

ESMPRO/ServerAgentService Ver.2 ユーザーズガイド(Linux編)

1章 製品概要

2章 監視機能

3章 通報機能

4章 OpenIPMIと追加機能

5章 注意事項

6章 FAQ

目 次




目 次	2
表 記	4
本文中の記号	4
外来語のカタカナ表記	4
商 標	5
本書に関する注意と補足	6
最新版	6
1 章 製品概要	7
1. 製品概要	8
2. 機能概要	10
2.1 CIM プロバイダ	10
2.2 監視サービス	11
2 章 監視機能	12
1. 監視設定	13
2. SNMP Trap	14
3. Syslog 監視	15
3 章 通報機能	17
1. 通報設定	18
2. 基本設定	20
2.1 通報手段の設定	21
2.1.1 マネージャ通報(SNMP)の基本設定	21
2.1.2 マネージャ通報(TCP_IP In-Band)の基本設定	22
2.1.3 マネージャ通報(TCP_IP Out-of-Band)の基本設定	23
2.2 その他の設定	24
3. 通報先リストの設定	25
3.1 通報先 ID の設定変更	26
3.1.1 通報手段がマネージャ通報(TCP_IP In-Band)の宛先設定	27
3.1.2 通報手段がマネージャ通報(TCP_IP Out-of-Band)の宛先設定	28
3.1.3 スケジュール設定	29
3.2 通報先 ID の追加	30
4. Syslog イベントの設定	31
4.1 通報先の指定(Syslog イベント)	33
4.1.1 監視イベントごとに通報先を指定する方法	33
4.1.2 ソースごとに通報先を一括指定する方法	35
4.2 Syslog イベントのソースの追加	37
4.3 Syslog イベントの追加	40
4.4 Syslog イベントのソースの削除	41

4.5 Syslog イベントの削除	42
4.6 Syslog イベントのテスト	43
4 章 OpenIPMI と追加機能	47
1. OpenIPMI を利用した OS ストール監視	48
1.1 Red Hat Enterprise Linux 6~7	49
2. コンフィグレーションツール	53
2.1 esmamset コマンド	54
2.2 esmsysrep コマンド	58
3. ツールについて	63
3.1 障害情報採取ツール(collectsa.sh)	63
3.2 必須パッケージチェックツール(check_packages.sh)	64
5 章 注意事項	66
1. ESMPRO/ServerAgentService	67
2. Red Hat Enterprise Linux	75
6 章 FAQ	77

表 記

本文中の記号

本書では 3 種類の記号を使用しています。これらの記号は、次のような意味をもちます。

	ソフトウェアの操作などにおいて、守らなければならないことについて示しています。
	ソフトウェアの操作などにおいて、確認しておかなければならないことについて示しています。
	知っておくと役に立つ情報、便利なことについて示しています。

外来語のカタカナ表記

本書では外来語の長音表記に関して、国語審議会の報告を基に告示された内閣告示に原則準拠しています。ただし、OS やアプリケーションソフトウェアなどの記述では準拠していないことがあります。誤記ではありません。

商 標

ESMPRO は日本電気株式会社の登録商標です。

Linux は、Linus Torvalds 氏の日本およびその他の国における商標または登録商標です。

Red Hat、Red Hat Enterprise Linux は、米国 Red Hat, Inc.の米国およびその他の国における商標または登録商標です。

その他、記載の会社名および商品名は各社の商標または登録商標です。

なお、本文には登録商標や商標に(TM)、(R)マークは記載していません。

本書に関する注意と補足

1. 本書の一部または全部を無断転載することを禁じます。
2. 本書に関しては将来予告なしに変更することがあります。
3. 弊社の許可なく複製、改変することを禁じます。
4. 本書について誤記、記載漏れなどお気づきの点があった場合、お買い求めの販売店までご連絡ください。
5. 運用した結果の影響については、4 項に関わらず弊社は一切責任を負いません。
6. 本書の説明で用いられているサンプル値は、すべて架空のものです。

この説明書は、必要なときすぐに参照できるよう、お手元に置いてください。

最新版

本書は作成日時点の情報をもとに作られており、画面イメージ、メッセージ、または手順などが実際のものと異なることがあります。変更されているときは適宜読み替えてください。

また、ユーザズガイドをはじめとする本製品に関する資料は、次の Web サイトから最新版をダウンロードできます。

<https://www.support.nec.co.jp/View.aspx?id=3170102037>

ESMPRO/ServerAgentService Ver. 2

1

製品概要

ESMPRO/ServerAgentService の製品概要について説明します。

1. 製品概要

ESMPRO/ServerManager、ESMPRO/ServerAgentService は、サーバーシステムの安定稼動と、効率的なサーバーシステム運用を目的としたサーバー管理ソフトウェアです。サーバーリソースの構成情報・稼動状況を管理し、サーバー障害を検出してシステム管理者へ通報することにより、サーバー障害の防止、障害に対する迅速な対処を可能にします。

サーバー管理の重要性

分散化システムにおいては、サーバーの安定稼動は必要不可欠です。また、安定稼動を保証するためには、サーバー管理の負担を軽減する必要があります。

サーバーの安定稼動

お客様の分散化システムの中核を担うサーバーの停止は、即、お客様の営業機会、利益の損失につながります。そのため、サーバーはつねに万全の状態稼動している必要があります。万が一サーバーで障害が発生した場合は、できるだけ早く障害の発生を知り、原因の究明、対処する必要があります。障害の発生から復旧までの時間が短ければ短いほど、利益(コスト)の損失を最小限にとどめることができます。

サーバー管理の負担軽減

分散化システムにおけるサーバー管理は多くの労力を必要とします。とくに大規模な分散化システム、遠隔地にあるサーバーとなればなおさらです。サーバー管理の負担を軽減することは、すなわちコストダウン(お客様の利益)につながります。

サーバー管理

では、サーバーをご利用のお客様がサーバー管理を行うには、どうすればよいのでしょうか？

このニーズに応えるため、サーバー管理ソフトウェア

「ESMPRO/ServerManager、ESMPRO/ServerAgentService、ServerAgent」

を提供しています。

ESMPRO/ServerManager、ESMPRO/ServerAgentService、ESMPRO/ServerAgent をご利用いただくことにより、お客様のサーバーを管理できるようになります。

VMware ESX では、コンソールオペレーティングシステムが、仮想カーネル(VMkernel)にあるため、Linux 版 ESMPRO/ServerAgent と同等の機能を提供しています。ただし、標準で添付している ESMPRO/ServerAgentService では、VMware ESX Server や仮想マシン(ゲスト OS)を監視できません。

VMware ESX のホスト OS(VMkernel)を監視するためのサーバー管理ソフトウェア製品として、

「ESMPRO/ServerAgent for VMware」

仮想マシン(ゲスト OS)を監視するためのサーバー管理ソフトウェア製品として、

「ESMPRO/ServerAgent for Guest OS (Windows/Linux)」

他社製サーバーを監視するためのサーバー管理ソフトウェア製品として、

「他社機版 ESMPRO/ServerAgent (Windows/Linux)」

をご用意しておりますので、詳細は次の Web サイトを参照してください。

<http://jpn.nec.com/esmsm/>

ESMPRO/ServerManager、ESMPRO/ServerAgentService とは？

ESMPRO/ServerManager、ESMPRO/ServerAgentService は、ネットワーク上のサーバーを管理・監視するサーバー管理ソフトウェアです。本製品を導入することにより、サーバーの構成情報・性能情報・障害情報をリアルタイムに取得・管理・監視できるほか、アラート通報機能により障害の発生を即座に知ることができるようになります。

ESMPRO/ServerManager、ESMPRO/ServerAgentService の利用効果

ESMPRO/ServerManager、ESMPRO/ServerAgentService は、多様化・複雑化するシステム環境におけるさまざまなニーズに対して十分な効果を発揮します。

サーバー障害を検出

ESMPRO/ServerManager、ESMPRO/ServerAgentService は、サーバーのさまざまな障害情報を収集し、異常を判定します。サーバーで異常を検出したとき、ESMPRO/ServerManager でアラート受信します。

サーバー障害を防止

ESMPRO/ServerManager、ESMPRO/ServerAgentService は、障害の予防対策として、事前に障害の発生を予測する予防保守機能をサポートしています。筐体内温度上昇や、ファイルシステムの空き容量、ハードディスクドライブ劣化などを事前に検出できます。

サーバー稼動状況を管理

ESMPRO/ServerManager、ESMPRO/ServerAgentService は、サーバーの詳細なハードウェア構成情報、性能情報を取得できます。取得した情報は ESMPRO/ServerManager をとおして参照できます。

分散したサーバーを一括管理

ESMPRO/ServerManager は、ネットワーク上に分散したサーバーを効率よく管理できる GUI インターフェースを提供します。

詳細は、次の Web サイトからダウンロードできる ESMPRO サーバ管理ガイドを参照してください。

<http://jpn.nec.com/esmsm/>

ダウンロード > ドキュメント

2. 機能概要

ESMPRO/ServerAgentService は、Common Information Model(CIM)プロバイダと監視サービスの機能を提供しています。ESMPRO/ServerAgentService には「サービスモード」と「非サービスモード」が存在します。サービスモードでは、CIM プロバイダと監視サービスの機能を提供します。非サービスモードでは、CIM プロバイダの機能を提供します。



ESMPRO/ServerAgentService がどちらのモードでインストールされているか確認するには、次のコマンドを実行してください。

```
# rpm -qa | grep Esmpro-Cmnsrv
```

Esmpro-Cmnsrv パッケージが表示されたときは、サービスモードです。

Esmpro-Cmnsrv-"バージョン情報"



ESMPRO/ServerAgentService を使用する前に EXPRESSBUILDER または Starter Pack、Web サイトのダウンロード物件に含まれる ESMPRO/ServerAgentService インストレーションガイド(Linux 編)の2章(3. インストールを終えた後に)を実施してください。

2.1 CIM プロバイダ

・ Esmpro-Provider パッケージ

機能名	クラス名
説明	
ESMPRO 情報プロバイダ	ESM_GeneralInformation ESM_VideoController ESM_Network ESM_Alive
Linux 標準プロバイダで不足している情報を提供します。	
CPU 負荷情報プロバイダ	ESM_Processor
1 分間の平均値の CPU 負荷情報を提供します。	
物理メモリ情報プロバイダ	ESM_PhysicalMemory
物理メモリ情報を提供します。	
仮想メモリ情報プロバイダ	ESM_VirtualMemory
仮想メモリ情報を提供します。	
ページファイル情報プロバイダ	ESM_PageFile
ページファイル情報を提供します。	

・ Esmpro-strgfs-Provider パッケージ

機能名	クラス名
説明	
ストレージ情報プロバイダ	ESM_StorageThread
ストレージ情報を提供します。	
ファイルシステム情報プロバイダ	ESM_FileSystemThread
ファイルシステム情報を提供します。	

2.2 監視サービス

・ Esmpro-Cmnsrv パッケージ

機能名	プロセス名	アラートのソース名
説明		
基幹サービス	ESMntserver	なし
ESMPRO/ServerAgentService のプロセス間の通信を制御します。		
監視スレッド起動・停止サービス	ESMcmn	なし
監視スレッドを起動または停止します。 監視スレッドは状態の変化に合わせ syslog への記録と CIM-Indication で通報します。		
Syslog 監視・通報サービス	ESMamvmain	なし
syslog に記録された文字列を監視し、syslog への記録と通報手段に合わせて通報します。 TCP/IP 通報する機能を提供します。		
SNMP 通報サービス	ESMntagent	なし
SNMP 通報する機能を提供します。		

- 監視スレッド

機能名	クラス名	アラートのソース名
説明		
CPU 負荷監視スレッド	ESM_Processor	ESMCPU PERF
CPU 負荷を監視します。		
物理メモリ使用量監視スレッド	ESM_PhysicalMemory	ESMMEMORYUSAGE
物理メモリ使用量を監視します。		
仮想メモリ使用量監視スレッド	ESM_VirtualMemory	ESMMEMORYUSAGE
仮想メモリ使用量を監視します。		
ページファイル使用量監視スレッド	ESM_PageFile	ESMMEMORYUSAGE
ページファイル使用量を監視します。		
ストレージ監視スレッド	ESM_StorageThread	ESM STORAGE SERVICE
ストレージを監視します。		
ファイルシステム監視スレッド	ESM_FileSystemThread	ESMFSSERVICE
ファイルシステムを監視します。		
CPU・メモリ縮退監視スレッド	なし	ESMCOMMONSERVICE
ESMcmn 起動時に CPU・メモリ縮退を監視します。		

・ Esmpro-Selsrv パッケージ

機能名	プロセス名	アラートのソース名
説明		
SEL 監視サービス	ESMsmsrv	ESMCOMMONSERVICE
ハードウェアのログを監視し、syslog への記録と通報手段に合わせて通報します。		

・ Esmpro-Expsrv パッケージ

機能名	プロセス名	アラートのソース名
説明		
エクスプレス通報サービス	なし	なし
通報サービス(プロセス名: ESMamvmain)にエクスプレス通報サービスの通報手段を追加します。		

監視機能

ESMPRO/ServerAgentService の監視機能について説明します。

1. 監視設定
2. SNMP Trap
3. Syslog 監視

1. 監視設定

本章では監視機能を説明します。各監視機能の設定は、コントロールパネル(ESMagntconf)で変更します。



非サービスモードでは、監視サービスはインストールされないため、設定はできません。



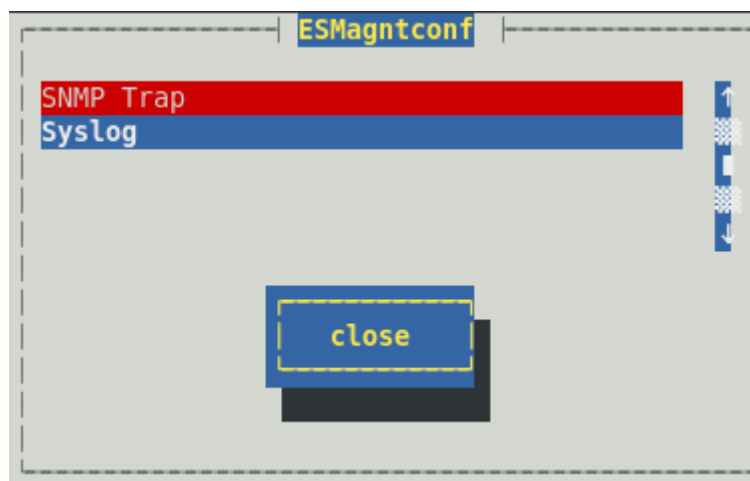
コントロールパネルを複数のコンソールから起動しないでください。後から実行したコンソールからは起動できず、『レジストリの読み込みに失敗しました。』と表示します。



ESMPRO/ServerAgentService を使用する前に EXPRESSBUILDER または Starter Pack、Web サイトのダウンロード物件に含まれる ESM PRO/ServerAgentService インストールガイド(Linux 編)の 2 章(3. インストールを終えた後に)を実施してください。

コントロールパネル(ESMagntconf)の起動方法は以下のとおりです。

1. root 権限のあるユーザーでログインします。
2. コントロールパネルが格納されているディレクトリに移動します。
cd /opt/nec/esmpro_sa/bin
3. コントロールパネルを起動します。
./ESMagntconf



コントロールパネル(ESMagntconf)のメイン画面

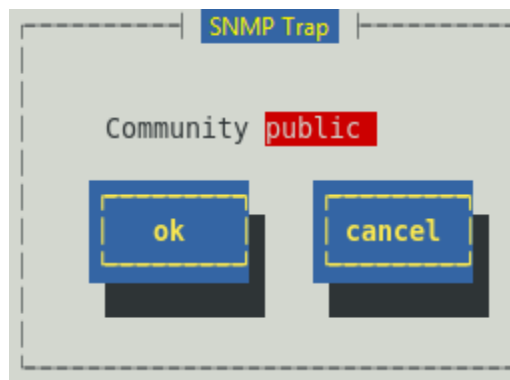
2. SNMP Trap

機 能

Syslog 監視機能で SNMP トラップを送信するときに使用する SNMP コミュニティー名を設定できます。

設 定

コントロールパネル(ESMagntconf)の「SNMP Trap」を選択して表示される[SNMP Trap]画面にて、設定ができます。



Community

Syslog 監視機能で SNMP トラップを送信するときに使用する SNMP コミュニティー名を選択します。リストに表示されるコミュニティ名は、SNMP 設定ファイル(snmpd.conf)に登録されているコミュニティ名です。使用可能な文字は半角英数字、最大文字数は 33 バイトまでです。

[ok]ボタン

設定した情報を登録し、この画面を閉じます。

[cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。

3. Syslog 監視

機 能

Syslog 監視機能は、Syslog イベントで設定されたキーワードが監視対象のファイルに記録されると、ESMPRO/ServerManager へ通報(アラート通報)します。Syslog イベントは、ESMPRO/ServerAgentService インストール時にあらかじめ登録している Syslog イベント以外に、システム環境に応じた新たなソース、イベントを追加/削除できます。Syslog イベントの追加/削除方法は、本書の 3 章(4. Syslog イベントの設定)を参照してください。

既定監視対象

監視対象となる syslog は、`/var/log/messages` となり変更はできません。

また、監視対象となる syslog ローテート後のファイル名は、`/etc/logrotate.conf` に `"dateext"` が

定義されていない : `/var/log/messages.n` [`n=1, 2, 3, ...`]

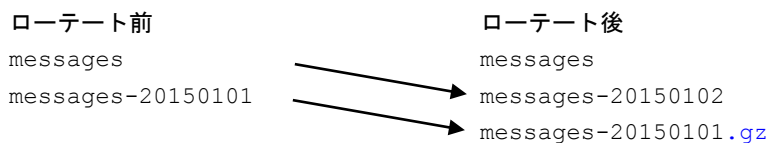
定義されている : `/var/log/messages-YYYYMMDD` [`YYYY=西暦年, MM=月, DD=日`]

であり、他の命名規則となっているとき、Syslog 監視機能では、監視できません。

また、`/etc/logrotate.d/syslog` に `"compress"` (圧縮する) が定義されているとき、ローテート後のファイルはテキストではないため、Syslog 監視機能では、監視できません。

Red Hat Enterprise Linux 6 では、既定値で `"dateext"` が定義されています。

Red Hat Enterprise Linux 7 では、既定値で `"dateext"` が定義されています。`"compress"` は定義されていませんが、ローテートするファイルの 1 つ前にローテートしたファイル (`messages-YYYYMMDD`) は gz 形式 (`messages-YYYYMMDD.gz`) に圧縮されますので、Syslog 監視機能では、監視できません。ただし、ESMPRO/ServerAgent が停止していない場合は gz 形式となる前に syslog を監視しているため、影響はありません。



追加監視対象

`/var/log/messages` の文字列を含まないファイルを監視対象として、1 つ追加できます。既定監視対象をチェックした後、追加監視対象のファイルをチェックするため、監視間隔のタイミングにより、時系列が逆転するときがあります。

追加することのできる監視対象は、syslog と同じ以下のフォーマットで出力されるファイルのみとなり、監視対象ファイルの一行目は監視しません。

`%b %d %H:%M:%S %HOSTNAME% %MESSAGE%`

`%b` ロケールによる省略形の月の名前 (Jan~Dec), `%d` 日(月内通算日数 2 桁) (1~31)

`%H` 時 (00~23), `%M` 分 (00~59), `%S` 秒 (00~59)

`%HOSTNAME%` ホスト名, `%MESSAGE%` メッセージ (通報内容)

ログローテートするファイルを指定した場合は、ログローテート後のファイルは監視対象となりません。

そのため、ログのファイル名の切り替わるタイミングで、追加監視対象ファイル後半の一部が監視できないときがあります。

ファイル監視対象

`/var/log/messages` の文字列を含まないファイルを監視対象として、1 つ追加できます。既定監視対象と追加監視対象をチェックした後、ファイル監視対象のファイルをチェックするため、監視間隔のタイミングにより、時系列が逆転するときがあります。

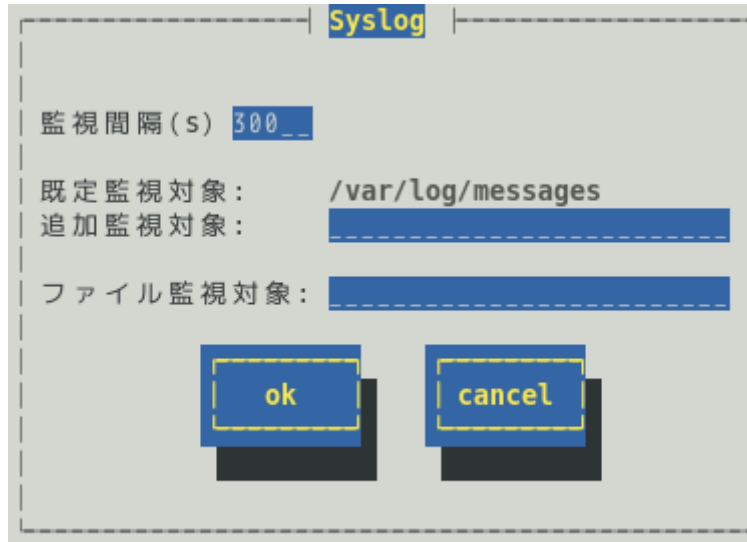
追加することのできる監視対象のファイルフォーマットに指定はありません。

ログローテートするファイルを指定した場合は、ログローテート後のファイルは監視対象となりません。

そのため、ログのファイル名の切り替わるタイミングで、ファイル監視対象のファイル後半の一部が監視できないときがあります。

設 定

コントロールパネル(ESMagntconf)の「Syslog」を選択して表示される[Syslog]画面にて、Syslog 監視の「監視間隔」、「既定監視対象」、「追加監視対象」、「ファイル監視対象」が設定できます。「追加監視対象」と「ファイル監視対象」にて"/var/log/messages"の文字列を含まないファイルを監視対象に設定できます。



