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8月

富士通株式会社

		改版履歴
版数	提供年月	変更内容
01	2017年7月	新規作成
02	2017年8月	 • 2.2.Red Hat Enterprise Linux への設定手順 に 2.2.3.一般ユーザーアカウント使用時の設定 を新規追加
		 ・2.3.SUSE Linux Enterprise Server への設定手順 に 2.3.4.一般ユーザーアカウント使用時の設定 を新規追加 ・3.4. KVM への設定手順 を新規追加

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	0	-	×	-	-	-	0
	7.x	0	-	×	-	-	-	0
SUSE Linux Enterprise	11	0	-	0	-	-	-	0
Server	12	0	-	0	-	-	-	0
Windows Server	2008R2	-	0	0	-	0	0	0
	2012	-	0	0	-	0	0	0
	2012R2	-	0	0	-	0	0	0
	2016	-	0	0	-	0	0	0
VMware ESXi	5.x	-	-	-	0	-	-	0
	6.x	-	-	-	0	-	-	0

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	ドメイン		
		の設定			
		WinRM	SPN	ISM-VA 設定	Kerberos 委任構成
vCenter Server	5.5 以降	-	-	0	-
	6.x 以降	-	-	0	-
Microsoft Failover Cluster	Windows	0	0	0	0
	Server				
	2012以降				
Microsoft System Center	2012以降	0	0	\bigcirc	0
KVM RedHat		-	-	0	0
KVM SUSELinuxEnterprise		-	-	0	0

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_CO	DE : 0 (0x0)
SERVICE_EXIT_C	ODE : 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="数值"}

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) <u>https://developer.microsoft.com/ja-jp/windows/downloads/windows-10-sdk</u>

[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。

-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
- <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。

- <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。

 $PS C:\Windows\system 32> ls \ cert: LocalMachine\my$

ディレクトリ: Microsoft.PowerShell.Security\Certificate::LocalMachine\my

Thumbprint

Subject

 $1C3E462623BAF91A5459171BD187163D23F10DD9 \qquad CN = 192.168.10.10$

(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
Copyright 2017 FUJITSU LIMITED

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 <u>http://go.microsoft.com/fwlink/?LinkID=135170</u>

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 ヘ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 ヘ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。

ドメインユーザーアカウント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. 一般ユーザーアカウント使用時の設定

root ユーザー以外の一般ユーザーアカウントで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) sudo コマンドの設定

該当ユーザーアカウントが、一般ユーザーアカウントのログインパスワードで sudo コ マンドが実行できるように監視対象サーバの設定を変更する必要があります。

以下は、user1 のログインパスワードで sudo コマンドが実行できるように設定する場合の例です。

1. /etc/sudoers ファイルを編集します。

```
# visudo
:
#Defaults targetpw ・・・コメントアウト
root ALL=(ALL) ALL
user1 ALL=(ALL) ALL ・・・user1を追加
:
```

2. user1 ユーザーで、監視対象サーバに ssh でログインします。sudo コマンドを実行 した際に user1 のパスワードが求められれば、設定完了です。

(2) 環境変数の設定

該当アカウントで、監視対象サーバに ssh でログインした後、プロンプト表示文字列が、 下記の条件を満たしていることを確認してください。下記の条件を満たしている場合、 プロンプト表示文字列の設定を変更しないでください。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。

- ・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) [user1@localhost ~]\$

環境変数 PS1 の設定値例)

[user1@localhost ~]\$ echo \$PS1 [¥u@¥h ¥W]¥\$

2.2.4. 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/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、該当アカウントの環境変数 PS1 の設 定が必要です。「2.2.3 一般ユーザーアカウント使用時の設定(2)環境変数の設定」を参 考に環境変数 PS1 を設定してください。

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。

	YaSI Control Center	
Software Hardware Sostem Network Devices Network Services Security and Users Virtualization Support Niscellaneous	AppArmor Configuration CA Management Common Server Certificate Firewall Linux Audit Framework (LAF) Security Center and Handening Sudo User and Group Management	
Help]		R.m][Q .)

