CA92344-2551-02

FUJITSU Software Infrastructure Manager V2.3
Infrastructure Manager for PRIMEFLEX V2.3
監視対象 OS、仮想化管理ソフトウェアに対する設定

2018 年 10 月

富士通株式会社

改版履歴		
版数	提供年月	変更内容
01	2018 年 8 月	新規作成
02	2018 年 10 月	1. 監視対象 OS・仮想化管理ソフトウェアごとに必要な設定一覧 ・監視対象 OS に SUSE 15 および Windows Server 2019 を追加 ・注意を追加 (ISM 2.3.0.b 以降) 2.1.3 ファイアーウォールのポート開放 ・Windows Server 2019 を追加 (ISM 2.3.0.b 以降) 2.3 SUSE Linux Enterprise Server への設定手順 ・SUSE 15 を追加 (ISM 2.3.0.b 以降)

FUJITSU Software Infrastructure Manager V2.3 および FUJITSU Software Infrastructure Manager for PRIMEFLEX V2.3 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。

以降、Infrastructure Manager を「ISM」、Infrastructure Manager for PRIMEFLEX を「ISM for PRIMEFLEX」と表記します。また、Infrastructure Manager と Infrastructure Manager for PRIMEFLEX を区別しないで説明する場合、両方を総称して「Infrastructure Manager」または「ISM」と表記します。

本書に記載の詳細や略語については、ISM または ISM for PRIMEFLEX の下記マニュアルを参照してください。

・ユーザーズマニュアル

・用語集

1. 監視対象 OS・仮想化管理ソフトウェアごとに必要な設定一覧

ISM 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	○	-	○	-	-	-	○
	15(ISM 2.3.0.b 以降)	○	-	○	-	-	-	○
Windows Server	2008R2	-	○	○	-	○	○	○
	2012	-	○	○	-	○	○	○
	2012R2	-	○	○	-	○	○	○
	2016	-	○	○	-	○	○	○
	2019(ISM 2.3.0.b 以降)	-	○	○	-	○	○	○
VMware ESXi	5.x	-	-	-	○	-	-	○
	6.x	-	-	-	○	-	-	○

表 1 監視対象 OS ごとに必要な設定一覧表

		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	○	○	○	○
KVM Red Hat		-	-	○	○
KVM SUSE Linux Enterprise		-	-	○	○

表 2 監視対象仮想化管理ソフトウェアごとに必要な設定一覧表

[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。

・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 に搭載される LAN/FC/CNA カードを管理するために、対象サーバの OS に pciutils および ethtool パッケージが導入されている必要があります。

・Linux のディスク速度、ネットワーク速度の性能監視のために、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。

・Linux のオペレーティングシステムログ、ServerView Suite ログを収集するために、対象サーバの OS に zip パッケージが導入されている必要があります。

　また、オペレーティングシステムログを収集するために、対象サーバの OS に rsyslog パッケージなどの syslog デーモンが導入されている必要があります。

・Linux の一般ユーザーアカウントで OS を管理するために、対象サーバの OS に sudo 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、ISM でもパスワードを変更してください。

2. 監視対象への設定手順（OS）

2.1. Windows への設定手順

ISM 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

(2-2)　　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

(2-2-1)　　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

(2-2-2)　　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〉
```

(2-3)　　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(2-2-1),(2-2-2)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。

(2-4)　　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）] > [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）] > [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）] > [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）] > [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”サーバ認証”となっていることを確認してください。

(3)　　WinRM サービスへの証明書に記載された拇印を登録

(3-1)　　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。

```
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
```

(3-2)　　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>"}
```

(3-3)　　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開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 または
Windows Server 2019(ISM 2.3.0.b 以降)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「ユーザーズマニュアル」(3.4.2 ISM-VA の初期設定)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「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

ISM 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「ユーザーズマニュアル」(3.4.2 ISM-VA の初期設定)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「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。

(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/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

ISM 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

SUSE Linux Enterprise Server 15(ISM 2.3.0.b 以降)

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。

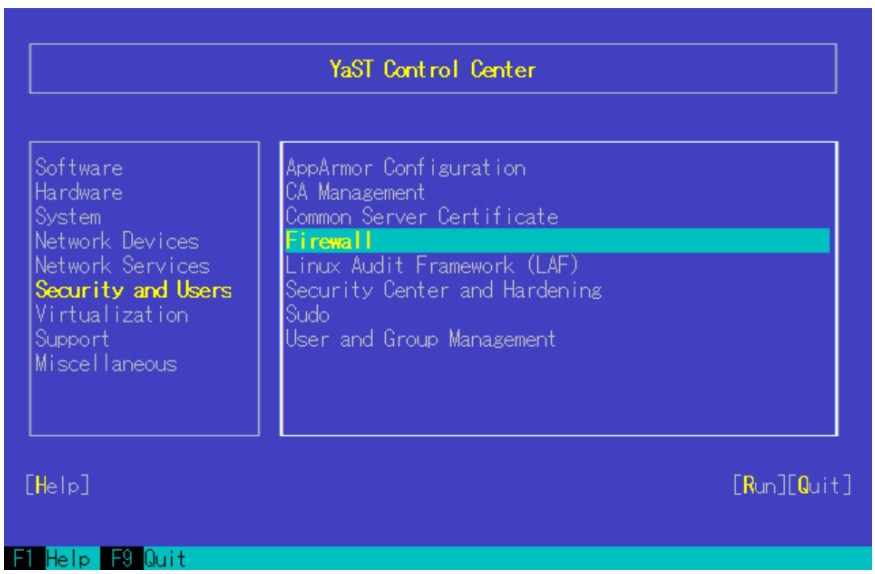
(1) SUSE Linux Enterprise Server 11 / 12

以下は、YaST を使用した場合のファイアーウォールの設定例です。

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

```
#yast
```

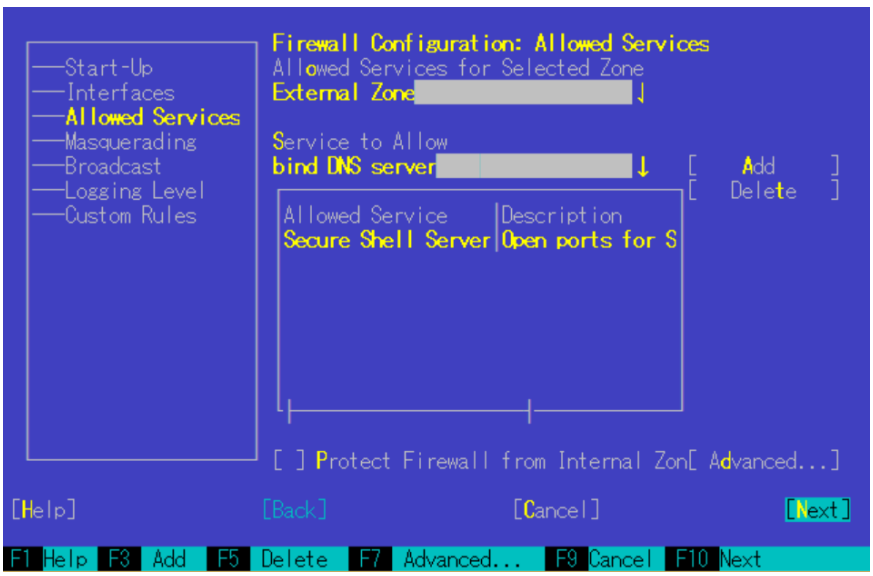
2. [Security and Users] > [Firewall] を選択し、[Enter]キーを押します。



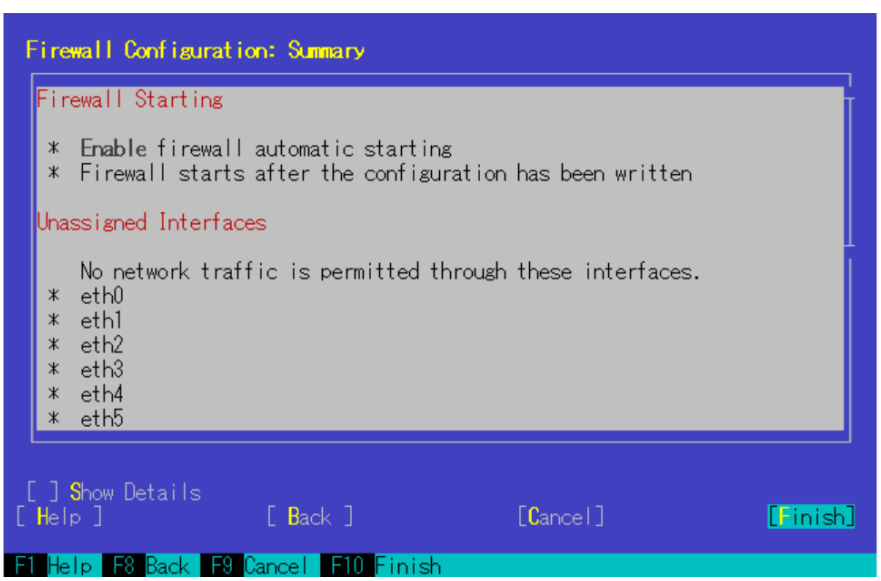
3. [Start-Up]画面から、[Service Start]の状態を「Enable Firewall Automatic Starting」にします。

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。



(2) SUSE Linux Enterprise Server 15 (ISM 2.3.0.b 以降)

SUSE Linux Enterprise Server 15 は、Yast を使用した Firewall の設定をサポートしていません。「firewall-cmd」を使用してファイアーウォールを設定します。

以下のコマンドを実行します。

```
#firewall-cmd --permanent --add-service=ssh
#firewall-cmd --reload
```

[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。ISM 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「ユーザーズマニュアル」(3.4.2 ISM-VA の初期設定)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「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、「One Command Manager 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。

```
# 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。「2.3.4 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

ISM 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 の有効化設定を実施してください。

・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 以降における 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「ユーザーズマニュアル」(3.4.2 ISM-VA の初期設定)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「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「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。「2.4 VMware 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「ユーザーズマニュアル」(3.4.2 ISM-VA の初期設定)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「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クラスタ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、監視対象クラスタ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］
```

コマンド実行結果に以下が出力されていれば、正しく登録されています。

```
HOST/[監視対象クラスタ IP]
```

(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「ユーザーズマニュアル」(3.4.2 ISM-VA の初期設定)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「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、クラスタノード名またはクラスタ名を右クリックし、[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]チェックボックスをオンにします。
7. [OK]を選択し全てのクラスタノードおよびクラスタに対して 5～6 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
 }
```

・ 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 ホストの 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。

```
# ifconfig （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
```

パスワードの入力を要求されるので、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
```

パスワードの入力を要求されるので、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

```
# authconfig --enablesssd --enablesssdauth --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。