監視間隔(s)

Syslog 監視機能の監視する間隔(秒)が設定できます。設定可能範囲は 10～3600 秒です。
既定値は 300 秒です。

既定監視対象

"/var/log/messages"からの変更、削除はできません。詳細は Syslog 監視の機能にある既定監視対象を参照してください。

追加監視対象

"/var/log/messages"の文字列を含まないファイルを監視対象として、パスの長さが 255 バイト以下となる絶対パスで設定できます。相対パスでの設定はできません。追加することのできる監視対象のファイルフォーマットは syslog と同じフォーマットです。詳細は Syslog 監視の機能にある追加監視対象を参照してください。

既定値は空白で、追加監視対象は設定されていません。

ファイル監視対象

"/var/log/messages"の文字列を含まないファイルを監視対象として、パスの長さが 255 バイト以下となる絶対パスで設定できます。相対パスでの設定はできません。追加することのできる監視対象のファイルフォーマットに指定はありません。詳細は Syslog 監視の機能にあるファイル監視対象を参照してください。

既定値は空白で、ファイル監視対象は設定されていません。

[ok]ボタン

設定した情報を登録し、この画面を閉じます。設定の変更は、次の監視間隔で有効になります。

[cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。

通報機能

ESMPRO/ServerAgentService の通報機能について説明します。

1. 通報設定
2. 基本設定
3. 通報先リストの設定
4. Syslog イベントの設定

1. 通報設定

本章では、どのようなイベントをどこの通報先にいつ通報するかといった通報設定の機能を説明しています。通報設定は、コントロールパネル(ESMamsadm)で設定します。



チェック

非サービスモードでは、監視サービスはインストールされないため、設定はできません。



ヒント

コントロールパネルを複数のコンソールから起動しないでください。後から実行したコンソールからは起動できず、『レジストリの読み込みに失敗しました。』と表示します。



ヒント

ESMPRO/ServerAgentService を使用する前に EXPRESSBUILDER または Starter Pack、Web サイトのダウンロード物件に含まれる ESMPRO/ServerAgentService インストールガイド(Linux 編)の 2 章(3. インストールを終えた後に)を実施してください。

マネージャ通報には、次の 3 種類があります。

1. マネージャ通報(SNMP)

ESMPRO/ServerAgentService が SNMP Trap(UDP トラップ)を送信します。ESMPRO/ServerManager 以外の「SNMP Trap 受信をサポートしているマネージャー」にも通報できます。

2. マネージャ通報(TCP_IP In-Band)

TCP/IP を利用して、ESMPRO/ServerManager に通報するため、信頼性の高い通報をする場合に使用します。

3. マネージャ通報(TCP_IP Out-of-Band)

TCP_IP In-Band と同様に TCP/IP を利用して、ESMPRO/ServerManager に通報しますが、PPP(Point to Point Protocol)を介して通報します。したがって、ESMPRO/ServerAgentService と ESMPRO/ServerManager が遠隔地に存在し、公衆回線を通して、通報する場合(Wide Area Network 環境)に使用します。また、ダイヤルアップ接続となるため、ESMPRO/ServerAgentService 側、ESMPRO/ServerManager 側のそれぞれにモデムと電話回線が必要となります。

上記のマネージャ通報以外に ESMPRO プロバイダの監視スレッドで、状態の変化に合わせマネージャーに CIM-Indication で通報します。ESMPRO/ServerManager で CIM-Indication を受信するには、ESMPRO/ServerManager(受信)側で、ESMPRO/ServerAgentService(送信)側を登録します。それにより、CIM-Indication のサブスクリプションが作成され、送信側から受信側に CIM-Indication を送信されます。

- ・ CPU 負荷監視スレッド (クラス名 : ESM_Processor)
- ・ 物理メモリ使用量監視スレッド (クラス名 : ESM_PhysicalMemory)
- ・ 仮想メモリ使用量監視スレッド (クラス名 : ESM_VirtualMemory)
- ・ ページファイル使用量監視スレッド (クラス名 : ESM_PageFile)
- ・ ストレージ監視スレッド (クラス名 : ESM_StorageThread)
- ・ ファイルシステム監視スレッド (クラス名 : ESM_FileSystemThread)
- ・ CPU・メモリ縮退監視スレッド (クラスなし)

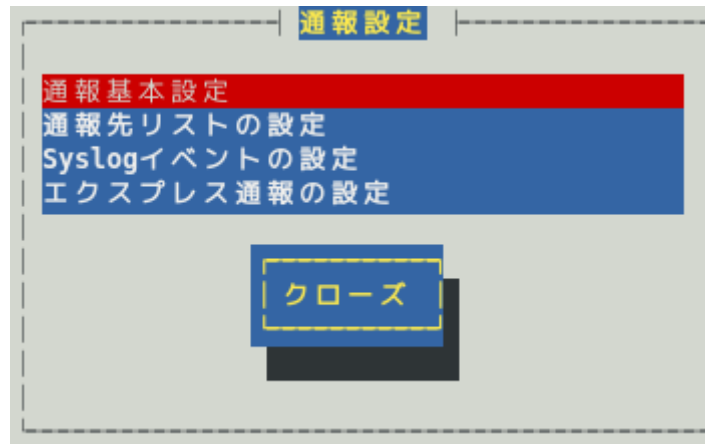


チェック

サブスクリプションには期限が設けられているため、ESMPRO/ServerManager(受信)側の OS が停止していた場合などにより、サブスクリプションの期限が切れると CIM-Indication を受信できません。

コントロールパネル(ESMamsadm)の起動方法は以下のとおりです。

1. root 権限のあるユーザーでログインします。
2. コントロールパネルが格納されているディレクトリに移動します。
cd /opt/nec/esmpro_sa/bin
3. コントロールパネルを起動します。
./ESMamsadm



コントロールパネル(ESMamsadm)のメイン画面

■ 通報手段として SNMP による通報をするとき

ESMPRO/ServerAgentService のインストール時にあらかじめ、監視イベントに対して SNMP 通報手段による通報設定がひととおり設定済みとなっています。通報基本設定にて、通報先となる ESMPRO/ServerManager が導入されているマシンの IP アドレスを設定するだけで、通報準備が整います。SNMP による通報をするときの設定につきましては、本書の 3 章(2.1.1. マネージャ通報(SNMP)の基本設定)を参照してください。

■ 通報手段として SNMP 以外による通報をするとき

以下の流れにしたがって設定してください。

1. 通報の基本設定をします。(通報基本設定)
TCP_IP In-Band による通報をするときの基本設定は、本書の 3 章(2.1.2. マネージャ通報(TCP_IP In-Band)の基本設定)を参照してください。
TCP_IP Out-of-Band による通報をするときの基本設定は、本書の 3 章(2.1.3. マネージャ通報(TCP_IP Out-of-Band)の基本設定)を参照してください。
2. 通報の宛先リストを設定します。(通報先リストの設定)
TCP_IP In-Band による通報をするときの宛先設定は、本書の 3 章(3.1.1. 通報手段がマネージャ通報(TCP_IP In-Band)の宛先設定)を参照してください。
TCP_IP Out-of-Band による通報をするときの宛先設定は、本書の 3 章(3.1.2. 通報手段がマネージャ通報(TCP_IP Out-of-Band)の宛先設定)を参照してください。
3. Syslog イベントの設定、および、Syslog イベントへの通報先を結びつけます。
Syslog イベントとは、Syslog 監視機能により検出した故障の監視イベントを指します。
Syslog イベントの設定は、本書の 3 章(4. Syslog イベントの設定)を参照してください。

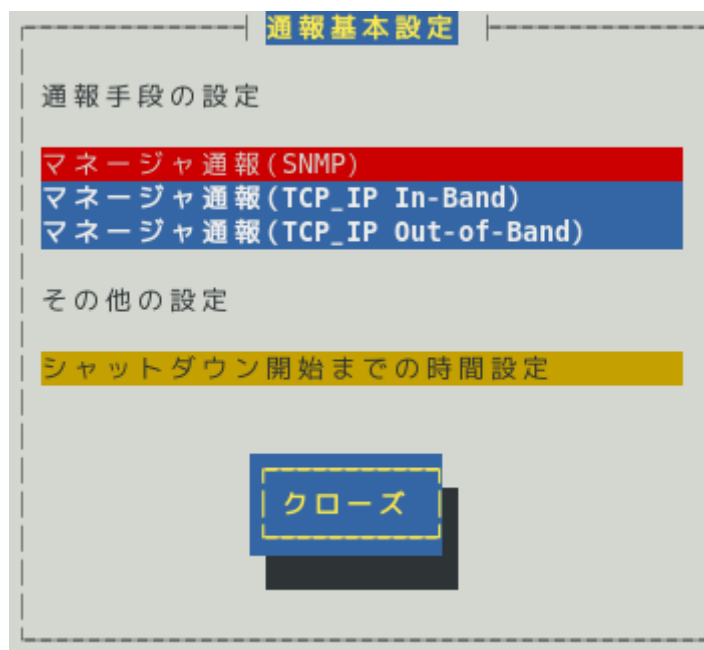
2. 基本設定

機 能

通報手段の有効/無効、マネージャ通報(SNMP)の Trap 送信先、エラー発生時のシャットダウン機能の有効/無効、シャットダウン開始までの時間を設定できます。通報手段を無効にすると、すべての監視イベントに設定されている当該通報手段による通報されなくなります。シャットダウンを無効にすると、各監視イベントの通報後動作でシャットダウン/リポートが設定されているときも、通報発生後のシャットダウン/リポートが実行されなくなります。

設 定

コントロールパネル(ESMamsadm)の「通報基本設定」を選択して表示される[通報基本設定]画面にて、通報の基本設定ができます。



通報手段一覧

通報手段が表示されます。

その他の設定

設定項目が表示されます。

[クローズ]ボタン

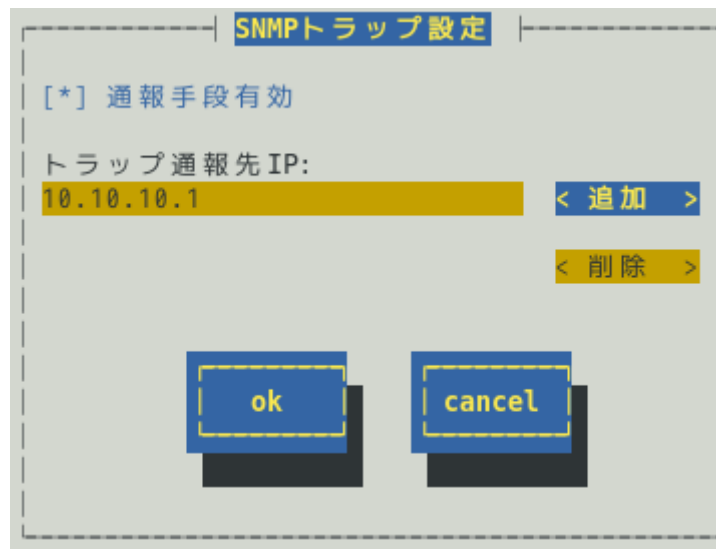
この画面を閉じます。

2.1 通報手段の設定

通報手段の有効/無効、マネージャ通報(SNMP)のトラップ通報先 IP が設定できます。

2.1.1 マネージャ通報(SNMP)の基本設定

[通報基本設定]画面の通報手段一覧から「マネージャ通報(SNMP)」を選択して表示される、[SNMP トラップ設定]画面にて、マネージャ通報(SNMP)の有効/無効、トラップ通報先 IP が設定できます。



The image shows a dialog box titled "SNMPトラップ設定" (SNMP Trap Setting). Inside the dialog, there is a section labeled "[*] 通報手段有効" ([*] Notification Method Enabled). Below this, there is a label "トラップ通報先 IP:" (Trap Notification Destination IP:). Underneath the label, the IP address "10.10.10.1" is displayed in a yellow box. To the right of the IP box, there are two buttons: "< 追加 >" (Add) and "< 削除 >" (Delete). At the bottom of the dialog, there are two buttons: "ok" and "cancel".

通報手段有効

SNMP による通報手段の有効(チェックあり) と無効(チェックなし)が<スペース>キーで設定できます。既定値は"有効"です。

トラップ通報先 IP

通報先に設定している IP アドレスが一覧で表示されます。ESMPRO/ServerAgentService から送信する Trap の宛先は、SNMP 設定ファイル(snmpd.conf)に設定される Trap Destination は使用しません。トラップ通報先 IP は、最大で 128 個まで設定できます。

[追加...]ボタン

トラップ通報先 IP に新しい通報先の IP アドレスを追加できます。

[削除...]ボタン

トラップ通報先 IP から削除したい通報先の IP アドレスを削除できます。

[ok]ボタン

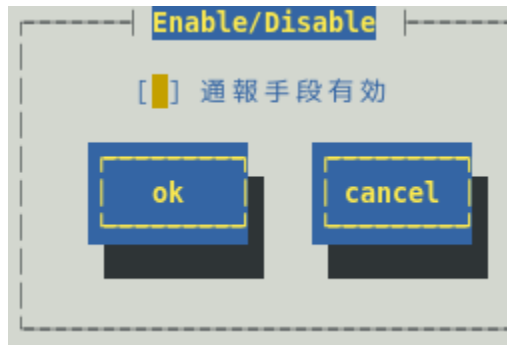
設定した情報を登録し、この画面を閉じます。

[cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。

2.1.2 マネージャ通報(TCP_IP In-Band)の基本設定

[通報基本設定]画面の通報手段一覧から「マネージャ通報(TCP_IP In-Band)」を選択して表示される、[Enable/Disable]画面にて、マネージャ通報(TCP_IP In-Band)の有効/無効が設定できます。



通報手段有効

TCP_IP In-Band による通報手段の有効(チェックあり)と無効(チェックなし)が<スペース>キーで設定できます。

[ok]ボタン

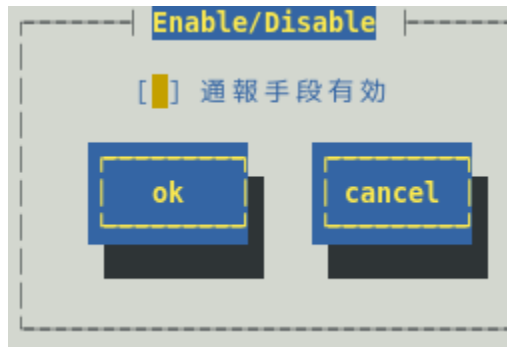
設定した情報を登録し、この画面を閉じます。

[cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。

2.1.3 マネージャ通報(TCP_IP Out-of-Band)の基本設定

[通報基本設定]画面の通報手段一覧から「マネージャ通報(TCP_IP Out-of-Band)」を選択して表示される、[Enable/Disable]画面にて、マネージャ通報(TCP_IP Out-of-Band)の有効/無効が設定できます。
TCP/IP Out-of-Band 通報を有効にするときは、ESMPRO/ServerManager 側の RAS(Remote Access Service) 設定の暗号化の設定は、「クリアテキストを含む任意の認証を許可する」を必ず選択します。



通報手段有効

TCP_IP Out-of-Band による通報手段の有効(チェックあり)と無効(チェックなし)が<スペース>キーで設定できます。

[ok]ボタン

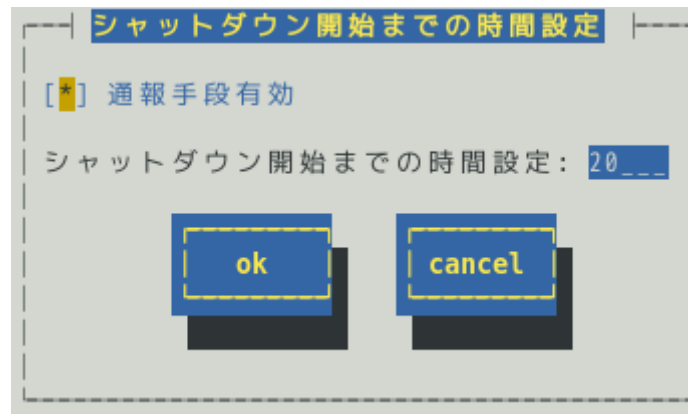
設定した情報を登録し、この画面を閉じます。

[cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。

2.2 その他の設定

[通報基本設定]画面のその他の設定から「シャットダウン開始までの時間設定」を選択して表示される、[シャットダウン開始までの時間設定]画面にて、シャットダウン開始までの時間が設定できます。



通報手段有効

通報によるシャットダウン機能の有効(チェックあり)と無効(チェックなし)が<スペース>キーで設定できます。

既定値は”有効”です。

シャットダウン開始までの時間設定

ESMPRO/ServerAgentService が OS のシャットダウンを開始するまでの時間が設定できます。

既定値は 20 秒です。

設定可能範囲は 0～1800 秒です。

通報後のアクションにシャットダウンを指定しているとき、ここで設定した時間が経過した後、OS のシャットダウンが開始します。

[ok]ボタン

設定した情報を登録し、この画面を閉じます。

[cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。

3. 通報先リストの設定

コントロールパネル(ESMamsadm)の「通報先リストの設定」を選択して表示される[通報先リストの設定]画面にて、通報先 ID の設定変更、追加、削除および通報スケジュールが設定できます。



通報先 ID 一覧

通報先 ID のリストが表示されます。

メッセージ

通報手段: 通報先 ID 一覧で選択された通報先 ID に設定されている通報手段が表示されます。

宛先情報: 通報先 ID 一覧で選択された通報先 ID に設定されている宛先情報が表示されます。

[追加...]ボタン

通報先 ID を追加できます。[追加...]ボタンを押すと、[ID 設定]画面が表示されます。

同一通報手段で異なる通報先を持つ通報先 ID を登録しておくと、同一手段で複数の宛先に通報できます。

[修正...]ボタン

通報先 ID 一覧で選択した通報先 ID に対して、通報先の設定が変更できます。

[修正...]ボタンを押すと、[ID 設定]画面が表示されます。

[削除...]ボタン

通報先 ID 一覧で選択した通報先 ID を削除できます。

通報先 ID を削除すると、各監視イベントに設定されている通報先 ID も削除されます。また、既定で設定している"SNMP"と"TCP_IP In-Band"、"TCP_IP Out-of-Band"の 3 つの通報先 ID は、削除できません。

[クローズ]ボタン

この画面を閉じます。

3.1 通報先 ID の設定変更

通報先リストに登録されている通報先 ID の設定変更ができます。[通報先リストの設定]画面の通報先 ID 一覧で変更したい通報先 ID を選択し、[修正]ボタンを押すと[ID 設定]画面が開きます。設定内容は、通報手段によって異なります。

ID設定

ID: SNMP

通報手段: Manager (SNMP)

宛先情報:
設定する必要はありません。

宛先設定... スケジュール... クローズ

● 設定方法

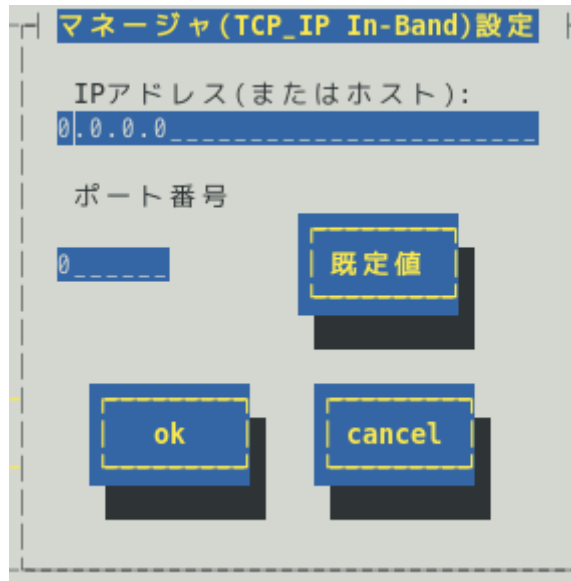
必要に応じて[宛先設定...]ボタンおよび[スケジュール...]ボタンを押して、宛先と通報スケジュールを設定します。

設定変更のとき、ID および通報手段の項目は、表示のみとなり、設定できません。

通報手段が「Manager(SNMP)」のときは、[宛先設定...]ボタンを押しても、ここでは設定する必要がないため、宛先設定画面は、表示されません。

3.1.1 通報手段がマネージャ通報(TCP_IP In-Band)の宛先設定

通報手段がマネージャ通報(TCP_IP In-Band)のとき、[ID 設定]画面で[宛先設定...]ボタンを押すと表示される[マネージャ(TCP_IP In-Band)設定]画面にて、宛先が設定できます。



IP アドレス(またはホスト)

通報先の ESMPRO/ServerManager が導入されたマシンの IP アドレス(またはホスト名)を指定します。省略することはできません。

ポート番号

ソケット間通信で使用するポート番号を設定できます。

このポート番号は、ESMPRO/ServerAgentService と通報先の ESMPRO/ServerManager で同じ値を設定してください。既定値は 31134 です。既定値に問題がないかぎり、設定を変更しないでください。

既定値に問題があるとき、6001 から 65535 の範囲で番号を変更してください。番号を変更したとき、通報先の ESMPRO/ServerManager がインストールされているマシンで設定ツールを実行し、[通報基本設定]の[通報受信設定]-[エージェントからの受信(TCP/IP)]の設定を変更してください。



