN	ISM-VA 設定	Kerberos 委任構成
vCenter Server	5.5 以降	-	-	○	-
	6.x 以降	-	-	○	-
Microsoft Failover Cluster	Windows Server 2012 以降	○	○	○	○
Microsoft System Center	2012 以降	○	○	○	○

表 2 監視対象仮想化管理ソフトウェア毎の必要設定一覧表

[注意]

・対象サーバを監視するためには、管理者権限を持つユーザーアカウントで OS 情報を登録する必要があります。

・Windows／Linux に搭載される Emulex LAN/FC/CNA カードを管理するためには、対象サーバの OS に Emulex OneCommand Manager CLI が導入されている必要があります。

・Windows／Linux に搭載される QLogic FC カードを管理するためには、対象サーバの OS に QLogic QConvergeConsole CLI が導入されている必要があります。

・Linux に搭載される LAN/FC/CNA カードを管理するためには、対象サーバの Linux で lspci コマンドが実行可能である必要があります。

・Emulex OneCommand Manager CLI、または QLogic QConvergeConsole CLI は最新のものを利用してください。LAN/FC/CNA カードには最新のドライバを適用してください。

・Linux のディスク速度、ネットワーク速度の性能監視をするためには、対象サーバの OS に sysstat パッケージが導入されている必要があります。

・Active Directory からドメインユーザーのパスワード変更した場合すぐに反映しなくても情報取得はできますが、速やかに ISM2.1 でもパスワード変更してください。

2. 監視対象への設定手順（OS）

2.1. Windows への設定手順

ISM2.1 は Windows Server がインストールされている監視対象機器に対して WS-Management プロトコルを使用します。通信方式は https プロトコル+Basic 認証を使用します。必要な設定は以下の通りです。

・WinRM サービスの起動確認
・WinRM サービスの設定
・ファイアーウォールのポート開放
・Windows PowerShell スクリプトの実行ポリシーを変更

2.1.1. WinRM サービスの起動確認

管理者権限でコマンドプロンプトを開いて以下のコマンドを実行し、WinRM サービスの起動を確認します。

```
>sc query winrm
```

以下の結果を確認し、STATE が RUNNING になっていることを確認します。

```
        TYPE                : 20  WIN32_SHARE_PROCESS
        STATE               : 4   RUNNING
                                  (STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE     : 0   (0x0)
        SERVICE_EXIT_CODE   : 0   (0x0)
        CHECKPOINT          : 0x0
        WAIT_HINT           : 0x0
```

WinRM サービスが起動されていない場合、以下のコマンドを実行し、WinRM サービスを起動します。

```
>sc start winrm
```

[注意]
WinRM サービスは、環境によって自動起動になっていない場合があります。WinRM サービスを自動起動(auto)、もしくは遅延自動起動(delayed-auto)するように設定してください。
以下は、自動起動に設定する場合の例になります。

```
>sc config winrm start=auto
```

2.1.2. WinRM サービスの設定

(1) WinRM サービスの設定

初期設定では Basic 認証が許可されていないため「(1-1)Basic 認証の許可」の設定を行います。

https 通信を使用するため Basic 認証の通信は暗号化されます。
管理者権限でコマンドプロンプトを開き、以下のコマンドを実行します。

```
>winrm quickconfig
```

以下のメッセージが表示された場合、WinRM サービスは実行されていますがリモートアクセス許可は設定されていないため以下の手順に進んでください。「WinRM サービスは、既にこのコンピューターで実行されています。」と表示されている場合は既に設定が完了しているため「(2)https 通信の設定」に進んでください。
「y」を入力後、[Enter]キーを押します。

```
WinRM サービスは、既にこのコンピューターで実行されています。
WinRM は、管理用にこのコンピューターへのリモート アクセスを許可するように設定されていません。
次の変更を行う必要があります:

ローカル ユーザーにリモートで管理権限を付与するよう LocalAccountTokenFilterPolicy を構成してください。
変更しますか [y/n]? y
```

以下のメッセージが表示されます。

```
WinRM はリモート管理用に更新されました。

ローカル ユーザーにリモートで管理権限を付与するよう LocalAccountTokenFilterPolicy を構成しました。
```

(1-1) Basic 認証の許可
以下のコマンドを実行します。

```
>winrm set winrm/config/service/Auth @{Basic="true"}
```

(1-2) 追加設定事項 (Windows Server 2008R2)
対象サーバの OS が Windows Server 2008 R2 の場合、以下のコマンドを実行して、カードの種類や数に応じて MaxConcurrentOperationsPerUser の数値を大きくします。
以下のコマンドを実行します。

```
>winrm set winrm/config/Service @{MaxConcurrentOperationsPerUser="数値"}
```