```
# authconfig --enablesssd --enablesssdauth --enablelocauthorize --enablemkhomedir
--update
```

(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 へドメイン情報の追加

「ユーザーズマニュアル」（3.4.2 ISM-VA の初期設定)を実施してください。

(15)　ISM-VA へ DNS 情報の追加

「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

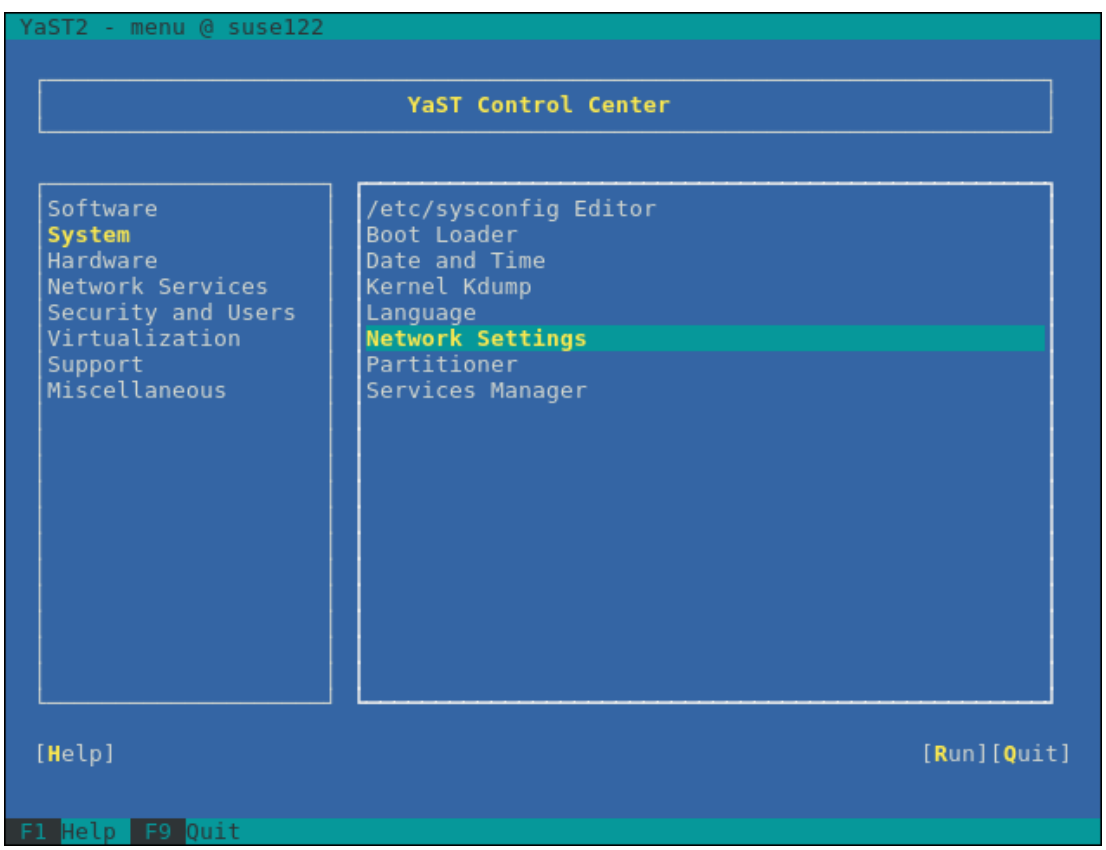
ターミナルより root ユーザーで以下のコマンドを実行します。

