取扱説明書補足資料－日本語

FUJITSU Software ServerView Suite ServerView Agents V7.20 以降 補足情報

2016/4

102-001 版

目次

■ はじめに

本書は、ServerView Agents V7.20 以降に関連する以下のマニュアルの補足情報です。本書をお読みになる前に、必ず以下のマニュアルもご覧ください。

- Installation ServerView Agents for Linux （sv-install-linux-agent-jp.pdf）
- Installation ServerView Agents for Windows （sv-install-windows-agent-jp.pdf）
- ServerView System Monitor （sv-ssm-jp.pdf）
- ServerView でのユーザ管理 （user-mgt-jp.pdf / sv-user-mgt-jp.pdf）

■ 対象バージョン

本書は、以下のバージョンの ServerView Agents (以下 Agents)を対象にしています。

本書の対象バージョン ： V7.20 以降

V5.00～V5.51 については、ServerView Agents 補足情報[002-007 版]を参照してください。

V6.00～V7.10 については、ServerView Agents 補足情報[002-020 版]以降を参照してください。

■ 補足情報

1 インストール要件

▸ Windows

1.1 ネットワークポートの設定

Windows Server 2008 の動的ポート割り当て設定で、開始ポートを変更すると ServerView Operations Manager と Agents が使用するポートと競合し、ServerView Operations Manager と Agents が起動できなくなる場合があります。開始ポート設定を変更する場合、ServerView Operations Manager と Agents の使用ポートと競合しないように注意してください。

ServerView Operations Manager と Agents が使用するポートは、マニュアル（高セキュリティ PRIMERGY サーバ管理：sm-security-jp.pdf)を参照してください。

2 インストール

▸ Windows

2.1 関連サービスの停止

次のいずれかのソフトウェアがインストールされ、サービスが起動している場合、Agents のインストール開始前にこれらのサービスを一時停止する必要があります。なお、Agents のインストール終了後はサービスの再開が必要です。

- REMCS エージェント（Windows）： F5EP00RMService サービス、REMCS RmAosfB サー

ビス

- HRM/server（Windows）： 5EP70_HRM_ctrl サービス
- RAS 支援サービス（Windows）： F5EP50 サービス

▸ Linux/VMware/Citrix XenServer/everRun MX 共通

2.2 snmpd.conf の localhost に対するコミュニティ名

snmpd.conf 内の以下の行は削除しないでください。存在しない場合は追加してください。

```
com2sec svSec localhost <コミュニティ名>
```

この行で指定したコミュニティ名は、Agents が内部アクセスする際に使用されます。
また、ブレードサーバの場合にはマネジメントブレードにアクセスする際にもこの行で指定したコミュニティ名が使用されます。マネジメントブレードでこの行で指定したコミュニティ名でのアクセスを許可するように設定してください。
この行が存在しなかった場合、Agents はコミュニティ名「public」で内部アクセスを行います。このとき、コミュニティ名「public」の通信が許可されていない場合、SNMP 認証エラーが発生します。

3 アンインストール

▸ Citrix XenServer/everRun MX 共通

3.1 /usr/sbin/srvmagt コマンド

Citrix XenServer/everRun MX 環境において、「/usr/sbin/srvmagt remove」コマンドを実行すると、Agents と ServerView RAID Manager がアンインストールされます。
Agents のみをアンインストールする場合は、「/usr/sbin/srvmagt remove」コマンド実行後、ServerView RAID Manager を再インストールしてください。
また、Agents のアップデートインストールを行なう場合は、ダウンロードモジュールに添付されている readme.txt の「6.インストール手順」の手順で行ってください。

4 その他

▸ 全 OS 共通

4.1 ServerView RAID Manager でのポート番号変更

ServerView RAID Manager のマニュアルにあるポート番号の変更を実施した場合、Agents としては正常動作保障外となります。実施した場合、以下の現象などが発生します。