アクセス制御を設定している場合は、指定したポートのアクセスを許可してください。

[既定値]ボタン

ボタンを押すと、既定値が設定されます。

[ok]ボタン

設定した情報を登録し、この画面を閉じます。

[cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。

3.1.2 通報手段がマネージャ通報(TCP_IP Out-of-Band)の宛先設定

通報手段がマネージャ通報(TCP_IP Out-of-Band)のとき、[ID 設定]画面で[宛先設定...]ボタンを押すと表示される[マネージャ(TCP_IP Out-of-Band)設定]画面にて、宛先が設定できます。

マネージャ(TCP_IP Out-of-Band)設定

IPアドレス(またはホスト):
0.0.0.0

リモートアクセスサービスのエントリ選択

電話番号: 0

ユーザ名:

パスワード:

ポート番号
0

既定値

ok cancel

IP アドレス(またはホスト)

通報先の ESMPRO/ServerManager が導入されたマシンの IP アドレス(またはホスト名)を指定します。
省略することはできません。

リモートアクセスサービスのエントリ選択

接続先の電話番号と、接続時に必要なユーザー名、パスワードを設定できます。

ポート番号

ソケット間通信で使用するポート番号を設定できます。

このポート番号は、ESMPRO/ServerAgentService と通報先の ESMPRO/ServerManager で同じ値を設定します。

既定値は 31134 です。既定値に問題がないかぎり、設定を変更しないでください。

既定値に問題があるとき、6001 から 65535 の範囲で番号を変更してください。番号を変更したとき、通報先の ESMPRO/ServerManager がインストールされているマシンで設定ツールを実行し、[通報基本設定]の[通報受信設定]-[エージェントからの受信(TCP/IP)]の設定を変更してください。



アクセス制御を設定している場合は、指定したポートのアクセスを許可してください。

[既定値]ボタン

ボタンを押すと、既定値が設定されます。

[ok]ボタン

設定した情報を登録し、この画面を閉じます。

[cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。

3.1.3 スケジュール設定

通報先 ID ごとに、通報スケジュールが設定できます。

スケジュール

リトライ間隔: 5 分

リトライ時間: 72 時間

通報時間帯

0-24,

例: 8-16, 19-23

ok cancel

リトライ間隔

通報リトライをする間隔が設定できます。
既定値は 5 分です。
設定可能範囲は 1～30 分です。

リトライ時間

最大リトライ可能時間が設定できます。
0 を設定したときは、通報リトライしません。
既定値は 72 時間です。
設定可能範囲は 0～240 時間です。

通報時間帯

通報時間帯(24 時間表記の 1 時間単位)を指定してください。指定した時間帯に発生した故障のみを通報します。通報をしない時間帯に発生したイベントは通報されず、通報をする時間帯になると通報します。(それまでイベントの通報は保留されます。)
既定値は 0-24 で、24 時間通報可能となっています。

[ok]ボタン

設定した情報を登録し、この画面を閉じます。

[cancel]ボタン

設定した情報を登録せずに、この画面を閉じます。

3.2 通報先 ID の追加

通報先 ID を追加します。設定内容は通報手段によって異なります。

ID設定

ID:

通報手段: MANAGER (SNMP)

宛先情報:

宛先設定... スケジュール... ok cancel

< 設定手順 >

- 1) 通報先 ID を半角英数字または半角スペース、半角ハイフン(-)、半角アンダーバー(_)を 31 文字以内で入力します。
- 2) 通報手段を<↑>か<↓>キーで選択します。
- 3) [宛先設定...]ボタンを押し、表示される画面にて宛先を設定します。
- 4) [スケジュール...]ボタンを押し、表示される画面で通報スケジュールを設定します。
- 5) [ok]ボタンを押します。

通報手段で「Manager(SNMP)」を選択したときは、[宛先設定...]ボタンを押しても、ここでは設定する必要がないため、宛先設定画面は表示されません。

4. Syslog イベントの設定

機 能

Syslog イベントの設定および通報先を結びつけます。監視対象のイベントが発生したとき、ここで結びつけた通報先に通報されます。Syslog イベントは、あらかじめ登録されているイベント以外に、システム環境に応じて新たなソース、監視イベントを任意に追加や削除できます。Syslog 監視は既定値では 300 秒間隔で監視しています。Syslog 監視の監視間隔は変更できます。Syslog 監視の監視間隔の設定方法につきましては本書の 2 章(3. Syslog 監視)を参照してください。

設 定

コントロールパネル(ESMamsadm)の「Syslog イベントの設定」を選択して表示される[Syslog イベントの設定]画面にて、Syslog イベントの設定ができます。

ソース名

ソースを<↑>か<↓>キーで選択し表示します。

ソースに対する処理

ソースに対する処理を<スペース>キーで選択できます。

本選択は Syslog イベントの設定内容ではなく、処理方法の選択です。

そのため、コントロールパネルの起動毎に「OFF」が選択されます。

以下の設定をするとき「OFF」を選択します。

- ・選択した「ソース名」のイベント ID に対して、通報先や監視イベントを設定するとき。
- ・監視イベントの追加や削除をするとき。

以下の設定をするとき「ON」を選択します。

- ・選択した「ソース名」のイベント ID すべてに対して、一括で通報先を設定するとき。
ただし、監視イベントの設定はできません。
- ・ソースの追加や削除(すべての監視イベントを削除)をするとき。

イベント ID

「ソースに対する処理」で「OFF」を選択しているときは、「ソース名」で選択されたイベント ID を<↑>か<↓>キーで選択し表示します。
「ソースに対する処理」で「ON」を選択しているときは、「イベント ID」に「すべて」と表示します。

Trap Name

選択されたイベント ID のトラップ名を表示します。

[クローズ]ボタン

[Syslog イベントの設定]画面を閉じます。
[クローズ]ボタンを押すと、Syslog 監視の間隔はリセットされ、[クローズ]ボタンを押した時間から Syslog 監視間隔(既定値は 300 秒)までは、Syslog イベントを検知しません。

[追加...]ボタン

[追加...]ボタンを押すと、[Syslog イベントの追加]画面が表示されます。
「ソースに対する処理」で「OFF」を選択しているときは、選択したソースの監視イベントを追加します。
「ソースに対する処理」で「ON」を選択しているときは、ソースを含め監視イベントを追加します。

[削除...]ボタン

[削除...]ボタンを押すと、
「ソースに対する処理」で「OFF」を選択しているときは、選択したソースの監視イベントを削除します。
「ソースに対する処理」で「ON」を選択しているときは、ソースを含め監視イベントすべてを削除します。

[設定...]ボタン

[設定...]ボタンを押すと、[Syslog アプリケーション設定]画面が表示されます。
「ソースに対する処理」で「OFF」を選択しているときは、選択したソースのイベント ID に対して、設定変更および通報先を設定できます。
「ソースに対する処理」で「ON」を選択しているときは、選択したソースのイベント ID すべてに対して、一括で通報先を設定できます。

[テスト]ボタン

「ソースに対する処理」で「OFF」を選択しているときは、選択した Syslog イベントのキーワードを含む"ESMamsadm: [TEST - AlertManager] (キーワード)"文字列を syslog に記録することにより、テストイベントを発生させて、監視対象イベントに結び付けた宛先への通報を実際にシミュレートできます。通報のみならず「通報後動作」も動作します。そのため、設定によってはシャットダウンされることもありますので、テストする通報の選択にはご注意ください。
「ソースに対する処理」で「ON」を選択しているときは、テストできません。



チェック

Syslog イベントの追加や削除、設定を変更したときは、Syslog イベントの情報を再読み込みさせる必要があります。

[クローズ]ボタンを押して、[Syslog イベントの設定]画面を閉じ、[通報設定]画面から、再度「Syslog イベントの設定」を選択します。その後、[テスト]ボタンを押します。

4.1 通報先の指定(Syslog イベント)

通報先の指定方法には、以下の方法があります。

1. 監視イベントごとに通報先を指定する方法(「ソースに対する処理」で「OFF」を選択しているとき)
2. ソースごとに通報先を一括指定する方法(「ソースに対する処理」で「ON」を選択しているとき)

4.1.1 監視イベントごとに通報先を指定する方法

監視イベントごとに個別に通報先を指定するときの方法を説明します。

通報先の設定と同時に、通報後の動作、対処法等の設定もできます。

< 設定手順 >

1. コントロールパネル(ESMamsadm)を起動し、「Syslog イベントの設定」を選択します。
[Syslog イベントの設定]画面が表示されます。

2. 「ソース名」でソースを<↑>か<↓>キーで選択します。
3. 「ソースに対する処理」で「OFF」に<スペース>キーでチェックします。
4. 「イベント ID」で設定したいイベント ID を<↑>か<↓>キーで選択します。
5. [設定...]ボタンを押します。
[Syslog アプリケーション設定]画面が表示されます。

Syslogアプリケーション設定

ソース名: ALERTMANAGER
 イベントID: 80000001
 キーワード1: AM FILE ERROR
 キーワード2:
 キーワード3:
 通報後動作: なし
 対処法: 保守員に連絡して下さい
 レポートカウント: 1

[<Detail>](#)
[<Detail>](#)
[<Detail>](#)

通報IDリスト:
 EXPRESSREPORT
 TCP_IP IN-BAND
 TCP_IP OUT-OF-BAND

< 追加 >
 < 削除 >

通報先:
 SNMP

監視時間帯
0-24,

ok
 cancel

6. 「通報 ID リスト」から通報したい通報 ID を選択します。
通報先の設定として、通報先に EXPRESSREPORT を追加できますが、Alive レベルが対象外のため、実際にエクスプレス通報されません。
7. [追加]ボタンを押します。
通報 ID が「通報 ID リスト」から「通報先」に移動します。
8. 通報 ID を通報対象から削除するには「通報先」から通報 ID を選択して、[削除]ボタンを押します。
通報 ID が「通報先」から「通報 ID リスト」に移動します。
9. [ok]ボタンを押します。

通報後動作

通報後のアクションを設定できます。[通報後のアクション]とは、このイベントが発生した後の動作を指し、「シャットダウン」「リブート」「なし」の3つから<↑>か<↓>キーで選択します。

対処法

通報する項目に対する対処方法を設定します。507 バイト(半角文字で 507 文字、全角文字で 253 文字)以下で指定します。日本語は使用できます。

レポートカウント

同一イベントを指定回数検出したときに通報をします。

監視時間帯

監視時間帯を指定できます。指定した時間帯に発生したイベントのみを通報します。
時間設定は 1 時間単位で指定できます。既定値では 24 時間通報可能となっています。

4.1.2 ソースごとに通報先を一括指定する方法

ソースごとに、ソース配下のすべての監視イベントに同じ通報先を一括して指定する方法を説明します。通報先を一括で設定した後、再度、[Syslog アプリケーション設定]画面を開いても、通報先一覧には何も表示されません。通報先の確認は「監視イベントごとに個別に通報先を指定する方法」にて、個々のイベントで確認します。

< 設定手順 >

1. コントロールパネル(ESMamsadm)を起動し、「Syslog イベントの設定」を選択します。
[Syslog イベントの設定]画面が表示されます。

Syslog イベントの設定

ソース名: ALERTMANAGER

ソースに対する処理: (*) ON () OFF

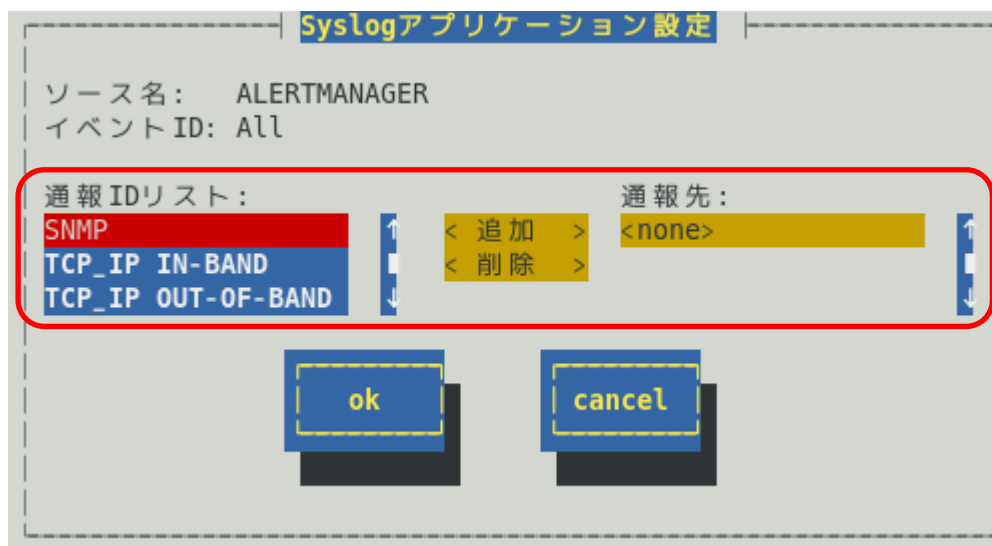
イベント ID: すべて

テスト

Trap Name:

追加... 削除... 設定... クローズ

2. 「ソース名」でソースを<↑>か<↓>キーで選択します。
3. 「ソースに対する処理」で「ON」に<スペース>キーでチェックします。
4. [設定...]ボタンを押します。
[Syslog アプリケーション設定]画面が表示されます。



5. 「通報 ID リスト」から通報したい通報 ID を選択します。
6. [追加]ボタンを押します。
通報 ID が「通報 ID リスト」から「通報先」に移動します。
7. 通報 ID を通報対象から削除するには「通報先」から通報 ID を選択して、[削除]ボタンを押します。
通報 ID が「通報先」から「通報 ID リスト」に移動します。
8. [ok]ボタンを押します。

4.2 Syslog イベントのソースの追加

システム環境に応じて、新たな Syslog イベントのソースを任意に追加できます。

ESMPRO/ServerAgentService 以外のアプリケーションが登録するイベントを監視したいときに設定します。ソース登録と同時に、1 件目の監視イベントをあわせて登録します。本機に登録できるイベント数は、以下のとおりですが、登録件数によりディスク使用量・メモリ使用量が増加しますので、設定には注意してください。

- ・ ESMPRO/ServerAgentService Ver.1 の場合 : 1024 件
- ・ ESMPRO/ServerAgentService Ver.2 の場合 : 2048 件

< 設定手順 >

1. コントロールパネル(ESMamsadm)を起動し、「Syslog イベントの設定」を選択します。
[Syslog イベントの設定]画面が表示されます。

2. 「ソースに対する処理」で「ON」に<スペース>キーでチェックします。
3. [追加...]ボタンを押します。
[Syslog イベントの追加]画面が表示されます。

Syslogイベントの追加

ソース名:

イベント ID:

キーワード 1:

キーワード 2:

キーワード 3:

Trap Name:

対処法:

4. 「ソース名」「イベント ID」「キーワード」「Trap Name」「対処法」を設定します。
5. [ok]ボタンを押します。
このとき、「通報後動作：なし」「レポートカウント：1」が設定されます。

ソース名 (必須項目)

ソース名を 40 文字以下の半角英字で始まる半角英数字(大文字)で指定します。ソース名は大文字使用しますので、小文字を設定しても大文字に変換しますが、アラートビューアで表示する「タイプ」と「製品名」は設定した半角英数字のままとなります。小文字で設定したとき、「ソース」は大文字、「タイプ」と「製品名」は小文字となります。

ESMPRO/ServerManager のアラートビューアの「ソース」と「タイプ」、「製品名」欄に表示されます。

イベント ID (必須項目)

以下の命名規則にしたがって、半角英数字 8 文字(16 進数表記[0-9,A-F])で指定します。

<監視イベント ID 命名規則>

“x0000yyy”形式で指定します。(例：40000101、800002AB、C0000101)

“x”には、4,8,Cの中から設定します。それぞれの意味は以下のとおりです。

4：情報系イベントを意味します。

ESMPRO/ServerManager のアラートビューアのアイコンが「緑色」で表示されます。

8：警告系イベントを意味します。

ESMPRO/ServerManager のアラートビューアのアイコンが「黄色」で表示されます。

C：異常系イベントを意味します。

ESMPRO/ServerManager のアラートビューアのアイコンが「赤色」で表示されます。

“yyy”には、0x001(1)～0xFFFF(4095)の範囲内で任意の 16 進数値を設定します。

キーワード 1 (必須項目)、キーワード 2、キーワード 3

syslog に記録されるメッセージを一意に特定できる文字列を、それぞれ 256 文字以下の半角英数字で指定します。すべてのキーワードを含むメッセージを syslog から検出(※)したときに、そのメッセージの

全文を ESMPRO/ServerManager に通報します。
ESMPRO/ServerManager のアラートビューアの「詳細」欄に表示されます。
※1 行における検出範囲は、行頭から 1024Byte まで。

Trap Name (必須項目)

通報メッセージの概要を 79 バイト(半角文字で 79 文字、全角文字で 39 文字)以下で指定します。日本語は使用できます。
ESMPRO/ServerManager のアラートビューアの「概要」欄に表示されます。

対処法

通報メッセージを受けたときの対処方法を 507 バイト(半角文字で 507 文字、全角文字で 253 文字)以下で指定します。日本語は使用できます。
ESMPRO/ServerManager のアラートビューアの「対処」欄に表示されます。

4.3 Syslog イベントの追加

すでに登録済みの Syslog イベントのソース配下に、システム環境に応じて新たな Syslog イベントを追加できます。

< 設定手順 >

1. コントロールパネル(ESMamsadm)を起動し、「Syslog イベントの設定」を選択します。
[Syslog イベントの設定]画面が表示されます。

2. 「ソース名」でソース名を<↑>か<↓>キーで選択します。
3. 「ソースに対する処理」で「OFF」に<スペース>キーでチェックします。
4. [追加...]ボタンを押します。
[Syslog イベントの追加]画面が表示されます。
5. 「イベント ID」「キーワード」「Trap Name」「対処法」を設定します。
各項目の設定内容は「5.2. Syslog イベントのソースの追加」に記載してある内容と同じです。
6. [ok]ボタンを押します。

4.4 Syslog イベントのソースの削除

Syslog イベント監視から、Syslog イベントのソースを削除できます。ソースを削除すると、その配下に登録されているすべての監視イベントも削除されます。また、ESMPRO/ServerAgentService が登録している既定のソースを削除することはできません。

< 設定手順 >

1. コントロールパネル(ESMamsadm)を起動し、「Syslog イベントの設定」を選択します。
[Syslog イベントの設定]画面が表示されます。

2. 「ソース名」で削除したいソース名を<↑>か<↓>キーで選択します。
3. 「ソースに対する処理」で「ON」に<スペース>キーでチェックします。
4. [削除...]ボタンを押します。

4.5 Syslog イベントの削除

Syslog イベント監視から、Syslog イベントを削除できます。ESMPRO/ServerAgentService が登録している既定の監視イベントを削除することはできません。

< 設定手順 >

1. コントロールパネル(ESMamsadm)を起動し、「Syslog イベントの設定」を選択します。
[Syslog イベントの設定]画面が表示されます。

2. 「ソース名」でソース名を<↑>か<↓>キーで選択します。
3. 「ソースに対する処理」で「OFF」に<スペース>キーでチェックします。
4. 「イベント ID」で削除したいイベント ID を<↑>か<↓>キーで選択します。
5. [削除...]ボタンを押します。

4.6 Syslog イベントのテスト

Syslog イベントのテストを実行して、SNMP 通報の送信テストができます。

< テスト手順 >

1. コントロールパネル(ESMamsadm)を起動し、「Syslog イベントの設定」を選択します。
[Syslog イベントの設定]画面が表示されます。

2. 「ソース名」でソース名を<↑>か<↓>キーで選択します。
3. 「ソースに対する処理」で「OFF」に<スペース>キーでチェックします。
4. 「イベント ID」でテストしたいイベント ID を<↑>か<↓>キーで選択します。
5. [設定...]ボタンを押します。
[Syslog アプリケーション設定]画面が表示されます。

Syslogアプリケーション設定

ソース名: ESMCPUPERF
 イベント ID: 40000067
 キーワード1: ESMCpuPerf
 キーワード2: 40000067
 キーワード3:
 通報後動作: なし
 対処法:
 レポートカウント: 1
 通報 ID リスト:
 EXPRESSREPORT
SNMP
 TCP_IP IN-BAND
 監視時間帯
 0-24,

<Detail>
 <Detail>
 <Detail>

<追加>
 <削除>

通報先:
 <none>

ok cancel

6. 「通報先」に「SNMP」が設定されているか、確認します。
 設定されていない場合、「通報 ID リスト」から「SNMP」を選択して、<追加>ボタンを押します。
 「通報先」に「SNMP」が追加されます。

Syslogアプリケーション設定

ソース名: ESMCPUPERF
 イベント ID: 40000067
 キーワード1: ESMCpuPerf
 キーワード2: 40000067
 キーワード3:
 通報後動作: なし
 対処法:
 レポートカウント: 1
 通報 ID リスト:
 EXPRESSREPORT
 TCP_IP IN-BAND
 TCP_IP OUT-OF-BAND
 監視時間帯
 0-24,

<Detail>
 <Detail>
 <Detail>

<追加>
 <削除>

通報先:
SNMP

ok cancel

7. 「通報後動作」が「なし」、「通報先」が SNMP となっていることを確認します。



「通報後動作」が「シャットダウン」や「リブート」の場合、テストであっても「通報後動作」が動作します。「通報先」がない場合、通報されません。

8. [ok]ボタンを押します。
[Syslog イベントの設定]画面が表示されます。



Syslog イベントの追加や削除、設定を変更したときは、Syslog イベントの情報を再読み込みさせる必要があります。

[クローズ]ボタンを押して、[Syslog イベントの設定]画面を閉じ、[通報設定]画面から、再度「Syslog イベントの設定」を選択します。その後、[テスト]ボタンを押します。

