取扱説明書補足資料－日本語

FUJITSU Software ServerView Suite ServerView Operations Manager V9.00 以降 補足情報

2020/08
201-003 版

目次

■ はじめに

本書は、ServerView Operations Manager V9 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。

- ServerView Operations Manager V9 （sv-operations-mgr-jp.pdf）
- ServerView Operations Manager V9 Installing ServerView Operations Manager Software under Linux （sv-install-linux-jp.pdf）
- ServerView Operations Manager V9 Installing ServerView Operations Manager Software under Windows （sv-install-windows-jp.pdf）
- ServerView Event Manager （sv-event-mgr-jp.pdf）
- ServerView Inventory Manager （sv-inventory-mgr-jp.pdf）
- ServerView Threshold Manager （sv-threshold-mgr-jp.pdf）
- ServerView Archive Manager （sv-archive-jp.pdf）
- ServerView Performance Manager （sv-performance-jp.pdf）
- Base Configuration Wizard （sv-base-config-wizard-jp.pdf）
- ServerView Online Diagnostics （sv-onldiag-jp.pdf）
- PrimeCollect （sv-primecollect-jp.pdf）
- ServerView でのユーザ管理 （sv-user-mgt-jp.pdf）
- セキュアな PRIMERGY サーバ管理 （sm-security-ja.pdf）
- ServerView Suite Asset Management (sv-asset-jp.pdf)
- FUJITSU Software ServerView Suite (sv-concepts-jp.pdf)
- ServerView Suite 説明書 (sv-documentation-jp.pdf)
- ServerView embedded Lifecycle Management (eLCM) 1.2 for iRMC S4 / S5 (sv-eLCM-overview-s4-jp.pdf / sv-eLCM-overview-S5-ja.pdf)
- ServerView Remote Management Frontend (sv-remfe-jp.pdf)
- PRIMERGY Server Events (sv-serverevents-41-jp.pdf)
- ServerView Suite 製品での SNMPv3 の 使用 (sv-snmpv3-jp.pdf)
- ServerView Update Management (sv-update-jp.pdf / sv-update-jp.pdf)

※マニュアル名の「x.xx」にはバージョン番号が入ります。

■ 対象バージョン

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

本書の対象バージョン ： V9 以降

V5.00～V5.51 については、ServerView Operations Manager 補足情報[001-009 版]を参照してください。

V6.00～V7.10 については、ServerView Operations Manager 補足情報[001-027 版]以降を参照してください。

V7.11～V8.51 については、ServerView Operations Manager 補足情報[101-021 版]を参照してください。

■ 補足情報

1 インストール要件

▸ Windows/Linux 共通

1.1 名前解決の設定

ブラウザからアクセスする際に、SVOM がインストールされたサーバのホスト名(ネットワーク上のコンピュータ名)もしくは「<ホスト名>.<DNS サフィックス>」を名前解決できるように設定されている必要があります。DNS サーバの設定、もしくは端末側の hosts ファイルにサーバのホスト名もしくは<ホスト名>.<DNS サフィックス>と IP アドレスを追加するなどして、名前解決できるように設定してください。

SVOM をインストールしたサーバにおいても、SVOM にブラウザでアクセスする場合には、自分自身のホスト名もしくは<ホスト名>.<DNS サフィックス>が名前解決できるように設定されている必要があります。

以下の方法で、名前解決が出来ているか確認してください。

- Windows の場合

  tracert <ホスト名>.<DNS サフィックス>

  例:

  ```
  tracert svomserver.psd.cs.fujitsu.co.jp
  ```

- Linux の場合

  traceroute <ホスト名>.<DNS サフィックス>

  例:

  ```
  traceroute svomserver.psd.cs.fujitsu.co.jp
  ```

なお、IPv6 と IPv4 の両方が有効になっている場合、ブラウザに入力したホスト名若しくは「＜ホスト名>.<DNS サフィックス>」に対して、SVOM のインストール時に入力したサーバの IP アドレスが先に解決される必要があります。

例えば、ホスト名もしくは「<ホスト名>.<DNS サフィックス>」に対して、インストール時に入力したサーバの IP アドレスが「192.168.0.2」などの IPv4 のアドレスであるのに対して、IPv6 のループバックアドレス「::1」などが先に解決される場合、一部の機能が正常に動作しません。

▸ Windows

1.2 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 SVOM/Agents が使用するポートと競合し、SVOM、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、SVOM/Agents の使用ポートと競合しない様に注意してください。

1.3 Windows Server 2008 R2 における SVOM インストールについて

Windows Server 2008 R2 に SVOM(同梱の SQL を含む)V8.20.02 以降をインストールする場合は、事前に.NET Framework4.x および同バージョンの日本語 Language Pack が必要です。
(マイクロソフトダウンロードサイト等からダウンロードして適用して下さい)

2 インストール

▸ Windows

2.1 ディレクトリサービスに Active Directory を使用している場合のアップデートインストール

SVOM が使用するディレクトリサービスに Active Directory を使用している場合で、アップデートインストールを行った場合、SVActiveDirectory.ldif を再度インポートする必要があります。

※ V7.20 以降で統合 RBAC 管理(ローカルのディレクトリサーバでの承認)を選択した場合は、SVActiveDirectory.ldif ファイルのインポートは必要ありません。

SVActiveDirectory.ldif のインポート方法の詳細は、マニュアル「ServerView でのユーザ管理」(sv-user-mgt-jp.pdf)の「ServerView ユーザ管理の Microsoft Active Directory への統合」を参照してください。

3 アンインストール

▸ Windows/Linux 共通

3.1 パフォーマンスマネージャのレポート設定

パフォーマンスマネージャのレポートを設定したまま SVOM をアンインストールすると、SVOM－Agents 間に設定の差異が生じます。SVOM をアンインストールする前に、必ずレポートの設定を解除してください。

▸ Linux

3.2 snmptrapd.conf の定義

SVOM をインストールした際、/usr/share/snmp/snmptrapd.conf に以下の行が追記されます。この行は SVOM をアンインストールした場合でも、削除されず残ったままとなります。

```
traphandle default
/opt/fujitsu/ServerViewSuite/web/cgi-bin/ServerView/SnmpTrap/SnmpTrapListen
```

※本書ではページの都合上 2 行で記載されていますが、実際には上記が 1 行で記載されます。

古いバージョンの SVOM をインストールしたことがある場合、古いパスの情報が残ったままとなるので、古いパスの情報は消してください。

4 サーバリストの管理

▸ Windows/Linux 共通

4.1 サーバ名に使える文字

サーバを登録する時、「サーバ名」を変更することができます。その場合、サーバ名に日本語や、記号（ ！" # $ % & ' ( ) = ~ | ^ ¥ @ [` { ; :] + * } , / < > ? _ など）、空白は使用しないでください。

4.2 マネジメントブレードの登録

マネジメントブレードをサーバリストに登録すると、配下のサーバブレードが監視可能となります。この場合、サーバブレードの IP アドレスはマネジメントブレードから自動的に取得されます。

マネジメントブレードは、サーバブレードに搭載されている LAN ポートを、MAC アドレスの小さい順、かつ、通信可能な順で IP アドレスを認識します。そのため、LAN ポートの状態変化によっては、サーバリスト上の監視 IP アドレスが変動することがあります。

IP アドレスの変動を避けるには、サーバのプロパティのブレードのネットワークアドレス設定でブレードにこのアドレスをいつも使用するにチェックを付け、指定可能なアドレスで監視 IP アドレスを選択して下さい。

4.3 LAN 冗長化を行っている場合の設定

サーバブレードでチーミングなどの LAN 冗長化を行っている場合、マネジメントブレードをサーバリストに登録した際に LAN 冗長化を行っているサーバブレードの IP アドレスが 0.0.0.0 と表示される場合があります。この場合、冗長化を行っているサーバブレードは独立したサーバとしてサーバリストに個別に登録してください。