- RAID 関連のステータスが取得できない。
- RAID Manager とのステータス連携ができない。

- Agents 起動時に RAID Manager と連携できない旨のエラーがログされる場合がある。

Windows

4.2 イベントログのソース名

Agents が OS のイベントログにログを記録する際のソース名は、以下のとおりです。なお、ログの種類は全て「アプリケーション」です。

- ServerView Agents・ServerView Remote Connector
- ServerView Server Control

4.3 Agents へのログイン

Agents へのログインユーザは、ローカルグループに所属している必要があります。ログイン可能なローカルグループの設定は「Agent Configuration」ツールで指定可能です。ServerView Installation Manager で Agents をインストールした場合やサイレントインストールを行った場合、デフォルトで「FUJITSU SVUSER」が設定されます。

ドメインユーザを使用する場合もローカルグループに所属させて下さい。なお、Active Directory などのドメインコントローラで、ローカルグループが作成できない環境ではドメイングループ指定で動作します。その際の「Agent Configuration」ツールの設定方法はローカルグループと同じです。

Linux/VMware/Citrix XenServer/everRun MX 共通

4.4 ブレードサーバの診断情報収集（PrimeCollect）

ブレードサーバの診断情報収集（PrimeCollect）を実行すると、アーカイブ取得処理によりマネジメントブレード（MMB）に対して snmpd.conf に設定された SNMP コミュニティを使用した SNMP 通信が行なわれます。

このとき、マネジメントブレードで snmpd.conf に設定された SNMP コミュニティによる SNMP 通信が許可されていない場合、マネジメントブレードに SNMP 通信の認証エラーが記録されます。

この場合、認証エラーを無視するか、マネジメントブレードで snmpd.conf に設定された SNMP コミュニティによる SNMP 通信を許可する設定をしてください。

4.5 シスログのソース名

Agents がシスログ（/var/log/messages）にログを格納する際の、ログの先頭文字列は以下のとおりです。

- Serverview:
- srvmagt_scs:
- vmeagt:
- ServerView RemoteConnector:

4.6 Agents が認識するネットワークインターフェース名

Agents が認識可能なネットワークインターフェース名は以下のとおりです。

eth, bond, vswif, br, xenbr, sha, eno, enp

上記外の名前のネットワークインターフェースは認識することができません。

4.7 しきい値情報保存ファイル

Agents では、しきい値監視を行うためのデータを定期的に採取して、/etc/srvmagt/VME/var/db/配下の vmeDb.db ファイルに保存します。

仮想化 OS の場合、ゲストマシンのデータについてもこのファイルに保存し、ファイルのサイズはゲストマシンの数に応じて大きくなります。ゲストマシン 1 つ当たりのデータ量は約 4MByte です。多数のゲストマシンが存在していた場合、その分ファイルサイズが大きくなります。

4.8 OpenSSL パッケージのアップデート

OpenSSL をアップデートした後、以下の確認/設定を行ってください。

OpenSSL のライブラリには以下の 3 か所でリンクを張っています。

- vmeagt

  /etc/srvmagt/VME/lib/

  libcrypto.so.x.x.x -> /usr/lib/libcrypto.so.xx

  libssl.so.x.x.x -> /usr/lib/libssl.so.xx

- SVRemoteConnector

  /opt/fujitsu/ServerViewSuite/SCS/lib/

  libcrypto.so.x.x.x -> /usr/lib/libcrypto.so.xx

  libssl.so.x.x.x -> /usr/lib/libssl.so.xx

- eecd(smtp) ※V6.00 以降。ServerView SystemMonitor で使用。

  /etc/srvmagt/smtp/lib/

  libcrypto.so.x.x.x -> /usr/lib/libcrypto.so.xx

  libssl.so.x.x.x -> /usr/lib/libssl.so.xx

OpenSSL のアップデートによりこのリンク先（/usr/lib/配下）が変更されている場合は、リンクを張りなおしてください。

例：リンク先（/usr/lib/libcrypto.so.xx や/usr/lib/libssl.so.xx）が、新たなリンク先（/usr/lib/libcrypto.so.yy や/usr/lib/libssl.so.yy）に変更された場合、リンクを張りなおしてください。