例：1500 に設定した場合（Windows Server 2012/2012R2 では、デフォルトが 1500 であるため 1500 を推奨します。）

```
>winrm set winrm/config/Service @{MaxConcurrentOperationsPerUser="1500"}
```

(2) https 通信の設定
https 通信をするためには、証明書の設定が必要になります。
(2-1) 必要なツールの準備
証明書を作成するために必要なツールは２つあります。証明書は実行環境に依存せず作成することができます。
・.NET Framework 4.5（ダウンロードサイト）

https://www.microsoft.com/ja-jp/download/details.aspx?id=30653

・Windows Software Development Kit（ダウンロードサイト）

https://developer.microsoft.com/ja-jp/windows/downloads/windows-10-sdk

[注意]

・上記 URL の Windows Software Development Kit は、Windows 7 SP1 または Windows 8.1、および Windows Server 2012 R2 または Windows Server 2016 の OS に対応しています。その他の OS にインストールする場合は、適切な Windows Software Development Kit をインストールしてください。

Windows Software Development Kit には証明書を作成するために必要な 2 つのツールが含まれています。

証明書作成ツール（makecert.exe）

https://msdn.microsoft.com/ja-jp/library/bfsktky3(v=vs.80).aspx

個人情報交換ファイル作成ツール(pvk2pfx.exe)

https://msdn.microsoft.com/en-us/library/windows/hardware/ff550672(v=vs.85).aspx

(3) 証明書の作成

証明書作成ツール、個人情報交換ファイル作成ツールを使用し、以下の 3 つのファイルを作成します。

・CER ファイル(証明書)

・PVK ファイル(秘密鍵ファイル)

・PFX ファイル(サービス証明書)

より詳細な証明書作成の流れについては、下記の URL を参照してください。

https://blogs.technet.microsoft.com/junichia/2010/11/09/azure-for-itpro-3

(4) 証明書、秘密鍵ファイルの作成

証明書、秘密鍵ファイルの作成では、対象サーバの環境に合わせてコマンドを実行する必要があります。

以下は、対象サーバのサーバ名を”192.168.10.10”, 証明書の有効期間を 2017 年 3 月 30 日に設定した場合のコマンド例です。

```
>makecert.exe -r -pe -n "CN=192.168.10.10" -e 03/30/2017 -eku 1.3.6.1.5.5.7.3.1 -ss My
-sr localMachine -sky exchange <証明書のファイル名.cer> -sv <秘密鍵のファイル名.pvk>
```

証明書の構成に関する詳しい設定については、下記の URL を参照してください。
https://technet.microsoft.com/ja-jp/library/ms186362(v=sql.105).aspx

(5)　サービス証明書の作成

以下のコマンドを実行します。

```
>pvk2pfx.exe -pvk <秘密鍵のファイル名.pvk> -spc <証明書のファイル名.cer> -pfx <サービス証明書のファイル名.pfx>
```

(6)　証明書、サービス証明書の登録

証明書スナップインを起動し(4),(5)で作成した証明書を登録します。

1. 対象サーバで mmc.exe を実行します。
2. [ファイル] > [スナップインの追加と削除] を選択します。
3. [利用できるスナップイン]から、「証明書」を選択し、[追加]します。
4. 「コンピューター アカウント」を選択し、[次へ] > [完了]を順に選択します。
5. [OK]を選択します。

(7)　SSL 証明書を登録

1. <証明書のファイル名.cer>を信頼されたルート証明機関に登録します。
   [コンソールルート] > [証明書（ローカルコンピューター）] > [信頼されたルート証明機関]を右クリックします。[すべてのタスク] > [インポート]から、<証明書のファイル名.cer>ファイルを選択し、証明書のウィザードインポートを完了します。
2. <証明書のファイル名.cer>を[信頼されたルート証明機関]に登録できたことを確認します。
   [コンソールルート] > [証明書（ローカルコンピューター）] > [信頼されたルート証明機関] > [証明書]の順に選択し、「発行先」と「発行者」が CN に指定したサーバ名となっていること、「目的」が”サーバー認証”となっていることを確認してください。
3. <サービス証明書のファイル名.pfx>を個人に登録します。
   [コンソールルート] > [証明書（ローカルコンピューター）] > [個人]を右クリックします。[すべてのタスク] > [インポート]から、<サービス証明書のファイル名.pfx>ファイルを選択し、証明書のウィザードインポートを完了します。
4. <サービス証明書のファイル名.pfx>を[個人]に登録できたことを確認します。
   [コンソールルート] > [証明書（ローカルコンピューター）] > [個人]の順に選択し、「発行先」と「発行者」が CN に指定したサーバ名となっていること、「目的」が”サーバー認証”となっていることを確認してください。

(8)　　WinRM サービスへの証明書に記載された拇印を登録

(8-1)　　拇印(Thumbprint)の確認

以下は、LocalMachine\my に証明書を保存した場合の確認方法です。

1. コマンドプロンプトから PowerShell を起動します。
2. 拇印を確認します。以下のコマンドを実行します。

```
>ls cert:LocalMachine\my
```