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

Start Us	Firewall Conf	isuration: Start-Up	
Interfaces	Service Star	t	
Allowed Services	(x) Enable F	irewall Automatic Starting	
Hissoueradina	() Disable	d Off-	
Broadcast	Seitch On ar	us: Firewall is running	
Lossing Level	Current Stat	tor Firewall Now	
Oaston Rules	(Save Settin	as and Restart Firewall Now	
(Hele)	(Bidi)	(Caros))	ONeit1

[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。

Start-Ub Interfaces Nasouerading Broadcast Broadcast	Firewall Configuration: Allowed Services Allowed Services for Selected Zone External Zone Service to Allow bind DNS server				
Ouston Rules	Allowed Servi Secure Shell	ce Description Server Open ports for S			
	E] Protect Fi	remail from Internal ZonL	Advanced]		
[Helo]	(Babba)	[Cancel]	(Next)		
Help BS Add BS	Delete 7 Ad	vanced F8 Cancel FI	Next		

 [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。

Firemil Starti	ne:		
* Enable fire * Firemall st	wall automatic startin arts after the config	ns uration has been writte	'n
Unassigned Inte	rfaces		
No network * eth0 * eth1 * eth2 * eth3 * eth4 * eth5	traffic is permitted (through these interface	s.
1 Store Details	1.00	(Berry 1)	

[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 ヘ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。

ドメインユーザーアカウント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. 一般ユーザーアカウント使用時の設定

root ユーザー以外の一般ユーザーアカウントで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) sudo コマンドの設定

該当ユーザーアカウントが、一般ユーザーアカウントのログインパスワードで sudo コ マンドが実行できるように監視対象サーバの設定を変更する必要があります。

以下は、user1 のログインパスワードで sudo コマンドが実行できるように設定する場合の例です。

1. /etc/sudoers ファイルを編集します。

# visud	0		
:			
#Defaults targetpw			・・・コメントアウト
root	ALL=(ALL)	ALL	
user1	ALL=(ALL)	ALL	・・・user1を追加
:			

- 2. user1 ユーザーで、監視対象サーバに ssh でログインします。sudo コマンドを実行 した際に user1 のパスワードが求められれば、設定完了です。
- (2) 環境変数の設定

該当ユーザーアカウントで、監視対象サーバに ssh でログインした後、プロンプト表示 文字列が、下記の条件を満たしていることを確認してください。下記の条件を満たして いる場合、プロンプト表示文字列の設定を変更しないでください。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。

- ・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) [user1@localhost ~]\$

環境変数 PS1 の設定値例)

[user1@localhost ~]\$ echo \$PS1 [¥u@¥h ¥W]¥\$

2.3.5. 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

 \flat

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、該当アカウントの環境変数 PS1 の設 定が必要です。「2.3.4 一般ユーザーアカウント使用時の設定 (2) 環境変数の設定」を参 考に環境変数 PS1 を設定してください。

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。
- 「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=displ ayKC&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=displ ayKC&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。
- 「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。

- 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

- 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 ヘ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 ヘ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 ヘ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。

3.4. KVM への設定手順

3.4.1. KVM Red Hat Enterprise Linux への設定手順(ドメインユーザー使用時)

KVM 情報を取得するため、監視対象で SSSD サービスを設定します。 必要なパッケージを以下に示します。

- krb5-workstation
- samba
- samba-client
- samba-common
- sssd

以降は、ターミナルより root ユーザーで設定してください。

(1) 「/etc/hosts」の編集

「/etc/hosts」ファイルを開きます。

vi /etc/hosts

- ・ 以下を追記してください。
 - ▶ 監視対象となる KVM サーバの IP アドレスと FQDN、ホスト名
 - ▶ ISM-VAのIPアドレス

例)

192.168.30.222 rhel73.win2016.local rhel73

192.168.30.228

※この設定はローカル(ホスト内)でのホスト名には反映されません。しかしこの設定 がないと後述の Active Directory への参加コマンド実行時にエラーとなります。

(2) 「/etc/krb5.conf」の編集

「/etc/krb5.conf」ファイルを開きます。

vi /etc/krb5.conf

・ セクション [libdefaults] の default_realm にドメイン名を大文字で設定します。

例)