4.4 サーバリストのエクスポート

サーバリストをエクスポートしたファイルは他サーバでもインポートすることが可能です。データベースや OS が違っていてもインポートすることが可能です。

ただし、Linux にインストールされた SVOM へインポートする場合は、Windows（Internet Explorer）で Linux の SVOM へアクセスしてインポートしてください。

エクスポートしたバージョン以降の SVOM にのみ、ファイルをインポートすることができます。

4.5 Citrix XenServer の監視

- XenCenter のプールサーバで管理されている仮想サーバに対して、SVOM を使用して監視する場合、XenCenter で使用している管理者権限のユーザアカウント(root など)を SVOM の「ユーザ/パスワード」に追加する必要があります。
- 複数の XenServer をまとめてリソースプールを作成している環境で XenServer や仮想サーバ

を SVOM で監視する場合、特定の XenServer に負荷がかかる可能性があります。XenServer、仮想サーバの情報を取得するために、サーバリストに登録されている XenServer、仮想サーバの数の分だけリソースプールのマスタノードとなっている XenServer にアクセスを行います。このため、多数の XenServer、仮想サーバが存在する環境ではマスタノードの XenServer に負荷がかかる可能性があります。負荷は環境によってことなりますので、事前に問題ないかの確認を行ってください。

なお、以下の設定を行うことにより、負荷を軽減させることができます。必要に応じて設定を変更してください。(詳細な手順についてはマニュアルを参照してください)

(1) サーバリストに登録されている仮想サーバのプロパティを開きます。
(2) [ネットワーク/SNMP] タブを開きます。
(3) タブ内にある [ポーリング間隔] の設定で [指定] を選択し、入力欄に 0 を設定します。

上記設定を行うことにより、設定を変更した仮想サーバの情報収集を行う定期的なポーリングを行わなくなります。

XenCenter の設定内容については、XenCenter の入手先へ確認してください。

4.6 VMware ESXi サーバの監視

VMware ESXi サーバの監視についての留意事項を以下のページにて公開しています。こちらの「VMware vSphere 5 におけるサーバ監視の留意事項」および「VMware vSphere 6 におけるサーバ監視の留意事項」も参照してください。

https://jp.fujitsu.com/platform/server/primergy/software/vmware/manual/ (PRIMERGY)
https://fujitsu.com/jp/products/computing/servers/primequest/products/1000/catalog/guide/vmware/index.html (PRIMEQUEST 1000 シリーズ)
https://fujitsu.com/jp/products/computing/servers/primequest/products/2000/catalog/guide/vmware/index.html (PRIMEQUEST 2000 シリーズ)
https://fujitsu.com/jp/products/computing/servers/primequest/products/3000/catalog/guide/vmware/index.html (PRIMEQUEST 3000 シリーズ)

4.7 VMware ESXi サーバの登録

監視対象サーバとして VMware ESXi サーバをサーバリストに登録する際、SVOM の[管理者設定] – [ユーザ/パスワード] にて、対象サーバの OS にログイン可能なユーザ名とパスワードを設定しておく必要があります。

VMware vSphere ESXi 6 サーバについては、ユーザ名とパスワードを事前登録せず、未認証のまま検出・登録を行うことが可能です。詳細は、「4.6 VMware ESXi サーバの監視」に記載の VMware のマニュアルページの「VMware vSphere ESXi 6 におけるサーバ監視の留意事項」を参照してください。

4.8 仮想サーバ

SVOM において、仮想化ソフトウェアをサーバリストに登録した場合、配下の仮想サーバに対して SNMP アクセスを行います。
仮想化ソフトウェアをサーバリストに登録した際に設定されているコミュニティ名が、配下の仮想サーバにも引き継がれます。サーバリストに登録後は、[サーバのプロパティ] － [ネットワーク/SNMP]タブを開いて、各仮想サーバのコミュニティ名について確認を行ってください。コミュニティ名が異なっている場合、認証エラーが生じます。
また、仮想サーバに対して以下を実施する場合、仮想サーバ上で SNMP サービスを起動させる必要があります。

- 接続状態変更トラップの有効。
- シングルシステムビューを開く（仮想サーバの場合、表示可能な項目に制限があります）。

4.9 サーバリストに表示される仮想(ゲスト)システムの IP アドレス

サーバリストに表示される仮想(ゲスト)システムの IP アドレスは、サーバのプロパティから任意の値を指定できます。対象の仮想(ゲスト)システムのサーバのプロパティを開き、サーバのアドレスタブのアドレス箇所に任意の値を入力してください。
ただし、次の場合は正しい IP アドレスに自動的に書き換えられます。

- 実際に割り当てられている IP アドレスではない
- 仮想化ソフトウェアが認識していない IP アドレス

4.10 仮想(ゲスト)システムに対する SNMP ポーリング

SVOM は、サーバリストに登録された仮想(ゲスト)システムに設定されている全ての IP アドレスに対して SNMP ポーリングを実施します。
特定の IP アドレスにのみ SNMP ポーリングを行うことは出来ません。
ただし、サーバのプロパティでポーリング間隔を 0 秒に設定することにより、該当の仮想(ゲスト)システムに対して SNMP ポーリングを一切行わないようにすることが可能です。

- サーバリストより SNMP アクセスを停止したい仮想(ゲスト)システムを選択し右クリックメニューからサーバプロパティを選択。
- ネットワーク/SNMP タブのポーリング間隔の項目で指定にチェックを付け、0 秒を指定。

ただし、上記設定を実施すると仮想(ゲスト)システムに対する SNMP ポーリングが無効となるため、仮想(ゲスト)システムのステータス監視が行われなくなります。

4.11 接続状態変更トラップ

[サーバのプロパティ] － [ネットワーク/SNMP]タブで設定可能な「接続状態変更トラップ」は、対象サーバのステータスが以下のように遷移した場合にトラップを送信します。

- ok → notmanageable
- ok → unknown
- snmpOK/cimOK → notmanageable
- snmpOK /cimOK→ unknown

- notmanageable → ok
- notmanageable → snmpOK/cimOK
- unknown → ok
- unknown → snmpOK/cimOK

上記の各ステータスの意味は以下の通りです。

ステータス	意味
ok	正常
snmpOK	ServerView Agent は応答していないが、SNMP は応答している
cimOK	ServerView CIM Provider は応答していないが、CIM Provider は応答している
notmanagble	SNMP または、CIM provider は応答していない
unknown	コンポーネントが利用不可

4.12 仮想(ゲスト)システムが表示される

基本設定ウィザードの VM 検索で設定した内容と、サーバリスト画面の実際のサーバ一覧が一致しない場合があります。(仮想(ゲスト)システムの監視を停止したが、サーバリストに残っている等)
対象のサーバを含むホスト OS をサーバリストから一度削除して、サーバブラウザから再登録をしてください。

4.13 iRMC を監視する場合の登録手順

監視対象サーバとして iRMC をサーバリストに登録する際、以下の手順で実施してください。

1) SVOM で「サーバブラウザ」画面を開きます。
2) 「サブネット / アドレス / ホスト名」欄に、監視対象の iRMC の IP アドレスを入力します。
3) 「SNMP 設定」に、監視対象の SNMP 情報を入力します。
4) 「検索」ボタンをクリックして検索結果を確認します。
5) 表示された項目を選択して、「追加」ボタンをクリックします。

以上で、監視対象の iRMC が「サーバリスト」画面に表示されます。

5 アラームモニタ

▸ Windows/Linux 共通

5.1 SNMP バージョン

SVOM は SNMPv1 に準拠したトラップのみをサポートしています。

6 アラーム設定

▸ Windows/Linux 共通

6.1 アラームルール名・アクション名

アラームルール名、及びアクション名に使用できる文字は、半角英数字と「_」のみとなります。
使用可能な文字以外の文字をアラームルール名やアクション名に使用した場合、使用したアラームルール、アクションを含めたすべてのアラームルール、アクションが正常に動作しない場合があります。