以下のように表示されます。

```
WinRM サービスは、既にこのコンピューターで実行されています。
PS C:\Windows\system32> ls cert:LocalMachine\my


ディレクトリ: Microsoft.PowerShell.Security\Certificate::LocalMachine\my
Thumbprint                                Subject
----------                                -------
1C3E462623BAF91A5459171BD187163D23F10DD9  CN=192.168.10.10
```

(8-2)　　WinRM リスナーに証明書に記載された拇印を登録

PowerShell を終了し、以下のコマンドを実行します。'HTTPS'と'@'の間にはスペースが必要です。

```
>winrm create winrm/config/listener?Address=*+Transport=HTTPS @{Hostname="<証明書を作成した時に設定した CN 名>";CertificateThumbprint="<作成した証明書の拇印>"}
```

(8-3)　　WinRM リスナーの登録確認

以下のコマンドを実行します。

```
>winrm get winrm/config/listener?Address=*+Transport=HTTPS
```

以下のようなコマンド結果が返ってくれば、WinRM のリスナーが登録できています。

```
Listener
    Address = *
    Transport = HTTPS
    Port = 5986
    Hostname = 192.168.10.10
    Enabled = true
    URLPrefix = wsman
    CertificateThumbprint = 1C3E462623BAF91A5459171BD187163D23F10DD9
    ListeningOn = 192.168.10.10, 127.0.0.1, ::1, 2001:258:8402:200:bd8a:1c1:c50d
:8704, fe80::5efe:192.168.10.10%13, fe80::bd8a:1c1:c50d:8704%12
```

2.1.3. ファイアーウォールのポート開放

WinRM サービスがリクエストの受付をできるように、WinRM リスナーで設定したポートを解放する必要があります。https 通信のデフォルトポート番号は、5986 です。

(1) Windows Server 2008 R2 の場合

以下のようなコマンドを実行します。

```
>netsh advfirewall firewall add rule name= <ファイアーウォールルール名> enable=yes localip=any remoteip=any protocol=tcp localport=<ポート番号> remoteport=any edge=no dir=in profile=domain,private,public action=allow
```

(例)ポート番号 5986 を解放するルールに、”WinRM”という名前を設定します。

```
>netsh advfirewall firewall add rule name=WinRM enable=yes localip=any remoteip=any protocol=tcp localport=5986 remoteport=any edge=no dir=in profile=domain,private,public action=allow
```

(2) Windows Server 2012 / 2012R2 / 2016 の場合

1. コマンドプロンプトから PowerShell を開きます。
2. 以下のようなコマンドを実行します。

```
>New-NetFirewallRule -DisplayName <ファイアーウォールルール名> -Action Allow -Direction Inbound -Enabled True -Protocol TCP -LocalPort <ポート番号>
```

例）ポート番号 5986 を解放するルールに、”WinRM”という名前を設定します。

```
>New-NetFirewallRule -DisplayName WinRM -Action Allow -Direction Inbound -Enabled True -Protocol TCP -LocalPort 5986
```

[注意]

ファイアーウォールの設定は、対象サーバの環境によって異なります。

2.1.4. Windows PowerShell の実行ポリシー変更

管理者権限で Windows PowerShell を開き、以下のコマンドを実行します。

```
>set-executionpolicy remotesigned
```

以下のメッセージが表示された場合、「Y」を入力後、[Enter]キーを押します。

```
実行ポリシーの変更
実行ポリシーは、信頼されていないスクリプトからの保護に役立ちます。実行ポリシーを変更すると、
about_Execution_Policies
のヘルプ トピック http://go.microsoft.com/fwlink/?LinkID=135170
で説明されているセキュリティ上の危険にさらされる可能性があります。実行ポリシーを変更しますか?
[Y] はい(Y)  [N] いいえ(N)  [S] 中断(S)  [?] ヘルプ (既定値は "Y"): Y
```

2.1.5. ドメインユーザーアカウント使用時の設定

ドメインユーザーアカウントでは、複数の異なるドメイン環境を同時に監視することはできません。

(1) Active Directory への SPN の追加

ドメインユーザーアカウントを使用し Windows Server の監視をする際には監視対象サーバのサービスプリンシパル名(SPN)を正しく Active Directory に登録する必要があります。以下の手順を実行し、監視対象サーバのサービスプリンシパル名を登録してください。

```
>setspn -A HOST/[監視対象 IP アドレス] [監視対象ホスト名]
```