また、OpenSSL をアップデートした後は、対象のライブラリをロードするために Agents を再起動してください。

```
#/usr/sbin/srvmagt stop
#/etc/init.d/srvmagt_scs restart
#/usr/sbin/srvmagt start
```

4.9 Agents のプロセス状態の確認

Agents for Linux が提供する CLI コマンド「srvmagt status」により、プロセスの状態を確認することができます。
この時、ServerView RAID Manager のプロセスである amDaemon についても同時に状態表示されますが、amDaemonの状態確認にはServerView RAID Managerが提供するCLIコマンド「amCLI -l」を使用してください。amCLIコマンドの詳細な使用方法は、「ServerView RAID Manager 補足情報」を参照してください。

4.10 ファイルシステムへのアクセスについて

Agents では、全ファイルシステムのスキャン(アクセス)を 60 秒間隔で行います。スキャンは順次ファイルシステムへアクセスされるため、ファイルシステム数によっては常にアクセスが行われている状態となります。これにより、自動的なアンマウントなどの設定が動作しない場合があります。

▸ VMware/Citrix XenServer/everRun MX 共通

4.11 ServerView System Monitor の制限

VMware/Citrix XenServer/everRun MX において、ServerView System Monitor は未サポートです。

4.12 VMware/Citrix XenServer/everRun MX でのログイン設定

VMware/Citrix XenServer/everRun MX に Agents をインストールした後、スレッシュホールドマネージャ、パフォーマンスマネージャの使用有無にかかわらず、以下のマニュアルの設定を行って下さい。

ServerView Operations Manager V6.10
Installing ServerView Agents for Linux SUSE, Red Hat, VMware ESX and Citrix XenServer
(ファイル名:sv-install-linux-agent-jp.pdf)
「3.5.2 エージェントの設定」ー「VMware ESX、Citrix Xen または Xen」

この設定を行わないと CPU 使用率上昇、メモリ使用量上昇といった現象が発生します。
なお、ここで設定するユーザは/etc/srvmagt/configファイルで設定されているグループに所属している必要があります。

▸ VMware ESX4.0/4.1

4.13 スケジュール(PowerOn/Off)の設定時刻

ESX4.0/4.1 を使用しているシステムでスケジュール(PowerOn/PowerOff)の設定を行った場合、意図しない時刻に PowerOn、PowerOff が行われる可能性があります。

ESX4.0/4.1 システムを使用する際には、BIOS は UTC 時刻に設定する必要があります。しかし、OS の上では Local 時刻で動作するため、スケジュールの設定は Local 時刻で行います。

スケジュールの時刻は BMC(iRMC)が管理します。iRMC の時刻は PowerOn 後の POST 時に BIOS から、OS 起動後に Agents から設定されます。
PowerOff されている間の iRMC の時刻は、OS 起動後に PowerOff したか OS 起動前に PowerOff したかによって異なります。OS 起動前であれば UTC 時刻、OS 起動後であれば Local 時刻で動作しています。

これにより、以下のような意図しない動作をすることがあります。

- Local 時刻で設定された PowerOn 時刻のスケジュールが、iRMC の時刻が UTC で動作している場合は UTC 時刻で PowerOn してしまいます。
  スケジュールを設定している場合は、毎回 OS が起動後、PowerOff するようにしてください。
  例: 時差+9 時間の場合、Local 時刻で 9:00 に PowerOn と設定してあると、18:00(UTC 時刻で 9:00)に PowerOn されます。
- PowerOff と PowerOn のスケジュールの時間差が UTC と Local 時刻の時差とほぼ同じ場合、PowerOn 直後に PowerOff されてしまうことがあります。
  PowerOn から OS 起動までの間は UTC 時刻で動作するため、PowerOff の設定時間が UTC 時刻で、PowerOn から OS 起動までの時間に来てしまうと PowerOff されてしまいます。
  PowerOff と PowerOn の間隔をさらに 15～30 分ほど長くする、もしくは短くしてタイミングをずらしてください。
  例: 時差が+9 時間で、Local 時刻で 21:05 に PowerOff し 6:00 に PowerOn する設定の場合、Local 時刻 21:05 に PowerOff 後、Local 時間 6:00 に PowerOn します。
  PowerOn から OS の起動するまでの間は UTC 時間で動作するため、iRMC は現在時刻を 21:00 と認識してしまいます。そのため、OS が起動する前に 6:05 になってしまうと、PowerOff を実行してしまいます。