```
# yast
```

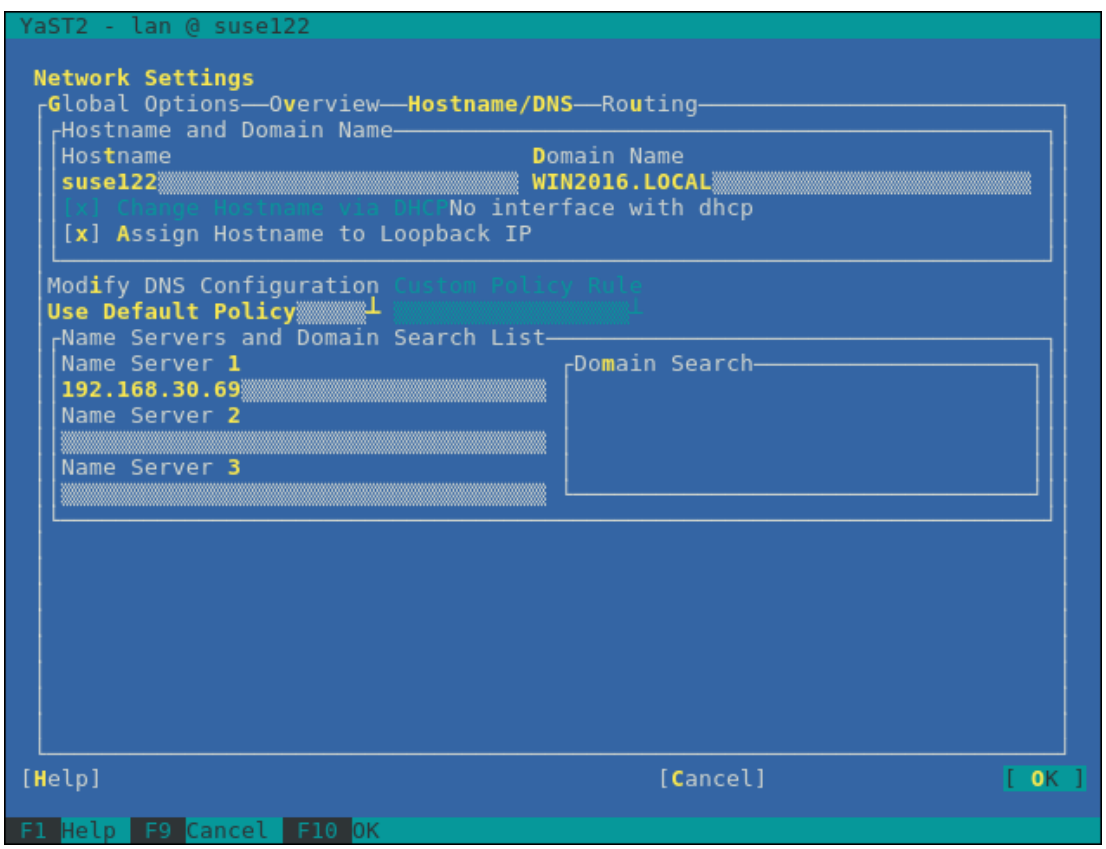
yast 内での項目の選択は、矢印キーと TAB キーを組み合わせて選択します。

(2) ホスト名／DNS の設定

1. System → Network Settings を選択し Enter キーを押します。

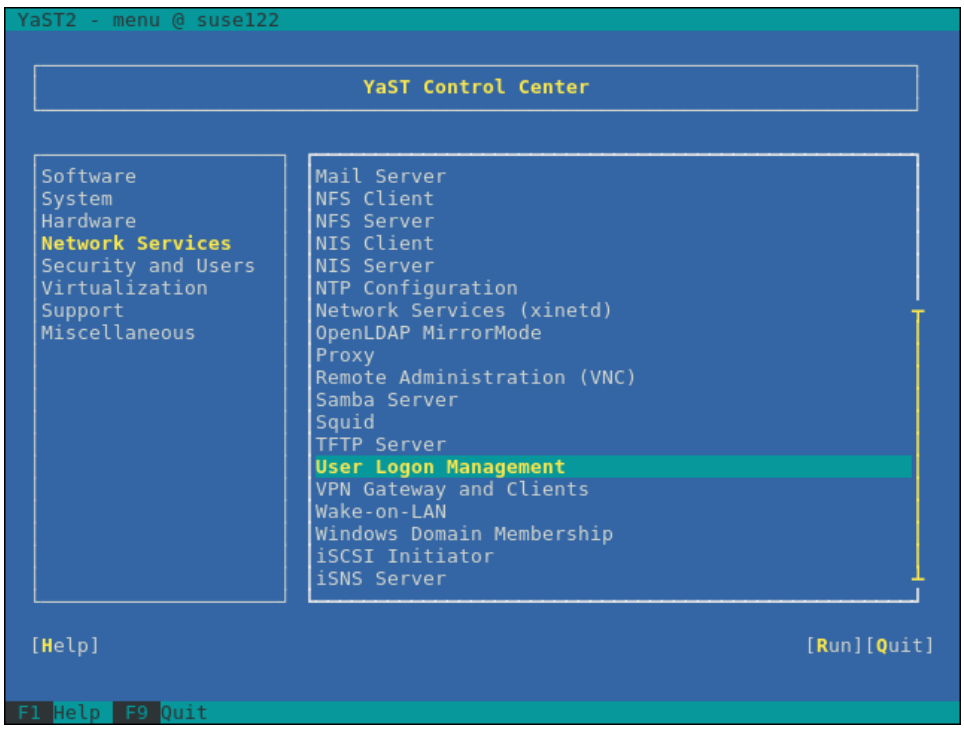


2. Hostname/DNS を選択し、以下の項目を設定してから OK を選択し、Enter キーを押します。
   - Hostname
   - Domain Name
   - Assign Hostname to Loopback IP
   - Name Server 1

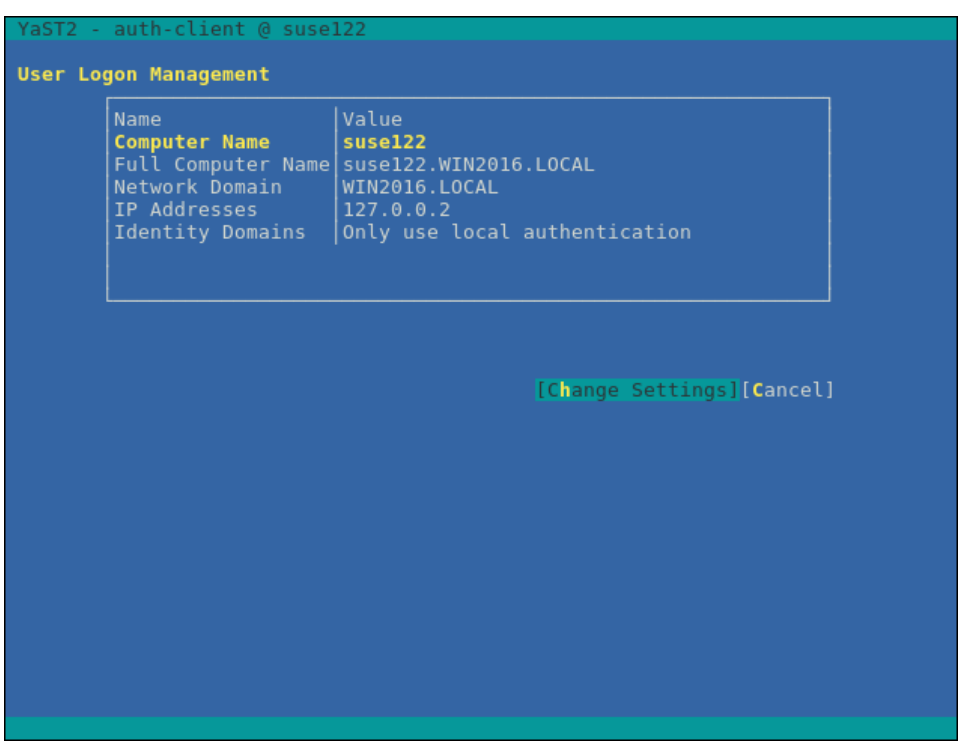


(3)　　SSSD サービスの設定

1.　Network Services → User Logon Management を選択し Enter キーを押します。

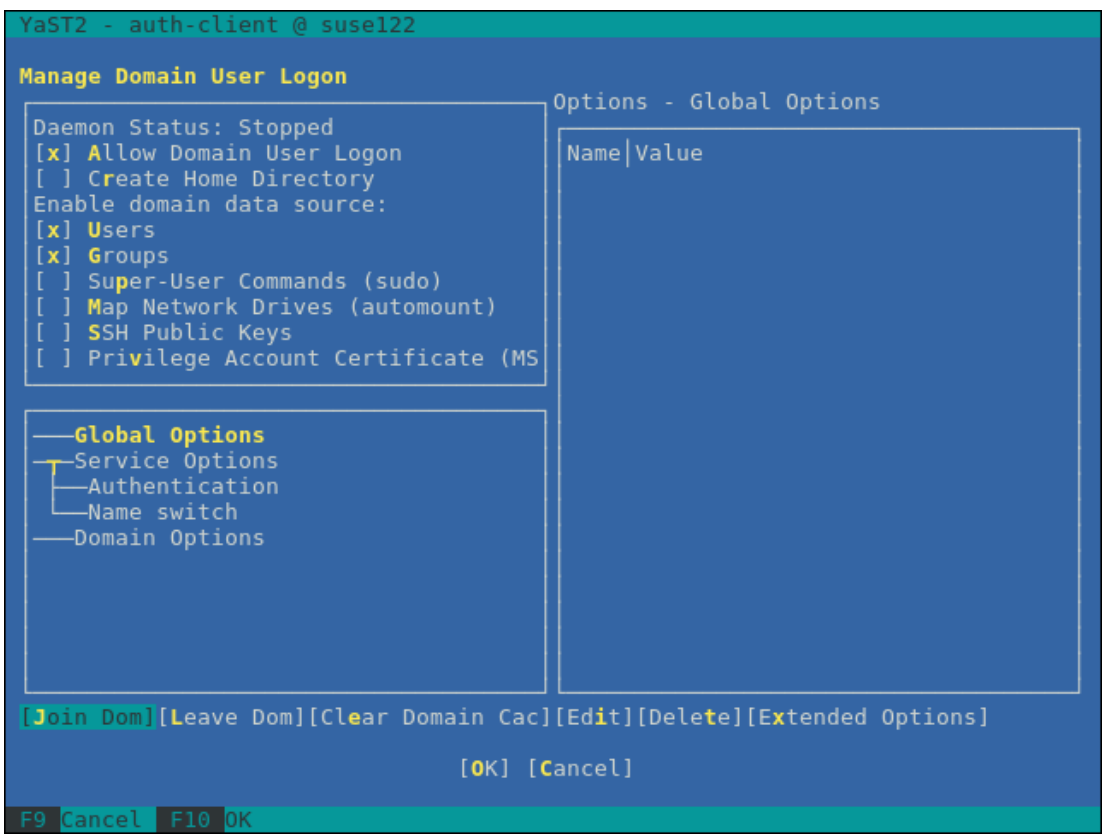


2.　Change Settings を選択し、Enter キーを押します。



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

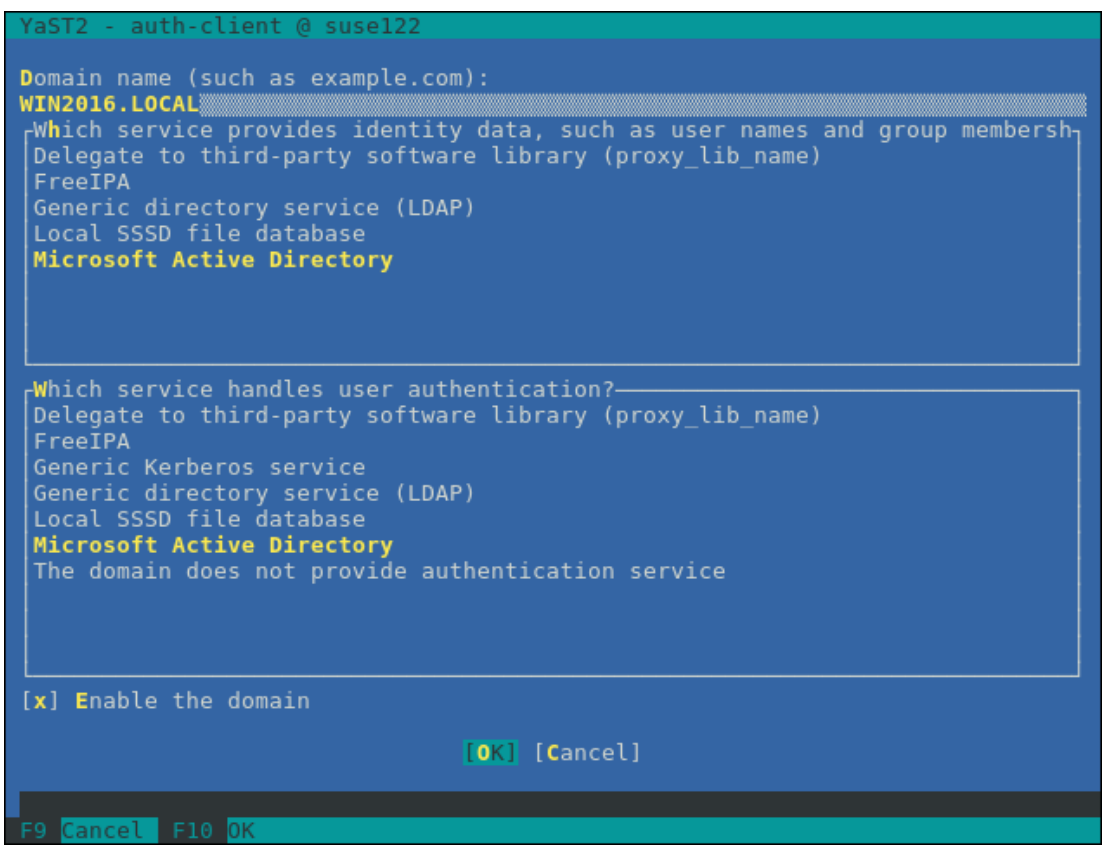


4. 以下の項目を設定してから OK を選択し、Enter キーを押します。

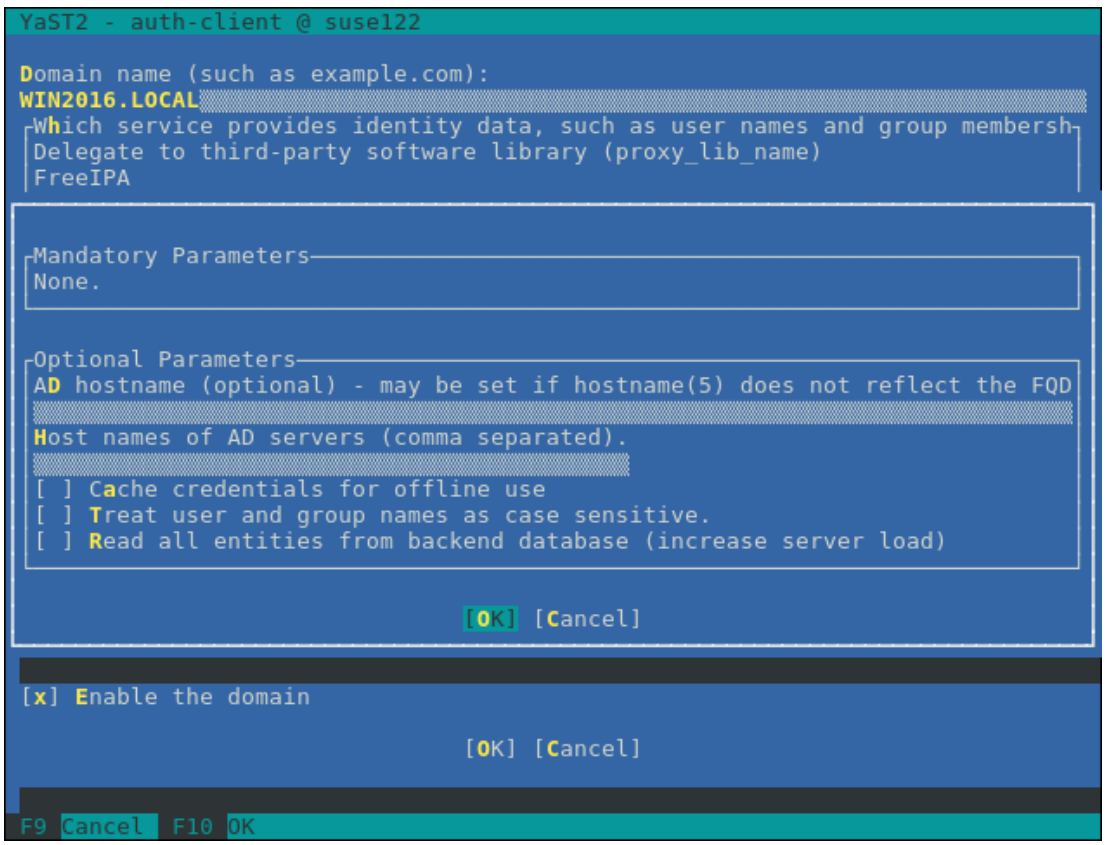
