取扱説明書補足資料－日本語

ServerView Suite
ServerView Agents
補足情報

2012/5

002-006

目次

■ はじめに

本書は、ServerView Agents V5 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)

■ 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 ： V5.00、V5.01、V5.10、V5.30、V5.50、V5.51

■ 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/Agents が使用するポートと競合し、ServerView Operations Manager、Agents が起動出来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/Agents の使用ポートと競合しない様に注意してください。

ServerView Operations Manager/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

▸ 共通

2.1 ダウングレード

現在お使いの Agents を、それよりも古いバージョンにダウングレードする場合、一旦現在インストール済みの Agents をアンインストールする必要があります。古いバージョンへのダウングレードインストール(上書きインストール)はできません。

Windows

2.2 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): F5EP70_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

2.3 snmpd.conf の変更

Agents をインストールした後に、snmpd.conf ファイルを編集した場合、編集後に Agents 及び snmpd を再起動する必要があります。

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 インストール後のコンピュータ情報変更

Agents をインストールした監視対象サーバのコンピュータ名、または IP アドレスを変更した場合、Agents に対して設定変更などの作業は必要ありません。

ただし、個別の環境用に snmpd.conf ファイルを編集している場合は、必要に応じて再度編集してください。

snmpd.conf ファイルを編集した後は、snmpd サービスと Agents を次の手順で再起動します。

1. スーパーユーザでログインします。
2. 次のコマンドを実行します。

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

3 アンインストール

▸ 共通

3.1 ASR の無効化

ASR 機能の設定をしたまま Agents をアンインストールした場合、 予期せぬ原因でサーバがシャットダウンされることがあります。

また、ASR の電源 OFF/ON のスケジュール機能を設定しているサーバから Agents をアンインストールする場合は、事前に必ず、スケジュール設定を全て無効にしてください。スケジュール設定を有効にしたまま Agents をアンインストールすると、スケジュール機能による電源 OFF が動作し、これによって、サーバの OS をシャットダウンせずに電源 OFF される場合があります。

▸ Citrix XenServer/everRun MX

3.2 /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、ServerView Agents と ServerView RAID がアンインストールされます。

ServerView 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 を再インストールしてください。

また、ServerView 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」の手順で行なってください。

4 サーバデータの詳細表示(シングルシステムビュー)

▸ 共通

4.1 ASR の設定

ASR の設定内容は、ServerView Operations Manager/Agents には保持されません。サーバ本体の BIOS／BMC(RSB／iRMC)に格納されます。

5 その他

Windows

5.1 Agents のサービスの再起動

Agents のサービス(サービス名:「ServerView Server Control」)を再起動する場合、「SNMP Service」も合わせて再起動する必要があります。

「ServerView Server Control」の再起動に際して、「SNMP Service」の再起動を行わなかった場合、正常にサーバ監視ができない場合があります。

5.2 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、以下の通りです。尚、ログの種類は全て「アプリケーション」です。

・ServerView Agents
・ServerView Virtualization Management Agents
・ServerView Remote Connector
・ServerView Server Control

Linux/VMware /Citrix XenServer/everRun MX

5.3 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、SNMP コミュニティ「public」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 SNMP コミュニティ「public」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 SNMP コミュニティ「public」による SNMP 通信を許可する設定を行なってください。

5.4 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、以下の通りです。

・Serverview:
・srvmagt_scs:
・vmeagt:
・ServerView RemoteConnector:

▸ VMware/Citrix XenServer/everRun MX

5.5 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。

6 トラブルシューティング

▸ 共通

6.1 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.

6.2 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。ServerView 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。

6.3 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()
```

- 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()
```

xx.xx.xx.xxにはIPアドレスがはいります。

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すメッセージです。

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>

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)

6.4 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 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 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

6.5 ServerView System Monitor が起動できない

ServerView System Monitor 等の ServerView Agents のツールが、JREのエラー等の影響によって正常に起動出来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」等で終了させ、一旦ツールを終了した後、再度起動を行ってください。

6.6 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。

- Agents バージョンを確認してください

  ServerView Agents for Windows V5.50 には、正常にログイン出来ない問題があります。

  以下の対処を行ってください。

  ① Agents Configuration ツールを起動し、「セキュリティ設定」タブに移動する。

  ② "パスワードによる保護を有効にする"のチェックを外す。

  ③ 「適用」ボタンをクリックする。

  ※設定以降、パスワードによる保護は行われません。

以上