9. [テスト]ボタンを押します。
テストメッセージが syslog に記録されます。
Syslog 監視の監視間隔(既定値 300 秒)を超えると、syslog に記録されたテストメッセージを検出し、SNMP 通報します。
10. [設定...]ボタンを押します。
[Syslog アプリケーション設定]画面が表示されます。

Syslogアプリケーション設定

ソース名: ESMCPUPERF
 イベントID: 40000067
 キーワード1: ESMCpuPerf
 キーワード2: 40000067
 キーワード3:
 通報後動作: なし
 対処法:
 レポートカウント: 1
 通報IDリスト:
 EXPRESSREPORT
 TCP_IP IN-BAND
 TCP_IP OUT-OF-BAND
 監視時間帯
 0-24,

<Detail>
 <Detail>
 <Detail>

通報先:
 <追加> SNMP
 <削除>

ok cancel

11. 手順6で「通報先」に「SNMP」を追加した場合、「通報先」から「SNMP」を選択して、<削除>ボタンを押します。
「通報先」から「SNMP」が削除されます。
12. [ok]ボタンを押します。
[Syslog イベントの設定]画面が表示されますので、[クローズ]ボタンを押して閉じます。

4

ESMPRO/ServerAgentService Ver. 2

OpenIPMI と追加機能

OpenIPMI を利用した OS ストール監視方法のご紹介と ESMPRO/ServerAgentService の追加機能について説明します。

1. OpenIPMI を利用した OS ストール監視
2. コンフィグレーションツール
3. ツールについて

1. OpenIPMI を利用した OS ストール監視

本章では、BMC 対応装置向けに OpenIPMI を利用した OS ストール監視を説明しています。



本章では、オープンソースソフトウェア(OSS)である OpenIPMI を利用した OS ストール監視の設定例についてご紹介します。なお、本章の記載内容については万全を期していますが、記載された設定内容や OSS である OpenIPMI の動作保証を行うものではありません。

機能

装置に搭載されているウォッチドッグタイマー(ソフトウェアストール監視用タイマー)を定期的に更新することにより、OS の動作状況を監視します。OS のストールなどにより応答がなくなり、タイマーの更新がされなくなると、タイマーがタイムアウトして自動的にタイムアウト後の動作に設定された復旧方法を実行します。

設定

ストール監視のタイムアウト、更新時間およびストール発生時の動作が設定できます。これによって OS 稼働中にストールが発生したときの復旧方法を設定できます。設定パラメーターは以下のとおりです。

タイムアウト時間 : timeout

OS がストールしたと判定する時間を秒数で設定してください。

既定値は 60 秒です。10 秒より設定可能です。

/etc/sysconfig/ipmi ファイルにて設定できます。

タイムアウト後の動作 : action

タイムアウト後の復旧方法を選択してください。既定値は「reset」です。

/etc/sysconfig/ipmi ファイルにて設定できます。

none	何もしません。
reset	システムをリセットし再起動を試みます。
power_off	システムの電源を切断します。
power_cycle	いったん電源 OFF し、直後に再度電源 ON します。

更新間隔 : interval

タイムアウト時間のタイマーを更新する間隔を秒数で設定してください。

既定値は 10 秒です。設定可能範囲は 1~59 秒です。

/etc/watchdog.conf ファイルにて設定できます。



使用するマシンの負荷状況によっては、OS がストール状態でなくても、ウォッチドッグタイマーの更新ができずにタイムアウトが発生する可能性があります。ご使用環境にて高負荷状態での評価した上でストール監視を設定してください。

1.1 Red Hat Enterprise Linux 6～7

対 象 O S

Red Hat Enterprise Linux 6 (以降、RHEL6 と表記します)

Red Hat Enterprise Linux 7 (以降、RHEL7 と表記します)

手 順

■ ストール監視機能の設定手順

root 権限のあるユーザーでログインして、設定をしてください。

1. 必要なパッケージを事前にインストールしてください。

1.1 下記の OpenIPMI パッケージをインストールしてください。

```
RHEL6, RHEL7
- OpenIPMI-*.rpm
- ipmitool-*.rpm
```

2. OpenIPMI を設定してください。

2.1 OpenIPMI の環境設定ファイル(/etc/sysconfig/ipmi)内のパラメーターの設定を下記のように vi コマンド等で修正してください。

```
-----
IPMI_WATCHDOG=no
-----
```

2.2 OpenIPMI を自動起動できるように設定してください。

```
# chkconfig ipmi on
```

3. WDT (Watchdog Timer)更新プログラムを設定してください。

3.1 下記の例を参考に、WDT 更新プログラムを作成してください。

この例ではファイル名を「ResetWDT」とします。

```
-----
#!/bin/sh
sleep 60      ← ご使用中の環境に合わせて WDT 開始の待ち時間を設定してください。
/usr/bin/ipmitool raw 0x6 0x24 0x4 0x01 0xa 0x3e 0x08 0x07 > /dev/null 2>&1 *1
while true
do
  /usr/bin/ipmitool raw 0x6 0x22 > /dev/null 2>&1
  sleep 30    ← 更新間隔に相当。秒数で指定してください。この例では 30 秒です。
done
-----
```

*1 Set Watchdog Timer コマンド実行時の ipmitool の引数は以下のとおりです。

```
raw    ... IPMI コマンドを指定して実行する際の引数(固定)
0x6    ... NetFunction (固定)
0x24   ... Command (固定)
```

- NetFunction(0x6) と Command(0x24) の組合せで、
Set Watchdog Timer コマンドを表します。
- 0x4 ... Timer Use
OS 動作中のスツール監視のとき 0x4 から変更の必要はありません。
下位 3 ビットで、スツール監視のフェーズを表しています。
[2:0]
000b = reserved
001b = BIOS FRB2
010b = BIOS/POST
011b = OS Load
100b = SMS/OS
101b = OEM
上記以外 = reserved (使用しません)
- 0x01 ... Timer Actions
上位 4 ビットでタイムアウト発生時の動作設定をします。
[7] reserved
[6:4] pre-timeout interrupt
000b = none(何もしません)
001b = SMI (使用しません)
010b = NMI/Diagnostic Interrupt (NMI を発生します)
011b = Messaging Interrupt (使用しません)
上記以外 = reserved(使用しません)
下位 4 ビットでタイムアウト発生後の動作設定をします。
[3] reserved
[2:0] timeout action
000b = no action (何もしません)
001b = Hard Reset (リセットします)
010b = Power Down (DC OFF します)
011b = Power Cycle (DC OFF 後、DC ON します)
上記以外 = reserved(使用しません)
- 0xa ... Pre-timeout interval
タイムアウト検出からタイムアウト後の動作に移行するまでの
時間を 1 秒単位で指定します。0xa のときは 10 秒となります。
- 0x3e ... Timer Use Expiration flags clear
0x3e のまま、変更の必要はありません。
- 0x08 ... Initial countdown value, lsbyte(100ms/count)
- 0x07 ... Initial countdown value, msbyte
Initial countdown value で、カウントダウン時間を設定します。
BMC のウォッチドッグタイマー機能は、1 count は 100 ミリ秒単位と
なっているため、カウントダウン時間を 180 秒に設定するとき、
 $180 \times 10 = 1800$ (10 進数) = 0x0708(16 進数)
lsbyte, msbyte の順に引数に指定するので 0x08 0x07 の順となる。



使用するマシンの負荷状況によっては、OS がストール状態であっても、ウォッチドッグタイマーの更新ができずにタイムアウトが発生する可能性があります。ご使用環境にて高負荷状態での評価した上でストール監視を設定してください。



コマンドの詳細は IPMI 仕様の“Set Watchdog Timer Command”の章を参照してください。
<http://www.intel.com/design/servers/ipmi/>

3.2 WDT 更新プログラムを/usr/sbin ディレクトリ配下にコピーしてください。

```
# install -p -m 755 ResetWDT /usr/sbin
```

3.3 下記の例を参考に、WDT 更新プログラムの起動スクリプトファイル(以降「WDT 起動スクリプト」という)を作成してください。

この例ではファイル名を「watchdog」とします。

```
-----
#!/bin/sh
#
# chkconfig: - 27 46
# description: software watchdog
#
# Source function library.

### BEGIN INIT INFO
# Provides: watchdog
# Required-Start:
# Should-Start: ipmi
# Required-stop:
# Default-Start: 2 3 5
# Default-stop:
# Short-Description: watchdog
# Description: software watchdog
### END INIT INFO

prog=/usr/sbin/ResetWDT

case "$1" in
    start)
        echo -n "Starting watchdog daemon: "
        ${prog} &
        echo
        ;;
    *)
        echo "Usage: watchdog {start}"
        exit 1
        ;;
esac
-----
```

「prog=」に WDT 更新プログラム(この例では ResetWDT)の格納パスを指定してください。

3.4 上記の WDT 起動スクリプトを install コマンドでコピーしてください。

```
# install -p -m 755 watchdog /etc/init.d
```

3.5 WDT 更新プログラムを自動起動できるように設定してください。

```
# chkconfig --add watchdog
# chkconfig watchdog on
```



Windows OS 上で、上記のプログラムおよびスクリプトファイルを作成するときには、ご使用中の Linux に対応したコードに変換してください。

4. OS を再起動してください。再起動にてストール監視機能が有効となります。

reboot

■ストール監視機能を無効にする手順

root 権限のあるユーザーでログインして、設定をしてください。

1. WDT 更新プログラムを自動起動しないように設定してください。
2. OS を再起動してください。再起動にてストール監視機能が無効となります。

■ストール監視機能の関連モジュールを削除する手順

root 権限のあるユーザーでログインして、設定をしてください。

1. WDT 更新プログラムを自動起動しないように設定してください。
2. WDT 更新プログラムおよび WDT 起動スクリプトを削除してください。
3. OS を再起動してください。

2. コンフィグレーションツール

/opt/nec/esmpro_sa/tools 配下にコンフィグレーションツール(以降、本ツールと表記)を提供しています。



非サービスモードでは、監視サービスはインストールされないため、設定はできません。

1. 本ツールを使用するには、ESMPRO/ServerAgentService Ver.1.0 以降が動作している必要があります。
必ず、ESMPRO/ServerAgentService Ver.1.0 以降をインストールして、動作させてください。
2. 本ツールを使用するには、root 権限が必要です。
必ず、root 権限のあるユーザーでログインしてください。
3. 本ツールは複数同時に使用することはできません。
また、ESMPRO/ServerAgentService のコントロールパネル(ESMagntconf, ESMamsadm)も起動しない
てください。
4. 本ツールの設定を ESMPRO/ServerAgentService に反映するため、以下のどちらかを実行してください。
 - ・以下のコマンドを実行して、ESMPRO/ServerAgentService のサービスを再起動します。
/opt/nec/esmpro_sa/bin/ESMRestart
 - ・以下のコマンドを実行して、OS を再起動します。
reboot
5. 本ツールは、コマンドラインインターフェースを使用する特性により、シェルスクリプトから実行する
ことも可能ですが、以下のような点に注意してください。
 - ・1 行目には「#!/bin/bash」を記述します。
 - ・ファイルの保存時には改行コードを Linux 改行コード(LF)とします。
Windows 標準のテキストエディタ(メモ帳)では、ファイル保存時に改行コードを Windows 改行コー
ド(CR+LF)に変換して保存されます。
 - ・設定項目に日本語を使用する場合は、文字コードは OS に合わせ、euc や UTF-8 を使用します。

esmamset コマンド

コマンドラインインターフェースを使用して、ESMPRO/ServerAgentService が使用する通報の情報を設定し
ます。esmamset コマンドでは、以下を設定できます。

1. SNMP コミュニティー名の設定
2. 通報手段(SNMP)の有効/無効設定
3. 通報手段(SNMP)の通報先 IP アドレスの追加または削除
4. 通報手段(TCP_IP In-Band)の有効/無効設定
5. 通報手段(TCP_IP In-Band)の IP アドレスの追加または削除
6. 通報手段(TCP_IP In-Band)で使用するポート番号の設定
7. ESMPRO/ServerAgentService からのシステムシャットダウン 有効/無効の設定
8. Syslog 監視の監視間隔の設定
9. Syslog 監視の追加監視対象の設定
10. Syslog 監視のファイル監視対象の設定

esmsysrep コマンド

コマンドラインインターフェースを使用して、ESMPRO/ServerAgentService が監視する Syslog 監視対象イ
ベントを設定します。esmsysrep コマンドでは、以下を設定できます。

1. Syslog 監視対象イベントの追加
2. Syslog 監視対象イベントの変更
3. Syslog 監視対象イベントの削除

2.1 esmamset コマンド

機 能

コマンドラインインターフェースを使用して、ESMPRO/ServerAgentService が使用する通報の情報を設定します。esmamset コマンドでは、以下を設定できます。

1. SNMP コミュニティ名の設定
2. 通報手段(SNMP)の有効/無効設定
3. 通報手段(SNMP)の通報先 IP アドレスの追加または削除
4. 通報手段(TCP_IP In-Band)の有効/無効設定
5. 通報手段(TCP_IP In-Band)の IP アドレスの追加または削除
6. 通報手段(TCP_IP In-Band)で使用するポート番号の設定
7. ESMPRO/ServerAgentService からのシステムシャットダウン 有効/無効の設定
8. Syslog 監視の監視間隔の設定
9. Syslog 監視の追加監視対象の設定
10. Syslog 監視のファイル監視対象の設定

設 定

esmamset コマンドの使用方法は以下のとおりです。

esmamset コマンドで実行した設定を動作中の ESMPRO/ServerAgentService に反映するには、ESMPRO/ServerAgentService の再起動(ESMRestart)が必要です。

```
# cd /opt/nec/esmpro_sa/tools
# ./esmamset [OPTION]
:
# /opt/nec/esmpro_sa/bin/ESMRestart
```

```
Usage:
esmamset [-r <rackname>] [-c <community>]
        [--mi <second>] [--cmo <filename>] [--fmo <filename>]
        [-s ON|OFF] [-d <delip|ALLIP ...>] [-a <addip ...>]
        [-t ON|OFF] [-i <ip>] [-p <port>]
        [-o ON|OFF]
        [-f <filename>]
        [-P]
        [-h]
```



ESMPRO/ServerAgentService は、日本語(2 バイト)文字を EUC コードで管理しています。そのため、日本語文字の入力や表示をさせる場合は、ネットワーク経由(ssh コマンドなど)で別の日本語端末からログインし、一時的に LANG 環境変数を日本語環境に変更してください。

- 1)現在の LANG 環境変数を確認します。

```
# echo $LANG
```

- 2)LANG 環境変数を ja_jp.eucJP に変更します。

```
# export LANG=ja jp.eucJP
```

- 3)esmamset または esmsysrep コマンドを実行します。

```
# cd /opt/nec/esmpro_sa/tools/
```

```
# ./esmamset [OPTION]
# ./esmsysrep [OPTION]
:
# /opt/nec/esmpro sa/bin/ESMRestart
4)LANG 環境変数を 1) の値に戻します。
# export LANG=xxxxxxx
```

[OPTION] 指定

[OPTION] には以下のオプションを指定します。複数のオプションを同時に指定することもできます。設定する値にスペースが含まれるときは、前後に"(ダブルクォーテーション)を付加してください。

オプション	説明
-r <rackname>	ESMPRO/ServerAgentService では使用しません。
-c <community>	コミュニティ名を設定します。使用可能な文字は半角英数字、最大で 33 バイトまで指定できます。 snmpd.conf に設定されていないコミュニティ名を指定したときは、設定は変更されませんので、先に snmpd.conf を修正してください。
--mi <second>	Syslog 監視の監視間隔(秒)を設定します。設定範囲は 10~3600(秒)です。
--cmo <filename>	/var/log/messages を含まない syslog と同じフォーマットの追加で監視対象とするファイルをフルパスで指定します。最大で 255 バイトまで指定できます。
--fmo <filename>	/var/log/messages を含まないファイル監視対象とするファイルをフルパスで指定します。最大で 255 バイトまで指定できます。
-s ON OFF	通報手段(SNMP)の有効/無効を設定します。 ON :有効 / OFF :無効
-d <delip ...>	通報手段(SNMP)に指定されている通報先 IP アドレスを削除します。 半角スペースを空格、2 つ以上の IP アドレスを同時に削除することもできます。
-d <ALLIP>	通報手段(SNMP)に指定されている通報先 IP アドレスをすべて削除します。
-a <addip ...>	通報手段(SNMP)に指定されている通報先 IP アドレスを追加します。 半角スペースを空格、2 つ以上の IP アドレスを同時に追加することもできます。最大で 255 個の IP アドレスを指定できます。
-t ON OFF	通報手段(TCP_IP In-Band)の有効/無効を設定します。 ON :有効 / OFF :無効
-i <ip>	通報手段(TCP_IP In-Band)の通報先 IP アドレスを指定します。
-p <port>	通報手段(TCP_IP In-Band)で使用するポート番号を指定します。ファイアウォールを設定している場合は指定したポートを開放してください。
-o ON OFF	ESMPRO/ServerAgentService からのシステムシャットダウンの有効/無効を設定します。 ON :有効 / OFF :無効
-f <filename>	配置ファイルを指定して読み込み、ファイルに記載の内容にしたがって、各種設定をします。配置ファイルは後述します。 配置ファイルを読み込んだ時点で、成功と判断するため、配置ファイル内で指定されたオプションが不正であっても戻り値は 0 (成功)を返却します。
-P	設定内容を一覧で表示します。esmamset コマンドで実行した設定を動作中の ESMPRO/ServerAgentService に反映するには、ESMPRO/ServerAgentService の再起動(ESMRestart)が必要です。
-h	ヘルプ (Usage:)を表示します。

配置ファイル

[OPTION]で指定する内容が記載されたテキストファイルのことを指します。配置ファイルを `-f` オプションで指定して読み込むことで、[OPTION]を指定したときと同じことができます。

配置ファイルは

```
keyname "value"
```

の形式で記載します。keyname と ダブルクォート(")の間には空白(スペースかタブ)を入れてください。また、改行コードが Linux 改行コード(LF)となるように注意してください。Windows 改行コード(CR+LF)で保存されたテキストファイルのときは、配置ファイルの内容を正しく読み込むことができません。

keyname の説明は下表を参照してください。

keyname(大文字)	説明
RACKNAME	ESMPRO/ServerAgentService では使用しません。
COMMUNITY	<code>-c</code> オプションで指定する内容と同じです。
SYSLOG-MONITOR-INTERVAL	<code>--mi</code> オプションで指定する内容と同じです。
CUSTOM-MONITORING-OBJECT	<code>--cmo</code> オプションで指定する内容と同じです。
FILE-MONITORING-OBJECT	<code>--fmo</code> オプションで指定する内容と同じです。
SNMP	<code>-s</code> オプションで指定する内容と同じです。
DELIP	<code>-d</code> オプションで指定する内容と同じです。
ADDIP	<code>-a</code> オプションで指定する内容と同じです。
IN-BAND	<code>-t</code> オプションで指定する内容と同じです。
IN-BANDIP	<code>-i</code> オプションで指定する内容と同じです。
IN-BANDPORT	<code>-p</code> オプションで指定する内容と同じです。
SHUTDOWN	<code>-o</code> オプションで指定する内容と同じです。

戻り値

esmamset コマンドの戻り値は以下のとおりです。

戻り値	説明
0	設定に成功しました。
1	設定に失敗しました。指定されているオプションの内容を確認してください。
2	設定に失敗しました。ESMPRO/ServerAgentService をインストールしてください。
4	設定に失敗しました。ログインしているユーザーにコマンドの実行権限がありません。

エラーメッセージ

esmamset コマンドのエラーメッセージは以下のとおりです。

メッセージ	説明	戻り値
Usage:	HELP 情報を表示します。	0
%s: Setting succeed!	指定された項目が設定成功、%s は項目名です。	0
%s: Setting failed!	指定された項目が設定失敗、%s は項目名です。	1
System Error!	システムエラーが発生しました。	1
Usage:	オプションが存在しません。	1
Please input a valid rackname after "-r" option (length<=63).	"-r"(rackname)のパラメーターが取得できません。または、rackname が最大長(63 バイト)を超えています。	1
Please input a valid community after "-c" option (length<=33).	"-c"(community)のパラメーターが取得できません。または、community が最大長(33 バイト)を超えています。	1
[%s] was not found in snmpd.conf file! The community [%s] must be	インプットされた community は snmpd.conf には存在しない。%s はインプットした community で	1