6.2 プログラム実行

- アクションの割り当ての「プログラム実行」で利用できるコマンドは CUI コマンドに限られます。
- コマンドラインに加えられるマクロを引数として使用する場合、受け取った内容によっては、データ内に空白があり、その前後でデータが分かれ、期待通りにデータが受け取れない可能性があります。その場合、マクロ部分を""(ダブルクォーテーション)で括ってください。
  例: “$_TRP” (トラップテキストの場合)
- 64bit Windows OS を使用している場合、アクションの割り当ての「プログラム実行」で、
  "C:¥WINDOWS¥System32¥"にあるプログラムを指定する際は、
  "C:¥WINDOWS¥Sysnative¥"を指定して下さい。
  SVOM は 32bit アプリケーションのため OS の仕様により、"C:¥WINDOWS¥System32¥"は自動的に"C:¥WINDOWS¥SysWOW64¥System32¥"にリダイレクトされてしまいます。
  "C:¥WINDOWS¥Sysnative¥"を指定することで"C:¥WINDOWS¥System32¥"にアクセスできるようになります。

  OS の仕様については以下を参照してください。
  https://msdn.microsoft.com/ja-jp/library/aa384187(v=vs.85).aspx

6.3 メール

アクションの割り当てで複数の「メール」のアクションを設定する場合、[メールプロパティ]タブで異なる SMTP の設定はできません。

6.4 メールの件名

- アクションの割り当てで「メール」のアクション設定する場合、件名に日本語(2バイト文字)を設定すると、SMTP によっては受信したメールの件名が文字化けする場合があります。その場合、件名には半角英数を使用してください。
- 件名に半角記号を使用した場合、メールの送信が失敗する、もしくは記号が件名に反映されない場合があります。 ((,), &, <, |, ;, +)

7 サーバデータの詳細表示(シングルシステムビュー)

▸ Windows/Linux 共通

7.1 ASR&R の設定

ASR&R の設定内容は、SVOM/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。

7.2 診断情報収集(PrimeCollect)

診断情報収集(PrimeCollect)を実行した際、CAS サーバエラーや証明書エラーなどが表示され正常に動作しない場合があります。この場合、以下の内容を確認してください。SVOM にアクセスするブラウザを実行している監視端末も対象となります。

- SVOM と対象サーバの間でネットワークポート 3170 番と 3172 番が開放されていること。
- 対象サーバから SVOM に対して名前解決が正しく行なわれていること。
- SVOM の証明書と対象サーバの証明書の整合性が取れていること。

8 MIB インテグレータ

▸ Windows/Linux 共通

8.1 ネットワーク機器からのトラップ

ネットワーク機器の MIB ファイルを登録することによって、その機器から送られたトラップの表示および、受信したトラップに対する動作の設定を行うことができます。

なお、あらかじめ対象のネットワーク機器をサーバリストに登録しておく必要があります。登録する際、サーバの種類は「Other」とします。

9 その他

▸ Windows/Linux 共通

9.1 SVOM がアクセスするネットワークポート

SVOM は SVOM のサーバブラウザ画面において、サーバを検索する際に、サーバブラウザ画面で指定したサブネット内のサーバに対して、以下のネットワークポートへアクセスを行います。

80, 135, 161, 443, 623, 3172, 5988, 5989, 9363, 16509, 16514

同じくサーバブラウザ画面で、サーバを登録する際には登録するサーバの上記ネットワークポートにアクセスを行います。またサーバを登録後は、登録されたサーバに対して、上記ネットワークポートにアクセスを行います。

SVOM は、ネットワークポートが共有されていても問題が起きない構造としておりますが、指定したサブ

ネット内、及び SVOM に登録したサーバで上記ネットワークポートへのアクセスを占有したい等の理由で不都合がある場合には、不都合のあるプロダクト側でポートを変更するなどの対処を行ってください。
※サーバの種類や OS によって、上記のアクセスが行われない場合があります。

9.2 サーバ名および IP アドレス変更後の操作

インストールしたサーバの IP アドレスやホスト名、DNS サフィックスを変更した場合、ServerView Operations Manager に変更を反映するため、以下の操作が必要です。

- Windows の場合

  以下の手順を実施してください。

  (1) [コントロールパネル]から、[プログラムと機能]を開く
  (2) [Fujitsu Software ServerView Application Server]を選択し、「変更」ボタンをクリック。変更インストールを実施
  (3) [Fujitsu Software ServerView Operations Manager]を選択し、「変更」ボタンをクリック。変更インストールを実施

- Linux の場合

  以下のコマンドを実行してください。

  ```
  # /opt/fujitsu/ServerViewSuite/svom/ServerView/Tools/ChangeComputerDetails.sh
  ```

  変更後の設定を確認するメッセージが表示されます。メッセージに従って入力を行ってください。

サーバリストに変更前のサーバ名や IP アドレスが監視対象として残ったままとなる場合があります。
その場合、SVOM が変更前の IP アドレスへアクセスし続けることになりますので、以下の手順で変更前のサーバ名及び IP アドレスの監視エントリを削除してください。

(1) サーバリストより削除対象のサーバ名を選択し、右クリックします。
(2) メニューから「削除」をクリックします。

9.3 ログインユーザのパスワードに使用可能な文字

ログインユーザのパスワードには、半角英数記号が使用可能です。ただし、UserAdministrator 権限を持つユーザが他のユーザのパスワードを設定する場合「"(ダブルクォーテーション)」を使用することはできません。その他の権限を持つユーザが自分自身のパスワードを設定する場合は、「"」も使用可能です。

9.4 SVOM 及び Agents に必要なユーザ設定

SVOM を運用するにあたって以下の 4 種のユーザ設定が存在します。

(A) SVOM のログインに用いられるユーザ設定
(B) SVOM から監視対象の Agents に値を設定する際に必要なユーザ設定
(C) SVOM が監視対象の OS/iRMC/ETERNUS DX に接続する際に用いられるユーザ設定

(D) SVOM のサービスに関連するユーザ設定

以下にこれらを説明します。

(A) SVOM のログインに用いるユーザ設定

- SVOM の起動画面で入力を求められます。
- SVOM の参照する ApacheDS(デフォルト)または ActiveDirectory に設定されています。
- ApacheDS を使用している場合、ユーザ名に以下の文字は使用することができません。
  - "=|[]:*;+,<>?/!#$'()^¥~@`{}
  - 空白
  - 日本語などの 2 バイト文字
- ApacheDS 使用時のユーザ/パスワードの最大文字数
  - ユーザ/パスワードとも 1000 文字以上可能

(B) SVOM から監視対象の Agents に値を設定する場合に必要なユーザ

- SVOM において以下を実施する場合にユーザ名/パスワードを求められます。
  - 表示識別灯を点灯させる場合
  - 「サーバの設定」画面でツリーから各サーバを選択した場合
  - パフォーマンスマネージャ画面で、レポートセットを作成し、「サーバへの適用」を実行した場合
- 監視対象の Agents で上記の操作を許可するグループを設定します。上記の操作を行う場合、表示されるダイアログに、監視対象の Agents で設定したグループに所属するユーザ/パスワードを入力します。
- ユーザ/パスワード入力の最大文字数
  - ユーザ:20 文字
  - パスワード:128 文字

監視対象の Agents で上記の操作を許可するグループの設定は、以下の方法で行います。

- ServerView Agents for Windows の場合
  (1) 「Agent Configuration」を起動します。
  スタート－[すべてのプログラム] - [Fujitsu] - [ServerViewSuite] - [Agents] - [AgentConfiguration]から起動します。
  (2) 「セキュリティ設定」タブを開きます。
  (3) 「パスワードによる保護を有効にする」にチェックを入れます。
  この項目にチェックを入れていない場合、上記の操作を行う場合にもユーザ名/パスワードは求められません。
  (4) 「ユーザグループ」に任意のグループ名を入力します。
  SVIM を使用して Agents をインストールした場合、もしくはインストールウィザードのセットアップレベル画面で選択肢を選ばずにインストールした場合、「FUJITSU

SVUSER」が入力されています。
この項目に何も入力せずに空白を設定した場合は、Administrators グループに所属するユーザが上記の操作を行うことができるようになります。