[libdefaults] dns_lookup_realm = true dns_lookup_kdc = true ticket_lifetime = 24h renew_lifetime = 7d forwardable = true default_realm = WIN2016.LOCAL

・ セクション [realms] を設定します。

例)

[realms]
WIN2016.LOCAL = {
kdc = 192.168.30.69
admin_server = WIN2016-ADVM.WIN2016.LOCAL
1

- ・ kdc には Kerberos のチケットを発行するサーバの IP アドレスを設定します。
- ・ admin_server には Kerberos 管理サーバの FQDN を設定します。
- 通常は kdc と admin_server は DNS サーバと Active Directory サーバと同じ サーバです。
- ・ セクション [domain_realm]を設定します。

例)

[domain_realm] win2016.local = WIN2016.LOCAL .win2016.local = WIN2016.LOCAL

※大文字・小文字は上記の例のようにし、実際に使用しているドメイン名を設定してく ださい。

(3) 「/etc/samba/smb.conf」の編集

「/etc/samba/smb.conf」ファイルを開きます。

vi /etc/samba/smb.conf

・ [global] セクション以外を全て削除し、[global] セクションを以下のように設定しま す。

例)

[global] workgroup = WIN2016 client signing = yes client use spnego = yes kerberos method = secrets and keytab log file = /var/log/samba/%m.log realm = WIN2016.LOCAL

security = ads

※workgroup と realm は実際に使用しているドメイン名を設定してください。

(4) 「/etc/sssd/sssd.conf」の作成

「/etc/sssd/sssd.conf」ファイルを開きます。初期状態で存在しないので、新規作成しま す。

vi /etc/sssd/sssd.conf

例)

[sssd] config_file_version = 2 services = pam,nss

domains = WIN2016.LOCAL

[pam]

[nss] filter_groups = root

filter_users = root

[domain/WIN2016.LOCAL]

id_provider = ad auth_provider = ad enumerate = false cache_credentials = false case sensitive = false

※[sssd] セクションの domains とセクション名 [domain/WIN2016.LOCAL] は実際に 使用しているドメイン名を設定してください。

ドメインユーザーのログイン時にホームディレクトリを自動作成する場合
 「/etc/sssd/sssd.conf」の[domain/ドメイン名]セクションに以下を追加します。

fallback_homedir = /home/%u

(5) 「/etc/sssd/sssd.conf」のパーミッションの変更

「/etc/sssd/sssd.conf」のパーミッションを 600 に変更します。

chmod 600 /etc/sssd/sssd.conf

※600 以外は sssd サービス起動時にエラーとなるので注意してください。

(6) ローカル (ホスト上) のホスト名設定

以下のコマンドで、ローカル(ホスト上)のホスト名を設定します。

hostnamectl set-hostname $\pi \land \land \circ O$ FQDN

例)

hostnamectl set-hostname rhel73.win2016.local

※この設定はローカル(ホスト内)でのホスト名の設定です。ネットワーク上でのホス ト名には反映されません。ホストの FQDN は(1)で設定した「/etc/hosts」のホストの FQDN と一致させてください。

(7) DNS サーバの IP アドレス設定

以下のコマンドで、DNS サーバの IP アドレスを設定し、インターフェイスの再起動を 行います。

nmcli connection modify インターフェイス名 ipv4.dns "DNS サーバの IP アドレス" # systemctl restart NetworkManager

・インターフェイス名を調べるには、以下のコマンドを実行します。

if config (Red Hat Enterprise Linux 6 以下) # ip addr (Red Hat Enterprise Linux 7 以上)

・設定を確認するには、以下のコマンドを実行します。

host Kerberos 管理サーバ名

例)

host WIN2016-ADVM.WIN2016.LOCAL

出力に IP アドレスが含まれていれば正しく設定されています。

(8) Kerberos 発券許可証の入手

以下のコマンドで、Kerberos 発券許可証を入手します。

kinit Administrator

パスワードを聞かれるので、ドメイン管理ユーザーAdministrator のパスワードを入力

します。

・ 設定を確認するには、以下のコマンドを実行します。

klist

ドメイン情報が出力されれば、正しく設定されています

失敗した場合は「/etc/krb5.conf」を確認してください。

(9) Active Directory への参加

以下のコマンドで、Active Directory に参加します。

net ads join -U Administrator

パスワードを聞かれるので、ドメイン管理ユーザーAdministrator のパスワードを入力 します。

設定を確認するには、以下のコマンドを実行します。

net ads info

サーバ情報(LDAP server と表示されます)とドメイン情報が出力されれば、正しく設 定されています。

失敗した場合はホスト名の設定と「/etc/samba/smb.conf」の設定を確認してください。 または後述のホスト名を変更後ログインできなくなった場合の項を参照してください。