メッセージ	説明	戻り値
set in snmpd.conf file.	す。	
Please input number range from 10 to 3600 after "--mi" option (Monitor Interval).	"--mi"(監視間隔)のパラメーターが取得できません。または、指定された値が無効(「10~3600」の数値)です。	1
Please input a readable file's name after "--cmo" option with full path (length<=255). And cannot be set "/var/log/messages".	"--cmo"(追加監視対象)のパラメーターが取得できません。追加監視対象のフルパスが必要で、読み込み権限が必要です。または、filename が最大長(255 バイト)を超えます。そして、「/var/log/messages」は設定できません。	1
Please input a readable file's name after "--fmo" option with full path (length<=255). And cannot be set "/var/log/messages".	"--fmo"(ファイル監視)のパラメーターが取得できません。ファイル監視のフルパスが必要で、読み込み権限が必要です。または、filename が最大長(255 バイト)を超えます。そして、「/var/log/messages」は設定できません。	1
The filenames of "File Monitoring Object (--fmo) and "Custom Monitoring Object (--cmo) must be different.	追加監視対象(--cmo)とファイル監視(--fmo)は、異なるファイルを指定する必要があります。	1
Please input ON or OFF after "-s" option (SNMP).	"-s"(SNMP)のパラメーターが取得できません。または、ON/OFF 以外の値が設定されています。	1
Please input valid IP address after "-d" option (SNMP).	削除したい IP が指定されない。"-d"のパラメーターが取得失敗しました。	1
Please input valid IP address after "-a" option (SNMP).	追加したい IP が指定されない。"-a"のパラメーターが取得失敗しました。	1
Please input ON or OFF after "-t" option (TCP_IP In-Band).	"-t"(TCP_IP In-Band)のパラメーターが取得できません。または、ON/OFF 以外の値が設定されています。	1
Please input valid IP address after "-i" option (TCP_IP In-Band).	"-i"(TCP_IP In-Band)のパラメーターが取得できません。または、IP アドレスが正しくありません。	1
Please input a port number range from 6001 to 65535 after "-p" option (TCP_IP In-Band).	"-p"(TCP_IP In-Band)のパラメーターが取得できません。または、指定されたポート番号が設定可能な範囲(6001~65535)と異なります。	1
Please input ON or OFF after "-o" option (Shutdown Delay).	シャットダウン開始"-o"(Shutdown Delay)のパラメーターが取得できません。または、ON/OFF 以外の値が設定されています。	1
Please input a config file after "-f" option.	設定ファイルを指定されていません。"-f" のパラメーターが取得できません。	1
Access %s failed!	ファイルのアクセスできません。%s は設定ファイル名です。	1
Skip the line in setting file, lineno=%d.	設定ファイルには問題があります。%d は設定ファイルの行番号です。	1
Please install ESMPRO/ServerAgentService.	ESMPRO/ServerAgentService がインストールされていません。	2
Please change to root user.	このツールを実行しているのは、root ユーザーではありません。	4

2.2 esmsysrep コマンド

機 能

コマンドラインインターフェースを使用して、ESMPRO/ServerAgentService が監視する Syslog 監視対象イベントを設定します。esmsysrep コマンドでは、以下を設定できます。

1. Syslog 監視対象イベントの追加
2. Syslog 監視対象イベントの変更
3. Syslog 監視対象イベントの削除

設 定

esmsysrep コマンドの使用方法は以下のとおりです。

esmsysrep コマンドで実行した設定を動作中の ESMPRO/ServerAgentService に反映するには、ESMPRO/ServerAgentService の再起動(ESMRestart)が必要です。

```
# cd /opt/nec/esmpro_sa/tools
# ./esmsysrep [ACTION] [SOURCE] [EVENT] [OPTION]
:
# /opt/nec/esmpro_sa/bin/ESMRestart
```

Usage:

```
esmsysrep --add -S <sourcename> -E <eventid> -K <keyword1> [OPTION]...
esmsysrep --mod -S <sourcename> -E <eventid> [-K <keyword1>] [OPTION]...
esmsysrep --del -S <sourcename> -E <eventid>
esmsysrep --list
esmsysrep --help
```

Action-selection option and specification:

```
--help    Show this help message
--list    List all event id's information
--add     Add an event id
--mod     Change the configuration of event id
--del     Delete an event id
```

Common option and specification:

```
-S <sourcename>    Specify the source name
-E <eventid>       Specify the event id
-K, -1 <keyword1> Specify the first keyword, and the argument of
                  -K will be used if -1 and -K are both specified.
                  It can't be omitted when --add is specified.
```

Other options(defaults in [] will be used if the options are not specified in --add):

```
-2 <keyword2>      Specify the second keyword. ["" ]
-3 <keyword3>      Specify the third keyword. ["" ]
-s <ON|OFF>        Set ON/OFF of the SNMP report method. [ON]
-i <ON|OFF>        Set ON/OFF of the TCP/IP IN-BAND report method. [OFF]
-o <ON|OFF>        Set ON/OFF of the TCP/IP OUT-OF-BAND report method. [OFF]
-t <trapname>      Set the trap name. ["" ]
```

```
-d <dealmethod>      Set the deal method. [""]  
-w <watchtime>       Set the watch time. ["0-24"]  
-c <reportcount>     Set the report count. [1]  
-r <NONE|SHUTDOWN|REBOOT> Set the action after a report. [NONE]
```



ESMPRO/ServerAgentService は、日本語(2 バイト)文字を EUC コードで管理しています。そのため、日本語文字の入力や表示をさせる場合は、ネットワーク経由(ssh コマンドなど)で別の日本語端末からログインし、一時的に LANG 環境変数を日本語環境に変更してください。

1)現在の LANG 環境変数を確認します。

```
# echo $LANG
```

2)LANG 環境変数を ja_jp.eucJP に変更します。

```
# export LANG=ja jp.eucJP
```

3)esmamset または esmsysrep コマンドを実行します。

```
# cd /opt/nec/esmpro sa/tools/
```

```
# ./esmamset [OPTION]
```

```
# ./esmsysrep [OPTION]
```

```
:
```

```
# /opt/nec/esmpro sa/bin/ESMRestart
```

4)LANG 環境変数を 1) の値に戻します。

```
# export LANG=xxxxxx
```

コマンド使用例

```
# ./esmsysrep --add -S TESTSOURCE -E 80000123 -K "test1234" -t " test trap"  
# /opt/nec/esmpro_sa/bin/ESMRestart
```

上記の例では、

- ・ソース名"TESTSOURCE"に、"80000123"のイベント ID を新規追加します。
- ・ESMPRO/ServerAgentService のサービスの再起動後、syslog(/var/log/messages)に、文字列"test1234"が記録されると、Syslog 監視機能にて検出し、イベント ID:80000123 を SNMP で通報します。
- ・アラートビューアで表示するトラップ名は" test trap"となります。

[ACTION] 指定

[ACTION] には以下のオプションを指定します。省略することはできません。

また、複数のオプションを同時に指定することはできません。

オプション	説明
--add	Syslog イベントを追加します。
--mod	既存の Syslog イベントを変更します。
--del	Syslog イベントを削除します。
--list	Syslog イベントの一覧を CSV 形式(コンマ区切り)で出力します。 "Source", "EventID", "KeyWord1", "KeyWord2", "KeyWord3", "Manager", "ALIVE (ALIVELevel)", "TrapName", "DealMethod", "WatchTime", "ReportCount", "AfterReport"
Source	アラートビューアで表示するソースを表示します。
EventID	アラートビューアで表示するイベント ID を表示します。
KeyWord1	Syslog 監視の通報対象文字列であるキーワード 1 を表示します。
KeyWord2	Syslog 監視の通報対象文字列であるキーワード 2 を表示します。

オプション	説明
KeyWord3	Syslog 監視の通報対象文字列であるキーワード 3 を表示します。
Manager	通報手段(SNMP)の有効または無効を表示します。 ON : 有効 / OFF : 無効
ALIVE (ALIVELevel)	エクスプレス通報サービスの有効または無効を表示します。 ON : 有効 / OFF : 無効 (通報レベルを表示します)
TrapName	アラートビューアで表示するトラップ名を表示します。
DealMethod	アラートビューアで表示する対処を表示します。
WatchTime	監視時間帯を表示します。
ReportCount	監視時間帯における、通報に必要な該当イベントの発生回数を 1~65535 の数字で表示します。
AfterReport	通報後の動作を表示します。 NONE : 何もしない SHUTDOWN: シャットダウン REBOOT : 再起動
--help	ヘルプ (Usage:)を表示します。

[SOURCE] 指定

[SOURCE] には以下のオプションを指定します。省略することはできません。

オプション	説明
-S <sourcename>	[ACTION]の対象となるソース名を半角英数字の大文字で指定します。

[EVENT] 指定

[EVENT] には以下のオプションを指定します。省略することはできません。

オプション	説明
-E <eventid>	<p>Syslog イベントを追加する場合、以下の命名規則にしたがって、[ACTION] の対象となるイベント ID を 16 進数(半角英数字 0~F)の 8 桁で指定します。</p> <p>＜監視イベント ID 命名規則＞</p> <p>“x0000yyy”形式で指定します。(例：40000101、800002AB、C0000101)</p> <p>“x”には、4,8,Cの中から設定します。それぞれの意味は以下のとおりです。</p> <ul style="list-style-type: none"> 4 : 情報系イベントを意味します。 ESMPRO/ServerManager のアラートビューアのアイコンが「緑色」で表示されます。 8 : 警告系イベントを意味します。 ESMPRO/ServerManager のアラートビューアのアイコンが「黄色」で表示されます。 C : 異常系イベントを意味します。 ESMPRO/ServerManager のアラートビューアのアイコンが「赤色」で表示されます。 <p>“yyy”には、0x001(1)~0xFFFF(4095)の範囲内で任意の 16 進数値を設定します。</p> <p>Syslog イベントを変更・削除する場合、該当するイベント ID を指定します。</p>

[OPTION] 指定

[OPTION] には以下のオプションを指定します。複数のオプションを同時に指定することもできます。
設定する値にスペースが含まれるときは、前後に" (ダブルクォーテーション) を付加してください。

オプション	説明
-K <keyword1> -1 <keyword1>	keyword1 を設定します。256 バイト以内の 1 バイト文字を使用します。-K と -1 を同時に指定したときは、-K の内容が設定されます。 [ACTION]が--add のときは省略することができません。
-2 <keyword2>	keyword2 を設定します。256 バイト以内の 1 バイト文字を使用します。 [ACTION]が--add のときの既定値は、""(空白)です。
-3 <keyword3>	keyword3 を設定します。256 バイト以内の 1 バイト文字を使用します。 [ACTION]が--add のときの既定値は、""(空白)です。
-s ON OFF	通報手段(SNMP)の有効または無効を設定します。 ON : 有効 / OFF : 無効 [ACTION]が--add のときの既定値は、"ON"です。
-i ON OFF	通報手段(TCP_IP In-Band)の有効または無効を設定します。 ON : 有効 / OFF : 無効 [ACTION]が--add のときの既定値は、"OFF"です。
-o ON OFF	通報手段(TCP_IP Out-of-Band)の有効または無効を設定します。 ON : 有効 / OFF : 無効 [ACTION]が--add のときの既定値は、"OFF"です。
-t <trapname>	アラートビューアで表示するトラップ名を設定します。79 バイト以内の文字列で、1 バイトまたは 2 バイト文字が使用できます。日本語も使用できます。 [ACTION]が--add のときの既定値は、""(空白)です。
-d <dealmethod>	アラートビューアで表示する対処を設定します。507 バイト以内の文字列で、1 バイトまたは 2 バイト文字が使用できます。日本語も使用できます。 [ACTION]が--add のときの既定値は、""(空白)です。
-w <watchtime>	監視時間帯を設定します。複数の時間帯を指定するときは、コンマ(,)区切りで設定します。 [ACTION]が--add のときの既定値は、"0-24"です。
-c <reportcount>	監視時間帯における、通報に必要な該当イベントの発生回数を 1~65535 の数字で設定します。 [ACTION]が--add のときの既定値は、"1"です。
-r <NONE SHUTDOWN REBOOT>	通報後の動作を設定します。<action>は以下のいずれかを設定します。 NONE : 何もしない SHUTDOWN: シャットダウン REBOOT : 再起動 [ACTION]が--add のときの既定値は、"NONE"です。

戻り値

esmsysrep コマンドの戻り値は以下のとおりです。

戻り値が 0 以外の場合は、コンソールにエラーメッセージを表示します。

戻り値	説明
0	設定に成功しました。
0 以外	設定に失敗しました。詳細はエラーメッセージを参照してください。

エラーメッセージ

esmsysrep コマンドのエラーメッセージは以下のとおりです。

メッセージ	説明	戻り値
Only root can execute the tool.	ログインしているユーザーに実行権限がありません。	1
プログラム名: error while loading shared libraries: ライブラリーの	ESMPRO/ServerAgentService がインストールされていません。	127

メッセージ	説明	戻り値
パス: cannot open shared object file: No such file or directory		
parameter error : "オプション名" is not specified.	省略不可の"オプション名"が指定されていません。	1
parameter error : argument of "オプション名" is too long.	"オプション名"に指定したパラメーターの文字列長が長すぎます。	1
parameter error : argument of "オプション名" is too short.	"オプション名"に指定したパラメーターの文字列長が短すぎます。	1
parameter error : argument of "オプション名" is invalid.	"オプション名"に指定したパラメーターは無効です。	1
parameter error : option "オプション名" requires an argument.	"オプション名"にパラメーターが指定されていません。	1
parameter error : invalid option "オプション名".	"オプション名"に指定したオプションは無効です。	1
parameter error : "オプション名".	"オプション名"に指定したオプションが不正です。	1
Can't make all of the keywords empty.	--mod の設定を反映すると、キーワード(1~3)が、すべて""(空白)となります。	1
Can't access "<sourcename>", which isn't the object source of this tool.	本コマンドで設定できないソース名が指定されました。	1
ESMntserver service is not started.	ESMntserver が起動していません。	1
Other program is accessing the syslog events setting.	他のプログラム(ESMamsadm など)が syslog 設定にアクセスしているため、アクセスできません。	1
"<sourcename>/<eventid>" already exists.	--add で指定したソース名/イベント ID は、すでに存在しています。	1
"<sourcename>/<eventid>" doesn't exist.	--mod または --del で指定したソース名/イベント ID は存在しません。	1
Access the "<sourcename>/<eventid>" failed.	[ACTION]に失敗しました。	1

3. ツールについて

ツールを使用するには、root ユーザーでログインしてください。

3.1 障害情報採取ツール(collectsa.sh)

機 能

本機または ESMPRO/ServerAgentService で発生した問題を調査するため、本機情報を収集します。

使 用 方 法

障害情報採取ツールの使用方法是以下のとおりです。

- 1) root ユーザーでログインします。
- 2) 任意のディレクトリに移動します。
- 3) 障害情報採取ツールを実行します。
CIM プロバイダの情報を採取するため、root のパスワードを入力します。
採取される情報に入力されたパスワードは含まれません。

```
# /opt/nec/esmpro_sa/tools/collectsa.sh -auth
Enter password for root :
```

カレントディレクトリに collectsa.tgz が作成されます。

- 4) NEC カスタマーサポートセンター経由でお問い合わせください。
NEC カスタマーサポートセンターの案内にしたがって、collectsa.tgz の提供をお願いします。

障害情報採取ツールの動作に問題が発生した場合

障害情報採取ツールが正しく動作しない(終了しない等)場合は、採取済みの情報を採取の上、NEC カスタマーサポートセンター経由でお問い合わせください。

- 1) 障害情報採取ツールを終了させます。
 - 1-1) 障害情報採取ツールを実行しているターミナルで、<Ctrl>+<C>キーを押します。
 - 1-2) 障害情報採取ツールが終了したことを確認します。

```
# ps aux | grep collectsa.sh |grep -v grep
```

たとえば下記のように表示された場合、collectsa.sh はバックグラウンドで実行されています。

```
root 11313 0.0 0.4 4196 1124 pts/0 T 14:46 0:00 /bin/bash ./collectsa.sh
```
 - 1-3) バックグラウンドで実行されていた場合は、プロセスを終了させます。

```
# kill -9 {pid}
```

(例) # kill -9 11313
- 2) カレントディレクトリに作成された collectsa ディレクトリを tgz 形式で圧縮します。

```
# tar czvf collectsa_dir.tgz collectsa/
```
- 3) NEC カスタマーサポートセンター経由でお問い合わせください。
NEC カスタマーサポートセンターの案内にしたがって、collectsa_dir.tgz の提供をお願いします。

3.2 必須パッケージチェックツール(check_packages.sh)

機 能

ESMPRO/ServerAgentService の動作に必要なパッケージを確認します。

OS インストール媒体をマウントするなど、必要なパッケージが格納されたディレクトリを準備できる場合、インストールすることも可能です。

使 用 方 法

```
root ユーザーでログインします。
# cd {check_packages.sh が格納されたディレクトリ}
【必須パッケージを確認する手順】
# sh ./check_packages.sh
【必須パッケージをインストールする手順】
# sh ./check_packages.sh -i {必要なパッケージが格納されたディレクトリ}
```

check_packages.sh が格納されたディレクトリは、インストールに使用する媒体により異なります。

EXPRESSBUILDER の場合 : {レビジョン}/lnx/pp/esmpro_sas/check_pkg/

Starter Pack の場合 : software/{レビジョン}/lnx/pp/esmpro_sas/check_pkg/

Web サイトからダウンロードした ZIP ファイルの場合 : check_pkg/

メ ッ セ ー ジ ー 覧

情報

{パッケージ名} ({アーキテクチャー}) package [{OK か NG}]
必須パッケージがインストールされている場合、"[OK]"
必須パッケージがインストールされていない場合、"[NG]"と表示します。

All packages are installed successfully.
必須パッケージのインストールに成功しました。

Please install the package of [NG].
必須パッケージチェックに表示します。
[NG]のパッケージをインストールしてください。

The package of [NG] will be installed.
必須パッケージをインストールする前に表示します。
[NG]のパッケージをインストールします。

Usage: {ツールのファイル名} [-i directory]
-i directory Install necessary packages those are not installed.
Directory is rpm packages's directory.
必須パッケージチェックツールの使用方法を表示します。

エラー

ERROR: Install {パッケージ名} failed, please confirm {ログファイル名} for detail information.
rpm コマンドで{パッケージ名}のインストールでエラーとなりました。

ログファイルの内容を確認し、対処してください。

ERROR: Install perl packages failed, please confirm {ログファイル名} for detail information.
rpm コマンドで perl パッケージのインストールでエラーとなりました。
ログファイルの内容を確認し、対処してください。

ERROR: Not found {RPM パッケージが格納されたディレクトリ} directory.
RPM パッケージが格納されたディレクトリが見つかりません。
check_packages.sh の引数が間違えていないか確認してください。

ERROR: Not found {フルパスの RPM パッケージ名}
RPM パッケージが格納されたディレクトリにインストールすべき
RPM パッケージが見つかりません。
表示されている RPM パッケージ名が存在するか確認してください。
アーキテクチャーまで一致する必要があります。

ERROR: The file {リストファイル名} is not exist. So exit.
必須パッケージのリストファイルが見つかりません。
リストファイルの格納先を確認してください。

ERROR: This architecture is not supported. So exit.
本ツールがサポートしていないアーキテクチャーです。
<https://www.support.nec.co.jp/View.aspx?id=3170102037>
→必須パッケージ一覧を参照し、必須パッケージの確認と不足している
RPM パッケージをインストールしてください。

ERROR: This kernel is not supported. So exit.
本ツールがサポートしていないカーネルバージョンです。
<https://www.support.nec.co.jp/View.aspx?id=3170102037>
→必須パッケージ一覧を参照し、必須パッケージの確認と不足している
RPM パッケージをインストールしてください。

ESMPRO/ServerAgentService Ver. 2

5

注意事項

ESMPRO/ServerAgentService の注意事項について説明します。

1. ESMPRO/ServerAgentService

2. Red Hat Enterprise Linux

「対象」に OS の Update や SP、バージョンを記載していないときは、Update や SP、バージョンに依存せず対象となります。

Linux サポート情報リストに、各ディストリビューションの注意・制限事項を公開しておりますので、こちら
も参照してください。

■Linux サポート情報リスト【Linux サービスセットご契約のお客様限定】

<https://www.support.nec.co.jp/View.aspx?id=3140001278>

1. ESMPRO/ServerAgentService

ESMPRO/ServerAgentService またはディストリビューションが限定されない OS に関する注意事項です。

ESMPRO/ServerAgentServiceの仕様

ESMPRO/ServerManagerのネットワーク情報の一部が"Unknown"と表示される場合がある

<追加> 10.201.04-030.05

対象：ESMPRO/ServerAgentService バージョン 2.0.5-0 以前(2.0.2-1 を除く)

詳細：ESMPRO/ServerAgentService がメモリ領域を拡張する際の処理に問題があり、ESMPRO/ServerManager の [構成情報] - [ネットワーク] - 各インターフェース配下の [一般情報] で表示される [タイプ] と [物理アドレス] が、"Unknown"と表示される場合があります。対象のインターフェースは、ネットワークインターフェースの数が 10 個以上ある環境で、10 番目、20 番目(10x2)、40 番目(20x2)、80 番目(40x2)...番目のインターフェースです。

表示のみの影響であり、その他の ESMPRO/ServerManager の表示や、ESMPRO/ServerAgentService の監視機能・通報機能に影響はありません。

対処：修正済みの ESMPRO/ServerAgentService バージョン 2.0.2-1、または、2.0.6-0 以降にアップグレードしてください。

ご使用環境に応じた最新バージョンが修正済みのバージョンかどうかは、以下のコンテンツから確認してください。

■モジュール、ドキュメントのダウンロードコンテンツ情報

<https://www.support.nec.co.jp/View.aspx?id=3140105860>

修正済みのバージョンが公開されていない場合は、監視対象サーバーにログインし、ifconfig コマンドを実行することで[タイプ]と[物理アドレス]を確認することができます。

ESMPRO/ServerManager で"Unknown"と表示されるインターフェース名を元に、

ifconfig 結果で合致するインターフェース(以下例の★1)を確認してください。

以下例の★2 が[タイプ]に該当し、★3 が[物理アドレス]に該当します。

```
ens3f3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
★1  inet xxx.xxx.xxx.xxx netmask xxx.xxx.xxx.xxx broadcast xxx.xxx.xxx.xxx
    inet6 fe80::d5fa:4509:a43a:d95 prefixlen 64 scopeid 0x20<link>
    ether 1c:1b:0d:fa:7f:a2 txqueuelen 1000 (Ethernet)
        ★3                                ★2
RX packets 243570 bytes 20733215 (19.7 MiB)
RX errors 0 dropped 1083 overruns 0 frame 0
TX packets 8 bytes 624 (624.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
device memory 0xc5800000-c58fffff
```