- Domain name
- Which service provides identity data, such as user names and group members

  Microsoft Active Directory
- Which service handles user authentication?

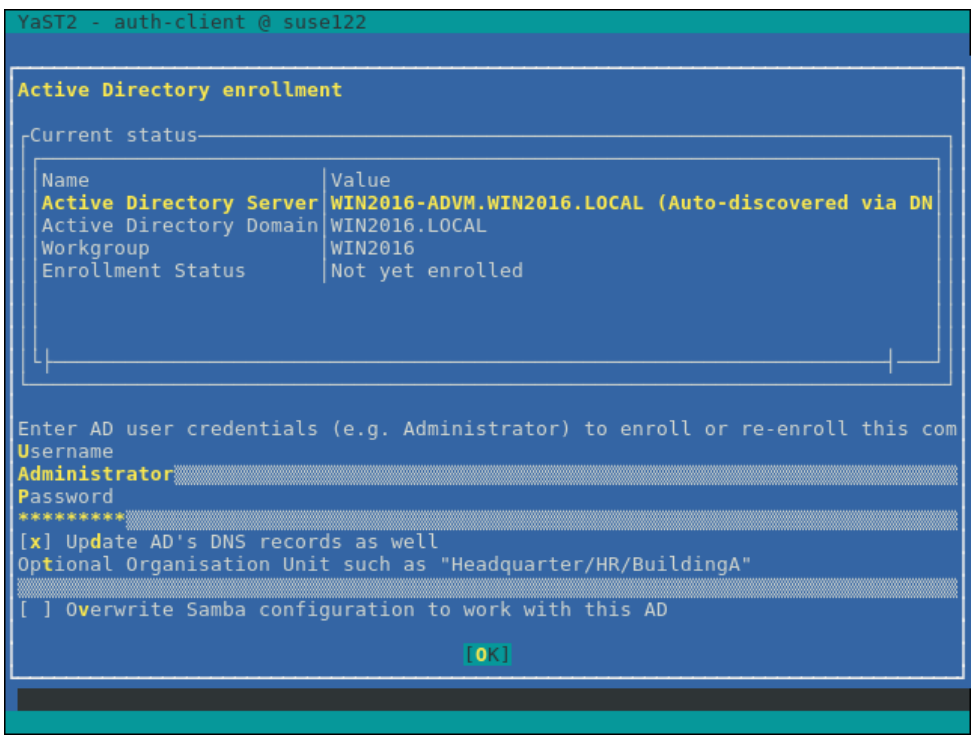
  Microsoft Active Directory
- Enable the domain



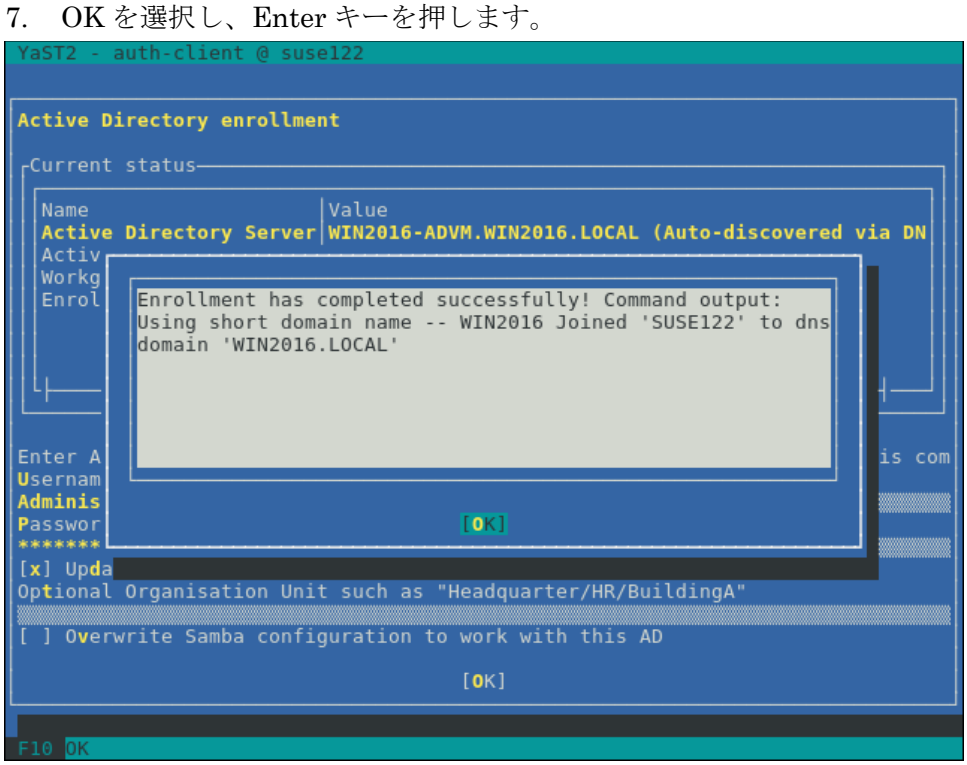
5.　全ての項目を空白またはチェックを外し、OK を選択し、Enter キーを押します。



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



7. OK を選択し、Enter キーを押します。

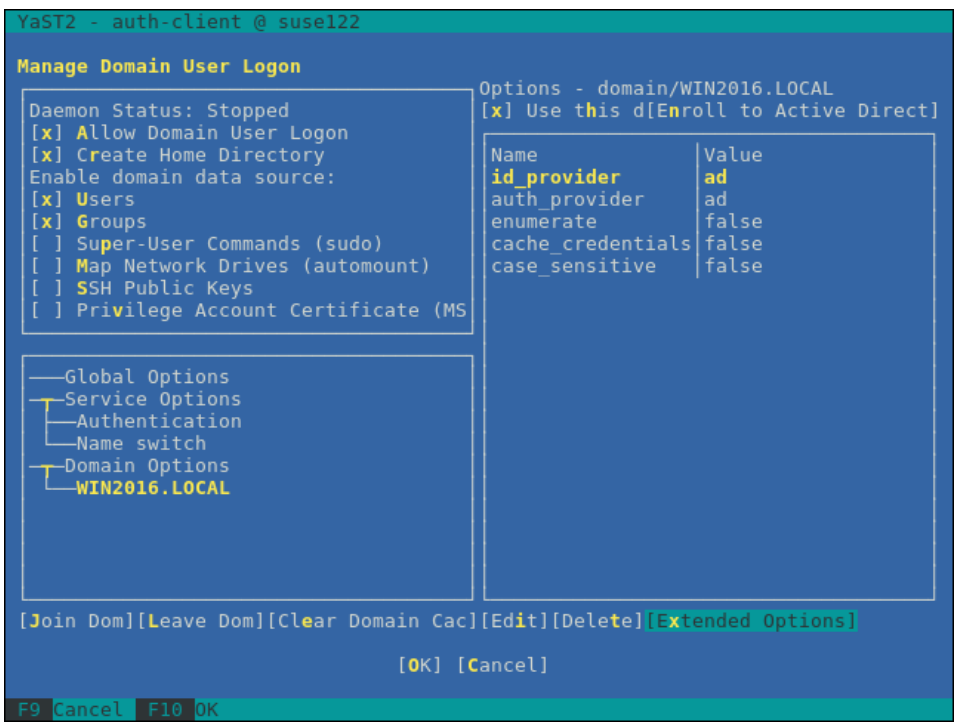


ドメインユーザーのホームディレクトリを作成する場合は 8.に進みます。

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。

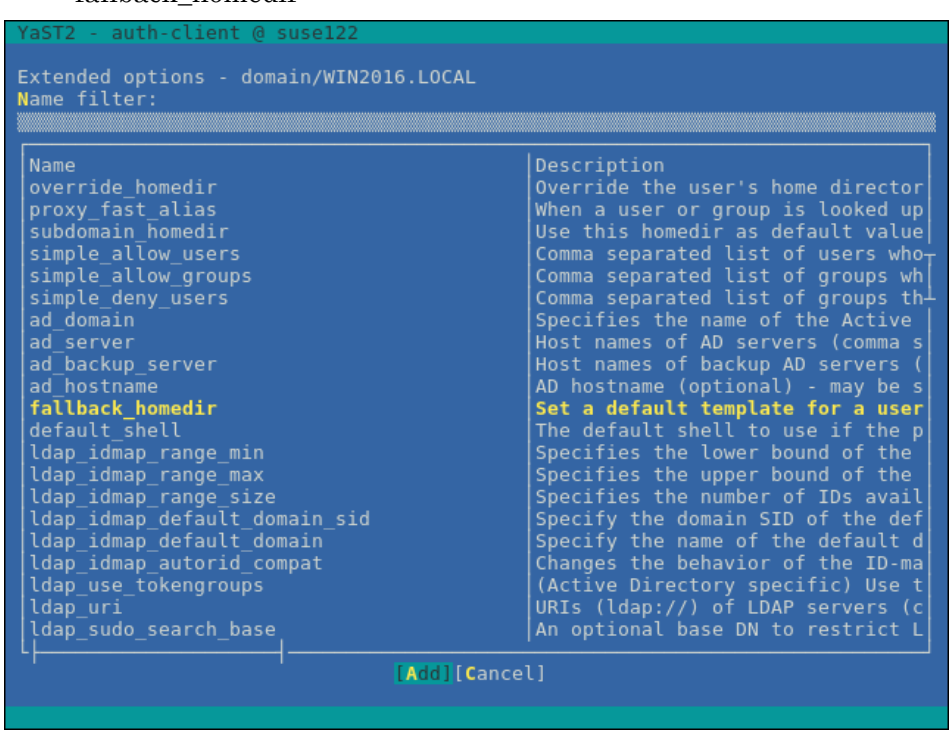
8. 以下の設定をしてから Extended Options を選択し、Enter を押します。

   - Create Home Directory



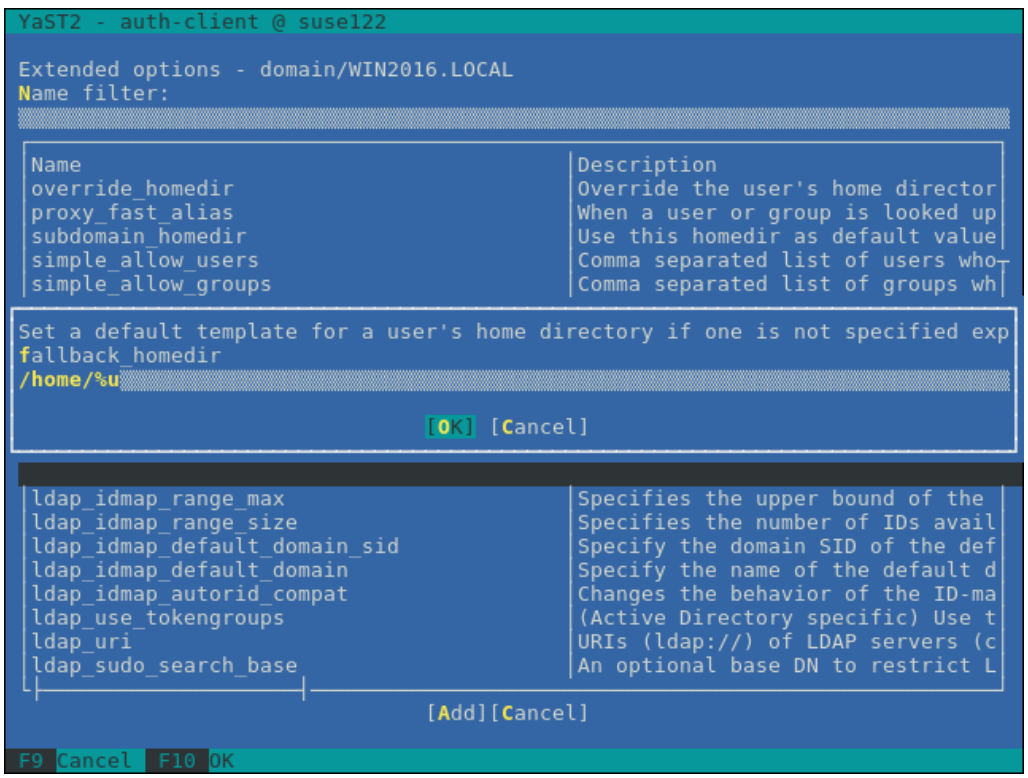