(10) システム認証の設定

以下のコマンドで、システム認証(監視先サーバの認証)の設定を行います。

このコマンドによって、関連設定ファイルが自動的に更新されます。

ドメインユーザーのホームディレクトリを自動作成しない場合

 $\label{eq:constraint} \mbox{ # authconfig --enablesssd --enablesssd auth --enablelocauthorize --update}$

 ドメインユーザーのホームディレクトリを自動作成する場合 あらかじめ、(4)「/etc/sssd/sssd.conf」の編集 で、「ドメインユーザーのログイン時 にホームディレクトリを自動作成する場合」を設定後、以下を実行してください。

 $\label{eq:constraint} \ensuremath{\texttt{#}}\xspace{\ensuremath{\texttt{authconfig}}\xspace{\ensuremath{\texttt{-enablesssd}}\xspace{\ensuremath{\texttt{authconfig}}\xspace{\ensuremath{\texttt{-enablesssd}}\xspace{\ensuremath{\texttt{authconfig}}\xspace{\ensuremath{authconfig}\xspace{\ensuremath{authconfig}\xs$

(11) SSSD (System Security Services Daemon)サービスの起動

以下のコマンドで SSSD サービスを起動します。

systemctl enable sssd

systemctl start sssd

サービスの起動を確認するには、以下のコマンドを実行します。

systemctl status sssd

正常に起動していれば、正しく設定されています。

失敗した場合は「/etc/sssd/sssd.conf」内容とファイルパーミッションを確認してください。

(12) ドメインユーザーでのログイン確認

・ ドメインユーザーの表記方法

ドメインユーザーの表記方法は下記のようにいくつか書き方があります。

- ユーザー名
- ・ 'ドメインプレフィックス\ユーザー名'
- ・ 'ドメインプレフィックス.ドメイン名サフィックス\ユーザー名'
- ・ 'ユーザー名@ドメインプレフィックス'
- ・ 'ユーザー名@ドメインプレフィックス.ドメイン名サフィックス'

例)

administrator

'win2016\administrator'

'win2016.local\administrator'

'administrator@win2016'

'administrator@win2016.local'

※「/etc/sssd/sssd.conf」の[domain/WIN2016.ドメイン名]で case_sensitive = false としているため、大文字・小文字の区別はしません。 ・ ドメインユーザーの存在確認

下記のコマンドのいずれかを用いて、ドメインユーザーの存在確認ができます。ユー ザー名は上記のユーザー名の表記方法のどれを用いても結構です。

#id ユーザー名

getent passwd ユーザー名

ユーザー情報が表示されれば、正しく設定されています。

・ ドメインユーザーでのログイン確認

以下のコマンドのいずれかを用いて、SSH プロトコルでのログイン確認ができます。 ユーザー名は上記のユーザー名の表記方法のどれを用いても結構です。

# ssh ユーザー名@監視対象サーバ IP アドレス	
#ssh -l ユーザー名 監視対象サーバ IP アドレス	

例)

ssh administrator@192.168.30.222
ssh 'administrator@win2016'@192.168.30.222
ssh -l 'win2016.local\administrator' 192.168.30.222