確認方法

```
>setspn -L [監視対象ホスト名]
```

削除方法

```
>setspn -D HOST/[監視対象 IP アドレス] [監視対象ホスト名]
```

(2) ISM-VA へドメイン情報の追加

ドメインユーザーアカウントでの監視を行う際には「ISM2.1 ユーザーズマニュアル」(3.4.2 ISM 初期設定)を実施してください。

(3) ISM-VA へ DNS 情報の追加

ドメインユーザーアカウントでの監視を行う際には「ISM2.1_ユーザーズマニュアル」(4.9 ネットワーク設定 DNS サーバ追加)を行い ISM-VA に DNS サーバの登録を実施してください。

2.2. Red Hat Enterprise Linux への設定手順

ISM2.1 では、Red Hat Enterprise Linux がインストールされている対象サーバと ssh(Secure SHell service)を使って通信します。必要な設定は以下の通りです。

・ssh サービスの起動

2.2.1. ssh サービスの起動確認

sshd を起動するように設定してください。OS のバージョンによって、コマンドが異な

ります。

(1) Red Hat Enterprise Linux 6 の場合

以下のコマンドを実行して、sshd の起動を確認します。

```
#chkconfig -list sshd
```

以下のように表示された場合は、sshd の起動が無効になっています。

```
sshd            0:off   1:off   2:off   3:off   4:off   5:off   6:off
```

対象サーバのランレベルに対応する番号の項目が off になっている場合には以下のコマンドを実行して、sshd を自動起動するようにしてください。

```
#chkconfig sshd on
```

(2) Red Hat Enterprise Linux 7 の場合

以下のコマンドを実行して、sshd の起動を確認します。

```
#systemctl is-enabled sshd
```

以下のように表示された場合は、sshd の起動が無効になっています。

```
disabled
```

sshd の起動が無効になっている場合には、以下のコマンドを実行してください。

```
#systemctl enable sshd
```

2.2.2. ドメインユーザーアカウント使用時の設定

ドメインユーザーアカウントでの監視を行う際には以下の点に注意して実施してください。

(1) ISM-VA へドメイン情報の追加

ドメインユーザーアカウントでの監視を行う際には「ISM2.1 ユーザーズマニュアル」(3.4.2 ISM 初期設定)を実施してください。

(2) ISM-VA へ DNS 情報の追加

ドメインユーザーアカウントでの監視を行う際には「ISM2.1_ユーザーズマニュアル」(4.9 ネットワーク設定 DNS サーバ追加)を行い ISM-VA に DNS サーバの登録を実施してください。

(3) ドメインユーザーアカウント名の制約

Active Directory に登録したドメインユーザー名を Linux で使用する場合には Linux のユーザー名の制限についても注意してください。

＜Linux ユーザー名として使えない代表例＞

・大文字、先頭文字の数字、ドットなどの記号

(4) Emulex カード情報収集時の制限

Avago/Emulex 社製カードが搭載された機器では「hbacmd」を使用しカード情報の収集

を行います。
root ユーザー権限以外でカード情報を収集する場合には、「hbacmd」に管理者権限を付与してください。
詳しくは、「OneCommandManager Command Line Interface User Manual」を参照してください。

(5) QLogic カード情報収集時の制限

ドメインユーザーアカウントでは QLogic 社製カードが搭載された機器の情報取得はせきません。OS 情報編集画面から root ユーザーを登録し情報取得を行ってください。

(6) ServerView ログ収集時の制限

ドメインユーザーアカウントでは ServerView ログの収集はできません。OS 情報編集画面から root ユーザーを登録し情報収集を行ってください。

(7) ファームウェアアップデート時の制限

ドメインユーザーアカウントではオンラインファームアップデートを実施できません。OS 情報編集画面から root ユーザーを登録しファームウェアアップデートを行ってください。

2.2.3. 監視に使用するアカウントの設定

(1) 「.bashrc」の設定

該当アカウントのホームディレクトリにある「.bashrc」ファイルを開きます。「.bashrc」ファイルがない場合は、作成してください。

```
#vi ~/.bashrc
```

「.bashrc」ファイルに「/sbin」、「/usr/sbin」、「/usr/local/sbin」のパスを追記してください。

```
PATH=$PATH:/sbin
PATH=$PATH:/usr/sbin
PATH=$PATH:/usr/local/sbin
```

(2) 環境変数の設定

ServerView のログ収集機能を実行するためには、ISM のノードに登録されている OS アカウントを使用し監視対象に ssh でログインした後、下記の条件を満たしていることを確認してください（※）。

・ログイン時に、ホームディレクトリに移動すること。
・ログイン時のプロンプト表示文字列に'~'が含まれていること。
・ログイン時のプロンプト表示文字列の'~'の後に'$'あるいは'#'が含まれていること。
例 1) [root@hostname ~]#

例 2) ADUSER\ismuser@hostname ~ $

※環境変数$PS1 の値を変更することでプロンプト表示文字列を変更できます。
環境変数$PS1 の設定値例）

```
[root@localhost ~]# echo $PS1
[¥u@¥h ¥W]¥$
```