9. 以下の項目を選択してから Add を選択し、Enter キー押します。

   - fallback_homedir

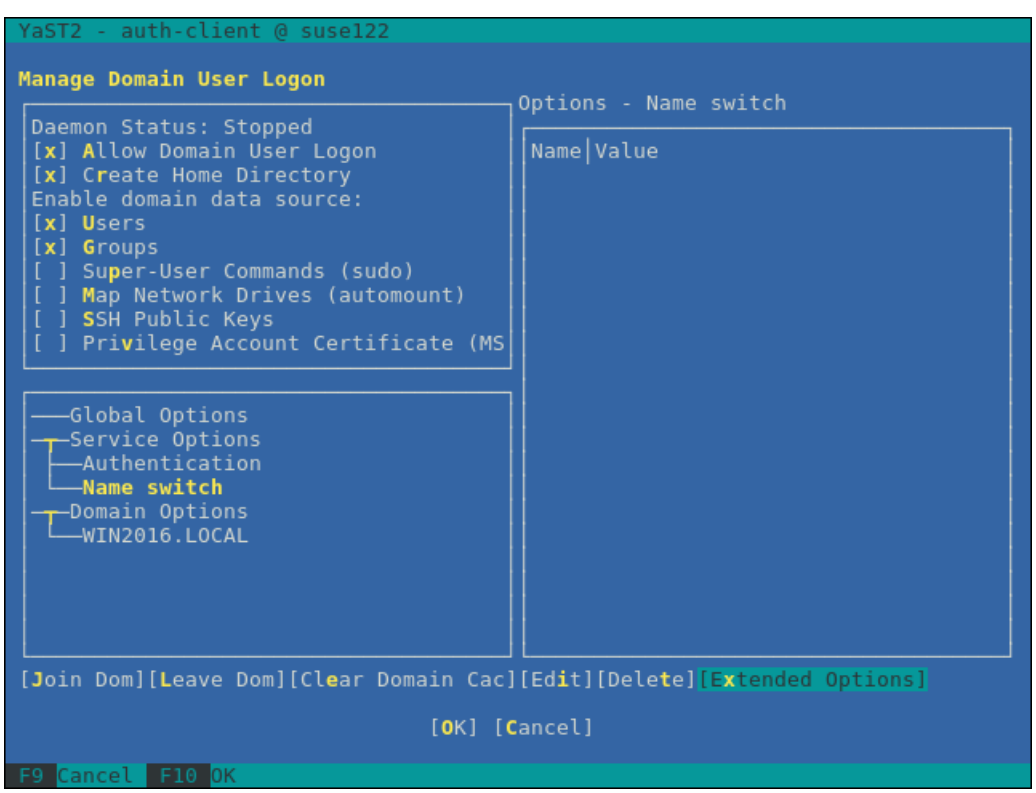


10. 以下の文字列を入力してから OK を選択し、Enter キーを押します。

- /home/%u

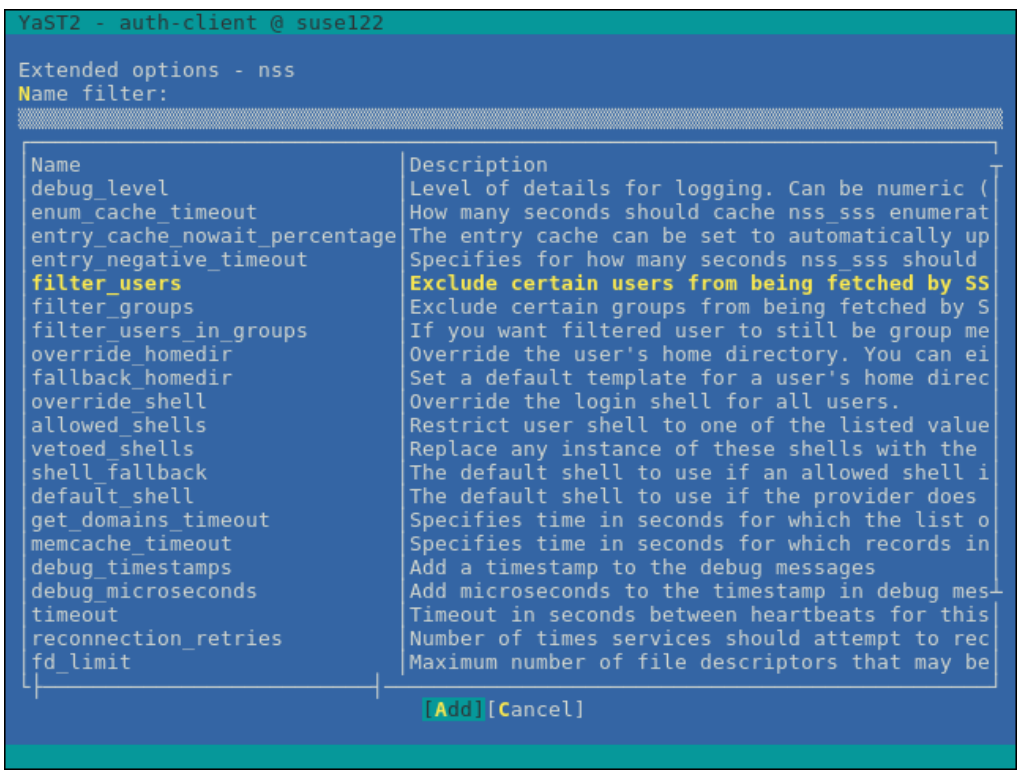


11. Name switch → Extended Options を選択し、Enter キーを押します。



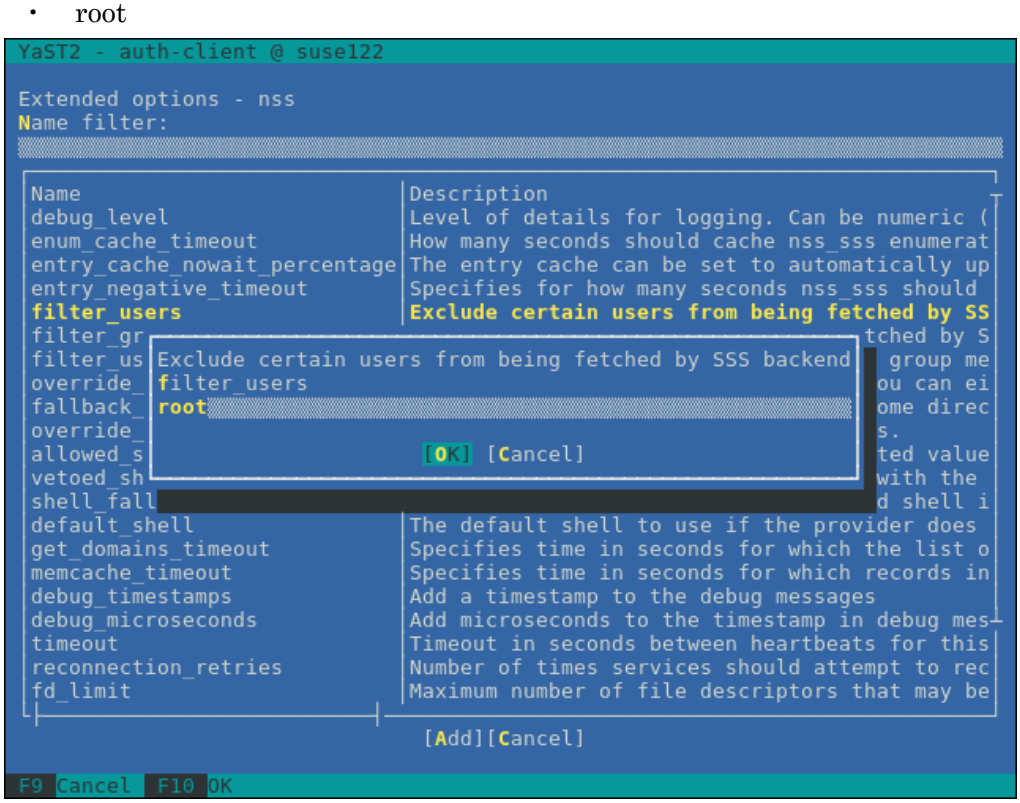
12. 以下の項目を選択してから Add を選択し、Enter キー押します。

- filter_users

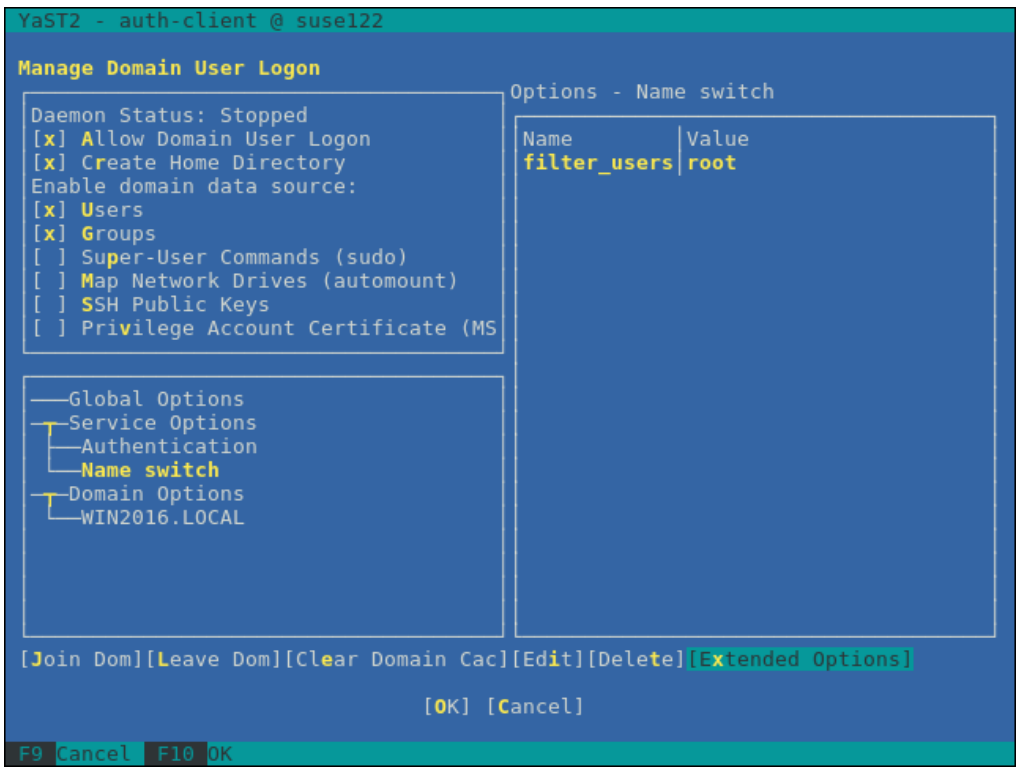


13. 以下の文字列を入力してから OK を選択し、Enter キーを押します。

- root

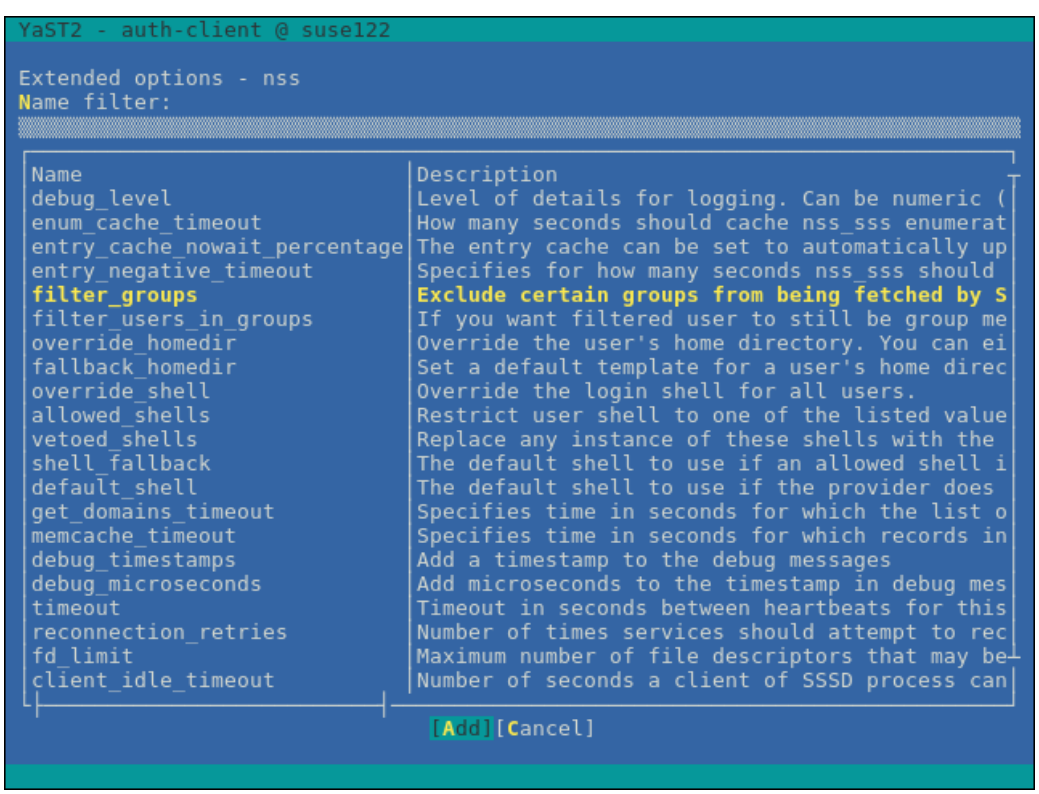


14. Name switch → Extended Options を選択し、Enter キーを押します。



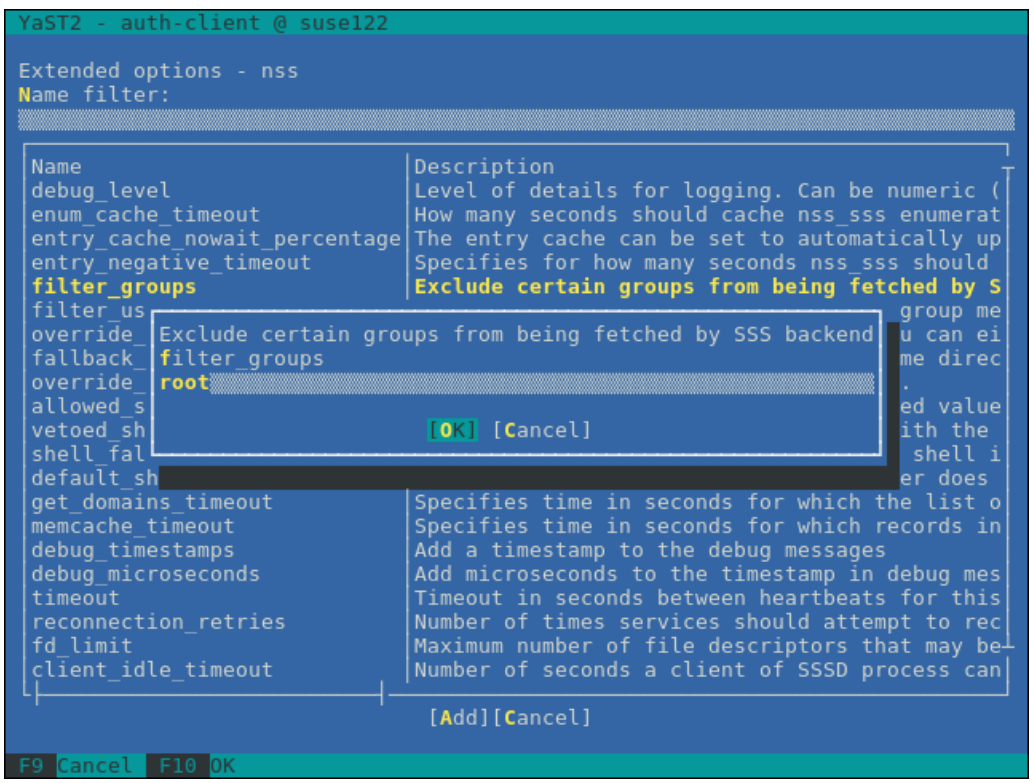
15. 以下の項目を選択してから Add を選択し、Enter キー押します。

- filter_groups

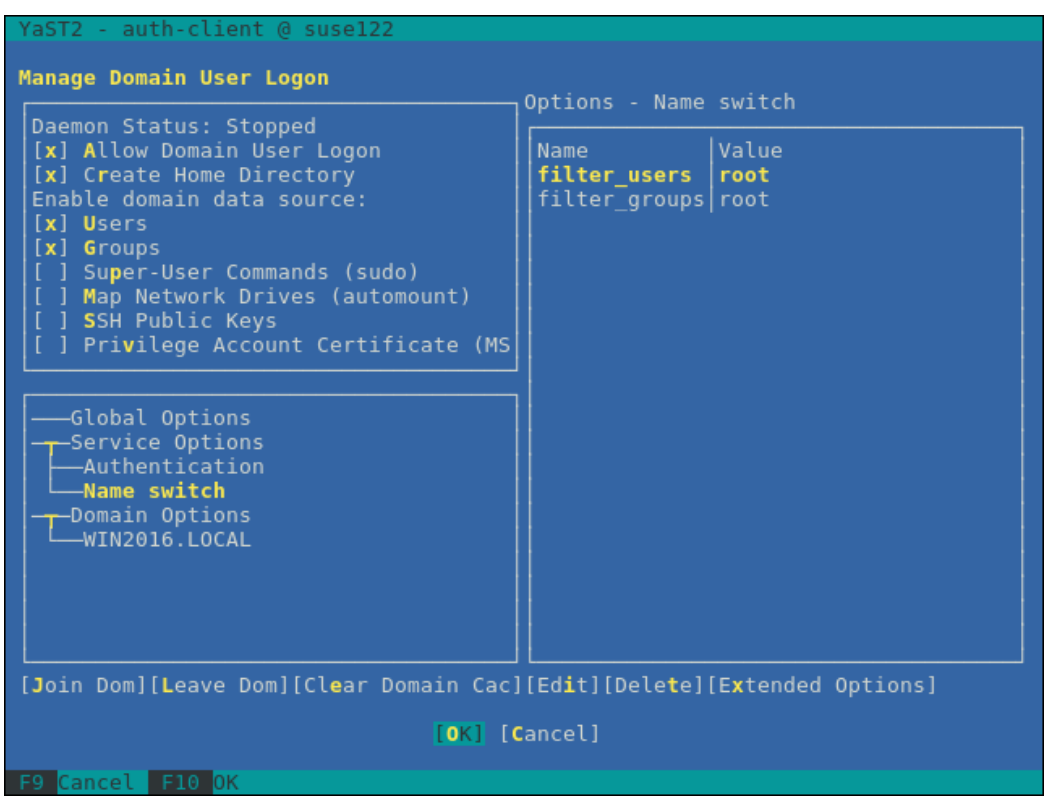