どの方法でもログインできれば、正しく設定されています。

(13) ドメインユーザーの設定

「3.4.3 一般ユーザーアカウント使用時の設定」にしたがって、ドメインユーザーの設定 を行ってください。

- トラブルシューティング
 - ホスト名を変更後ログインできなくなった場合
 ネットワーク上のホスト名とローカルのホスト名の両方を変更した後、以下の2
 つのコマンドを実行します。

net ads join -U Administrator

systemctl restart sssd

それでもログインに失敗する場合は、過去の設定が「/etc/krb5.keytab」に残って いる可能性があるため、以下のコマンドで/etc/krb5.keytab を削除してから、上記 のコマンドを再実行します。

rm /etc/krb5.keytab

(14) ISM-VA ヘドメイン情報の追加

「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。

(15) ISM-VA へ DNS 情報の追加

「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。

3.4.2. KVM SUSE Linux Enterprise Server への設定手順(ドメインユーザー使用時 KVM 情報を取得するため、監視対象で SSSD サービスを設定します。

以降の設定は、ターミナルより yast コマンドを使うか、GUI のメニューより YaST を 使って行ってください。ここでは yast コマンドを用いた方法について示します。

(1) yast コマンドの起動

ターミナルより root ユーザーで以下のコマンドを実行します。

yast

yast 内での項目の選択は、矢印キーと TAB キーを組み合わせて選択します。

- (2) ホスト名/DNS の設定
- 1. System \rightarrow Network Settings を選択し Enter キーを押します。

YaST Control Center	
Software System Hardware Network Services Security and Users /irtualization Support Miscellaneous	<pre>/etc/sysconfig Editor Boot Loader Date and Time Kernel Kdump Language Network Settings Partitioner Services Manager</pre>
lelpl	[Run][Quit

- 2. Hostname/DNS を選択し、以下の項目を設定してから OK 選択し、Enter キーを押 します。
 - Hostname
 - Domain Name
 - Assign Hostname to Loopback IP
 - Name Server 1

<pre>/aST2 - lan @ suse122 Network Settings Global Options—Overview—Hostname/ Hostname and Domain Name- Hostname suse122 Ist Change Rostname vie Unit [x] Assign Hostname to Loopback IP</pre>	DNS—Routing Domain Name WIN2016.LOCAL erface with dhcp	
Modify DNS Configuration Use Default Policy Name Servers and Domain Search Lis Name Server 1 192.168.30.69 Name Server 2 Name Server 3	t	
[Help]	[Cancel]	[0K
F1 Help F9 Cancel F10 OK		

- (3) SSSD サービスの設定
- 1. Network Services \rightarrow User Logon Management を選択し Enter キーを押します。

YaST Control Center		
Software System Hardware Network Services Security and Users Virtualization Support Miscellaneous	Mail Server NFS Client NFS Server NIS Client NIS Server NTP Configuration Network Services (xinetd) OpenLDAP MirrorMode Proxy Remote Administration (VNC) Samba Server Squid TFTP Server User Logon Management VPN Gateway and Clients Wake-on-LAN Windows Domain Membership iSCSI Initiator iSNS Server	
Help]		[Run][Quit

2. Change Settings を選択し、Enter キーを押します。



- 3. 以下の項目にチェックを入れ、Join Dom を選択し、Enter キーを押します。
 - Allow Domain User Logon
 - Users
 - Groups

YaST2 - auth-client @ suse122	
Manage Domain User Logon	Options - Global Options
Daemon Status: Stopped [x] Allow Domain User Logon [] Create Home Directory Enable domain data source: [x] Users [x] Groups [] Super-User Commands (sudo) [] Super-User Commands (sudo) [] Map Network Drives (automount) [] SSH Public Keys [] Privilege Account Certificate (MS 	Name Value
[Join Dom][Leave Dom][Clear Domain Cac] [OK] [C	[Edit][Delete][Extended Options] ancel]
TEA BOURDER FTO OK	

- 4. 以下の項目を設定してから OK を選択し、Enter キーを押します。
 - Domain name
 - Which service provides identity data, such as user names and group members Microsoft Active Directory
 - Which service handles user authentication?