▸ Windows/Linux 共通

4.14 ServerView System Monitor の Update Check

ServerView System Monitor の Update Check の繰り返しタイミングの最大値は 99 です。

5 トラブルシューティング

▸ 全 OS 共通

5.1 イベントログ/シスログに「Communication ～ lost.」のメッセージが出力される

システムやネットワークの高負荷により BMC(iRMC)との通信がタイムアウトした場合などに、以下のメッセージが出力されます。

Communication with the Server Management controller in cabinet <キャビネット番号> of server <サーバ名> lost.

このメッセージの後に以下が出力されていれば、通信が再確立されサーバの監視が継続されますので問題ありません。

Communication with the Server Management controller in cabinet <キャビネット番号> of server <サーバ名> established again.

5.2 イベントログ/シスログに「Communication link failed」のメッセージが出力される

以下のメッセージが出力される場合があります。

ServerView received the following alarm from server <サーバ名>: Communication link failed at the station <ネットワークインタフェースの station 番号>

※ネットワークインタフェースの station 番号は、このメッセージ（SNMP トラップ）を送信するハードウェアや OS において割り当てられている任意の番号です。

このメッセージは、LAN Switch などのハードウェアや OS 標準の SNMP サービス（Windows）/snmpd デーモン（Linux, VMware, Citrix XenServer/everRun MX）が、LAN（ネットワークインタフェース）の Link Down を検出することにより送信する SNMP トラップです。Agents がこの SNMP トラップを送信することはありません。Link Down は、LAN ケーブルが抜けたり、LAN Switch が故障したりした場合などの LAN 異常時に発生します。

SVOM はこの SNMP トラップを受信し、表示およびログ出力を行ないます。

この SNMP トラップが送信された原因を特定するには、SNMP トラップを送信したソフトウェア（OS 標準の SNMP サービス/snmpd デーモン）やハードウェアにおいて行なう必要があります。ServerView では、この SNMP トラップが送信された原因を特定することはできません。

最初に、<サーバ名>よりメッセージ（SNMP トラップ）の送信元を特定し、<ネットワークインタフェースの station 番号>を確認してください。次に、ネットワークインタフェースの station 番号が割り当てられている LAN インタフェースに異常が無いかどうかを確認してください。

5.3 イベントログ/シスログに ServerView Remote Connector の警告メッセージが出力される

以下のメッセージが出力される場合があります。

- Windows 環境の場合

イベントログ アプリケーション
イベント ID 2370
ソース: ServerView Remote Connector
詳細:
IP=xx.xx.xx.xx
SOAP-ENV:Receiver
SSL_ERROR_SSL
error:140890B2:SSL routines:SSL3_GET_CLIENT_CERTIFICATE:no certificate returned
SSL_accept() failed in soap_ssl_accept()
または
イベント ID 2370
ソース: ServerView Remote Connector
詳細:
There is a request from IP=172.26.70.12 whose SSL-Key-Certificate cannot be verified.
Please contact the owner of that system (to prevent requests or to add SSL-CA-Certificate).