16. 以下の文字列を入力してから、OK を選択し、Enter キーを押します。

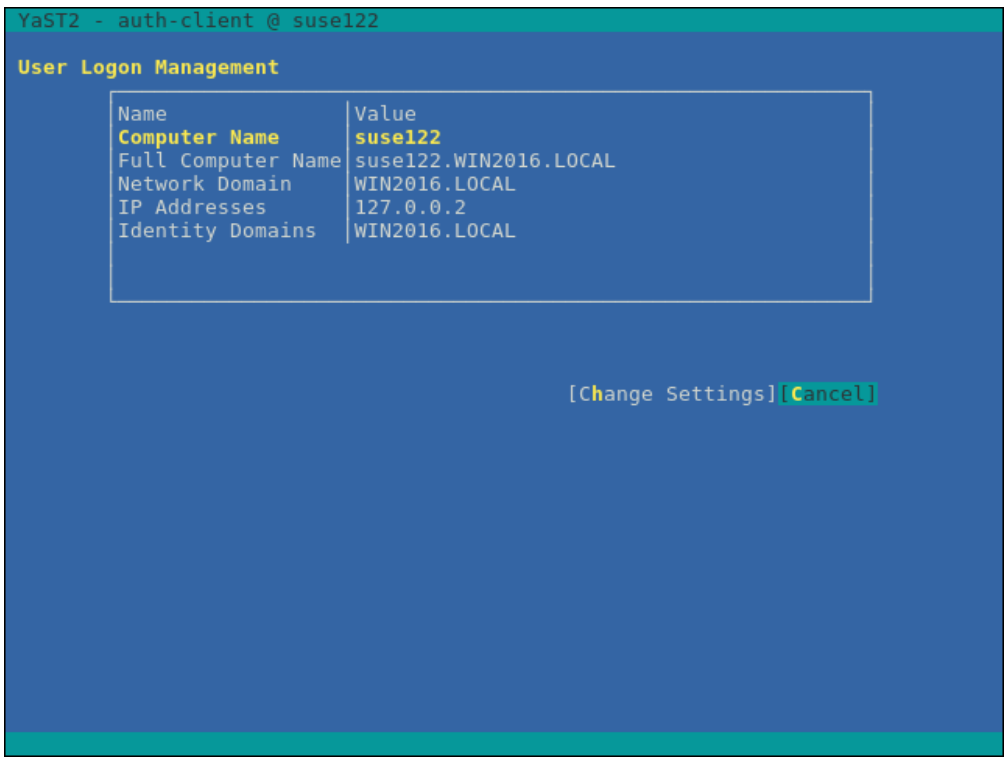
- root



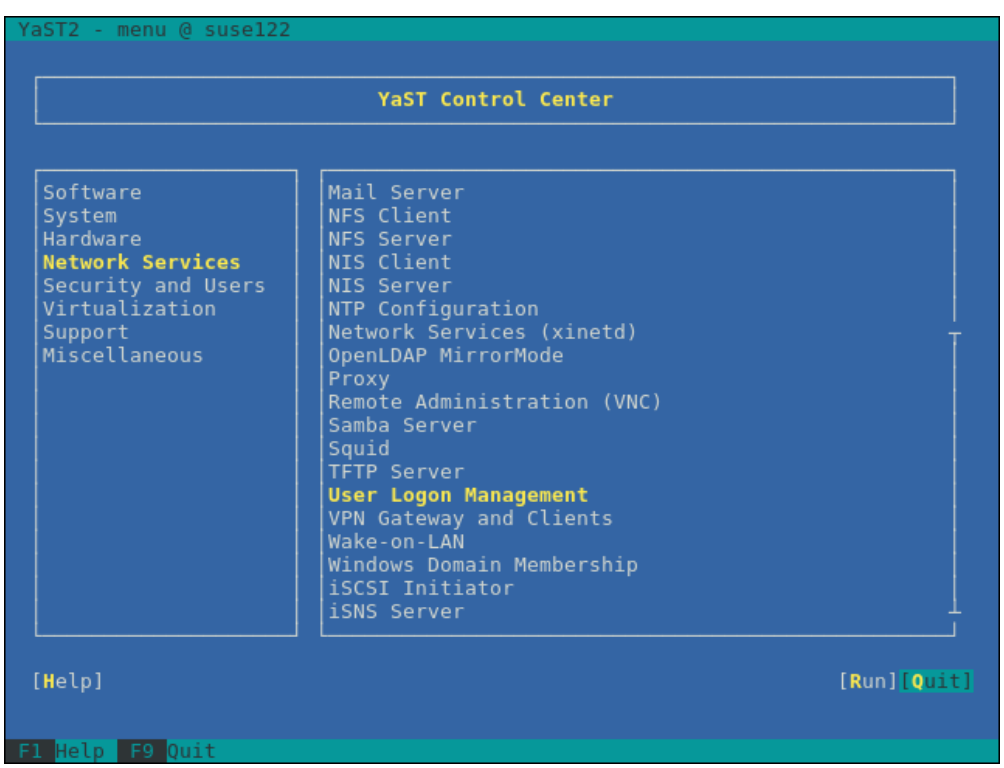
17. OK を選択し、Enter キーを押します。



18. Cancel 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。



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 **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。

(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 へドメイン情報の追加

「ユーザーズマニュアル」（3.4.2 ISM-VA の初期設定)を実施してください。

(7)　　ISM-VA へ DNS 情報の追加

「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。

3.5. IPCOM への設定手順

3.5.1. 仮想マシン情報取得コマンド実行権限設定手順

admin ユーザーで IPCOM の仮想情報を取得する場合は、監視対象 IPCOM サーバ上で admin ユーザーをグループ libvirt に追加し、仮想マシン情報取得コマンド実行権限を与える必要があります。

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