Microsoft Active Directory

• Enable the domain

YaST2 - auth-client @ suse122
Domain name (such as example.com): WIN2016.LOCAL Which service provides identity data, such as user names and group membersh Delegate to third-party software library (proxy_lib_name) FreeIPA Generic directory service (LDAP) Local SSSD file database Microsoft Active Directory
Which service handles user authentication? Delegate to third-party software library (proxy_lib_name) FreeIPA Generic Kerberos service Generic directory service (LDAP) Local SSSD file database Microsoft Active Directory The domain does not provide authentication service
[x] Enable the domain
[OK] [Cancel]
F9 Cancel F10 0K

5. 全ての項目を空白またはチェックを外し、OKを選択し、Enterキーを押します。

YaST2 - auth-client @ suse122
Domain name (such as example.com): WIN2016.LOCAL Which service provides identity data, such as user names and group membersh Delegate to third-party software library (proxy_lib_name) FreeIPA
-Mandatory Parameters
Optional Parameters AD hostname (optional) - may be set if hostname(5) does not reflect the FQD Host names of AD servers (comma separated). [] Cache credentials for offline use [] Treat user and group names as case sensitive. [] Read all entities from backend database (increase server load)
[OK] [Cancel]
[x] Enable the domain
[OK] [Cancel]
F9 Cancel F10 OK

- 6. 以下の項目を設定してから OK を選択し、Enter キーを押します。
 - Username
 - Password
 - Update AD's DNS records as well

YaST2 - auth-client @ suse122		
Active Directory enrollme	it	
Current status		
Name Active Directory Server Active Directory Domain Workgroup Enrollment Status	Value WIN2016-ADVM.WIN2016.LOCAL (Auto-discovered via DN WIN2016.LOCAL WIN2016 Not yet enrolled	
Enter AD user credentials Username Administrator Password	(e.g. Administrator) to enroll or re-enroll this com	
[x] Up d ate AD's DNS record Op t ional Organisation Unit	ds as well t such as "Headquarter/HR/BuildingA"	
[] Overwrite Samba configuration to work with this AD		
[OK]		

7. OKを選択し、Enter キーを押します。

rasiz - auth-client @ suseizz		
Active Directory enrollment		
Current status		
Name Value Active Directory Server WIN2016-ADVM.WIN2016.LOCAL (Auto-discovered via DN		
Activ		
Enrol Enrollment has completed successfully! Command output: Using short domain name WIN2016 Joined 'SUSE122' to dns domain 'WIN2016.LOCAL' Enter A is com		
Usernam		
<pre>[x] Upda Optional Organisation Unit such as "Headquarter/HR/BuildingA" [] Overwrite Samba configuration to work with this AD</pre>		
[0 K]		
F10 OK		

ドメインユーザーのホームディレクトリを作成する場合は 8.に進みます。 ドメインユーザーのホームディレクトリを作成しない場合は 11.へ進みます。 8. 以下の設定をしてから Extended Options を選択し、Enter を押します。

Create Home Directory

Edit][Delete][Ext	ended Options]
E	dit][Delete] <mark>[Ext</mark> cel]

- 9. 以下の項目を選択してから Add を選択し、Enter キー押します。
 - fallback_homedir

YaST2 - auth-client @ suse122	
Extended options - domain/WIN2016.LOCAL	
Name filter:	
Name	Description
override homedir	Override the user's home director
proxy fast alias	When a user or group is looked up
subdomain homedir	Use this homedir as default value
simple allow users	Comma separated list of users who
simple_allow_groups	Comma separated list of groups wh
simple deny users	Comma separated list of groups th
ad_domain	Specifies the name of the Active
ad_server	Host names of AD servers (comma s
ad_backup_server	Host names of backup AD servers (
ad_hostname	AD hostname (optional) - may be s
fallback_homedir	Set a default template for a user
default_shell	The default shell to use if the p
ldap_idmap_range_min	Specifies the lower bound of the
ldap_idmap_range_max	Specifies the upper bound of the
ldap_idmap_range_size	Specifies the number of IDs avail
ldap_idmap_default_domain_sid	Specify the domain SID of the def
ldap_idmap_default_domain	Specify the name of the default d
ldap_idmap_autorid_compat	Changes the behavior of the ID-ma
ldap_use_tokengroups	(Active Directory specific) Use t
ldap_uri	URIs (ldap://) of LDAP servers (c
Ldap_sudo_search_base	An optional base DN to restrict L