2.3. SUSE Linux Enterprise Server への設定手順

ISM2.1 では、SUSE Linux Enterprise Server がインストールされている対象サーバと ssh(Secure Shell service)を使って通信します。必要な設定は以下の通りです。

・ssh サービスの起動確認

・ファイアーウォールのポート開放

2.3.1. ssh サービスの起動確認

SUSE Linux Enterprise Server では、デフォルトでは sshd の起動が無効になっています

sshd を起動するように設定してください。OS のバージョンによって、コマンドが異なります。

(1) SUSE Linux Enterprise Server 11

以下のコマンドを実行して、sshd の起動を確認します。

```
#chkconfig -list sshd
```

以下のように表示された場合は、sshd の起動が無効になっています。

```
sshd            0:off   1:off   2:off   3:off   4:off   5:off   6:off
```

対象サーバのランレベルに対応する番号の項目が off になっている場合には以下のコマンドを実行して、sshd を自動起動するようにしてください。

```
#chkconfig sshd on
```

(2) SUSE Linux Enterprise Server 12

以下のコマンドを実行して、sshd の起動を確認します。

```
#systemctl is-enabled sshd
```

以下のように表示された場合は、sshd の起動が無効になっています。

```
disabled
```

sshd の起動が無効になっている場合には、以下のコマンドを実行してください。

```
#systemctl enable sshd
```

2.3.2. ファイアーウォールのポート開放

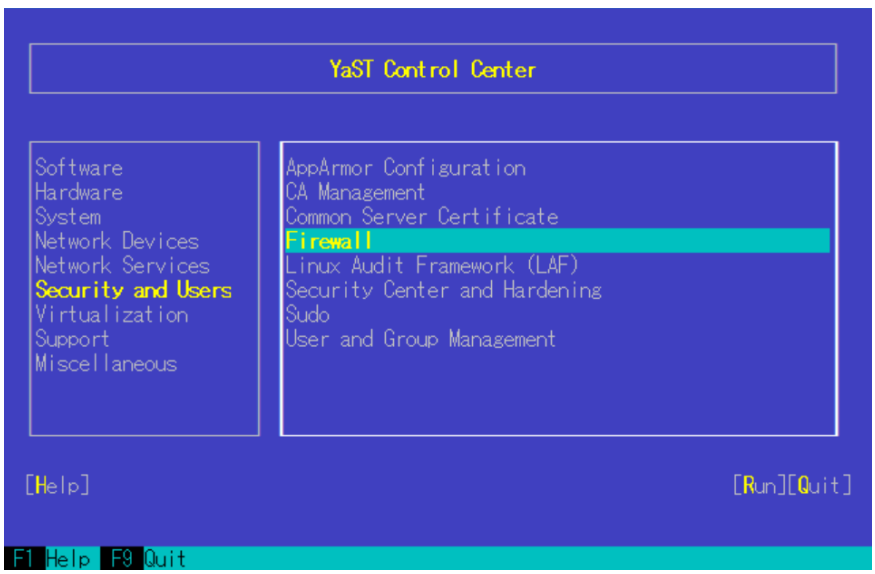
SUSE Linux Enterprise Server のファイアーウォールは、デフォルトで ssh のポート

を閉じています。ファイアーウォールの設定から、ssh 通信を許可する必要があります。ファイアーウォールの設定は、対象サーバの環境によって異なります。以下では例として、YaST を使用した場合のファイアーウォールの設定になります。