(5) 「適用」ボタンをクリックします。

- ServerView Agents for Linux の場合
  ファイル「/etc/srvmagt/config」の「UserGroup」に任意のグループ名を設定します。その後、ServerView Agents for Linux を再起動します。
  デフォルトでは、以下の値が設定されています。
  UserGroup=svagtuser

(C) SVOM が監視対象の OS/iRMC/ETERNUS DX に接続するためのユーザ

- SVOM において以下を実施する場合に、予め SVOM の画面の[監視] － [ブラウジング設定] － [ユーザ/パスワード] に対象のサーバの OS にログイン可能なユーザ名とパスワードを設定しておく必要があります。
  - VMware ESXi サーバを CIM 監視する場合
  - iRMC 監視を行う場合(「4.13 iRMC を監視する場合の登録手順」を参照)
    ※ iRMC のデフォルトのユーザ/パスワード admin/admin は初期設定されています
  - サーバリスト上から「電源制御」を行う場合
  - 仮想 OS のホストをサーバリストに登録する場合
  - スレッシュホールドマネージャを使用する場合
  - シングルシステムビューの項目「パフォーマンス」を有効にする場合
  - ストレージ情報を表示する場合
- ユーザ/パスワード入力の最大文字数
  - ユーザ:256 文字
  - パスワード:文字数に制限はありません。

(D) SVOM のサービスに関連するユーザ

- Windows 環境に SVOM をインストールする際に、SVOM のサービスである「ServerView ApplicationService」および「ServerView Download Service」を実行するユーザを設定する必要があります。
- 通常、インストール時以外には設定 / 変更の必要はありません。
- ユーザ/パスワードの最大文字数
  - ユーザ:20 文字
  - パスワード:63 文字

9.5 SVOM サービス停止中の注意

バックアップなどの採取により SVOM 関連のサービスを停止している間は、サーバの監視やトラップの受領などが行われません。

9.6 関連ファイルの編集

SVOM/Agents 関連ファイルの編集、追加、削除などは、動作に影響を及ぼす可能性がありますので、マニュアルに記載されている内容以外は一切行わないでください。

9.7 SVOM がアクセスする IP アドレス

サーバリストに登録されている監視対象サーバの IP アドレスに対して通信ができなかった場合、SVOM では監視対象サーバが持つ他の IP アドレスに対してもアクセスを行う可能性があります。

9.8 サードパーティ製 MIB について

SVOM には予めサードパーティより入手した MIB が組み込まれています。
これらサードパーティ製の MIB に関するお問い合わせは、各ベンダへお願いします。
MIB は以下のフォルダに格納されています。

Windows:

<SVOM インストールフォルダ>¥ServerView Suite¥ServerView¥ServerView Services¥scripts¥ServerView¥common¥mibs¥

Linux:

/opt/fujitsu/ServerViewSuite/web/cgi-bin/ServerView/common/mibs/

各 MIB ファイルをテキストエディタで開くと、SNMPv1 形式の場合は先頭近くのコメントに、SNMPv2 形式の場合は"DESCRIPTION"**行に MIB の作成ベンダ名が記載されています。**
記載されておらず、ベンダ名が不明であればお問い合わせください。
なお、SVOM に組み込まれている MIB は、SVOM の公開当時のバージョンです。
適宜、ベンダより対応する MIB を入手してください。
SVOM にて対応可能な MIB のトラップ定義の注釈形式は、Novell NMS で提唱される形式に準じます。

▸ Windows

9.9 システムバックアップ

SVOM は常時ファイルの書き換えやデータベースへのアクセスを行っています。システムバックアップ時には、必要に応じて以下の順に SVOM のサービスを停止してください。

(1) ServerView Download Service
(2) ServerView Services
(3) ServerView ApplicationService
(4) ServerView Apache Directory Server (*)
(5) ServerView Remote Connector
(6) SQL Server（SQLSERVERVIEW）

システムバックアップを行った後、以下の通り、停止したのと逆の順番でサービスを開始してください。

(1) SQL Server(SQLSERVERVIEW)
(2) ServerView Remote Connector
(3) ServerView Apache Directory Server (*)
(4) ServerView ApplicationService
(5) ServerView Services
(6) ServerView Download Service

*:インストール手順により存在しない場合があります。

9.10 Microsoft SQL Server の更新プログラムの適用

Microsoft SQL Server の更新プログラムを適用する場合、SVOM のサービスが停止している場合があります。その場合、以下の手順でサービスの停止/開始を行ってください。

以下の(1)～(3)のサービスのうちいずれか 1 つでも停止していた場合、(1)～(3)の順に停止します。
既に停止されているサービスは、そのまま停止しておきます。
以下のサービスのうち、存在するものがすべて開始されていた場合は、対処の必要はありません。

(1) ServerView Download Service
(2) ServerView Services
(3) ServerView ApplicationService
(4) ServerView Apache Directory Server (*)

Microsoft SQL Server の更新プログラムを適用した後、以下の通り、停止したのと逆の順番でサービスを開始してください。

(1) ServerView Apache Directory Server (*)
(2) ServerView ApplicationService
(3) ServerView Services
(4) ServerView Download Service

*:インストール手順により存在しない場合があります。

Linux

9.11 cron に登録されるジョブ

定期的にデータのバックアップを行うため次のジョブが cron に登録されます。

ジョブ説明:

Weekly :1 週間(曜日、時刻はシステム稼働に依存)ごとにデータベースをバックアップします。
Daily :1 日(時刻はシステム稼働に依存)ごとにデータベースの差分をバックアップします。

これらのジョブを、cron から削除したり、無効にしたりしないでください。動作時刻はシステムの稼働状

況に依存します。詳しくは、cron の仕様を確認してください。
バックアップデータは、次のディレクトリ配下に格納されます。
/var/fujitsu/ServerViewSuite/ServerViewDB/backup

9.12 追加されるユーザ/グループ

SVOM をインストールすると、ユーザ: svuser, postgpls、グループ: svgroup, postgpls が作成されます。
これらユーザ/グループのユーザ ID、グループ ID、ログインシェル、ホームディレクトリなどの変更は、動作に影響を及ぼすので、一切行わないでください。

9.13 OpenSSL パッケージのアップデート

OpenSSL パッケージのアップデートを行うと以下のメッセージが表示され、SVOM が停止します。

```
Please be patient, it may be a lengthy operation ...
Shutting down sv_watchdogd: [  OK  ]
Note:
If you uninstalled openssl, then ServerViewOperationsManager cannot work.
You need to install openssl, and execute the commands described below.
If you upgraded openssl, please check whether ServerViewOperationsManager works.
If not, the links to libraries may be wrong. Please execute the following commands
...(略)
```

SVOM では、OpenSSL のライブラリにリンクを張っています。そのため、SVOM がインストールされた状態で OpenSSL パッケージのアップデートを行うと、ライブラリへのリンクが切れ、SVOM のプロセス「SVServerListService」が起動できません。この場合、以下の確認/対処を行ってください。
SVOM、SVRemoteConnector では、それぞれ以下の箇所でリンクを張っています。

- SVOM
  - /usr/lib/serverview
  - libcrypto.so -> /usr/lib/libcrypto.so.x.x.x
  - libssl.so -> /usr/lib/libssl.so.x.x.x
- 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

OpenSSL のアップデートによってリンク先(/usr/lib 配下)が変更されている場合は、リンクの張り直しを行ってください。
また、OpenSSL をアップデートした場合は、対象のライブラリをロードするために SVOM、SVRemoteConnector の再起動を行ってください。

```
# /usr/bin/sv_services restart -withSCS
```

9.14 Update Manager 使用時のサーバリストへサーバブレードの二重登録

Update Manager の機能を使用する際は同じサーバブレードを二重に登録(マネジメントブレード、および独立して表示されるサーバブレード)しないでください。

二重に登録を行っているサーバブレードに対し Update Manager でアップデートを行う場合は独立して表示されるサーバブレードで登録した方を削除してから行ってください。