- Linux/VMware /Citrix XenServer/everRun MX 環境の場合

ServerView Remote Connector[PID]:
WARN2370: WARN: SSL sends error for the 'handshake tests'. This request will be ignored ! It might be missing encryption or problems with authentications. For more technical information see following data: IP=xxx.xxx.xxx.xxx SOAP-ENV:Receiver SSL_ERROR_SSL error:140890B2: SSL routines:SSL3_GET_CLIENT_CERTIFICATE:no certificate returned SSL_accept() failed in soap_ssl_accept()
または
ServerView Remote Connector[PID]:
WARN2377: WARN:There is a request from IP=xxx.xxx.xxx.xxx whose SSL-Key-Certificate cannot be verified. Please contact the owner of that system (to prevent requests or to add SSL-CA-Certificate).

「xxx.xxx.xxx.xxx」には IP アドレスが入ります。
このメッセージは、SVOM からの要求に対して、監視対象サーバにインストールされている ServerView Remote Connector が SVOM へのクライアント認証に失敗したことを示します。このメッセージが出力された場合は、以下の確認を行なってください。

- マニュアル「ServerView でのユーザ管理 中央認証および役割ベースの権限」

（user-mgt-jp.pdf）の「4 CMS と管理対象ノードでの SSL 証明書の管理」を実施しているか確認してください。

- <システム名>.scs.xml の「<wcc:host><システム名></wcc:host>」で指定された<システム名>が SVOM をインストールしているサーバであるかどうか確認してください。
- <システム名>.scs.xml の「<wcc:host><システム名></wcc:host>」で指定された<システム名>を使用して、監視対象サーバから<システム名>に通信できるかどうか確認してください。
  例： # ping <システム名>
- OS のテンポラリフォルダに「SCSCA*」というファイルがあるか確認してください。このファイルが削除されていると ServerView Remote Connector の警告メッセージが発生します。
  デフォルトは以下のパスです。
  Windows 環境
  C:¥Windows¥Temp¥
  Linux/VMware /Citrix XenServer/everRun MX 環境
  /tmp または/var/tmp
  「SCSCA*」というファイルが無い場合、ServerView Remote Connector を再起動してください。
  上記確認後もメッセージが出力される場合は、SVOM の再インストールにより証明書を再作成し、マニュアル「ServerView でのユーザ管理 中央認証および役割ベースの権限」（user-mgt-jp.pdf）の「4 CMS と管理対象ノードでの SSL 証明書の管理」を実施してください。

このメッセージが出ていた場合、SVOM からの接続テスト実行結果が一部エラーとなる場合があります。

また、SVOM から以下の機能が使用できない可能性があります。

- PrimeCollect 実行
- オンライン診断実行
- サーバの設定実行
- スレッシュホールドマネージャによるしきい値設定
- パワーモニタによる電力消費データの取得
- アップデートマネージャの情報取得
  （監視対象サーバに UpdateAgent がインストールされている場合）

5.4 イベントログ/シスログに ServerView Virtualization Management Agent の警告メッセージが出力される

以下のメッセージが出力される場合があります。

- Windows 環境の場合

イベントログ　アプリケーション
イベント ID 1
ソース: ServerView Virtualization Management Agent
詳細:
SCCI : can't connect too the eecd daemon

- Linux/VMware /Citrix XenServer/everRun MX 環境の場合

vmeagt [PID]: SCCI : can't connect too the eecd daemon

Agents は Hyper-V、Xen、VMware モードの確認を行い、一致していない場合に物理サーバの構成であるか否かをSCCIを使用して確認しますが、その際、eecdと接続が出来なかった場合に出力されます。

SCCI は ServerView Virtualization Management Agent 以外でも使用されているため、サービス起動時または負荷の影響などで一度だけ発生した場合、および SVOM で監視ができている場合は、その後の SCCI 動作は正常に行われているため無視して問題ありません。

5.5 認証エラートラップが送信される

許可されていないコミュニティ名で Agents がインストールされたサーバにアクセスしている可能性があります。

アクセス先（Agents がインストールされたサーバ）の SNMP コミュニティ名とアクセス元（SVOM サーバ）のコミュニティ名が正しいか確認してください。

SVOM の「サーバのプロパティ」に設定されているコミュニティ名と、Agents 側の以下の設定が同じであることを確認してください。

- Windows 環境の場合
  OS のサービスより「SNMP Service」のプロパティを開き、セキュリティタブに設定されているコミュニティ名
- Linux/VMware 環境の場合
  snmp フォルダにある snmpd.conf を開き、アクセス設定のコミュニティ名