1. 以下のコマンドを実行して、YaST Control Center を表示します。

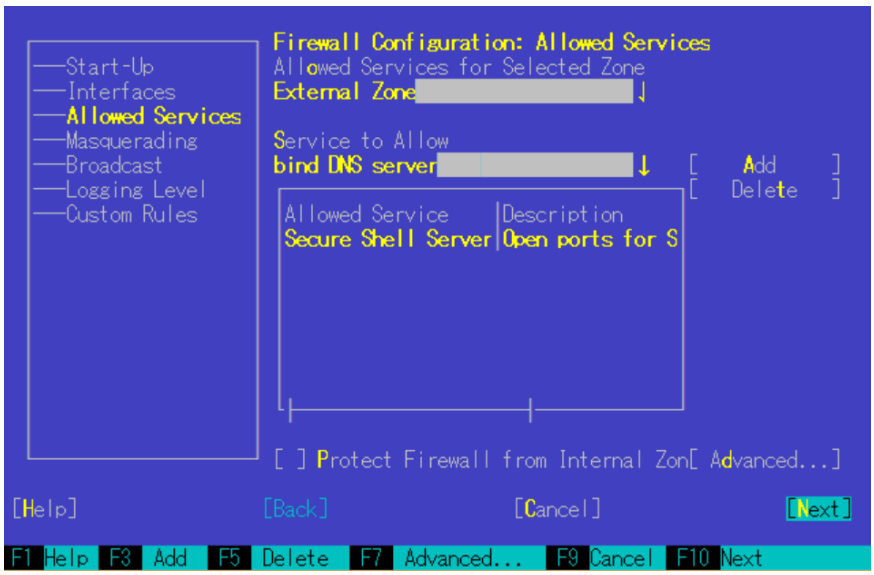
```
#yast
```

2. [Security and Users] > [Firewall] を選択し、[Enter]キーを押します。

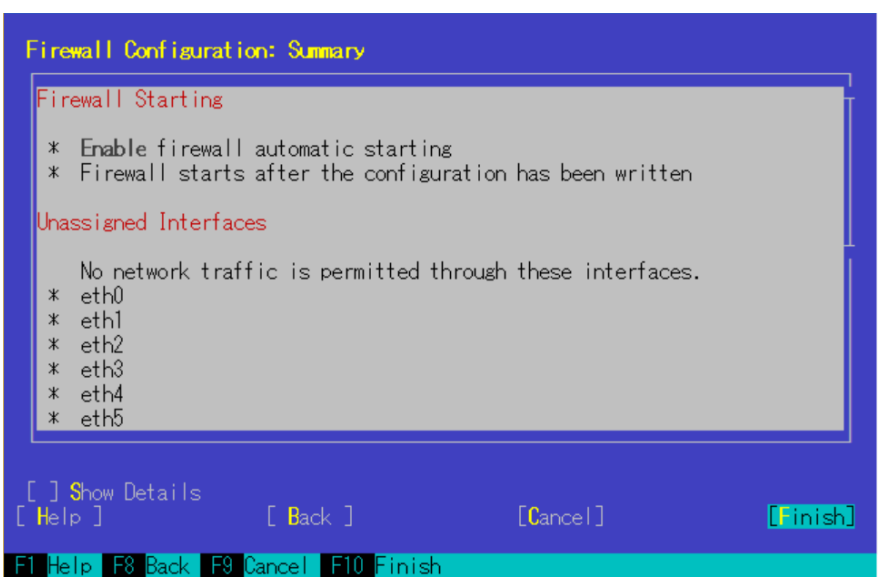


3. [Start-Up]画面から、[Sevice Start]の状態を「Enable Firewall Automatic Statrting」にします。

4. [Allowed Services] > [Service to Allow]から、「Secure Shell Server」を選択し、[Add]へ移動して[Enter]キーを押します。
5. Allowed Service に「Secure Shell Server」が追加されているのを確認し、[Next]へ移動して[Enter]キーを押します。



6. [Firewall Configuration: Summary]画面が表示された後、[Finish]へ移動し、[Enter]キーを押して、ファイアーウォールの設定を完了します。



[注意]

・SUSE Linux Enterprise Server では、デフォルトで root ユーザーのログインができません。ISM2.1 で対象サーバを監視するには root ユーザーでのログインを許可するか、もしくは root ユーザー権限と同等のユーザーアカウントを設定する必要があります。ssh で root ユーザーによるログインを許可する場合には、/etc/ssh/sshd_config に以下の設定をしてください。

PermitRootLogin　yes

2.3.3. ドメインユーザーアカウント使用時の設定

(1) ISM-VA へドメイン情報の追加

ドメインユーザーアカウントでの監視を行う際には「ISM2.1 ユーザーズマニュアル」（3.4.2 ISM 初期設定)を実施してください。

(2) ISM-VA へ DNS 情報の追加

ドメインユーザーアカウントでの監視を行う際には「ISM2.1_ユーザーズマニュアル」(4.9 ネットワーク設定 DNS サーバ追加)を行い ISM-VA に DNS サーバの登録を実施してください。

(3) Emulex カード情報収集時の制限

Avago/Emulex 社製カードが搭載された機器では「hbacmd」を使用しカード情報の収集を行います。

root ユーザー権限以外でカード情報を収集する場合には、「hbacmd」に管理者権限を付与してください。

詳しくは、「OneCommandManager Command Line Interface User Manual」を参照してください。

(4) QLogic カード情報収集時の制限

ドメインユーザーアカウントでは QLogic 社製カードが搭載された機器の情報取得はできません。OS 情報編集画面から root ユーザーを登録し情報取得を行ってください。

(5) ServerView ログ収集時の制限

ドメインユーザーアカウントでは ServerView ログの収集はできません。OS 情報編集画面から root ユーザーを登録し情報収集を行ってください。

(6) ファームウェアアップデート時の制限

ドメインユーザーアカウントではオンラインファームアップデートを実施できません。OS 情報編集画面から root ユーザーを登録しファームウェアアップデートを行ってください。