OSやESMPRO/ServerAgentService停止時に、syslogにsegfaultやcore出力のメッセージが発生するときがある

<追加> 10.201.04-030.05

対象：すべての ESMPRO/ServerAgentService バージョンで、ESMPRO/ServerManager に未登録のとき

詳細：OS や ESMPRO/ServerAgentService 停止時に、サービスの停止タイミングにより、

syslog に以下のメッセージが記録されるときがあります。

「XXXXX」は、状況により異なります。

```
kernel: cimprovagt[XXXXXX]: segfault at XXXXX ip XXXXX sp XXXXX error XXXXX
```

```
abrt[XXXXXX]: Saved core dump of pid XXXXX to /var/opt/nec/pfc/core/cimprova  
gt-XXXXX.core at /var/lib/Pegasus/cache/trace (XXXXX bytes)
```

OS や ESMPRO/ServerAgentService 停止時にのみ発生する現象であり、次回の OS またはサービス起動時の動作に影響はありません。

対処：ESMPRO/ServerManager に ESMPRO/ServerAgentService を登録してください。

ESMPRO/ServerManager を使用しない場合は、内部ファイルを修正します。

- 1) root ユーザーでログインします。
- 2) /opt/nec/esmpro_sa/data/monitor.ini を、以下のように変更します。
サービスやシステムの再起動は不要です。

```
[CimAlert]
RetryCount=0
WaitTime=0
```

ファイルシステム監視スレッドの監視対象となるドライブ

対象：すべての ESMPRO/ServerAgentService バージョンでサービスモードのとき

詳細：ファイルシステム監視スレッドの空き容量監視対象となるドライブは、次の条件に一致するドライブとなります。

- ・全容量 : 100MB 以上
- ・ドライブタイプ : Fixed
- ・ファイルシステムタイプ : ext2、ext3、ext4、xfs

アンマウントした時に、ファイルシステムの情報を誤検出するときがある

対象：すべての ESMPRO/ServerAgentService バージョンでサービスモードのとき

詳細：ファイルシステム監視スレッドは、監視間隔毎にマウントポイントを確認し、ファイルシステム情報を取得しています。監視中にマウントポイントがアンマウントされた場合、正常なファイルシステム情報が取得出来ません。

対処：アンマウント前に一時的にファイルシステム監視スレッドを停止します。

以下の手順 4) と手順 7) にある ESMPRO/ServerAgentService を再起動すると、ファイルシステム監視以外の ESMPRO/ServerAgentService が提供している監視機能がすべて再起動されます

<手順>

- 1) root 権限のあるユーザーでログインします。
- 2) /opt/nec/esmpro_sa/data/class.xml をバックアップします。
- 3) /opt/nec/esmpro_sa/data/class.xml から ESM_FileSystemThread の<Class>～</Class>までの記載を削除します。
- 4) 以下のコマンドで ESMPRO/ServerAgentService を再起動します。
/opt/nec/esmpro_sa/bin/ESMRestart
- 5) ファイルシステムをアンマウントします。
- 6) 手順 2) でバックアップしたファイルをリストアします。
- 7) 以下のコマンドで ESMPRO/ServerAgentService を再起動します。
/opt/nec/esmpro_sa/bin/ESMRestart

アンマウントしたファイルシステムの空き容量監視しきい値について

対象：すべての ESMPRO/ServerAgentService バージョンでサービスモードのとき

詳細：ファイルシステム監視スレッドが動作中にアンマウント/マウントしたドライブの空き容量しきい値は、アンマウント時に監視対象から外れたときに初期値を設定する場合があります。

対処：ファイルシステムのアンマウント/マウント操作時、一時的にファイルシステム監視スレッドを停止し

ます。

以下の手順 4)と手順 7)にある ESMPRO/ServerAgentService を再起動すると、ファイルシステム監視以外の ESMPRO/ServerAgentService が提供している監視機能がすべて再起動されます

<手順>

- 1) root 権限のあるユーザーでログインします。
- 2) /opt/nec/esmpro_sa/data/class.xml をバックアップします。
- 3) /opt/nec/esmpro_sa/data/class.xml から ESM_FileSystemThread の<Class>~</Class>までの記載を削除します。
- 4) 以下のコマンドで ESMPRO/ServerAgentService を再起動します。
/opt/nec/esmpro_sa/bin/ESMRestart
- 5) ファイルシステムをアンマウント/マウントします。
- 6) 手順 2)でバックアップしたファイルをリストアします。
- 7) 以下のコマンドで ESMPRO/ServerAgentService を再起動します。
/opt/nec/esmpro_sa/bin/ESMRestart

USBフロッピーディスクが空き容量しきい値設定対象となる

対象：Linux OS

詳細：USB フロッピーディスクをマウントすると、ドライブタイプが"Fixed"となる場合があります。

[ESMPRO/ServerAgentService 設定]-[ファイルシステム]-[しきい値]に表示するドライブは、ドライブタイプが"Fixed"のファイルシステムを表示しますが、フロッピーディスクの容量は 100MB 未満であるため空き容量の状態は監視せず、しきい値も変更することはできません。

ESMamvmainが高負荷となるときがある

対象：すべての ESMPRO/ServerAgentService バージョンでサービスモードのとき

詳細：ESMamvmain サービスは Syslog 監視機能を提供しています。syslog(/var/log/messages)などの監視対象となっているファイルに書き込みが多い場合は、ESMamvmain サービスも高負荷となります。

対処：監視対象となっているファイルの書き込みを抑止してください。

OSまたはサービス起動時に、ESMsmsrvサービスが停止するときがある

対象：すべての ESMPRO/ServerAgentService バージョンでサービスモードのとき

詳細：ESMPRO/ServerAgentService は OpenIPMI ドライバーを使用して、Baseboard Management Controller(BMC)からハードウェアの情報を取得します。

ESMPRO/ServerAgentService 以外に BMC へアクセスするソフトウェアが存在すると競合が発生し、ESMsmsrv サービスが停止するときがあります。また、ESMPRO/ServerAgentService が初めて起動した時と Sensor Data Record(SDR)が更新された場合に、すべての SDR データにアクセスする動作となるため、競合が発生しやすくなります。

弊社は、センサーが多く存在する装置で、ESMPRO/ServerAgentService がすべての SDR へアクセスする場合の処理と ipmiutil の処理で競合が発生する事を確認しております。この時、ESMsmsrv サービスが停止しますが、ipmiutil の処理は完了します。そのため、次回の ESMsmsrv サービスが起動する時に競合は発生しません。

ESMPRO/ServerAgentService 以外に BMC へアクセスするソフトウェアを使用される場合は、十分な評価を実施の上、運用を開始するようお願いします。

対処：以下のコマンドを実行して、ESMPRO/ServerAgentService のサービスを再起動します。

```
# /opt/nec/esmpro_sa/bin/ESMRestart
```

NMIボタンを押したときに、syslogにメッセージが記録されるときがある

対象：すべての ESMPRO/ServerAgentService バージョンでサービスモードのとき

詳細：NMI ボタンを押したとき、ESMsmsrv サービスが処理をするタイミングにより、syslog にメッセージが記録されるときがあります。

```
ESMsmstrv: ###ERR###RPC###: RPC: プログラムが登録されていません
```

対処: NMI ボタンでシステム停止する場合に発生する現象であり、次回の OS 起動時の動作に影響はありません。

他製品から SEL クリアされると通報が漏れるときがある

対象: BMC 対象装置で、すべての ESMPRO/ServerAgentService バージョンでサービスモードのとき

詳細: ESMPRO/ServerAgentService は、新しい SEL の記録がないかを 1 分間隔で確認します。

ESMPRO/ServerAgentService が確認した後から次の確認までの 1 分間に他製品から SEL クリアされると、ESMPRO/ServerAgentService が読み込んでいない SEL はクリアされ通報できません。

対処: 他製品から SEL クリアしないように注意してください。

EXPRESSSCOPE エンジン 3 や BMCConfiguration の SEL 領域 Full 時の動作で"古い SEL を上書き"から別の設定または別の設定から"古い SEL を上書き"へ変更した場合、SEL はクリアされます。

rpcbind と network サービスについて

対象: すべての ESMPRO/ServerAgentService バージョン

詳細: ESMPRO/ServerAgentService では、rpcbind と network サービスの機能を利用しています。

ESMPRO/ServerAgentService 運用中に rpcbind と network サービスの停止や再起動をされたとき、ESMPRO/ServerAgentService は正常に動作できません。

対処: 以下のコマンドを実行して、ESMPRO/ServerAgentService のサービスを再起動します。

```
# /opt/nec/esmpro_sa/bin/ESMRestart
```

OS またはサービス停止時に、syslog にメッセージが記録されるときがある

対象: すべての ESMPRO/ServerAgentService バージョンでサービスモードのとき

詳細: OS またはサービス停止時、syslog に以下のメッセージが記録されるときがあります。「XXXXXX」は英数字で、状況により異なります。

```
###ERR###RPC###: RPC XXXXX
```

対処: OS またはサービス停止時のみに発生する現象であり、次回の OS またはサービス起動時の動作に影響はありません。

OS 起動時の SNMP 通報遅延が発生するときがある

対象: すべての ESMPRO/ServerAgentService バージョンでサービスモードのとき

詳細: OS 起動時に通報の準備ができていない時に通報対象の現象が発生したとき、リトライ処理をします。

通報対象の現象が発生するタイミングにより、OS 起動時に通報されるときとリトライ(5 分)後に通報されるときがあります。

対処: OS が起動してから 5 分以上経過後に、アラートビューアへ表示されるメッセージを確認してください。

SNMP 通報の通報手段が有効でないときにも SNMP 通報が送信されるときがある

対象: すべての ESMPRO/ServerAgentService バージョンでサービスモードのとき

詳細: OS 起動時に通報の準備ができていない時に通報対象の現象が発生したとき、リトライ処理をします。

リトライ処理は、SNMP の通報手段(ON/OFF)に関係なく通報を処理するため、リトライ処理をするタイミングでトラップ通報先 IP が設定されたとき、SNMP 通報の通報手段が OFF のときでも通報します。

対処: 通報させたくないとき、OS 起動後 5 分以上経ってから設定してください。

障害情報採取ツールを実行中にコンソールの表示または syslog にメッセージが記録されるときがある

詳細：障害情報採取ツール(collectsa.sh)を実行中、コンソールの表示または syslog に以下のメッセージが記録されることがあります。

```
BUG: scheduling while atomic: kipmi0
```

collectsa.sh では ipmitool を使用して情報を採取する処理があり、ipmi ドライバーの既知問題が発生した場合にメッセージが記録されます。ipmi ドライバーの排他制御方法に問題があるため、システムの動作状況や、現象発生タイミングによっては、運用中にカーネルパニックなどの致命的な問題が発生する可能性があります。この不具合は、kernel-2.6.32-504.el6 以降のカーネルで修正されておりますので、カーネルアップデートをご検討ください。

■System logs include a message similar to "kernel: BUG: scheduling while atomic: kipmi0"

<https://access.redhat.com/solutions/691403>

■BUG: scheduling while atomic in acpi_ipmi

<https://access.redhat.com/solutions/656603>

```
kernel: process 'sysctl' is using deprecated sysctl (syscall)
net.ipv6.neigh.vswif0.base_reachable_time; Use
net.ipv6.neigh.vswif0.base_reachable_time_ms instead.
kernel: process 'cp' is using deprecated sysctl (syscall)
net.ipv6.neigh.vswif0.base_reachable_time; Use
net.ipv6.neigh.vswif0.base_reachable_time_ms instead.
kernel: process 'cp' is using deprecated sysctl (syscall)
net.ipv6.neigh.default.retrans_time; Use
net.ipv6.neigh.default.retrans_time_ms instead.
```

カーネルパラメータの名称が変更されることを示す警告です。旧名称のカーネルパラメータにアクセスしたことを示すメッセージです。システムのエラーを示すものではなく、システムへの影響はありません。

```
kernel: ACPI Error: No handler for Region [OEM2] (ffff88105999d780) [IPMI]
(20090903/evregion-319)
kernel: ACPI Error: Region IPMI(7) has no handler (20090903/exfldio-295)
kernel: ACPI Error (psparse-0537): Method parse/execution failed
[¥_SB_.PMI0._PMM] (Node ffff88105999f470), AE_NOT_EXIST
```

「/sys/bus/acpi/devices/ACPI000D:00/power1_average」を含む、/sys/bus 配下の全ファイル(サブディレクトリ含む)をコピーしていることが原因です。ACPI テーブルの IPMI 領域を介した電源管理機能が利用できないことを示すメッセージです。システムのエラーを示すものではなく、システムへの影響はありません。

```
kernel: netlink: 12 bytes leftover after parsing attributes.
```

snmpd からカーネルに渡されたデータが規定より 12byte 長いことを示すメッセージです。システムのエラーを示すものではなく、システムへの影響はありません。

■[RHEL6]注意・制限事項

<https://www.support.nec.co.jp/View.aspx?id=3140100260>

ID:06225 syslog に netlink 関連のメッセージが出力されることがあります。

```
kernel: CPUFREQ: ondemand sampling_rate_max sysfs file is deprecated - used
by: cp
kernel: CPUFREQ: Per core ondemand sysfs interface is deprecated -
sampling_rate_max
kernel: CPUFREQ: Per core ondemand sysfs interface is deprecated -
sampling_rate_min
kernel: CPUFREQ: Per core ondemand sysfs interface is deprecated -
sampling_rate
kernel: CPUFREQ: Per core ondemand sysfs interface is deprecated - up_threshold
kernel: CPUFREQ: Per core ondemand sysfs interface is deprecated -
ignore_nice_load
kernel: CPUFREQ: Per core ondemand sysfs interface is deprecated -
powersave_bias
```

sys/devices/system/cpu/cpu0/cpufreq/ondemand/配下の将来廃止される予定のファイルにアクセスしたことを示すメッセージです。システムのエラーを示すものではなく、システムへの影響はありません。

■[RHEL6]注意・制限事項

<https://www.support.nec.co.jp/View.aspx?id=3140100260>

ID:06122 syslog に CPUFREQ 関連のメッセージが出力されることがあります。

```
kernel: mbox_read: Bad State
kernel: mbox_read: Bad State
```

lpfc ドライバーが作成した/sys/class/scsi_host/hostX 配下のファイルにアクセスしたことを示すメッセージです。システムのエラーを示すものではなく、システムへの影響はありません。

■https://www.express.nec.co.jp/linux/supported-driver/faq/fibre/faq_fibre_0009.html

Q&A > Fibre Channel コントローラ > 「kernel: mbox_read: Bad State」と表示される原因について

WebSAM AlertManagerとの通報連携するためには、レジストリーを登録する

対象：すべての ESMPRO/ServerAgentService バージョン

詳細：Syslog イベントの設定で追加したイベントを WebSAM AlertManager で通報連携するとき、ESMPRO/ServerManager をインストールしたマシンに、以下のレジストリーを登録してください。

対処：レジストリーに以下のキー、名前、データを設定してください。

xxxx が新しく設定するアラートタイプの名前です。

アラートタイプ(xxxx)には以下を設定してください。

- ・ Syslog 監視で設定した通報ソース名
Syslog 監視では、通報ソース名がアラートタイプに変換されるため。
- ・ 以下のアラートタイプ
AM

64bit OS では、以下の記述の HKEY_LOCAL_MACHINE¥SOFTWARE¥NEC を HKEY_LOCAL_MACHINE¥SOFTWARE¥Wow6432Node¥NEC に読み替えてください。

```
[HKEY_LOCAL_MACHINE¥SOFTWARE¥NEC¥NVBASE¥AlertViewer¥AlertType¥xxxx]
"WavDefault"="Server.wav"
"AniDefault"="Default.bmp"
"Image"="Default.bmp"
"SmallImage"="Default.bmp"
```

=の左辺が名前、右辺がデータです。データはいずれも文字列型(REG_SZ)です。

Windows XP(Home Edition は除く), 2000/2003, Vista では追加したアラートタイプのキー (~¥AlertType¥xxxx) に対して、以下のアクセス権を設定してください。

Administrators	フルコントロール
Everyone	読み取り
SYSTEM	フルコントロール
ESMPRO ユーザーグループ (*)	フルコントロール

(*) ESMPRO ユーザーグループ は、ESMPRO/ServerManager インストール時に指定した、ESMPRO を使用するユーザーを管理するためのグループ名です。これはインストール時にユーザーが指定するグループ名ですが、以下のレジストリーにも格納されています。

```
[HKEY_LOCAL_MACHINE¥SOFTWARE¥NEC¥NVBASE]  
名前 : LocalGroup
```

以下の製品ページ FAQ もご参考にしてください。

http://www.nec.co.jp/middle/WebSAM/products/p_am/faq.html

Q43. アラートタイプの追加手順を教えてください。

→[目的のアラートタイプが選択画面に表示されない場合]

Linux OSに含まれるパッケージの仕様

ESMPRO/ServerAgentServiceのメモリ使用量が増加するときがある

対象 : Red Hat Enterprise Linux 6, 他の OS でも現象を確認しています。

詳細 : dlopen 関数が動的ライブラリーを二重ロードし、かつ失敗した場合に、(32+ファイル名)バイトメモリリークが発生します。二重ロードがともに成功した場合、または一重ロードで失敗した場合はいずれもメモリリークは発生しません。

弊社の評価で、net-snmp-libs パッケージに含まれる libsnmp.so ライブラリーの snmp_sess_init 関数が確保したメモリを開放しないためにメモリが増加することを確認しています。

snmp_sess_init 関数は通報する際に使用しており、使用しているプロセスと 1 回と 10 回、100 回の測定結果(単位は KB)は、次のとおりです。

プロセス名	1 回 (KB)	増加量 (KB)	10 回 (KB)	増加量 (KB)	50 回 (KB)	増加量 (KB)	100 回 (KB)
ESMntagent	3636	876	4512	12	4524	16	4540
ESMamvmmain	3320	212	3532	0	3532	4	3536
ESMcmn	5940	0	5940	0	5940	20	5960

この結果から 10 回までに、数十パーセントの増加は見られますが、それ以降は僅かな増加となっており、メモリ使用量が同じサイズで増加し続ける現象ではないことを確認しています。しかし、プロセスのメモリ使用量が大きくなった場合は、回避策でメモリの開放をお願いします。

回避 : メモリを開放するために、ESMPRO/ServerAgentService のサービスを再起動します。

```
# /opt/nec/esmpro_sa/bin/ESMRestart
```

ESMPRO/ServerManagerの表示

ハードディスクドライブ情報の表示

対象 : Linux OS

詳細 : [構成情報]-[ストレージ]で表示しているハードディスクドライブ情報は、/proc/scsi/scsi の情報を元にしており、実際のハードウェアと異なる情報が表示される場合があります。SATA ディスクは、T10 SCSI/ATAtranslation の仕様に従い、Vendor に'ATA'という文字列が入ります。

Host: scsi0 Channel: 00 Id: 00 Lun: 00 Vendor: ATA Model: SSDSA2SH064G1GC Rev: 445C Type: Direct-Access ANSI SCSI revision: 05

物理メモリ、仮想メモリとページファイル使用量の表示

対象：すべての ESMPRO/ServerAgentService バージョン

詳細：[構成情報]-[システム]-[メモリ]で表示している物理メモリ、仮想メモリとページファイルの使用可能容量は、/proc/meminfo の情報を元に以下の計算式で算出しています。

物理メモリ使用量 = MemTotal - MemFree

仮想メモリ使用量 = (MemTotal - MemFree) + (SwapTotal - SwapFree)

ページファイル使用量 = SwapTotal - SwapFree

MemTotal と MemFree の値は、Buffers と Cached を含んだ値となるため、OS の状況によっては、高い値が表示されることがあります。

OS環境により、UUID/GUIDが異なることがある

対象：Linux OS

詳細：[サーバ状態]で表示している GUID は、dmidecode コマンドより、[構成情報]-[ハードウェア]-[装置情報]-[システムマネージメント]の UUID/GUID は、SMBIOS から情報を取得しています。dmidecode のバージョンが 2.10 以降のときは、SMBIOS のバージョンを判断しています。SMBIOS のバージョンが 2.6 以降のときは UUID をバイトオーダーへ入れ替える処理があります。その影響により、UUID/GUID が異なることがあります。

例) SMBIOS Ver.2.6 の値

12345678 ABCD EFGH IJKL MNOPQRSTUVWXYZ

波下線の部分が 4byte 2byte 2byte 単位でバイト交換される。

78563412 CDAB GHEF IJKL MNOPQRSTUVWXYZ

2. Red Hat Enterprise Linux

Red Hat Enterprise Linux に関する注意事項です。

Linux OSに含まれるパッケージの仕様

openwsmand サービスが停止するときがある

<更新> 10.201.04-030.02

対象 : Red Hat Enterprise Linux

詳細 : 弊社の評価で、複数のプロセスから openwsmand を経由して、CIM プロバイダへアクセスした際に、openwsmand サービスが停止するときがあることを確認しております。ESMPRO/ServerManager は openwsmand を経由して、CIM プロバイダへアクセスします。

本現象は、複数の ESMPRO/ServerManager に登録したり、ESMPRO/ServerAgentService 側のサーバーで、wsman コマンドや他のプロセスにより、発生する可能性があります。

```
systemd: openwsmand.service: main process exited, code=killed, status=6/ABRT
systemd: Unit openwsmand.service entered failed state.
systemd: openwsmand.service failed.
```

回避 : 複数の ESMPRO/ServerManager に登録している場合は、1 つの ESMPRO/ServerManager にのみ登録してください。

wsman コマンドを使用している場合、以下の wbemcli コマンドを使用します。

例) 以下は改行なしで実行してください。

```
# wbemcli ei -nl -t http://root:{root のパスワード}@localhost:5988/root/ESMPRO/AS:ESM_Processor
```