5.6 ServerView System Monitor が起動できない

ServerView System Monitor などの Agents のツールが、JRE のエラーなどの影響によって正常に起動できない場合があります。

エラーのポップアップがある場合は「OK」などで終了させ、一度ツールを終了した後、再度起動してください。

5.7 ServerView System Monitor にログイン出来ない

ServerView System Monitorの起動時、Agentsの設定によりユーザ ID、パスワードの要求が行われます。この際、ログインが正常に行われずエラーが表示される場合や、再度ログインが要求される場合

があります。以下の確認を行って下さい。

- ログインに使用するユーザ ID、パスワードを確認してください。
  入力するユーザ ID、パスワードはサーバの OS で作成、許可されている必要があります。サーバの OS 上、または監視対象サーバが利用可能なディレクトリサービス上でユーザ ID、およびパスワードの作成を行って下さい。
- ログインに使用するユーザ ID が管理グループに属しているか確認してください。
  Agents の設定によっては、ユーザ ID は管理グループに属している必要があります。グループの有効設定、およびユーザ ID がそのグループに属している事を確認してください。
  以下の Agents ツール、設定ファイルで確認出来ます。
  Windows
  Agents Configuration ツール （デフォルトは「FUJITSU SVUSER」グループが設定）
  Linux
  /etc/srvmagt/config 設定ファイル （デフォルトは「SVUSER」グループが設定）
- JRE の版数を確認してください。
  SVOM で使用している JRE バージョンを確認してください。バージョン 1.6.0_29 では、ログインの制御が正常に動作しない場合があります。1.6.0_29 以外のバージョンを使用してください。

▸ Linux/VMware/Citrix XenServer/everRun MX 共通

5.8 インストール時に VersionView.sav のエラーメッセージが表示される

インストール時に以下のメッセージが出力される場合があります。

```
Waiting for Inventory data 0 giving up after 300 seconds!
Starting ServerView Agents:VersionView.sav does not exist!
Starting aborted with status 1 (General error)
```

VersionView.sav はインストール時、およびそこから 2 時間おきに採取したインベントリデータが保持されるファイルです。
インストール時に 300 秒たってもファイルが作成されなかった場合に上記メッセージが出力されますが、このメッセージが出力された後もインベントリデータ収集、およびファイル作成は続行されます。しばらく（約 30 分程度）待って、VersionView.sav ファイルが作成されていることを確認してください。作成されていれば Agents の動作には問題ありません。
しばらく時間経過した後もファイルが作成されない場合、以下の点を確認して下さい。

- snmpd.conf に設定間違いはないか？
  snmpd.conf を手動で変更している場合、変更内容の記述に間違いがないか確認して下さい。
- snmp（ポート 161 番）へのアクセスがファイヤーウォール等で制限されていないか確認して下さい。

5.9 バージョンアップ後に FAN や温度センサが監視できない

Agents for Linux V5.10 以前のバージョンから V5.30 以降のバージョンにバージョンアップを行うと、FAN や温度、電圧センサ、および電源の情報が表示されない場合があります。原因は、V5.30 以降では OS の IPMI ドライバのみを使用するようになったため、そのドライバが削除されている場合、ハードウェアからセンサ情報が取得できないためです。

以下の環境で発生します。

- Agents for Linux V5.10 以前のバージョンで、ServerView の IPMI ドライバを使用する設定（OS の IPMI ドライバをローディングしない設定）を行っていた。
- その設定を行っている状態で V5.30 以降のバージョンのインストールを行った。