2.3.4. 監視に使用するアカウントの設定

(1) 「.bashrc」の設定

該当アカウントのホームディレクトリにある「.bashrc」ファイルを開きます。「.bashrc」ファイルがない場合は、作成してください。

```
#vi ~/.bashrc
```

「.bashrc」ファイルに「/sbin」、「/usr/sbin」、「/usr/loca/sbin」のパスを追記してください。

```
PATH=$PATH:/sbin
PATH=$PATH:/usr/sbin
PATH=$PATH:/usr/local/sbin
```

(2)　　環境変数の設定

ServerView のログ収集機能を実行するためには、ISM2.1 のノードに登録されている OS アカウントを使用し監視対象に ssh でログインした後、下記の条件を満たしていることを確認してください（※）。

・ログイン時に、ホームディレクトリに移動すること。
・ログイン時のプロンプト表示文字列に'~'が含まれていること。
・ログイン時のプロンプト表示文字列の'~'の後に'$'あるいは'#'が含まれていること。
　例 1) [root@hostname ~]#
　例 2) ADUSER\ismuser@hostname ~ $

※環境変数$PS1 の値を変更することでプロンプト表示文字列を変更できます。
環境変数$PS1 の設定値例）

```
[root@localhost ~]# echo $PS1
[¥u@¥h ¥W]¥$
```

2.4. VMware ESXi への設定手順

ISM2.1 では、VMware ESXi がインストールされている対象サーバと vSphere API, CIM プロトコルを使用して通信します。必要な設定は以下の通りです。

・VMware ESXi での SSLv3 のサポートの有効化

2.4.1. VMware ESXi 5.5、VMware ESXi 6.0 における SSLv3 のサポートの有効化

(1)　　SSH サービスの起動

すでに SSH サービスが起動中の場合、本設定は必要ありません。

1. vSphere Client で対象サーバ上の VMware ESXi にログインします。
2. [構成]タブの[セキュリティプロファイル]を選択し、サービスの[プロパティ]を選択します。
3. 「SSH」を選択し、[オプション]を選択します。
4. 「サービスコマンド」の[開始]を選択して SSH サービスを開始し、[OK]を選択します。

[注意]

VMware ESXi の SSH を有効にすると、vSphere Client 上に以下のメッセージが表示されます。

構成の問題 　ホストの SSH は有効になっています

(2)　CIM サーバの SSLv3 を有効化

SSLv3 のサポートが CIM サーバ(ポート 5989)に対して無効になっています。sfcb.cfg ファイルを編集し、SSLv3 を有効にします。

1. SSH で VMware ESXi がインストールされている対象サーバに管理者権限でログインします。
2. チャレンジレスポンス認証を使用してログインします。
3. /etc/sfcb/sfcb.cfg ファイルを編集して、以下の 1 文を追加し、SSLv3 を有効にします。

enableSSLv3: true

sfcbd-watchdog を再起動します。以下のコマンドを実行します。

#/etc/init.d/sfcbd-watchdog restart

[注意]

vSphere ESXi 5.5 Update 2 以前のリリースについてセキュリティパッチ(ESXi550-201501101-SG)を適用していない場合には POODLE セキュリティ脆弱性が発生する可能性があります。必ずセキュリティパッチを適用してから SSLv3 の有効化設定をお願いいたします。

・VMware Security Patching Guidelines for ESXi and ESX (2020972)
https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2020972

・VMware ESXi 5.5, Patch ESXi550-201501101-SG: Updates esx-base (2099273)
https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2099273

(3)　SSH サービスの停止

1. vSphere Client で対象サーバ上の VMware ESXi にログインします。
2. [構成]タブの[セキュリティプロファイル]を選択し、サービスの[プロパティ]を選択します。
3. 「SSH」を選択し、[オプション]を選択します。
4. 「サービスコマンド」の[停止]を選択して SSH サービスを停止し、[OK]を選択しま

す。

2.4.2. VMware ESXi 6.5 における SSLv3 のサポートの有効化

(1) SSH サービスの起動

すでに SSH サービスが起動中の場合、本設定は必要ありません。

1. VMware Host Client で対象サーバ上の VMware ESXi にログインします。
   Web ブラウザから、https://<ESXi の IP アドレス>/ui/にアクセスします。
2. [ホスト]の[管理]を選択し、ESXi の管理画面を開きます。
3. [サービス]タブを選択し、サービスの一覧から「SSH」を選択します。
4. 「起動」を選択します。

[注意]