9.15 Update Manager でアップデートした PSP に含まれるドライバに対し、手動で更新/削除を行った場合

PSP に含まれるドライバに対し、手動でインストール/アンインストールを行った場合、Update Manager で正常にバージョン管理できません。

PSP に含まれるドライバに対し、PrimeUp を利用してインストール/アンインストールを行う場合は「sv-update-mgr-jp.pdf」の「アップデートマネージャを使用しないアップデート可能なコンポーネントのインストール/アンインストール」を参照してください。

9.16 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、SVOM としては正常動作保障外となります。

Agents においても動作保証外であり、実施した場合、RAID 関連のステータスが取得できず、RAID Manager とのステータス連携ができません。そのため、SVOM としてもシングルシステムビューにおいて以下の事象などが生じます。

- 「外部記憶装置」の各項目、およびステータスが正しく表示されない。
- 「RAID 設定」(RAID Manager の起動)のリンクが表示されない、またはリンクが有効ではない。

9.17 ファイルシステムが XFS のシステム上で SVOM を使用する場合

ファイルシステムがXFSのシステムでは、inode番号が2の32乗を超える場合があり、32ビットのstat()など一部のシステム関数がエラーとなります。このような場合、SVOM の動作にも影響が生じ、正常に動作しない可能性があります。

以下のいずれかの対処が必要になります。

- ファイルシステムのサイズを1Tバイト未満になるようにパーティションを分割する。
- ファイルシステムに XFS を使用しない(ext3、ext4 などを使用する)。

9.18 ServerView Apache Directory Server サービスについて

ServerView Operations Manager のインストール時に「ディレクトリサーバの選択」画面において、「既存の外部ディレクトリサービスを使用する」を選択、かつ「既存のディレクトリサービスでの承認」を選択した場合、「ServerView Apache Directory Server」サービスはインストールされません。

9.19 Linux OS のパッケージアップデートについて

Linux OS では個々のパッケージのアップデートが可能です。
使用しているServerViewのサポート対象となっているOSであってもパッケージをアップデートすることにより、ServerView が正常に動作しなくなる可能性があります。
この場合、最新の ServerView を使用していただくことより動作する可能性があります。
最新版をご使用いただいても動作しない場合、アップデートしたパッケージを元の版数に戻してServerView をご使用ください。

9.20 ServerView Operations Manager V9.01.02 または V9.01.04 へログインする際の設定

ServerView Operations Manager V9.01.02 またはV9.01.04 をインストールしている場合、Internet Explorer を使用してから ServerView Operations Manager にログインするためには、Windows Server の[IE セキュリティ強化の構成]が[有効]になっている必要があります。
また、クライアント側も Windows Server を使用している場合は、クライアント側の同設定も[有効]になっている必要があります。
[IE セキュリティ強化の構成]が[無効]の場合、以下の手順で設定を変更するか、V9.02.02 以降の版数にアップグレードしてください。

[IE セキュリティ強化の構成]設定の確認方法

・Windows Server のタスクバーから[サーバーマネージャー]を起動します。

・[ローカルサーバー]をクリックし、[IE セキュリティ強化の構成]が[有効]か[無効]かをチェックします。

設定が[無効]だった場合、[有効]への設定変更方法

・上記確認画面の[IE セキュリティ強化の構成]-[無効]をクリックします。

・[Administrators グループ]と[Users グループ]を[オン(推奨)]に設定して、[OK]をクリックします。

・[サーバーマネージャー]を閉じます。

10トラブルシューティング

▸ Windows/Linux 共通

10.1 接続テストが正常とならない

- すべての項目が正常にならない場合

状況	原因	対処
PINGの通信ができていません。	LANが接続されていない、またはLANの接続経路が確立されていない場合があります。	PING が通りますか？PING を有効にしてください。PING の応答がない場合、接続テストは

	対象のサーバがファイアウォールで通信遮断されている場合があります。	実行されません。PING が通るようにLAN 環境を見直してください。

- 「SNMP」の項目が正常にならない場合

状況	原因	対処
SNMP サービスから応答がありません。	ファイアウォールなどでSNMP(ポート 161/162)通信が遮断されていませんか？	ファイアウォールの設定を確認してください。
	SNMP Service サービスは起動していますか？	SNMP Service サービスを起動してください。
	SNMP Service サービスの設定で管理サーバの IP からの書き込みが抑止されていませんか？	SNMP の設定(SNMP Service サービスのプロパティ、snmpd.conf)を確認してください。

- 「ノードタイプ」の項目が正常にならない場合

状況	原因	対処
ServerView Agents から応答がありません。	ServerView Agents がインストールされていますか？	ServerView Agents をインストールしてください。
	ServerView Agents のサービス(ServerView Server Control サービス、eecd サービス)が起動していますか？	ServerView Agents のサービスが停止している場合は起動してください。 ServerView Agents のサービスが起動している場合は、再起動してください。

- 「テストトラップ」の項目が正常にならない場合

状況	原因	対処
トラップを受けていません。	管理サーバからトラップを受け付ける設定になっていますか？	管理サーバ側の SNMP Trap サービスが起動しているか確認してください。 SNMP の設定(SNMP Service サービスのプロパティ、snmpd.conf)を確認してください。

	対象サーバのトラップ送信先はあっていますか？	対象サーバ側の SNMP の設定(SNMP Service サービスのプロパティ、snmpd.conf)で送信先を確認してください。
	設定ファイルを変更していませんか？	Linux の場合、/usr/share/snmp/snmptrapd.conf にトラップ受信設定が記述されています。 このファイルに変更を加えると、トラップが受信できなくなる場合があります。 設定を確認してください。
アラームモニタ画面では受信したトラップが確認できる。	トラップを受信し、SVOM が認識するまでに時間が掛かっている可能性があります。	対象サーバの「サーバのプロパティ」－「ネットワーク/SNMP」タブ－「タイムアウト(秒)」を5から延ばすことで回避できる場合があります。また、アラームモニタ画面でテストトラップの受信ができている場合、エラー検知などのトラップも問題なく受信できます。

10.2 サーバが管理不可能と表示される

サーバが管理不可能と表示された場合は、次の項目を確認してください。

- ネットワーク環境の確認項目
  - LAN ケーブルが正しく接続されていますか？LAN ケーブルを正しく接続してください。
  - ネットワーク機器(ルータ、HUB など)は正常に動作していますか？ネットワーク機器を確認してください。
  - 「監視対象サーバ」←→「SVOM をインストールしたサーバ」間のネットワーク機器において、SNMP プロトコルの通信ポート(udp 161 番、及び udp 162 番)が遮断されていませんか？遮断されている場合は、遮断解除設定を行ってください。

- SVOM をインストールしたサーバの確認項目
  - 監視対象サーバに対して、ping が通りますか？ping が通らない場合、ネットワーク周りの設定を確認してください。
  - 監視対象サーバの IP アドレスは正しいですか？監視対象サーバの IP アドレスを確認し、正しい IP アドレスを設定してください。
  - 監視対象サーバで設定されている SNMP Service サービスのコミュニティが、「サーバのプロパティ」－「ネットワーク/SNMP」タブ－「コミュニティ名」に設定されていますか？コミ

ュニティ名が異なる場合、コミュニティ名を合わせてください。また、同じコミュニティ名が設定されている場合でも、前後に空白が設定されている可能性もあります。不要な空白は削除してください。

- ネットワークあるいはコンピュータの負荷が高い場合、時間内に処理が終了せず、「管理不可能」アイコンが表示される場合があります。この場合は、次の手順でポーリング間隔、タイムアウト値、更新間隔を変更することで、負荷を低減し、タイムアウト値の延長を行うことができます。
  (1) 「サーバの一覧」から問題があるサーバを右クリックし、表示されたメニューから「サーバのプロパティ」→「ネットワーク/SNMP」タブの順にクリックします。
  (2) 環境に合わせて設定値を変更します。

項目	説明
ポーリング間隔	サーバをポーリングする時間の間隔です。ここで指定した間隔ごとに、システムの情報をサーバに要求します。(デフォルト 60 秒)
タイムアウト	要求に対するサーバからの応答に待機する時間です。(デフォルト 5 秒)
更新間隔	表示内容を更新する間隔です。(デフォルト 60 秒)

