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

2019/07
102-013 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（セキュアな 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

2.2 SNMP サービスの設定について

SNMP サービスのセキュリティタブの設定において、「これらのホストから SNMP パケットを受け付ける」を選択する場合、次の3つの設定値を入力してください。

- SVOM のホスト名または IP アドレス
- 自身のサーバのホスト名または IP アドレス
- ループバックアドレス(127.0.0.1 または localhost)

これらの設定がない場合、SNMP 認証エラーが発生します。

2.3 System Configuration 機能の使用について

ServerView Agents の SystemConfiguration 機能を使用する場合は、Java 実行環境を対象サーバにインストールする必要があります。

※ 監視のみを行う場合、あるいは ServerView Operations Manager で、System Configuration Manager を用いて設定を行う場合は監視対象サーバに Java 実行環境をインストールするは必要ありません。

ServerView Suite DVD 2 で提供される JRE の使用を推奨します。

▸ Linux/Citrix XenServer/everRun MX 共通

2.4 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。

2.5 OS をアップグレードする場合の注意事項

OS/カーネルのアップデートを行う場合(RedHat Enterprise Linux 7.4 -> 7.5 の場合など)は以下の手順で関連パッケージの再インストールが必要となります。
※修正カーネル（errata kernel）を適用する場合は、下記の手順を行う必要はありません。

1. ServerView Agents のアンインストール
2. smbus ドライバのアンインストール（smbus ドライバがインストールされている環境の場合）
3. OS/カーネルのアップデート
4. システムの再起動
5. smbus ドライバのインストール（手順 2 で smbus ドライバをアンインストールした場合）
6. ServerView Agents のインストール

※アンインストールを行うため、ServerView Agents の設定は引き継がれません。ServerView Agents 関連の設定とは、電源スケジュールや ASR 機能、ソフトウェアウォッチドッグ、ブートウォッチドッグ監視などの項目です。アップデートインストール後、再度設定し直してください。

- ServerView Agents for Liunx のアンインストール/インストール手順については、インストールガイド(sv-install-linux-agent-jp.pdf)を参照してください。
  ※アンインストール手順では、ソフトウェアウォッチドッグ、BOOT ウォッチドッグ、電源 ON/OFF 設定を必ず無効にしてください。予期せぬ再起動が発生する場合があります。

- smbus ドライバのアンインストール手順については、ServerView Agents for Linux V8.40.04 以降に同梱されている、smbus_driver.txt を参照してください。

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。

4.2　バージョンのダウングレード方法

ServerView Agents はダウングレードインストールには対応していません。一度アンインストールしてから、対象のバージョンをインストールしてください。

また、Update Agent も併せて再インストールしてください。これは、Agents のバージョンと依存関係があるためです。

Linux の smbus ドライバは、上位互換のため再インストールの必要はありません。

4.3　アラーム通知対象

ServerView Agents は BMC (iRMC) または BIOS から取得するセンサ情報、状態、および前回チェック時との比較によりアラームを通知します。そのため、SEL に格納されている全てのログが通知対象というわけではありません。

▸ Windows

4.4　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

4.5　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、対象のドメインユーザをローカルグループに所属させる必要があります。

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。

4.6　監査ポリシーの設定

Agents のインストールディレクトリ、またはインストールディレクトリより上位のドライブ、およびディレクトリに対し、監査ポリシーを適用しないでください。

適用した場合、セキュリティログにアクセスログが入り続けることがあります。

Linux/Citrix XenServer/everRun MX 共通

4.7 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。

4.8 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:

4.9 Agents が認識するネットワークインタフェース名

Agents が認識可能なネットワークインタフェース名は以下のとおりです。

eth*, bond*, sha*, vswif*, br*, xenbr*, en*, mic*, lo*, peth*, vmnic*, cip*, sit*

上記外の名前のネットワークインタフェースは認識することができません。

4.10 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。

4.11 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

  [32bit OS の場合]

  /etc/srvmagt/VME/lib/

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

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

[64bit OS の場合]