/etc/modprobe.conf に以下の行があれば削除し、OS を再起動してください。

install ipmi_* /bin/false

5.10 ServerView System Monitor で日本語文字列が正しく文字が表示されない

ServerView System Monitor で日本語文字列が正しく文字が表示されないことがあります。

使用する Java が他のアプリケーションによって置き換えられてしまっている可能性があります。

ServerView System Moitor は /usr/bin/java にリンクされている Java を使用します。これがサポート対象外の Java に置き換えられてしまっている場合は、サポート対象の Java のリンクへ設定を戻してください。富士通 Linux サポートパッケージ（FJ-LSP）をインストールすると Java のリンクがサポート外の Java に置き換えられることが確認されています。

5.11 Buffer I/O error が記録される場合がある

DISK のロックを行うようなツールを使用する場合は、Agents の機能により以下のエラーが発生する可能性があります。

kernel: Buffer I/O error on device sdx, logical block y

（sdx はデバイス名、block y はブロック番号）

Agents の仕様で監視対象の構成チェックを行う際に、OS が検知することにより発生します。

※一部のプロセス（hdagt）を停止する事により軽減することがか可能です。プロセスを停止する方法は、FNS-19976 の「3.発生を未然に防止する方法」を参照し、vme を hd に読み替えて実施願います。

5.12 ServerView System Monitor にアクセスすると ServerView Remote Connector の警告メッセージがログに出力される

Linux 環境にインストールされた ServerView System Monitor（Web 版）にアクセスすると /var/log/messages に以下のようなログが出力されます。

```
ServerView Remote Connector[PID]: WARN2370:  SSL sends error for the 'handshake tests'. This request will be ignored ! It might be missing encryption or problems with authentications. For more technical information see following data: IP=xxx.xxx.xxx.xxx SOAP-ENV:Receiver EOF was observed that violates the protocol. The client probably provided invalid authentication information. SSL_accept() failed in soap_ssl_accept()
```

このログはブラウザ側の制約のため、Remote Connector 側では抑止できません。
System Monitor の表示に問題がなければそのままお使いください。

▸ Windows

5.13 インストール時にイベントログにエラーメッセージが入ることがある

インストール時に以下のメッセージが出力される場合があります。

> ログの名前: System
> ソース: SNMP
> 説明:
> レジストリ キー
> SYSTEM¥CurrentControlSet¥Services¥SNMP¥Parameters¥ExtensionAgents をアクセスしているときに SNMP サービスはエラーを検出しました。

Agents V6.20 以前をインストールした事のある環境に Agents V6.20 をインストールした時、このメッセージが表示されます。Agents の動作に問題はありません。

5.14 WMI のエラーや WMI を使用するコマンドが異常終了することがある

Agents では自身が収集する情報を WMI コマンドで提供可能にするため、インストール時にデフォルトで「FSCSV_*」クラスが組み込まれます。
通常の「WIN32_*」クラスも、一部、この「FSCSV_*」クラスを経由または利用することになるため、WMI のエラーや WMI を使用するコマンド（systeminfo 等）の結果表示が遅い等の現象が発生する場合があります。
以下の方法で回避可能です。
ただし、この回避を行うと、SVOM のマニュアルに記載されている WMI コマンドを使用した、独自に作成したコマンドが動作しなくなります。独自にコマンドを作成していない場合は影響ありません。

(1) 「コントロールパネル」→「プログラムと機能」を開いて下さい。
(2) 「Fujitsu ServerView Agents」を右クリックし「変更」を実行して下さい。
(3) Agents のインストールウィザードが起動しますので「次へ」を押して下さい。
(4) 「プログラムの保守」画面では「変更」にチェックが付いた状態で「次へ」を押して下さい。
(5) 「カスタムセットアップ」画面では[Windows Managerment インテグレーション]をクリックし「X この機能を使用できないようにします」を選択して「次へ」を押して下さい。
(6) 「インストール」ボタンを押すと、変更インストールが開始されます。
SNMP サービスと Agent のサービスが再起動されますが、OS の再起動は不要です。

以上