```
# sudo gpasswd -a admin libvirt
```

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

```
# sudo gpasswd -d admin libvirt
```

3.6. OpenStack への設定手順

3.6.1. コントローラーノードへの設定手順

(1) SSL モジュールのインストール

コントローラーノードにすでにインストールされている場合は必要ありません。

以下は yum コマンドを使用してインストールする場合の例です。

```
# yum install mod_ssl
```

(2) SSL 証明書の用意

HTTPS 通信用の SSL 証明書ファイルおよび SSL 証明書キーファイルを用意する必要があります。

SSL 証明書の用意には以下の 3 つの手段があります。

- SSL 証明書ファイルと SSL 証明書キーファイルがすでにインストールされている場合にそのファイルを流用する
- 認証局から発行する
- 自己証明書を作成する

[注意]

Version 3 のみ使用可能です。

以下のコマンドにて Version 情報を調べることが可能です。

```
# openssl x509 -text -noout -in certificate_file_path
※certificate_file_path には証明書ファイルのフルパスを入力してください
```

OpenStack インストール時に自動でファイルが作成されることがありますが、Version 3 以外で作成されている場合があります。必ず Version 3 で作成した証明書を使用してください。

[参考]自己証明書の作成方法例

```
# openssl genrsa -rand /proc/uptime 2048 > server.key
# openssl req -new -key server.key -x509 -sha256 -days 365 -set_serial $RANDOM
-extensions v3_req -out server.crt
※Common Name には IP アドレス、FQDN またはホスト名を入力してください
```

用意した SSL 証明書をコントローラーノードに格納します。

SSL 証明書ファイル: /etc/pki/CA/certs/

SSL 証明書キーファイル: /etc/pki/CA/private/

(3)　　割り当てポートの決定

Proxy サーバに割り当てるポートを決定します。

コントローラーノードにて他のサービスで使用されていないポートを選んでください。

1-1023 は使用不可です。

(4)　　OpenStack endpoint 情報の取得

・　OpenStack 環境変数設定ファイルの用意

以下の手順でダウンロードします(下記手順はお使いのバージョン／プラットフォームにより異なる場合があります)。

1. OpenStack Dashboard に admin ユーザーでログインします。
2. 右上の admin アイコンを選択します。
3. OpenStack RC File v3 を選択しダウンロードします。

また、OpenStack インストール時に作成されているファイルを使用することもできます。

・　endpoint の取得

後述のコマンドをコントローラーノード上で実行し、以下の 4 種類の URL 情報および 2 種類のバージョン情報を取得します。バージョン情報は URL の最後の vx の部分を取得してください。また URL は/vx の部分までを取得してください。

- Service Type が identity、Interface が public となっている項目の URL、バージョン
- Service Type が network、Interface が public となっている項目の URL
- Service Type が image、Interface が public となっている項目の URL
- Service Type が compute、Interface が public となっている項目の URL、バージョン

```
source <OpenStack 環境変数設定ファイル>; unset OS_SERVICE_TOKEN;  export OS_PASSWORD=< OpenStack_PASSWORD>; openstack endpoint list
```

例)

```
source keystonerc_admin; unset OS_SERVICE_TOKEN;  export OS_PASSWORD=password; openstack endpoint list
```

出力結果例)

```
+----------------------------------+----------+-------------+-------------+---------+----------+-------------------------------------------------+
| ID                               | Region   | Service Name | Service Type | Enabled | Interface | URL                                             |
```

```
+----------------------------------+----------+-------------+-------------
+---------+----------+-------------------------------------------------+
| 01d7dd66d19947d5870acec413876ba2 | RegionOne | keystone     | identity     |
True    | public    | http://192.168.30.86:5000/v3                    |
| 04005c8d71a544e596b9e40083fa7206 | RegionOne | placement    | placement    |
True    | internal  | http://192.168.30.86:8778/placement             |
| 0797675ff3c64da58a57a4988ec44a2b | RegionOne | cinderv2     | volumev2     |
True    | admin     | http://192.168.30.86:8776/v2/%(tenant_id)s      |
| 09ae73e20c004030ae04a7f5d8bf048a | RegionOne | placement    | placement    |
True    | admin     | http://192.168.30.86:8778/placement             |
| 12d9cbc0b1de4bf5a63d6819ec274685 | RegionOne | swift        | object-store |
True    | internal  | http://192.168.30.86:8080/v1/AUTH_%(tenant_id)s |
| 201c7c5ecef54c0691c043eafe6087ae | RegionOne | neutron      | network      |
True    | admin     | http://192.168.30.86:9696                       |
| 32920d76f674494d9a9dd98e06c9e229 | RegionOne | gnocchi      | metric       |
True    | internal  | http://192.168.30.86:8041                       |
| 3ff445febbee434aafc70c964dc3dbdc | RegionOne | ceilometer   | metering     |
True    | internal  | http://192.168.30.86:8777                       |
| 42f8a5c483ef43f18e736b622c2d5cf8 | RegionOne | cinderv2     | volumev2     |
True    | internal  | http://192.168.30.86:8776/v2/%(tenant_id)s      |
| 4aba919df7f947bbaf7a19918fadd01e | RegionOne | swift        | object-store |
True    | admin     | http://192.168.30.86:8080/v1/AUTH_%(tenant_id)s |
| 4b8c976fe4e742018b0fd4177dcae429 | RegionOne | cinderv3     | volumev3     |
True    | admin     | http://192.168.30.86:8776/v3/%(tenant_id)s      |
| 5b61335921c247689906b1bf390a45e7 | RegionOne | cinderv2     | volumev2     |
True    | public    | http://192.168.30.86:8776/v2/%(tenant_id)s      |
| 676ec9c2044947fea66b15f6168465de | RegionOne | gnocchi      | metric       |
True    | admin     | http://192.168.30.86:8041                       |
| 6855184db088496baabb85f5a70021f4 | RegionOne | aodh         | alarming     |
True    | internal  | http://192.168.30.86:8042                       |
| 8944c76fb0784089b1f7f56c94388530 | RegionOne | nova         | compute      |
True    | public    | http://192.168.30.86:8774/v2.1/%(tenant_id)s    |
| 930030ede13049439e2933665e91a3b4 | RegionOne | cinderv3     | volumev3     |
True    | public    | http://192.168.30.86:8776/v3/%(tenant_id)s      |
| 9503ad1f5e754993838fa53fd5d58690 | RegionOne | nova         | compute      |
True    | admin     | http://192.168.30.86:8774/v2.1/%(tenant_id)s    |
```