/etc/srvmagt/VME/lib64/

libcrypto.so.x.x.x -> /usr/lib64/libcrypto.so.xx

libssl.so.x.x.x -> /usr/lib64/libssl.so.xx

- SVRemoteConnector

  [32bit OS の場合]

  /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

  [64bit OS の場合]

  /opt/fujitsu/ServerViewSuite/SCS/lib64/

  libcrypto.so.x.x.x -> /usr/lib64/libcrypto.so.xx

  libssl.so.x.x.x -> /usr/lib64/libssl.so.xx

- eecd(smtp) ※ServerView SystemMonitor で使用。

  [32bit OS の場合]

  /etc/srvmagt/smtp/lib/

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

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

  [64bit OS の場合]

  /etc/srvmagt/smtp/lib64/

  libcrypto.so.x.x.x -> /usr/lib64libcrypto.so.xx

  libssl.so.x.x.x -> /usr/lib64/libssl.so.xx

OpenSSL のアップデートによりこのリンク先（/usr/lib/配下、/usr/lib64/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/lib64/libcrypto.so.xx や/usr/lib64/libssl.so.xx）が、新たなリンク先（/usr/lib64/libcrypto.so.yy や/usr/lib64/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
```

4.12 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。

4.13 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。

4.14 smbus ドライバのアップデートについて

smbus ドライバのアップデートを実行する際は、ServerView Agents for Linux V7.20.24 以降に同梱されている、smbus_driver.txt を参照してください。

4.15 ドライバモニタの制限

ドライバモニタでは、起動時に /var/log/ 配下の messages ファイルを全て調査しますが、そのファイル数の上限は 255 です。messages のバックアップファイル数が 255 を超えた場合、ServerView Agents の起動が失敗します。（ログローテート等により）同フォルダにバックアップを作成する場合、255 を超えないようにしてください。255 を超えてバックアップが必要な場合、別フォルダに作成してください。

▸ Citrix XenServer/everRun MX 共通

4.16 ServerView System Monitor の制限

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

Citrix XenServer/everRun MX において、Web 版 ServerView System Monitor の Update 機能は未サポートです。

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

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 Agents for Linux Vx.xx
(SUSE, Red Hat, 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」－「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。

everRun

4.18 everRun による制限のため、everRun のゲスト OS に対するスレッシュホールドマネージャおよびパフォーマンスマネージャの機能は利用できません。

Windows/Linux 共通

4.19 ServerView System Monitor の Update Check

Java 版 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, 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/ 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/ 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 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 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

5.5 ServerView System Monitor 等の Agents ツールが起動できない

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。

5.6 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。

5.7 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

ServerView System Monitor (Web 版)にアクセスすると以下のようなメッセージが出力される場合があります。

- Windows 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:
> 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 の場合

> 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

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。

5.8　SVOM のスレッシュホールドマネージャで監視ができない

SVOM のスレッシュホールドマネージャで Agents V7.30 以降のしきい値監視を行う場合、
SVOM の版数は V7.11.12 以降にする必要があります。

5.9　SystemMonitor のアップデート機能で[アップデート開始]ボタンが無効になる場合がある

System Monitor の アップデート機能において
[アップデート開始]ボタンが無効になる場合があります。
以下の方法を試してください。

1.System Monitor 画面を閉じる
2.フォルダの削除
C:¥ProgramData¥ServerView Suite¥Managed Node¥Server Control¥EM_UPDATE¥
3.ServerView Agents を再起動
Windows： スタートページの「Restart agents」を実行
Linux：# /usr/sbin/srvmagt restart　を実行

---

*EM_UPDATE の情報を再構成するため再起動の完了に時間がかかります。

▸ Linux/Citrix XenServer/everRun MX 共通

5.10 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。

5.11 アップデートインストール時に以下の警告メッセージが表示される

アップデートインストール時に以下のメッセージが複数出力される場合があります。