  - ✧ これらの項目の適切な値は、負荷の状況によって異なります。何度か設定を試してみて最適な値を決定してください。
  - ✧ タイムアウト値に大きすぎる値を設定すると、本当に管理不可能な場合の反応も遅れてしまいます。大きすぎる値(12 秒以上)は設定しないようにしてください。

- 監視対象サーバ(Windows)の確認項目
  - ファイアウォールにより、ICMP(PING)または SNMP ポート(udp 161 番)が遮断されていませんか？遮断されている場合は、遮断解除設定を行ってください。ファイアウォールの詳細については、インストールしているファイアウォールソフトウェアのマニュアルをご覧ください。
  - ServerView Agents がインストールされていますか？インストールされていない場合は、インストールしてください。
  - SVOM で、「サーバのプロパティ」に設定した SNMP コミュニティ名が、「SNMP Service」のプロパティに設定されていますか？コミュニティ名が異なる場合、コミュニティ名を合わせてください。また、同じコミュニティ名が設定されている場合でも、前後に空白が設定されている可能性もあります。不要な空白は削除してください。
  - ServerView Agents(SNMP Service サービス、ServerView Server Control サービス)が起動していますか？起動していない場合、起動してください。
  - ServerView Agents(SNMP Service サービス、ServerView Server Control サービス)が正常動作していない可能性があります。ServerView Agents を再起動してください。

再起動しても、解決しない場合は、ServerView Agents を再インストールしてください。

- SNMP を使用する他製品の影響により、管理不可能となっている可能性があります。他製品の SNMP を無効化してください。

- 監視対象サーバ(Linux)の確認項目
  - ファイアウォールにより、ICMP(PING)または SNMP ポート(udp 161 番)が遮断されていませんか？遮断されている場合は、遮断解除設定を行ってください。ファイアウォールの詳細については、インストールしているファイアウォールソフトウェアのマニュアルをご覧ください。なお、OS 標準のファイアウォール(パケットフィルタ)としては、iptables、tcpwrapper(/etc/hosts.deny, /etc/hosts.allow)などがあります。
  - ServerView Agents がインストールされていますか？インストールされていない場合は、インストールしてください。
  - SVOM で、「サーバのプロパティ」に設定した SNMP コミュニティ名が、snmpd.conf に設定されていますか？コミュニティ名が異なる場合、コミュニティ名を合わせてください。また、同じコミュニティ名が設定されている場合でも、前後に空白が設定されている可能性もあります。不要な空白は削除してください。
  - ServerView Agents(snmpd, eecd, srvmagt, srvmagt_scs)が起動していますか？起動していない場合、起動してください。
  - ServerView Agents(snmpd, eecd, srvmagt, srvmagt_scs)が正常動作していない可能性があります。ServerView Agents を再起動してください。再起動しても、解決しない場合は、ServerView Agents を再インストールしてください。
  - SNMP を使用する他製品の影響により、管理不可能となっている可能性があります。他製品の SNMP を無効化してください。
  - snmpd.confの中に「com2sec svSec localhost <SNMPコミュニティ名>」行がない可能性があります。この行がない場合は追加してください。

10.3 SVOM 起動時にエラーが表示される（HTTP 500、HTTP 404 や Internet Explore ではこのページは表示できません など）

- SVOM が使用するネットワークポートが他のプログラムによって占有されていないか確認してください。
  SVOM が使用するネットワークポートは、マニュアル「ServerView Operations Manager V9 Installing ServerView Operations Manager Software under Windows」(sv-install-windows-jp.pdf)、もしくは「ServerView Operations Manager V9 Installing ServerView Operations Manager Software under Linux」(sv-install-linux-jp.pdf)を参照してください。
- SVOM をインストールしたサーバの名前解決ができることを確認してください。
  サーバ側 (SVOM をインストールするサーバ)と、クライアント側(ウェブブラウザで SVOM にアクセスする端末)の両方で、名前解決ができるように設定されている必要があります。

以下のコマンドを実行して、正常に名前解決が行われていることを確認します。

- Windows の場合

  tracert <サーバのコンピュータ名>.<DNS サフィックス >

- Linux の場合

  traceroute < サーバのコンピュータ名>.<DNS サフィックス >

- インストール時にファイルが正しくコピーされなかった可能性があります。
  一度アンインストールして、インストール先のフォルダ内のファイル・フォルダを全て削除した後、再度インストールを行ってください。
- ブラウザのアップデートの適用を行ってください。
  ブラウザが Internet Explorer 11 で、かつ、ブラウザ上、およびシステムのイベントログにそれぞれ以下のメッセージが確認できる場合、Windows Update などを使用し、ブラウザのアップデートの適用してください。
  - ブラウザ上に表示されるメッセージ

    > このページは表示できません
    > Web アドレス https://< システム名>.< ドメイン名>:3170 が正しいか確かめてください。

    > このページは表示できません
    > [詳細設定] で SSL 3.0、TLS 1.0、TLS 1.1、TLS 1.2 を有効にして、
    > https://< システム名>.< ドメイン名>:3170 にもう一度接続してください。

  - システムのイベントログに記録されるメッセージ

    > ソース:Schannel
    > ID:36887
    > リモート エンドポイントから致命的な警告を受け取りました。
    > TLS プロトコルで定義されているこの致命的な警告のコードは 40 です。

10.4 SVOM の画面読み込みに時間が掛かる

Web ブラウザに不要なデータが格納されている可能性があります。以下の一時ファイルを削除してください。

- Web ブラウザのインターネット一時ファイル
  - Internet Explorer の場合:
    [ツール]－[インターネットオプション]を起動し、「全般」タブの「閲覧の履歴」枠で「削除」を開き、インターネット一時ファイルの削除を行ってください。
  - FireFox の場合:
    [ツール]－[オプション]を起動し、「詳細」を選択、「ネットワーク」タブの「キャッシュされた Web ページ」項目にある「今すぐ消去」を実行してください。

10.5 SVOM から監視対象サーバにログインできない

SVOM から監視対象のサーバへ設定を行う際、Agents 側サーバ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）
- 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。

10.6 [メンテナンス]－[システムイベントログ]の内容が文字化けする

監視サーバと監視対象サーバが異なるプラットフォームの場合（Linux にインストールされた SVOM から Windows サーバを監視、または、Windows にインストールされた SVOM から Linux サーバを監視する場合）、かつ、監視対象サーバにおいて、システムイベントログに「原因」「対処方法」などの詳細情報が保持されている場合、シングルシステムビューの下記画面にて文字化けが生じます。
[シングルシステムビュー]－[メンテナンス]－[システムイベントログ]画面の「原因」、「対処方法」
その場合、iRMC の WebUI の[イベントログ]－[SEL の表示]画面にて確認してください。

10.7 「スレッシュホールドマネージャの画面右上に「設定が不整合です」と表示される

「設定が不整合です」の表示は、Agents と SVOM 間で監視テーブルの差異（監視項目やサーバのタイプ）がある場合に表示されます。
仮想 OS のホストサーバを通常のサーバとしてサーバリストへ登録すると、Agents と SVOM にサーバタ

イプの差異が生じるため「設定が不整合です」が表示されます。
監視テーブルの監視対象項目で、「平均値」の値が「N/A」ではなく正しく表示されていれば監視は行われています。

10.8 SVOM の画面が正常に動作しない（画面がすべて閉じる、フリーズする）

SVOM の画面がすべて閉じる、フリーズするなど正常に動作しないなどの事象が発生した場合は、SVOM の画面を一度閉じて開き直してください。この時、デスクトップ上に「hs_err_pid*****.log」という名前のファイルが作成される場合がありますが、ファイルは削除して問題ありません。
これらの事象は SVOM が使用している JRE(Java Runtime Environment)の障害によるものです。
なお、この事象による SVOM の内部の動作(SNMP トラップの受信処理やメールの転送処理など)への影響はありません。

10.9 シングルシステムビューが英語表示される

シングルシステムビューの表示内容の処理とブラウザの表示のタイミングによって内容が英語で表示される場合があります。表示のみの問題であり、監視には問題ありません。
事象が発生した場合、ブラウザを開き直してください。