```
| 9541b01381404c4cb200dcbeea0168c4 | RegionOne | keystone     | identity     |
True    | admin     | http://192.168.30.86:35357/v3                |
| 98f00b9d75564ba29e92ccd5fdccb376 | RegionOne | keystone     | identity     |
True    | internal  | http://192.168.30.86:5000/v3                 |
| 9ae897c5ae704d9aa142b7b61c728468 | RegionOne | aodh         | alarming     |
True    | admin     | http://192.168.30.86:8042                    |
| 9bdc57b0a32e40148e2a049ba9211e8b | RegionOne | placement    | placement    |
True    | public    | http://192.168.30.86:8778/placement          |
| b0ea3c01f909451bafb57ccc2e5a6e32 | RegionOne | glance       | image        |
True    | admin     | http://192.168.30.86:9292                    |
| b75f5ae0fc8644fc9859ef37d4a4afc5 | RegionOne | ceilometer   | metering     |
True    | public    | http://192.168.30.86:8777                    |
| b7de11ad749b4d0f9b593446794c355c | RegionOne | swift        | object-store |
True    | public    | http://192.168.30.86:8080/v1/AUTH_%(tenant_id)s |
| b82ce3bd754a46289838cdc4ec17fd0f | RegionOne | cinder       | volume       |
True    | public    | http://192.168.30.86:8776/v1/%(tenant_id)s   |
| be3d757e64a945f8b0cdf784f0167ff8 | RegionOne | neutron      | network      |
True    | internal  | http://192.168.30.86:9696                    |
| c70161c0b104474f8f1d15fee74b222f | RegionOne | gnocchi      | metric       |
True    | public    | http://192.168.30.86:8041                    |
| c89faf6e8b9d4b3f9823d1a7e490e45b | RegionOne | cinder       | volume       |
True    | internal  | http://192.168.30.86:8776/v1/%(tenant_id)s   |
| cbd56dff0a5d4fe4b1a705e820115fd6 | RegionOne | ceilometer   | metering     |
True    | admin     | http://192.168.30.86:8777                    |
| dab0b8fa23c943a787803e0fd5e00450 | RegionOne | nova         | compute      |
True    | internal  | http://192.168.30.86:8774/v2.1/%(tenant_id)s |
| dbaf3b9d826d49ec8955623bf57cd7ec | RegionOne | neutron      | network      |
True    | public    | http://192.168.30.86:9696                    |
| e2fff591156f4176a13aad68c7e0e000 | RegionOne | glance       | image        |
True    | internal  | http://192.168.30.86:9292                    |
| ecda799534b144e7a48dbe8c4e99836a | RegionOne | cinderv3     | volumev3     |
True    | internal  | http://192.168.30.86:8776/v3/%(tenant_id)s   |
| f9052dd300904e8c80fca87fdb8bc2a1 | RegionOne | glance       | image        |
True    | public    | http://192.168.30.86:9292                    |
| fa9b861b2e14423baba72aa08bf2953d | RegionOne | aodh         | alarming     |
True    | public    | http://192.168.30.86:8042                    |
```

```
| fd768ee6e3844bd982e27b6cd3501c5b | RegionOne | cinder       | volume       |
True    | admin     | http://192.168.30.86:8776/v1/%(tenant_id)s      |
+----------------------------------+-----------+--------------+--------------
+---------+-----------+-------------------------------------------------+
```

取得例)

Service Type	URL	バージョン
identity	http://192.168.30.86:5000/v3	v3
network	http://192.168.30.86:9696	-
image	http://192.168.30.86:9292	-
compute	http://192.168.30.86:8774/v2.1	v2.1

・　バージョン情報付きの endpont の取得

network と image について curl コマンドでバージョン情報付 URL および URL のバージョンを取得します。

バージョン情報は URL の最後の vx の部分を取得してください。

結果が複数件ある場合、status が CURRENT の href キーを使用してください

network の場合

以下のコマンドを実行してください。

```
# curl -k <network の url>
```

例)

```
# curl -k "http://192.168.30.86:9696"
```

出力結果例)

```
{"versions": [{"status": "CURRENT", "id": "v2.0", "links": [{"href":
"http://192.168.30.86:9696/v2.0/", "rel": "self"}]}]}
```

取得例)

Service Type	URL	バージョン
network	http://192.168.30.86:9696/v2.0	v2.0

image の場合

以下のコマンドを実行してください。

```
# curl -k <image の url>
```

例)

```
# curl -k "http://192.168.30.86:9292"
```

出力結果例)

{"versions": [{"status": "CURRENT", "id": "v2.5", "links": [{"href": "http://192.168.30.86:9292/v2/", "rel": "self"}]}, {"status": "SUPPORTED", "id": "v2.4", "links": [{"href": "http://192.168.30.86:9292/v2/", "rel": "self"}]}, {"status": "SUPPORTED", "id": "v2.3", "links": [{"href": "http://192.168.30.86:9292/v2/", "rel": "self"}]}, {"status": "SUPPORTED", "id": "v2.2", "links": [{"href": "http://192.168.30.86:9292/v2/", "rel": "self"}]}, {"status": "SUPPORTED", "id": "v2.1", "links": [{"href": "http://192.168.30.86:9292/v2/", "rel": "self"}]}, {"status": "SUPPORTED", "id": "v2.0", "links": [{"href": "http://192.168.30.86:9292/v2/", "rel": "self"}]}, {"status": "DEPRECATED", "id": "v1.1", "links": [{"href": "http://192.168.30.86:9292/v1/", "rel": "self"}]}, {"status": "DEPRECATED", "id": "v1.0", "links": [{"href": "http://192.168.30.86:9292/v1/", "rel": "self"}]}]}

取得例)

Service Type	URL	バージョン
image	http://192.168.30.86: 9292/v2	v2

(5) Apache SSL 設定の変更

1. 下記例を参考に任意の名称で設定ファイルを作成します。ただし、拡張子は「.conf」である必要があります。

```
Listen <手順 3 で決定したポート番号>
<VirtualHost *:<手順 3 で決定したポート番号>>
    ServerName <コントローラーノードの IP アドレス、FQDN またはホスト名>
    SSLEngine on
    SSLProtocol all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
    SSLCipherSuite HIGH:MEDIUM:!aNULL:!MD5:!SEED:!IDEA:!3DES:!RC4:!DH
    SSLHonorCipherOrder on
    SSLCertificateFile    <SSL 証明書ファイルのフルパス>
    SSLCertificateKeyFile <SSL 証明書キーファイルのフルパス>
    LogLevel notice
    ErrorLog /var/log/httpd/ssl_openstack_api_error.log
    ServerSignature Off
    CustomLog /var/log/httpd/ssl_openstack_api_access.log combined
    <Location /identity>
        ProxyPass  <手順 4 で取得した identity の URL>
```

```
        Header  set  x-openstack-api-version 〈手順 4 で取得した identity のバージョン〉
    </Location>
    <Location /network>
        ProxyPass  〈手順 4 で取得した network の URL〉
        Header set x-openstack-api-version 〈手順 4 で取得した network のバージョン〉
    </Location>
    <Location /compute>
        ProxyPass  〈手順 4 で取得した compute の URL〉
        Header set x-openstack-api-version 〈手順 4 で取得した compute のバージョン〉
    </Location>
    <Location /image>
        ProxyPass  〈手順 4 で取得した image の URL〉
        Header set x-openstack-api-version 〈手順 4 で取得した image のバージョン〉
    </Location>
</Virtualhost>
```

例)

```
Listen 5001
<VirtualHost *:5001>
    ServerName 192.168.30.86
    SSLEngine on
    SSLProtocol all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
    SSLCipherSuite HIGH:MEDIUM:!aNULL:!MD5:!SEED:!IDEA:!3DES:!RC4:!DH
    SSLHonorCipherOrder on
    SSLCertificateFile    /etc/pki/CA/certs/server.crt
    SSLCertificateKeyFile /etc/pki/CA/private/server.key
    LogLevel notice
    ErrorLog /var/log/httpd/ssl_openstack_api_error.log
    ServerSignature Off
    CustomLog /var/log/httpd/ssl_openstack_api_access.log combined
    <Location /identity>
        ProxyPass  http://localhost:5000/v3
```

```
        Header set x-openstack-api-version v3
    </Location>
    <Location /network>
        ProxyPass  http://localhost:9696/v2.0
        Header set x-openstack-api-version v2.0
    </Location>
    <Location /compute>
        ProxyPass  http://localhost:8774/v2.1
        Header set x-openstack-api-version v2.1
    </Location>
    <Location /image>
        ProxyPass  http://localhost:9292/v2
        Header set x-openstack-api-version v2
    </Location>
</Virtualhost>
```

2. Apache SSL 設定ファイルを格納します。

以下に格納してください。

```
/etc/httpd/conf.d/
```

3. Apache 設定再読み込みします。

以下コマンドをターミナルにて root ユーザーで実行してください。

```
systemctl reload httpd
```

(6) ファイアーウォールの設定

以下コマンドを使用して設定したポートを許可してください。

ポート許可状況確認コマンド

```
iptables -nL --line-numbers
```

ポート開放コマンド

```
iptables -I INPUT 1 -p tcp --dport [port] -s [ISM の IP アドレス] -j ACCEPT
```

ポート開放コマンド例).

```
iptables -I INPUT 1 -p tcp --dport 5001 -s 192.168.0.101 -j ACCEPT
```

設定保存コマンド

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

ポート閉鎖コマンド

```
iptables -D INPUT [No]
```

ポート閉鎖コマンド例)

```
iptables -D INPUT 1
```

3.6.2. 仮想ネットワーク分析機能使用時の設定

(1) 「/etc/nova/nova.conf」の編集

/etc/nova/nova.conf ファイルを開きます

```
# vi /etc/nova/nova.conf
```

以下の 2 項目をそれぞれ 1 行で追加してください。

・キー: scheduler_available_filters、値: 任意

・キー: scheduler_default_filters、値: SameHostFilter

例)

```
scheduler_available_filters = nova.scheduler.filters.all_filters
scheduler_default_filters =

SameHostFilter,RetryFilter,AvailabilityZoneFilter,RamFilter,DiskFilter,Compu
teFilter,ComputeCapabilitiesFilter,ImagePropertiesFilter,ServerGroupAntiAffi
nityFilter,ServerGroupAffinityFilter
```

(2) nova サービスの再起動

コントローラーノードにて以下のコマンドを実行します。

コマンドは全て 1 行で記述してください。

```
for service in api consoleauth conductor scheduler novncproxy; do  systemctl
restart openstack-nova-$service; done
```