```
警告：ファイル xxxxxxxxxxxxxx：削除に失敗しました：そのようなファイルやディレクトリはありません
```

xxxxxxxxxxxxxx は削除対象のファイル、ディレクトリ名

アップデート前バージョンのファイルを削除する際に表示されます。

既に削除済み、またはアップデート後バージョンにしか存在しないファイルを削除しようとして表示されるメッセージですので、無視してください。

5.12 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ため、すべての DISK にアクセスを行います。

このため、OS がエラーを検知することにより発生します。

例えば、ETERNUS DX series のアドバンスト・コピー機能を使用した場合、本現象が発生する場合があります。

監視機能に問題はありませんが、エラー出力を抑制したい場合は、リモートマネージメントコントローラ等の Agents を使用しない別の監視方法をご検討ください。

PRIMERGY/PRIMEQUEST のサーバ運用管理については以下をご参照ください。

http://jp.fujitsu.com/platform/server/primergy/svs/

5.13 System Monitor のメール送信機能においてテスト送信が失敗する場合があります

Linux の 64bit 環境において、System Monitor(Web 版)のメール送信機能のテスト送信が失敗する場合があります。

テスト送信が失敗する場合は、以下のパッケージがインストールされているか確認してください。

- compat-libstdc++-33.i686 (※)
- openssl.i686

(※) RHEL7 の場合、インストール DVD に同梱されていません。オンライン上からダウンロードしてください。

5.14 ドライバモニタが過去のエラーを繰り返し検出します

OS のシスログに検出対象となるメッセージが出力されていた場合、ServerView Agents の再起動時に

再度ドライバモニタのエラーを検出します。検出対象となるメッセージがローテーションされ過去のシスログからも削除されると再検出はしません。

5.15 他サーバのドライバモニタ対象ログが自サーバのログとして処理される場合があります

OS のシスログの転送先に設定されている場合、転送されたログを自サーバ発生したのログとして処理する場合があります。

ドライバモニタはシスログに格納されるログを解析対象としていますが、対象のログが転送されたログなのか自サーバのログなのかの区別がつきません。

そのため、ドライバモニタ（ServerView Agents）が動作しているサーバにログを転送する場合は、rsyslog.conf で転送されたログの除外を設定してください。

例）local（ファシリティ)として転送されたログを、ドライバモニタの対象外として設定する。

※事前に、転送元サーバにてログの転送設定をファシリティ local7 と設定している場合。

現）/etc/rsyslog.conf

```
        :
*.info;mail.none;news.none;authpriv.none;cron.none
                                |/opt/fujitsu/ServerViewSuite/HWLog/path/syslog_fifo
```

変更）/etc/rsyslog.conf （";local7.none"を追記）

```
*.info;mail.none;news.none;authpriv.none;cron.none;local7.none
                                |/opt/fujitsu/ServerViewSuite/HWLog/path/syslog_fifo
```

▸ Windows

5.16 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

V7.20.22 以前のデフォルトでのインストール環境、および V7.30.10～V7.31.18 のカスタムセットアップで[Windows Managerment インテグレーション]機能を有効にしてインストールした環境の場合、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「FSCSV_*」クラスが組み込まれます。

※ 既に[Windows Managerment インテグレーション]が有効になっている環境から、V7.20.10～V7.31.18 へアップデートした場合、[Windows Managerment インテグレーション]は有効のままとなります。

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。

5.17 ハードの情報が表示されない場合の確認

Agents がハードから情報を取得できず、ServerView Operations Manager や SererView System Monitor でハード情報が表示されない場合、以下を確認してください。

OS アプリケーションログ:

Server Control 1 EM_XXXX: WMI instance 'Microsoft_IPMI' could not be connected (hres = 0x80041013). Check if Microsoft Generic IPMI Compliant Device is running asic hardware server management not available.

※EM_XXXX はエラーを検出した Agents の内部モジュール名が入ります。

上記のエラーは、Agents がハードと通信を行う際に使用する OS の IPMI ドライバのエラーです。このエラーがある場合はハードとの通信ができません。

Agents を再起動しても解消しない場合、OS 観点での調査が必要です。

以上