他のプロセスが openwsmand を経由して CIM プロバイダへアクセスしている場合は、該当のプロセスを停止する等ご検討ください。

対処 : openwsmand サービスを起動します。

```
# systemctl start openwsmand.service
```

ESMPRO/ServerAgentService を再起動します。

```
# /opt/nec/esmpro_sa/bin/ESMRestart
```

OpenIPMI (kipmi0 プロセス) とハードウェア/ファームウェアとの交流に問題が発生し、ESMPRO/ServerAgentService の動作に影響がある

対象 : Red Hat Enterprise Linux 6

詳細 : ESMPRO/ServerAgentService のサービスモードでは OpenIPMI(kipmi0)を経由して、ハードウェア(BaseboardManagementController(BMC))にアクセスし、SystemEventLog(SEL)を監視しています。OpenIPMI (kipmi0 プロセス)とハードウェア/ファームウェアとの交流に問題が発生する場合があります、下記の影響があります。

- ・ BMC にアクセスできなくなるため、SEL 監視サービス(ESMsmsrv)が停止、あるいは、正常に動作できず、syslog への記録とエクスプレス通報されない場合がある。
- ・ カーネルヘルパースレッド kipmi0 の CPU 使用量が 100% になるときがあり、この時、再起動するまで 100% のままになります。再起動すると元に戻りますが、その後不定期に 100% になります。

対処 : ESMPRO/ServerAgentService での対処はありません。

ご使用の装置の BMC ファームウェアアップデートモジュールで修正している場合、適用してください。

■型番・モデル名から探す サポート・ダウンロード NEC

<http://support.express.nec.co.jp/pcserver/number.php>

ご使用の製品型番またはモデル名を検索し、BMC ファームウェアアップデートモジュールのリリー

スノートを確認します。

参照：本件に関する情報は、下記も参照してください。

■kipmi カーネルヘルパースレッド kipmi0 が、CPU の負荷を高くする

<https://access.redhat.com/ja/solutions/402953>

■[RHEL6]注意・制限事項 ID:06236

<https://www.support.nec.co.jp/View.aspx?id=3140100260>

SELinuxが有効の時、障害情報採取ツール(collectsa.sh)を実行すると、syslogにメッセージが記録される

対象：Red Hat Enterprise Linux 6

詳細：障害情報採取ツールでは、/proc 配下のファイルを収集しております。SELinux が有効の時、/proc 配下へのアクセスが制限され、syslog に複数のメッセージが記録されます。

```
SELinux is preventing cp ...
```

対処：障害情報採取ツールで、アクセス制限されたファイルが収集されませんが、OS の動作には影響ありません。

ESMPRO/ServerAgentService Ver. 2

6

FAQ

ESMPRO/ServerAgentService の FAQ です。

ESMPRO/ServerManagerへの登録や、接続チェックに失敗する、または、

ESMPRO/ServerAgentServiceが起動しない

登録済みの設定内容を確認してください

ESMPRO/ServerManagerに登録されているサーバー名、IPアドレスを確認してください。登録されているサーバーの「マシン名」または「IPアドレス」が登録しようとするサーバーの「マシン名」「IPアドレス」と重なっていないか確認してください。重なっていると登録できません。

ESMPRO/ServerManagerのバージョンを確認してください

<更新> 10.201.04-030.02

ESMPRO/ServerManagerのバージョンが、ESMPRO/ServerAgentServiceのバージョンに対応したバージョンかどうか、確認してください。

ESMPRO/ServerAgentService Ver.1.0 は ESMPRO/ServerManager Ver.6.06 以降 (Windows)

ESMPRO/ServerAgentService Ver.1.1 は ESMPRO/ServerManager Ver.6.08 以降 (Windows)

ESMPRO/ServerAgentService Ver.1.3 は ESMPRO/ServerManager Ver.6.08 以降 (Windows)

ESMPRO/ServerAgentService Ver.2.0 は ESMPRO/ServerManager Ver.6.20 以降 (Windows)

また、ESMPRO/ServerManagerから管理対象サーバーを監視する場合は、監視対象となるサーバー用のEXPRESSBUILDER内のESMPRO/ServerManager、もしくはそれより新しいバージョンのESMPRO/ServerManagerを利用してください。

対応していない場合、ESMPRO/ServerManagerをバージョンアップしてください。

最新版を利用することを推奨します。最新版は以下のWebサイトから入手できます。

<http://jpn.nec.com/esmsm/download.html>

自己署名証明書を許容する設定になっているか確認してください

ESMPRO/ServerManagerの画面右上にある[環境設定]を選択し、[ネットワーク]タブのWS-Man 通信にある[自己署名証明]が、「許容する」になっているか確認してください。

通信プロトコルはHTTPSか確認してください

<更新> 10.201.04-030.02

ESMPRO/ServerManagerに登録するとき、SNMP (ESMPRO/ServerAgent)/ WS-Man の設定が以下になっているか確認してください。

- ・ [管理]は、「登録」に設定する。
- ・ [管理対象]は、「WS-Man」を選択する。
- ・ [通信プロトコル]は、「HTTPS」を選択する。
- ・ [ユーザ/パスワード]は、「root」と、そのパスワードを入力する。

アクセス制限の設定を確認してください

<更新> 10.201.04-030.05

ESMPRO/ServerManagerから監視するとき、以下のポートを利用しています。お使いの環境でアクセス制限の設定をされているとき、以下のポートに対してアクセスを許可する設定か確認してください。

openwsmand 5986/tcp

詳細につきましては、本書の下記項を確認してください。

ESMPRO/ServerAgentServiceが使用するポート番号を教えてください

/etc/hosts.deny、/etc/hosts.allowの設定内容を確認してください

/etc/hosts.deny と /etc/hosts.allow ファイルの設定を確認してください。/etc/hosts.deny で原則禁止の設定を

しているときは、/etc/hosts.allow ファイルで tog-pegasus や openwsmand、rpcbind、snmpd のアクセスの許可を設定してください。

詳細につきましては、本書の下記項を確認してください。

ESMPRO/ServerAgentService が使用するポート番号を教えてください

本件に関する設定は、次の Web サイトを参照してください。

Linux サービスセット : /etc/hosts.deny、/etc/hosts.allow を使ったアクセス制限(TCP wrappers)の方法を教えてください。【Linux サービスセットご契約のお客様限定】

<https://www.support.nec.co.jp/View.aspx?id=3150005102>

<過去事例>

/etc/hosts.deny に"ALL : ALL"が記述されており、/etc/hosts.allow に rpcbind が 127.0.0.1(localhost)を許可する記述がありませんでした。

<過去事例の対処>

/etc/hosts.allow に"rpcbind : 127.0.0.1"と記述し、rpcbind のローカルアクセスを許可します。

または、"ALL : 127.0.0.1"と記述し、すべてのローカルアクセスを許可します。

その後、ESMRestart コマンドで ESMPRO/ServerAgentService を再起動します。

```
# /opt/nec/esmpro_sa/bin/ESMRestart
```

rpcbindが起動していることを確認してください

以下のコマンドを実行して、rpcbind が起動していることを確認してください。

```
# ps ax | grep rpcbind
```

- 起動しているときは、何もする必要はありません。

- 起動していないときは、rpcbind の設定を変更した後、rpcbind を起動し、サービスを再起動します。

```
# /sbin/chkconfig --level 35 rpcbind on
```

```
# /etc/init.d/ rpcbind start
```

```
# /opt/nec/esmpro_sa/bin/ESMRestart
```

Red Hat Enterprise Linux 7 では、ESMntserver に紐づいて rpcbind は起動しますので、設定は不要です。

SELinux機能の設定状況を確認してください

SELinux の設定が「無効」以外の場合は、「無効」に変更してください。



SELinux の設定を「無効(Disabled)」以外に設定されている場合は、SELinux のポリシー設定ファイルで適切なセキュリティコンテキストの設定をしてください。設定を行わないと、利用するソフトウェアでセキュリティ違反の警告またはエラーが発生し、正常に動作しない可能性があります。

「無効」以外を使用する場合は、SELinux のセキュリティコンテキストについて十分ご理解の上、設定を変更してください。

1) root ユーザーでログインします。

2) SELinux のカレント設定を確認します。

・カレント設定が「無効」の場合は、次のように表示されます。

```
# getenforce
```

```
Disabled
```

・カレント設定が「有効」の場合は、次のように表示されます。

```
# getenforce
```

```
Enforcing
```

・カレント設定が「警告のみ」の場合は、次のように表示されます。

```
# getenforce
```

Permissive

カレント設定が「無効」以外の場合は、以下の手順にしたがい、「無効」に変更します。

- 3) /etc/sysconfig/selinux をエディターで開き、以下の行を探します。

SELINUX=<カレント設定>

- 4) 上記の行を編集し、ファイルを保存します。

- ・「無効」にする場合は、以下に変更します。

SELINUX=disabled

- ・「有効」にする場合は、以下に変更します。

SELINUX=enforcing

- ・「警告だけ」にする場合は、以下に変更します。

SELINUX=permissive

- 5) システムを再起動します。

reboot

自己署名証明書が作成されているか確認してください

openwsman が動作するためには、自己署名証明書が必要です。

下記のファイル(自己署名証明書)が作成されているか、確認してください。

/etc/openwsman/servercert.pem

/etc/openwsman/serverkey.pem

存在しない場合、下記コマンドで自己署名証明書を作成してください。

/etc/openwsman/owsmangencert.sh

コマンドを実行すると、情報の入力を求められますので、項目に合わせて入力します。

項目を空白にする場合、'!'を入力します。"server name"は必須項目(required)となりますので、本機のホスト名(eg. ssl.domain.tld; required!!!)を入力します。

openwsmandが自動起動する設定か確認してください

- ・ Red Hat Enterprise Linux 6 のとき

openwsmand のランレベル 3, 5 の設定を確認します。

```
# /sbin/chkconfig --list openwsmand
```

```
openwsmand 0:off 1:off 2:off 3:off 4:off 5:off 6:off
```

- on のときは、設定に問題はありません。

- off のときは、openwsmand の設定を変更し、サーバーを再起動します。

```
# /sbin/chkconfig --level 35 openwsmand on
```

- ・ Red Hat Enterprise Linux 7 のとき

openwsmand の設定を確認します。

```
# systemctl is-enabled openwsmand.service
```

```
enabled
```

- enabled のときは、設定に問題はありません。

- disabled のときは、openwsmand の設定を変更し、サーバーを再起動します。

```
# systemctl enable openwsmand.service
```

```
ln -s '/usr/lib/systemd/system/ openwsmand.service'
```

```
'/etc/systemd/system/multi-user.target.wants/ openwsmand.service'
```

```
# systemctl start openwsmand.service
```


ベーシック認証のパスワードファイルが作成されているか確認してください

Red Hat Enterprise Linux 6 で openwsman が動作するためには、ベーシック認証(Basic Authentication)のパスワードファイルが必要です。

パスワードファイル(/etc/openwsman/simple_auth.passwd)が作成されているか、確認してください。

Red Hat Enterprise Linux 7 の場合、不要です。

作成されていない場合は、以下のコマンドで作成してください。

指定するユーザーは root、パスワードは root のパスワードを入力します。

```
# htpasswd -c /etc/openwsman/simple_auth.passwd root
New password:
Re-type new password:
Adding password for user root
```

ESMntserverのメッセージがsyslogへ記録され、OSの起動に時間が掛かる

下記メッセージが表示される原因として考えられるのは、rpcbind が起動されていない可能性や ESMPRO/ServerAgentService が使用するポートが開放されていない可能性が考えられます。

```
###ERR### Please check /opt/nec/esmpro_sa/work/ESMntserver.ready or fopen is
failed(errno:2)
```

以下を確認してください。

- ・ rpcbind が起動していることを確認してください。

- ・ /etc/sysconfig/iptables の内容を確認してください。

システム内のプログラム間通信で使用されるループバック・インターフェースへの通信を許可する設定があるか確認してください。ファイアウォールを利用していないときは問題ありません。

例) -A INPUT -i lo -j ACCEPT

- ・ /etc/hosts.deny と /etc/hosts.allow の内容を確認してください。

/etc/hosts.allow に対し、ループバックアドレスを許可する設定があるか確認してください。

例) ALL : 127.0.0.1

コントロールパネル(ESMagntconf, ESMamsadm)に関する質問

コントロールパネルが起動できない

syslog に以下のメッセージが記録されている場合、rpcbind に対する 127.0.0.1(localhost)からの要求が拒否されています。コントロールパネルは rpcbind の機能を使用していますので、/etc/hosts.deny と /etc/hosts.allow の内容を見直してください。

```
rpcbind: connect from 127.0.0.1 to <アクション>: request from unauthorized host
<プロセス名>: ###ERR###RPC###: RPC: ポートマッパーの失敗です - RPC: 認証エラー
```

<過去事例>

/etc/hosts.deny に "ALL : ALL" が記述されており、/etc/hosts.allow に rpcbind が 127.0.0.1(localhost) を許可する記述がありませんでした。

<過去事例の対処>

/etc/hosts.allow に "rpcbind : 127.0.0.1" と記述し、rpcbind のローカルアクセスを許可します。または、"ALL : 127.0.0.1" と記述し、すべてのローカルアクセスを許可します。

その後、ESMRestart コマンドで ESMPRO/ServerAgentService を再起動します。

```
# /opt/nec/esmpro_sa/bin/ESMRestart
```

コントロールパネルが起動できない

コントロールパネルの起動には、root ユーザーで実行する必要があります。ログインしているユーザーの実行権限を確認してください。

```
例) [root@localhost bin]# コントロールパネルは起動できます。
      [admin@localhost bin]$ コントロールパネルは起動できません。
```

コントロールパネルが起動できない

ディストリビューションやバージョンにより、必須パッケージは異なります。ESMPRO/ServerAgentService 必須パッケージを確認していただき、ESMPRO/ServerAgentService が動作に必要な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。ESMPRO/ServerAgentService 必須パッケージは ESMPRO/ServerAgentService ドキュメントに公開しています。

■ESMPRO/ServerAgentService ドキュメント

<https://www.support.nec.co.jp/View.aspx?id=3170102037>

必須パッケージ一覧 > ESMPRO/ServerAgentService (Linux 版) 必須パッケージ一覧

コントロールパネルで日本語の表示、および入力ができない

コントロールパネル(ESMagntconf, ESMamsadm)を日本語で表示させるためには、以下の手順を実行してください。

1. ネットワーク経由(ssh コマンド)で別の日本語端末からログインします。
2. root 権限がないときは、root ユーザーに昇格します。
su -
3. LANG 環境変数を確認します。
echo \$LANG
4. LANG 環境変数が日本語(ja_JP.~)ではない場合は、一時的に日本語に変更します。
export LANG=ja_JP.UTF-8 または ja_JP.eucJP
5. コントロールパネルを起動します。
cd /opt/nec/esmpro_sa/bin
./ESMagntconf
6. 作業終了後に、手順 2.で確認した LANG 環境変数に変更します。

コントロールパネルで日本語の入力に切り替えできない

ESMPRO/ServerAgentService のコントロールパネルは、newt パッケージの機能を利用しています。newt パッケージのバージョンにより、切り替え方法が異なります。<Space>キーまたは<Ctrl>+<Space>キーを押して、入力の切り替えできるか確認してください。

ESMPRO/ServerAgentServiceのサービスに関する質問

ESMPRO/ServerAgentServiceのサービスの起動に失敗する

syslog に以下のメッセージが記録されている場合、rpcbind に対する 127.0.0.1 (localhost)からの要求が拒否されています。ESMPRO/ServerAgentService のサービスは rpcbind の機能を使用していますので、/etc/hosts.deny と/etc/hosts.allow の内容を見直してください。

```
rpcbind: connect from 127.0.0.1 to <アクション>: request from unauthorized host
<プロセス名>: ###ERR###RPC###: RPC: ポートマッパーの失敗です - RPC: 認証エラー
```

<過去事例>

/etc/hosts.deny に"ALL : ALL"が記述されており、/etc/hosts.allow に rpcbind が 127.0.0.1(localhost)を許可する記述がありませんでした。

<過去事例の対処>

/etc/hosts.allow に"rpcbind : 127.0.0.1"と記述し、rpcbind のローカルアクセスを許可します。または、"ALL :

127.0.0.1"と記述し、すべてのローカルアクセスを許可します。

その後、ESMRestart コマンドで ESMPRO/ServerAgentService を再起動します。

```
# /opt/nec/esmpro_sa/bin/ESMRestart
```

ESMPRO/ServerAgentServiceのサービスを一括で停止や起動させたい

root 権限のあるユーザーでログインし、ESMRestart コマンドを実行します。

【停止させるとき】

引数に"stop"を指定して、ESMRestart コマンドを実行します。

```
# /opt/nec/esmpro_sa/bin/ESMRestart stop
```

【起動させるとき】

引数に"start"を指定して、ESMRestart コマンドを実行します。

```
# /opt/nec/esmpro_sa/bin/ESMRestart start
```

【再起動させるとき】

引数を指定せず、ESMRestart コマンドを実行します。

```
# /opt/nec/esmpro_sa/bin/ESMRestart
```

ESMPRO/ServerAgentServiceの機能や仕様に関する情報を教えてください

NetworkManagerを無効またはインストールしない場合、どのような影響がありますか

Red Hat Enterprise Linux 7 および Oracle Linux 7 の場合、ネットワークが起動した後に ESMPRO/ServerAgentService のサービスを起動させるため、NetworkManager-wait-online.service を使用しています。

NetworkManager を無効またはインストールしない場合、NetworkManager-wait-online.service が使用できません。そのため、OS 起動時にネットワークが起動する前に ESMPRO/ServerAgentService のサービスが起動した場合、CIM Indication が通報先へ到達しないときがあります。

ESMPRO/ServerAgentServiceの必須パッケージは、ディストリビューターから提供されているものを使用する必要がありますか

機能に影響がある場合がありますので、ESMPRO/ServerAgentService の必須パッケージは、ディストリビューターが提供しているパッケージをご使用ください。

<過去事例>

ディストリビューターから提供されている openssl パッケージのバージョンは openssl-1.0.1e だが、openssl-1.1.0c をコンパイル(make)してインストールしたところ、openwsmand が起動しない状態となりました。

その影響により、ESMPRO/ServerAgentService が正常に動作できない事象が発生しました。

原因は、openwsmand が利用している SSLv23_server_method 関数が、openssl-1.1.0c で削除されたことが原因でした。

```
-----/var/log/wsmand.log 抜粋-----
```

```
Jan 6 15:59:02 [9526] Using SSL
```

```
Jan 6 15:59:02 [9526] Initializing http server
```

```
★Jan 6 15:59:02 [9526] set_ssl: cannot find SSLv23_server_method
```

```
-----
```

ウイルスチェックの除外対象ファイルはありますか

ESMPRO/ServerAgentService のバージョンは問わず、インストールディレクトリ(/opt/nec/esmpro_sa)配下と、Syslog 監視対象ファイルをスキャン対象外としてください。

インストールディレクトリ(/opt/nec/esmpro_sa)配下：

過去のお問い合わせで、ウイルス対策ソフトのスキャンにより、ESMPRO/ServerAgentService のファイル

が圧縮ファイル爆弾(zip bomb)として検出された事例がありました。検出の原因は、インストールディレクトリ配下にあるファイルの解凍後のディレクトリやファイル数が多いためであり、問題ありません。

また、ウィルス対策ソフトでオンアクセススキャンを実施している場合、ファイルアクセスが遅くなり、データ取得に時間がかかり、サーバアクセス不能と検知されることがあります。

Syslog 監視対象ファイル：

ウィルス対策ソフトが利用している fsnotify_mark プロセスのステータスが、D (割り込み不可能なスリープ状態)となる場合があります。

--ps -axlw 実行例-----

```
F  UID  PID  PPID  PRI  NI    VSZ   RSS  WCHAN  STAT  TTY      TIME  COMMAND
1    0   231    2    -   -     0     0  -      -    ?         0:00 [fsnotify_mark]
1    0    -    -   20    0     -    -  synchr D    -         0:00 -
```

この影響で、Syslog 監視対象ファイルにアクセスできなくなる事例がありました。

原因はカーネル側(fsnotify)にあり、3.10.0-327.29.1.el7 で修正されています。

ESMPRO/ServerAgentServiceがsyslogへ記録するロケールは変更できますか

ESMPRO/ServerAgentService は、ロケールのデフォルト以外での動作をサポートしておりません。そのため、ロケールのデフォルト以外に変更する事もできません。ロケールのデフォルトは以下のとおりです。

UTF-8

Red Hat Enterprise Linux 6 以降

OSの時刻を変更(進める、または遅らせる)した場合、ESMPRO/ServerAgentServiceに与える影響について教えてください

OSの時刻を変更(進める、または遅らせる)した場合でも、ESMPRO/ServerAgentService は、特に影響はございません。

ESMPRO/ServerAgentServiceが使用するポート番号を教えてください

<更新> 10.201.04-030.04

ESMPRO/ServerManager(以降、ESMPRO/SM と表記)から ESMPRO/ServerAgentService(以降、ESMPRO/SAS と表記)がインストールされた装置を監視するとき、以下のポートを利用しています。お使いの環境でファイアウォールの設定をされるときは、これらへのアクセスを許可する設定にしてください。

表中「自動割当」のか所は、OS により使用可能なポートを一定の範囲内で割り振られます。そのため固定することはできません。ポートの範囲は以下のファイルを参照してください。

/proc/sys/net/ipv4/ip_local_port_range

■ESMPRO/SAS ↔ ESMPRO/SM

機能	ESMPRO/SAS	方向	ESMPRO/SM	備考
サーバー監視(WS-Man)	5986/tcp	← →	自動割当	openwsmand (HTTPS)
CIM-Indication 設定	—	← →	ICMP	ping(ICMP) 疎通確認
CIM-Indication 予約	5989/tcp	← →	自動割当	tog-pegasus (HTTPS)
CIM-Indication 送信	自動割当	→ ←	6736/tcp	tog-pegasus (HTTPS)
マネージャ通報(SNMP)	自動割当	→	162/udp	SNMP Trap