10. 以下の文字列を入力してから、OKを選択し、Enterキーを押します。

/home/%u



11. Name switch \rightarrow Extended Options を選択し、Enter キーを押します。

YaST2 - auth-client @ suse122		
Manage Domain User Logon		
Manage Domain User Logon Daemon Status: Stopped [x] Allow Domain User Logon [x] Create Home Directory Enable domain data source: [x] Users [x] Groups [] Super-User Commands (sudo) [] Map Network Drives (automount) [] SSH Public Keys [] Privilege Account Certificate (MS	Options - Name switch Name Value	
Join Dom][Leave Dom][Clear Domain Cac [OK] [1 [9 Cancel F10 OK	[Edit][Delete][Extended_Options] Cancel]	

- 12. 以下の項目を選択してから Add を選択し、Enter キー押します。
 - filter_users

YaST2 - auth-client @ suse122 Extended options - nss Name filter:		
Name filter: Name debug_level enum_cache_timeout entry_cache_nowait_percentage entry_negative_timeout filter_users filter_groups filter_users_in_groups override_homedir fallback_homedir override_shell allowed_shells vetoed_shells shell_fallback default_shell get_domains_timeout memcache_timeout debug_microseconds timeout reconnection_retries fd_limit	Description Level of details for logging. Can be numeric (How many seconds should cache nss_sss enumerat The entry cache can be set to automatically up Specifies for how many seconds nss_sss should Exclude certain users from being fetched by SS Exclude certain groups from being fetched by S If you want filtered user to still be group me Override the user's home directory. You can ei Set a default template for a user's home direc Override the login shell for all users. Restrict user shell to one of the listed value Replace any instance of these shells with the The default shell to use if an allowed shell i The default shell to use if the provider does Specifies time in seconds for which the list o Specifies time in seconds to the timestamp in debug mes- Timeout in seconds between heartbeats for this Number of times services should attempt to rec Maximum number of file descriptors that may be	
	[Add][Cancel]	

13. 以下の文字列を入力してから、OKを選択し、Enterキーを押します。

• root

YaST2 - auth-client @ suse122		
Extended options - nss Name filter:		
Name debug_level enum_cache_timeout entry_cache_nowait_percentage entry_negative_timeout filter_users filter_or	Description Level of details for logging. Can be numeric How many seconds should cache nss_sss enumerat The entry cache can be set to automatically up Specifies for how many seconds nss_sss should Exclude certain users from being fetched by SS	t (
filter_us Exclude certain user override_ filter_users fallback_ root	rs from being fetched by SSS backend group me ou can ei ome direct	
allowed_s	[OK] [Cancel] s. ted value with the	e
shell_fall default_shell get_domains_timeout memcache_timeout debug_timestamps debug_microseconds timeout reconnection_retries fd_limit	d shell i The default shell to use if the provider does Specifies time in seconds for which the list of Specifies time in seconds for which records in Add a timestamp to the debug messages Add microseconds to the timestamp in debug mes Timeout in seconds between heartbeats for this Number of times services should attempt to reconstruct Maximum number of file descriptors that may be	
F9 Cancel F10 OK		

14. Name switch \rightarrow Extended Options を選択し、Enter キーを押します。



15. 以下の項目を選択してから Add を選択し、Enter キー押します。

• filter_groups

1	YaST2 - auth-client @ suse122	
Extended options - nss Name filter:		
	Name debug_level enum_cache_timeout entry_cache_nowait_percentage entry_negative_timeout filter_groups filter_users_in_groups override_homedir fallback_homedir override_shell allowed_shells vetoed_shells shell_fallback default_shell get_domains_timeout memcache_timeout debug_timestamps debug_microseconds timeout reconnection_retries fd_limit client_idle_timeout	Description Level of details for logging. Can be numeric (How many seconds should cache nss_sss enumerat The entry cache can be set to automatically up Specifies for how many seconds nss_sss should Exclude certain groups from being fetched by S If you want filtered user to still be group me Override the user's home directory. You can ei Set a default template for a user's home direc Override the login shell for all users. Restrict user shell to one of the listed value Replace any instance of these shells with the The default shell to use if an allowed shell i The default shell to use if the provider does Specifies time in seconds for which the list o Specifies time in seconds for which records in Add a timestamp to the debug messages Add microseconds to the timestamp in debug mes Timeout in seconds between heartbeats for this Number of times services should attempt to rec Maximum number of file descriptors that may be- Number of seconds a client of SSSD process can
[Add][Cancel]		