10.10 トラップの受信に時間がかかる

トラップの処理は 1 件/秒です。多数のトラップを同時に受信した場合は順次処理されるため、テストトラップ等の意図したトラップや、事象発生時のトラップの受信処理が遅れる場合があります。
トラップ受信の対象機器の構成を見直し、トラップ受信量の軽減を行ってください。

10.11 Single System View が開かない

- Web ブラウザに不要なデータが格納されている可能性があります。以下の一時ファイルを削除してください。
  - Web ブラウザのインターネット一時ファイル

    Internet Explorer の場合

    [ツール]－[インターネットオプション]を起動し、「全般」タブの「閲覧の履歴」枠で「削除」を開き、インターネット一時ファイルの削除を行ってください。

    FireFox の場合

    [ツール]－[オプション]を起動し、「詳細」を選択、「ネットワーク」タブの「キャッシュされた Web ページ」項目にある「今すぐ消去」を実行してください。

10.12 識別灯が点けられない

- Agent の SNMP セキュリティ設定で ServerView SET オペレーションを有効にしていることを確認してください。
  なお、サーバ上での不正な SNMP SET 操作を防止するため、設定とサービスツールに対するパスワード認証の設定をお勧めします。

- ServerView Agents for Windows の場合
  (1) 「Agent Configuration」を起動します。
  スタート－[すべてのプログラム] - [Fujitsu] - [ServerViewSuite] - [Agents] - [AgentConfiguration]から起動します。
  (2) 「セキュリティ設定」タブを開きます。
  (3) 「ServerView SET オペレーションをこのサーバ上で有効にする」にチェックを入れます。
  (4) 「適用」ボタンをクリックします。
- ServerView Agents for Linux の場合
  ファイル「/etc/srvmagt/config」の「AgentPermission」の値を「3」に設定します。その後、ServerView Agents for Linux を再起動します。
  日本語 OS 環境の場合のデフォルトは、値が「3」に設定されています。

- ファイアウォールの設定を確認してください。
  ファイアウォールにより、ICMP(PING)またはSNMPポート(udp 161 番)が遮断されていませんか？遮断されている場合は、遮断解除設定を行ってください。ファイアウォールの詳細については、インストールしているファイアウォールソフトウェアのマニュアルをご覧ください。
- 識別灯が搭載されていない機種では識別灯ボタンは表示されません。
  TX1310M1、TX100S3 など、識別灯の搭載されていない機種では、識別灯の項目は表示されません。

10.13 ウォッチドッグの設定・解除ができない

- Agent の SNMP セキュリティ設定で ServerView SET オペレーションを有効にしていることを確認してください。
  なお、サーバ上での不正な SNMP SET 操作を防止するため、設定とサービスツールに対するパスワード認証の設定をお勧めします。
  - ServerView Agents for Windows の場合
    (1) 「Agent Configuration」を起動します。
    スタート－[すべてのプログラム] - [Fujitsu] - [ServerViewSuite] - [Agents] - [AgentConfiguration]から起動します。
    (2) 「セキュリティ設定」タブを開きます。
    (3) 「ServerView SET オペレーションをこのサーバ上で有効にする」にチェックを入れます。
    (4) 「適用」ボタンをクリックします。
  - ServerView Agents for Linux の場合
    ファイル「/etc/srvmagt/config」の「AgentPermission」の値を「3」に設定します。その後、ServerView Agents for Linux を再起動します。
    日本語 OS 環境の場合のデフォルトは、値が「3」に設定されています。
- ファイアウォールの設定を確認してください。

ファイアウォールにより、ICMP(PING)またはSNMPポート(udp 161番)が遮断されていませんか？遮断されている場合は、遮断解除設定を行ってください。ファイアウォールの詳細については、インストールしているファイアウォールソフトウェアのマニュアルをご覧ください。

- ブートウォッチドック機能が搭載されていない場合。
  TX1310M1、TX100S3 など、ブートウォッチドッグが搭載されていない機種では、ブートウォッチドック設定の項目が表示されません。
- ESXi サーバに CIM Provider V7.01 以降をインストールしている環境の場合。
  ソフトウェアウォッチドッグをシステム監視にのみ使用することができますが、以下の条件を満たす設定が必要です。
  異常時動作： 継続稼動
  タイムアウト時間： 4 分以上

10.14 PrimeCollect のリモート取得ができない

- Remote Connector サービスが停止している可能性があります。
  リモートからの PrimeCollect 取得には、監視対象サーバで Remote Connector サービスが正常に動作している必要があります。診断情報収集(PrimeCollect)が選択できない場合、ServerViewRemote Connector サービスが正常に動作しているか確認してください。
- ファイアウォールの設定を確認してください。
  ファイアウォールにより、3170 番と 3172 番が遮断されていませんか？遮断されている場合は、遮断解除設定を行ってください。ファイアウォールの詳細については、インストールしているファイアウォールソフトウェアのマニュアルをご覧ください。
- 監視対象サーバから SVOM に対して名前解決が正しく行なわれていない可能性があります。
  監視対象サーバから SVOM に対して名前解決が正しくできるように設定されている必要があります。
  以下のコマンドを実行して、正常に名前解決が行われていることを確認してください。
  - Windows の場合
    tracert <サーバのコンピュータ名>.<DNS サフィックス>
  - Linux の場合
    traceroute <サーバのコンピュータ名>.<DNS サフィックス>
- 証明書が正しくインストールされていない可能性があります。
  監視対象サーバのイベントログ/システムログに以下のメッセージが表示される場合があります。これは、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。
  - 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 アドレスがはいります。

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。

- 監視対象サーバが VMware の場合
  監視対象が VMwareESXi の場合、リモートから PrimeCollect を取得することはできません。
- 監視対象が iRMC の場合
  監視対象サーバに ServerView エージェントまたは ServerView Agentless Service が必要となります。詳しくは、ServerView PrimeCollect 取扱説明書「4 eLCM PrimeCollect」を参照してください。

10.15 System Event Log が表示されない

事象が発生した場合、一度ブラウザを閉じて再度開き直してください。

10.16 接続状態変更トラップを対象としたアラームルールが動作しない

以下の条件を満たす場合、接続状態変更トラップを対象としたアラームルールの
アクションが動作しないことがあります。その場合、アラームルール作成時に "サーバの割り当て画面" で「すべてのサーバ」を選択してください。

- SVOM を仮想(ゲスト)システムにインストールしている。
- "サーバの割り当て" に、仮想化ソフトウェア配下の仮想(ゲスト)システムの SVOM を設定している。
- 対象となるアラームが接続状態変更トラップ(アラームの名前:Server changed state)である。

10.17 サーバブラウザにて監視対象のサーバが検索結果に表示されない

サーバブラウザでサブネット内を検索した際に意図せず検索停止が表示されることがあります。
その場合は再度検索を実施してください。

10.18 接続テストの結果画面が表示されない

SVOM V9.10.02 以降で接続テストを行うと結果画面に何も表示されない場合があります。
以下のフォルダ配下に"enforceSNMP4J"という名前の空ファイルを作成してください。

> Windows の場合

<インストールフォルダ>¥Fujitsu¥ServerView Suite¥svom¥bin¥ServerView¥SnmpView¥

> Linux の場合

/opt/fujitsu/ServerViewSuite/svom/bin/ServerView/SnmpView/

Windows

10.19 SQL Server が出力するイベントログメッセージ

SQL Server(SQLSERVERVIEW)サービス起動時に、以下のメッセージがイベントログに出力される場合がありますが、SVOM の動作に影響はありませんので無視してください。

レベル　　:エラー
イベント ID :17053
ソース　　:MSSQL$SQLSERVERVIEW
DoDevIoCtlOut() DeviceIoControl() : オペレーティング システム エラー 234(データがさらにあります。)が発生しました。