VMware ESXi の SSH を有効にすると、VMware Host Client 上に以下のメッセージが表示されます。

このホストでは SSH が有効です。 管理に必要な場合を除き、SSH を無効にする必要があります。

(2) CIM サーバの SSLv3 を有効化

SSLv3 のサポートが CIM サーバ(ポート 5989)に対して無効になっています。
sfcb.cfg ファイルを編集し、SSLv3 を有効にします。

1. SSH で VMware ESXi がインストールされている対象サーバに管理者権限でログインします。
2. チャレンジレスポンス認証を使用してログインします。
3. /etc/sfcb/sfcb.cfg ファイルを編集して、以下の 1 文を追加し、SSLv3 を有効にします。

enableSSLv3: true

sfcbd-watchdog を再起動します。以下のコマンドを実行します。

#/etc/init.d/sfcbd-watchdog restart

(3) SSH サービスの停止

1. VMware Host Client で対象サーバ上の VMware ESXi にログインします。
   Web ブラウザから、https://<ESXi の IP アドレス>/ui/にアクセスします。
2. [ホスト]の[管理]を選択し、ESXi の管理画面を開きます。
3. [サービス]タブを選択し、サービスの一覧から「SSH」を選択します。
4. 「停止」を選択します。

2.4.3. ドメインユーザーアカウント使用時の設定

(1) ISM-VA へドメイン情報の追加

ドメインユーザーアカウントでの監視を行う際には「ISM2.1 ユーザーズマニュアル」（3.4.2 ISM 初期設定)を実施してください。

(2) ISM-VA へ DNS 情報の追加

ドメインユーザーアカウントでの監視を行う際には「ISM2.1_ユーザーズマニュアル」(4.9 ネットワーク設定 DNS サーバ追加)を行い ISM-VA に DNS サーバの登録を実施してください。

3. 監視対象への設定手順（仮想化管理ソフトウェア）

3.1. vCenter Server への設定手順

3.1.1. ISM-VA へ DNS 情報の追加

vCenter に ESXi ホストを FQDN で登録している環境で監視を行う際には「ISM2.1_ユーザーズマニュアル」(4.9 ネットワーク設定 DNS サーバ追加)を行い ISM-VA に DNS サーバの登録を実施してください。

3.1.2. ドメインユーザーアカウント使用時の設定

(1) vCenter Server に登録されている各ホストへの設定

vCenter Server から情報を取得するためには、vCenter Server に登録されている各ホストへの設定が完了している必要があります。「2.4VMware ESXi への設定手順」を参照し、各ホストへの設定を実施してください。

(2) ISM-VA へドメイン情報の追加

ドメインユーザーアカウントでの監視を行う際には「ISM2.1 ユーザーズマニュアル」（3.4.2 ISM 初期設定)を実施してください。

(3) ISM-VA へ DNS 情報の追加

ドメインユーザーアカウントでの監視を行う際には「ISM2.1_ユーザーズマニュアル」(4.9 ネットワーク設定 DNS サーバ追加)を行い ISM-VA に DNS サーバの登録を実施してください。

3.2. Microsoft Failover Cluster への設定手順

3.2.1. ドメインユーザーアカウント使用時の設定

(1) クラスタを構成する各ホストへの WinRM 設定

Microsoft Failover Cluster から情報を取得するためには、クラスタを構成する各ホストへの設定が完了している必要があります。「2.1. Windows への設定手順」を参照し、各ホストへの設定を実施してください。

(2) Active Directory への SPN の追加

ドメインユーザーアカウントを使用し Windows Server の監視をする際には監視対象サ

ーバのサービスプリンシパル名(SPN)を正しく Active Directory に登録する必要があります。以下の手順を実行し、監視対象サーバのサービスプリンシパル名を登録してください。

```
>setspn -A HOST/[監視対象クラスタ IP] [監視対象クラスタ名]
```

確認方法

```
> setspn -L [監視対象クラスタ名]
```

(3) ISM-VA へドメイン情報の追加

ドメインユーザーアカウントでの監視を行う際には「ISM2.1 ユーザーズマニュアル」（3.4.2 ISM 初期設定)を実施してください。

(4) ISM-VA へ DNS 情報の追加

ドメインユーザーアカウントでの監視を行う際には「ISM2.1_ユーザーズマニュアル」(4.9 ネットワーク設定 DNS サーバ追加)を行い ISM-VA に DNS サーバの登録を実施してください。

(5) Active Directory へ Kerberos 委任の構成

1. Active Directory サーバにログオンします。
2. サーバー・マネージャーを開きます。
3. [ツール]ボタンから[Active Directory ユーザーとコンピューター]を選択します。
4. ドメインを展開し、[コンピューター]フォルダを展開します。
5. 右側ウィンドウで、クラスタノード名を右クリックし、[プロパティ]を選択します。
6. [委任]タブで、[任意のサービスへ委任でこのコンピューターを信頼する]チェックボックスがオンになっていることを確認します。
7. [OK]を選択し全てのクラスタノードに対して 3～4 を実施してください。

3.3. Microsoft System Center への設定手順

「2.1. Windows への設定手順」を参照し Microsoft System Center のインストールされている各ホスト・仮想マシンに対して設定を実施して下さい。