16. 以下の文字列を入力してから、OKを選択し、Enterキーを押します。

• root

YaST2 - auth-client @ suse122		
Extended options - nss Name filter		
Name debug_level enum_cache_timeout entry_cache_nowait_percentage entry_negative_timeout filter_groups	Description Level of details for logging. Can be numeric (How many seconds should cache nss_sss enumerat The entry cache can be set to automatically up Specifies for how many seconds nss_sss should Exclude certain groups from being fetched by S	
filter_us override_ fallback_ override_ allowed_s vetoed_sh shell fal	ups from being fetched by SSS backend u can ei me direc [OK] [Cancel] [Cancel]	
<pre>default_sh get_domains_timeout memcache_timeout debug_timestamps debug_microseconds timeout reconnection_retries fd_limit client_idle_timeout</pre>	er does Specifies time in seconds for which the list o Specifies time in seconds for which records in Add a timestamp to the debug messages Add microseconds to the timestamp in debug mes Timeout in seconds between heartbeats for this Number of times services should attempt to rec Maximum number of file descriptors that may be Number of seconds a client of SSSD process can	
[Add][Cancel]		
F9 Cancel F10 OK		

17. OKを選択し、Enterキーを押します。







19. Quit を選択し、Enter キーを押します。

YaST Control Center		
Software System Hardware Network Services Security and Users Virtualization Support Miscellaneous	Mail Server NFS Client NFS Server NIS Client NIS Server NTP Configuration Network Services (xinetd) OpenLDAP MirrorMode Proxy Remote Administration (VNC) Samba Server Squid TFTP Server User Logon Management VPN Gateway and Clients Wake-on-LAN Windows Domain Membership iSCSI Initiator iSNS Server	
Help]		[Run][Quit

以上で SSD サービスの設定は終了です。

- (4) ドメインユーザーでのログイン確認
 - ・ ドメインユーザーの表記方法

ドメインユーザーの表記方法は下記のようにいくつか書き方があります。

- ユーザー名
- 'ドメインプレフィックス\ユーザー名'
- ・ 'ドメインプレフィックス.ドメイン名サフィックス\ユーザー名'
- 'ユーザー名@ドメインプレフィックス'
- ・ 'ユーザー名@ドメインプレフィックス.ドメイン名サフィックス'

例)

administrator

'win2016\administrator'

'win2016.local\administrator'

'administrator@win2016'

'administrator@win2016.local'

- ※ドメインのオプションの設定で case_sensitive false としているので、大文字・小文字の区別はしません。
- ・ ドメインユーザーでのログイン確認

以下のコマンドのいずれかを用いて、SSH プロトコルでのログイン確認ができます。 ユーザー名は上記のユーザー名の表記方法のどれを用いても結構です。

# ssh	#ssh ユーザー名@監視対象サーバ IP アドレス	
# ssh	-1 ユーザー名	監視対象サーバ IP アドレス

例)

ssh administrator@192.168.30.222

ssh 'administrator@win2016'@192.168.30.222

ssh -l 'win2016.local\administrator' 192.168.30.222

どの方法でもログインできれば、正しく設定されています。

(5) ドメインユーザーの設定

「3.4.3 一般ユーザーアカウント使用時の設定」にしたがって、ドメインユーザーの設定 を行ってください。

(6) ISM-VA ヘドメイン情報の追加

「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。

(7) ISM-VA へ DNS 情報の追加

「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。

3.4.3. 一般ユーザーアカウント使用時の設定

KVM 情報は基本的には root ユーザーのみで取得できます。

root ユーザー以外のユーザー(ドメインユーザーも含みます)で KVM 情報を取得する 場合は監視対象 Linux サーバ上で、対象ユーザーをグループ libvirt に追加する必要があ ります。

ユーザーをグループ libvirt に追加する場合、root ユーザーで以下を実行してください。

gpasswd -a ユーザー名 libvirt

※ユーザー名は全て小文字で設定してください。

 ユーザーをグループ libvirt から削除する場合、root ユーザーで以下を実行してくだ さい。

gpasswd -d ユーザー名 libvirt

※ドメインユーザーも上記コマンドでグループ追加・削除が可能です。