10.20 ROR/VIOM 共存環境で SVOM の画面が正常に表示されない

Windows 環境において、SVOM と ServerView Resource Orchestrator(ROR) / ServerView Virtual-IO Manager(VIOM)が共存する環境の場合、SVOM 起動時またはログイン時に以下のメッセージが表示される場合があります。

LDAP エラー:
ユーザ検索ベースに関する問題があったため、ディレクトリサービスとの通信が失敗しました。
could not connect to server

この不具合を暫定回避するためには、「ServerView Apache Directory Server」サービスを再起動してください。
SVOM V8.50 以降の場合は、予防措置としてタスクスケジューラに登録されている SVApacheDSRestartTask を有効にしてください。これを有効にすることで、毎週日曜 0 時 0 分に ApacheDS が再起動します。
また、ご使用の環境に合わせて ApacheDS を再起動する時間を変更できます。タスクスケジューラに登録されている SVApacheDSRestartTask を実行する時間を変更してください。

10.21 受信したメールの日本語部分が文字化けする

SVOM V7.20.08 以降においてアラーム設定等で送信されたメールの日本語部分が
文字化けする場合、以下のファイルを作成してください。

<install folder>¥ServerView¥ServerView Services¥scripts¥ServerView¥SnmpTrap
“mail_enforce932” という名前の空ファイルを作成

Linux

10.22 SnmpTrapListen プロセスが増加する

通常、SnmpTrapListen プロセスはトラップ受信処理が完了すると終了します。
トラップ受信処理時にポート 162 の内部通信が出来ない状況では SnmpTrapListen プロセスが終了されずに残ってしまいます。
SnmpTrapListen プロセスが複数残っている場合は、ポート 162 の内部通信が正常に行えるように設定を行い、SVOM のサービスを再起動してください。

VMware

10.23 ブレードサーバ上の VMware ESXi の IP アドレスが 0.0.0.0 と表示され、監視できない

サーバリストにて、ブレードサーバ上の VMware ESXi の IP アドレスが 0.0.0.0 と表示されて監視ができない問題が発生する場合があります。本問題を未然に防止するため、以下の確認を行い、その後に VMware ESXi を登録してください。登録後に問題が発生した場合も、同様の確認を行ってください。

1. ネットワークインターフェイス「vmkX」に仮想 MAC アドレスが割り当てられていないか

ESXi のネットワークインターフェイス「vmkX」に仮想 MAC アドレスが割り当てられている状態で発生します。仮想 MAC アドレス は VMware 社に固有の接頭値「00:50:56:xx:xx:xx」であるか否かで確認できます。

※vmkX の X には、現在使用しているインターフェイスの番号が入ります。

【vmkX に割り当てられている MAC アドレスの確認方法】

(1) vSphere Client で vCenter Server(もしくは ESXi)にログインします。
(2) インベントリから、対象の VMware ESXi を選択します。
(3) 右ペインの構成タブをクリックします。
(4) ハードウェアの「ネットワーク」をクリックして仮想スイッチの一覧から、SVOM で登録している VMkernel Port を持つ仮想スイッチのプロパティをクリックします。
(5) 仮想スイッチのプロパティの中で、ポートの一覧から SVOM で指定している VMkernel Port を選択します。
(6) 右の画面の「NIC 設定」内の MAC アドレスを確認します。

【対処方法】

- ESXi Shell から行う場合:
  (1) 次のコマンドを実行します。
  ```
  # esxcfg-advcfg -s 1 /Net/FollowHardwareMac
  ```
  (2) ESXi サーバを再起動します。
  (3) ESXi サーバ再起動後、次のコマンドを実行します。
  ```
  # esxcfg-advcfg -g /Net/FollowHardwareMac
  ```

Value of FollowHardwareMac is 1

設定が有効になっていることを確認します。

(4) SVOM 上でブレードシャーシの再登録を行います。

- 「Restore Network Setting」を実行する場合:
  (1) VMware ESXi のコンソール画面で「Restore Network Setting」を実行します。
  (2) SVOM 上でブレードシャーシの再登録を行います。
  注意) 上記を実施した場合、ESXi のネットワーク設定で、仮想スイッチ、ポートグループ、vmknics の設定が初期化されます。実行後は、ネットワーク設定の内容を確認してください。

また、以下の手順で通常の MAC アドレスが割り振られた事例も存在します。

(1) VMware ESXi のコンソール画面で <F2> キーを押し、Customize System メニューを起動します。
プロンプトが表示されたら、root ユーザでログインします。

(2) [Configure Management Network] -> [Network Adapters]を選択します。

(3) vmkX (Management Network) で使用する物理 NIC(vmnic)を 1 つ選択し、Enter キーを押下します。

(4) Esc キーを押下し、以下のメッセージが表示されたら「Y」を選択して設定を反映します。

Configure Management Network: Confirm
You have made changes to the host's management network.
Applying these changes may result in a brief network outage,
disconnect remote management software and affect running virtual
machines. In case IPv6 has been enabled or disabled this will
restart your host.
Apply changes and restart management network?

(5) [Restart Management Network] を選択します。以下のメッセージが表示されたら、Y を選択します。

Restart Management Network: Confirm
Restarting the management network will result in a brief network
outage. It may disconnect remote management software and affect
running virtual machines.
Restart management network now?

2. VMware ESXi による MAC アドレス情報を更新しない不具合が生じていないか

ESXi には、NIC カードなどハード交換を行った後も MAC アドレス情報を更新しない不具合があります。OS が保持している MAC アドレスとマネジメントブレードが認識しているサーバブレードの MAC アドレスが一致しているかを確認してください。

詳細は、VMware 社 の以下の Knowledge Base を確認してください。

Knowledge Base：1031111

vmk0 management network MAC address is not updated when NIC card is replaced or vmkernel has duplicate MAC address (1031111)

10.24 VMware vSphere ESXi 5/6 サーバの監視が出来ない場合

VMware vSphere ESXi 5/6 サーバの監視を ServerView ESXi CIM Provider を使用して行う場合、CIMProvider は VMware vSphere ESXi 5/6 の sfcbd サービス機能を使用しています。

このため sfcbd サービスが正常に動作していないと VMware vSphere ESXi 5/6 サーバの監視が正常に行えません。監視が正常に行えていない場合、sfcbd サービスが正常に動作しているか確認してください。

また、sfcbd サービスを再起動することにより、正常に監視が行えるようになる場合があります。

【sfcbd サービスの再起動方法】

- ESXi Shell から行う場合
  (1) VMware vSphere ESXi 5/6 サーバの ESXi Shell にログオンします。
  (2) 次のコマンドを実行し、sfcbd サービスを停止します。
  # /etc/init.d/sfcbd-watchdog stop
  (3) 次のコマンドを実行し、sfcbd サービスの状態を確認します。
  # /etc/init.d/sfcbd-watchdog status
  「sfcbd is not running」と出力されれば停止しています。
  (4) 次のコマンドを実行し、sfcbd サービスを起動します。
  # /etc/init.d/sfcbd-watchdog start
  (5) 次のコマンドを実行し、sfcbd サービスの状態を確認します。
  # /etc/init.d/sfcbd-watchdog status
  「sfcbd is running」と出力されれば正常に起動しています。
- vSphere Client から行う場合
  (1) vSphere Client から vCenter Server または ESXi ホストにログインします。
  (2) 左側に表示されるインベントリ パネルから対象の ESXi ホストを選択し、「構成」タブ - 「ソフトウェア」 - 「セキュリティプロファイル」を選択します。
  (3) サービスの「プロパティ」をクリックし、サービス プロパティを開きます。
  (4) 「CIM サーバ」を選択し、「オプション」ボタンをクリックします。
  (5) サービス コマンドで「停止」をクリックします。
  (6) サービス コマンドで「開始」をクリックします。
  ※「再起動」コマンドの場合、タイムアウトして失敗する場合があります。このため、「開始」をクリックしてください。
  (7) vSphere vSphere ESXi 5/6 サーバの ESXi Shell にログオンします。
  (8) 次のコマンドを実行し、sfcbd サービスの状態を確認します

/etc/init.d/sfcbd-watchdog status

「sfcbd is running」と出力されれば正常に起動しています。

以上