機能	ESMPRO/SAS	方向	ESMPRO/SM	備考
マネージャ通報 (TCP/IP in Band, TCP/IP Out-of-Band)	自動割当	→ ←	31134/tcp	
マネージャ経由 エクスプレス通報サービス	自動割当	→ ←	31136/tcp	
HTTPS(マネージャ経由) エクスプレス通報サービス	自動割当	→ ←	31138/tcp	

※openwsmand のポート番号は、/etc/openwsman/openwsman.conf の[server]にある ssl_port に設定されています。

※マネージャ経由の通報を使用する場合、ESMPRO/SM 側に WebSAM AlertManager が必要です。

※方向が双方向のか所は、上段の矢印は通信を開始した方向を示し、下段は折り返しの通信を示します。

※SNMP 以外で使用するポート番号は、通報の設定画面より設定します。

※iptables または firewalld を使用したポートの開放例は以下のとおりです。

使用しないサービス(iptables または firewalld)は停止してください。

- iptables を利用したポートの開放例は以下のとおりです。

事前に iptables や iptables-services(RHEL7/OL7)のインストールが必要です。

```
# iptables -I INPUT -p tcp --dport 5986 -s <ESMPRO/SM の IP アドレス> -j ACCEPT
# iptables -I INPUT -p icmp -j ACCEPT
# iptables -I OUTPUT -p icmp -j ACCEPT
# iptables -I INPUT -p tcp --dport 5989 -s <ESMPRO/SM の IP アドレス> -j ACCEPT
# iptables -I OUTPUT -p tcp --dport 6736 -j ACCEPT
# iptables -I OUTPUT -p udp --dport 162 -j ACCEPT
# iptables -I OUTPUT -p tcp --dport 31134 -j ACCEPT
# iptables -I OUTPUT -p tcp --dport 31136 -j ACCEPT
# iptables -I OUTPUT -p tcp --dport 31138 -j ACCEPT
# service iptables save
```

- firewalld を使用したポートの開放例は以下のウェブサイトを参照して、使用するポートを解放してください。

Linux サービスセット : firewalld (ファイアウォール機能) の基本的な使用方法について教えてください。

<https://www.support.nec.co.jp/View.aspx?id=3150110809>

※TCP Wrappers を使ったアクセス制御をするときは以下のウェブサイトを参照して、使用するポートを解放してください。

Linux サービスセット : /etc/hosts.deny、/etc/hosts.allow を使ったアクセス制限(TCP wrappers)の方法を教えてください。

<https://www.support.nec.co.jp/View.aspx?id=3150005102>

■ ESMPRO/SAS ↔ メールサーバー

機能	ESMPRO/SAS	方向	メールサーバー	備考
エクスプレス通報サービス (インターネットメール)	自動割当	→	25/tcp	SMTP
		←		
		→	110/tcp	POP3
		←		

※方向が双方向のか所は、上段の矢印は通信を開始した方向を示し、下段は折り返しの通信を示します。

※使用するポート番号は、通報の設定画面より設定します。

※iptables または firewalld を使用したポートの開放例は以下のとおりです。

使用しないサービス(iptables または firewalld)は停止してください。

- iptables を利用したポートの開放例は以下のとおりです。

事前に iptables や iptables-services(RHEL7/OL7)のインストールが必要です。

```
# iptables -I OUTPUT -p tcp --dport 25 -j ACCEPT
# iptables -I OUTPUT -p tcp --dport 110 -j ACCEPT
```

```
# service iptables save
```

- ・firewalld を使用したポートの開放例は以下のウェブサイトを参照して、使用するポートを解放してください。

Linux サービスセット : firewalld (ファイアウォール機能) の基本的な使用方法について教えてください。

<https://www.support.nec.co.jp/View.aspx?id=3150110809>

- ※TCP Wrappers を使ったアクセス制御をするときは以下のウェブサイトを参照して、使用するポートを解放してください。

Linux サービスセット : /etc/hosts.deny、/etc/hosts.allow を使ったアクセス制限(TCP wrappers)の方法を教えてください。

<https://www.support.nec.co.jp/View.aspx?id=3150005102>

■ESMPRO/SAS ↔ HTTPS サーバー

機能	ESMPRO/SAS	方向	HTTPS サーバー	備考
エクスプレス通報サービス(HTTPS)	自動割当	→ ←	443/tcp	HTTPS

※使用するポート番号は、通報の設定画面より設定します。

※iptables または firewalld を使用したポートの開放例は以下のとおりです。

使用しないサービス (iptables または firewalld) は停止してください。

- ・iptables を利用したポートの開放例は以下のとおりです。

事前に iptables や iptables-services(RHEL7/OL7)のインストールが必要です。

```
# iptables -I OUTPUT -p tcp --dport 443 -j ACCEPT
```

```
# service iptables save
```

- ・firewalld を使用したポートの開放例は以下のウェブサイトを参照して、使用するポートを解放してください。

Linux サービスセット : firewalld (ファイアウォール機能) の基本的な使用方法について教えてください。

<https://www.support.nec.co.jp/View.aspx?id=3150110809>

- ※TCP Wrappers を使ったアクセス制御をするときは以下のウェブサイトを参照して、使用するポートを解放してください。

Linux サービスセット : /etc/hosts.deny、/etc/hosts.allow を使ったアクセス制限(TCP wrappers)の方法を教えてください。

<https://www.support.nec.co.jp/View.aspx?id=3150005102>

ESMPRO/ServerAgentService は以下のポートを使用しています。

iptables を使ったパケットフィルタリング設定をするときは、これらへのアクセスを許可する設定にしてください。

■ローカルホスト内のプロセス間通

機能	ポート番号	備考
ESMPRO/ServerAgentService	自動割当	
rpcbind	111/tcp	
	111/udp	
tog-pegasus	5988/tcp	HTTP
	5989/tcp	HTTPS
openwsmand	5986/tcp	HTTPS

※rpcbind, tog-pegasus のポート番号は変更できません。

※openwsmand のポート番号は、/etc/openwsman/openwsman.conf の[server]にある ssl_port に設定されています。

※iptables を利用したポートの開放例は以下のとおりです。

使用しない場合、サービス (iptables) は停止してください。

事前に iptables や iptables-services(RHEL7/OL7)のインストールが必要です。

```
# iptables -A INPUT -i lo -j ACCEPT
# service iptables save
```

※TCP Wrappers を使ったアクセス制御をするときは以下のウェブサイト参照して、使用するポートを解放してください。

Linux サービスセット : /etc/hosts.deny、/etc/hosts.allow を使ったアクセス制限(TCP wrappers)の方法を教えてください。

<https://www.support.nec.co.jp/View.aspx?id=3150005102>

ESMPRO/ServerAgentServiceのサービス(プロセス)の機能を教えてください

本書の1章「2. 機能概要」を参照してください。

ESMPRO/ServerAgentServiceが出力するログについて教えてください

ESMPRO/ServerAgentService が出力するログは、ESMPRO/ServerAgentService ログ情報資料を参照してください。

■ESMPRO/ServerAgentService ドキュメント

<https://www.support.nec.co.jp/View.aspx?id=3170102037>

内部ログ情報 > ESMPRO/ServerAgentService (Linux 版) 内部ログ情報

RAID構成のストレージ監視はできますか？

ESMPRO/ServerAgentService のストレージ監視機能はハードディスクドライブ単体構成のみのサポートであり、RAID 構成のストレージ監視はできません。RAID 構成のストレージ監視は、RAID 管理ユーティリティを導入することにより Syslog 監視機能を利用した通報機能のみサポートします。

■RAID コントローラ関連 – 掲載情報

<http://www.express.nec.co.jp/linux/supported-help/raid/raid.asp>

NICのLink Up/Downが通報されない

ESMPRO/ServerAgentService はネットワークを監視していないため、NIC の Link Up/Down は検出できません。NIC の Link Up/Down 時に、システムから syslog(/var/log/messages)に記録されるメッセージがあるとき、Syslog イベントを追加することで通報できます。ただし、Link Down のときは、ネットワークが使用できない状態のため、通報されない可能性があります。

MIB定義ファイルは、どこに格納されていますか？

ESMPRO/ServerAgentService が拡張している ESMPRO MIB(1.3.6.1.4.1.119.2.2.4.4)の定義ファイルは、OS 種別(Windows、Linux、VMware 等)を問わず装置に添付されている EXPRESSBUILDER または Starter Pack に格納しております。

EXPRESSBUILDER: {レビジョン}/lnx/pp/esmpro_sas/MIBS

Starter Pack: software/{レビジョン}/lnx/pp/esmpro_sas/MIBS

ESMPRO/ServerAgentServiceの通報に関する情報を教えてください

ESMPRO/ServerAgentServiceが通報する内容を教えてください

ESMPRO/ServerAgentService が通報する内容は ESMPRO/ServerAgentService アラート一覧を参照してください。ESMPRO/ServerAgentService アラート一覧は ESMPRO/ServerAgentService ドキュメントに公開しています。

■ESMPRO/ServerAgentService ドキュメント

<https://www.support.nec.co.jp/View.aspx?id=3170102037>

アラート一覧

ESMPRO/ServerAgentService Ver.1, Ver.2 (Linux 版) アラート一覧

ESMPRO/ServerAgentServiceが送信するSNMPトラップ内の文字コード

ESMPRO/ServerAgentService が送信する SNMP トラップ内の日本語文字コードは、OS で使用している日本語文字コードに影響されず S-JIS に変換して送信しています。ESMPRO/ServerManager のアラートビューアは問題ありませんが、SNMP トラップを受信するソフトウェアの仕様によっては、S-JIS が表示できず文字化けする可能性があります。

ESMPRO/ServerAgentServiceが送信するSNMPトラップ内のAgentAddress

ESMPRO/ServerAgentService は、以下の処理で取得した IP アドレスを SNMP トラップの AgentAddress フィールドに埋め込み送信します。

- 1) システムコールの gethostname() 関数から、ホスト名を取得します。
- 2) システムコールの gethostbyname() 関数から、1) で取得したホスト名を検索し、最初に一致するホスト名の IP アドレスを取得します。
gethostbyname() 関数の取得データは、/etc/hosts の定義と関連しています。
もし /etc/hosts に 1) で取得したホスト名が存在しない場合、または、取得した IP アドレスがローカルホスト(127.0.0.1)の場合は、UDP のソケット通信を利用して通信に使用する IP アドレスを取得し、TRAP 送信元の IP アドレスとして埋め込みます。

ESMPRO/ServerManager のアラートビューアは、SNMP トラップの AgentAddress フィールドに埋め込まれている IP アドレスを元に、自身に登録されているサーバの情報(IP アドレス)を検索し、最初に合致するホスト名を表示します。

そのため、検索に合致しない場合は「不明なサーバ」、別サーバの情報に合致した場合は別サーバのホスト名が表示されます。

上記 1) のホスト名が "server1" の場合に、/etc/hosts の内容によってどのような IP アドレスを取得し、トラップの送信元 IP アドレスとして埋め込むかの例を記載します。

(/etc/hosts の設定例 1) 通信に使用する IP アドレスを埋め込みます。

```
127.0.0.1 server1 localhost.localdomain localhost
10.1.2.1 server1
10.1.2.2 server2
```

(/etc/hosts の設定例 2) 10.1.2.1 となります。

```
10.1.2.1 server1
127.0.0.1 server1 localhost.localdomain localhost
10.1.2.2 server2
```

(/etc/hosts の設定例 3) 10.1.2.1 となります。

```
127.0.0.1 localhost.localdomain localhost
10.1.2.1 server1
10.1.2.2 server2
```

(/etc/hosts の設定例 4) 通信に使用する IP アドレスを埋め込みます。

```
127.0.0.1 localhost.localdomain localhost
10.1.2.2 server2
```

ESMPRO/ServerAgentServiceがsyslogに記録するメッセージを教えてください

ESMPRO/ServerAgentService が syslog に記録するメッセージは ESMPRO/ServerAgentService アラート一覧の通報メッセージを参照してください。

<例(BMC 対応装置)>

```
Sep 13 07:46:26 test-host ESMsmshr: SRC:ESMCommonService, ID:80000065, MSG:システムの温度が高くなっています。 センサ番号: 3 位置: フロントパネルボード 1 現在の温度: 42
```


度 (C) しきい値: 42 度 (C)

上記メッセージとアラート一覧の対応としては、以下のとおりです。

SRC:ESMCommonService = ソース名
ID:80000065 = イベント ID
MSG:システムの温... = 通報メッセージ

ESMPRO/ServerAgentService アラート一覧は ESMPRO/ServerAgentService ドキュメントに公開していません。

■ ESMPRO/ServerAgentService ドキュメント

<https://www.support.nec.co.jp/View.aspx?id=3170102037>

アラート一覧

ESMPRO/ServerAgentService Ver.1, Ver.2 (Linux 版) アラート一覧

ESMPRO/ServerAgentServiceがsyslogに記録するメッセージのファシリティとプライオリティを教えてください

ESMPRO/ServerAgentService が syslog に記録するメッセージのファシリティとプライオリティは以下のとおりです。

情報	ファシリティ	: user	プライオリティ	: info
警告	ファシリティ	: user	プライオリティ	: warning
異常	ファシリティ	: user	プライオリティ	: err

任意のメールアドレスへの通知やパトロールランプを鳴動させる方法を教えてください

任意のメールアドレスへの通知やパトロールランプを鳴動させる方法はありません。

ESMPRO/ServerManager(Windows)をインストールしている管理側(Windows)に WebSAM AlertManager を導入することにより、運用環境に合わせた通報手段を提供しています。

【WebSAM AlertManager - 特長・機能の抜粋】

- ・システム管理者がどこからでも障害状況の確認ができる mail 通報
- ・サーバーの異常をサーバーのオペレーターに通知するポップアップ通報
- ・サーバーの異常情報をリモートプリンターにも印刷可能なプリンター書き出し
- ・サーバーの異常を検出した場合に、業務アプリケーションと連携して障害回避、障害復旧処理をする事を可能とするアプリケーションの実行
- ・サーバーの異常を検出した場合に、パトロールランプを鳴動させるパトロールランプ通報
- ・サーバーの異常情報履歴をファイル保存するファイル出力

■ WebSAM AlertManager - 特長・機能

http://www.nec.co.jp/middle/WebSAM/products/p_am/kinou.html

設定を変更したときに再設定する必要がある項目を教えてください

ESMPRO/ServerAgentService側のrootパスワードを変更されるとき

- ・ ESMPRO/ServerAgentService 側の設定を変更する項目
RHEL7 の場合、設定を変更する項目はありません。
RHEL6 の場合、ベーシック認証のパスワードファイルを、再作成してください。
- ・ ESMPRO/ServerManager 側の設定を変更する項目
システム管理(WS-Man)にてサーバーを監視している場合、ESMPRO/ServerManager の接続設定画面にてパスワードを変更してください。変更後、管理対象サーバーの接続チェックを実行してください。

ESMPRO/ServerManager側のAdministratorパスワードを変更されるとき

- ・ ESMPRO/ServerAgentService 側の設定を変更する項目
設定を変更する項目はありません。
- ・ ESMPRO/ServerManager 側の設定を変更する項目
設定を変更する項目はありません。

ESMPRO/ServerAgentService側のIPアドレスを変更されるとき

<更新> 10.201.04-030.05

- ・ ESMPRO/ServerAgentService 側の設定を変更する項目

自己署名証明書を再作成してください。

```
# /etc/openwsman/owsmangencert.sh --force
```

その後、openwsmand サービスと ESMPRO/ServerAgentService を再起動してください。

- ・ openwsmand サービスの再起動

RHEL7 の場合 : # systemctl restart openwsmand.service

RHEL6 の場合 : # /etc/init.d/openwsmand restart

- ・ ESMPRO/ServerAgentService の再起動

```
# /opt/nec/esmpro_sa/bin/ESMRestart
```

- ・ ESMPRO/ServerManager 側の設定を変更する項目

ESMPRO/ServerManager の接続設定画面にて、変更した本機または BMC/iLO の該当する IP アドレスを変更してください。

変更後、管理対象サーバーの接続チェックを実行してください。

システム管理(SNMP)にて、リモートウェイクアップ機能を使用している場合、リモートウェイクアップ設定画面にて、MAC アドレスと IP ブロードキャストアドレスを変更してください。

ESMPRO/ServerManager側のIPアドレスを変更されるとき

- ・ ESMPRO/ServerAgentService 側の設定を変更する項目

マネージャ通報(SNMP/TCP_IP)に ESMPRO/ServerManager マシンの IP アドレスを指定しているときは、3 章の以下を参照して、コントロールパネル(ESMamsadm)から通報先の設定を変更してください。

2.1.1. マネージャ通報(SNMP)の基本設定

3.1.1. 通報手段がマネージャ通報(TCP_IP In-Band)の宛先設定

3.1.2. 通報手段がマネージャ通報(TCP_IP Out-of-Band)の宛先設定

また、snmpd に対して IP アドレスによるアクセスを制限しているときは、設定を変更してください。

```
/etc/snmp/snmpd.conf
```

```
/etc/hosts.allow
```

```
/etc/hosts.deny
```

- ・ ESMPRO/ServerManager 側の設定を変更する項目

以下の手順で ESMPRO/ServerManager のサービスを再起動してください。サービスの再起動の代わりに ESMPRO/ServerManager がインストールされている装置を再起動していただくことも対応可能です。

■サービス停止順

- 1.DianaScope ModemAgent
- 2.ESMPRO/SM Web Container
- 3.ESMPRO/SM Event Manager
- 4.ESMPRO/SM Base AlertListener
- 5.ESMPRO/SM Common Component
- 6.Alert Manager Socket(R) Service(*)
- 7.ESMPRO/SM Base Service
- 8.Dmi Event Watcher(*)
- 9.ESM Alert Service
- 10.ESM Command Service
- 11.ESM Remote Map Service
- 12.ESM Base Service
- 13.Alert Manager HTTPS Service(*)
- 14.Alert Manager WMI Service

■サービス開始順序

- 1.Alert Manager WMI Service
- 2.Alert Manager HTTPS Service(*)
- 3.ESM Base Service
- 4.ESM Remote Map Service
- 5.ESM Command Service
- 6.ESM Alert Service
- 7.Dmi Event Watcher(*)
- 8.ESMPRO/SM Base Service
- 9.Alert Manager Socket(R) Service(*)
- 10.ESMPRO/SM Common Component
- 11.ESMPRO/SM Base AlertListener
- 12.ESMPRO/SM Event Manager
- 13.ESMPRO/SM Web Container
- 14.DianaScope ModemAgent

* 設定によりサービスが停止している場合があります。

サービスが停止している場合、サービスを開始する必要はありません。

ESMPRO/ServerAgentService側のホスト名を変更されるとき

<更新> 10.201.04-030.05

- ・ ESMPRO/ServerAgentService 側の設定を変更する項目

自己署名証明書を再作成してください。

```
# /etc/openwsman/owsmangencert.sh --force
```

その後、openwsmand サービスと ESMPRO/ServerAgentService を再起動してください。

- ・ openwsmand サービスの再起動

RHEL7 の場合 : # systemctl restart openwsmand.service

RHEL6 の場合 : # /etc/init.d/openwsmand restart

- ・ ESMPRO/ServerAgentService の再起動

```
# /opt/nec/esmpro_sa/bin/ESMRestart
```

また、エクスプレス通報サービスを利用している場合、エクスプレス通報サービス セットアップガイド (Linux/VMware 編)の1章「3.6 開局ファイルの再読み込み」を参照し、開局ファイルの再読み込みを実施してください。

- ・ ESMPRO/ServerManager 側の設定を変更する項目

管理しているサーバーのコンポーネント名を新しいホスト名にしたい場合は、ESMPRO/ServerManager の接続設定画面にてコンポーネント名を変更してください。

なお、本操作は必須ではありません。旧コンポーネント名のまま管理することで問題ない場合は、コンポーネント名の変更は不要です。

ESMPRO/ServerManager側のホスト名を変更されるとき

- ・ ESMPRO/ServerAgentService 側の設定を変更する項目

マネージャ通報(SNMP/TCP_IP)に ESMPRO/ServerManager マシンの IP アドレスを指定しているときは、3章の以下を参照して、コントロールパネル(ESMamsadm)から通報先の設定を変更してください。

2.1.1. マネージャ通報(SNMP)の基本設定

3.1.1. 通報手段がマネージャ通報(TCP_IP In-Band)の宛先設定

3.1.2. 通報手段がマネージャ通報(TCP_IP Out-of-Band)の宛先設定

また、snmpd に対して IP アドレスによるアクセスを制限しているときは、設定を変更してください。

```
/etc/snmp/snmpd.conf
```

```
/etc/hosts.allow
```

```
/etc/hosts.deny
```

- ・ ESMPRO/ServerManager 側の設定を変更する項目

<ESMPRO/ServerManager インストールフォルダー>

¥ESMWEB¥wbserver¥webapps¥esmpro¥WEB-INF¥service¥options.txt 中の "SM_NAME=xxxx" と記載されている行を削除してください。

その後、以下の手順で ESMPRO/ServerManager のサービスを再起動してください。サービスの再起動の代わりに ESMPRO/ServerManager がインストールされている装置を再起動していただくことでも対応可能です。

■サービス停止順

- 1.DianaScope ModemAgent
- 2.ESMPRO/SM Web Container
- 3.ESMPRO/SM Event Manager
- 4.ESMPRO/SM Base AlertListener
- 5.ESMPRO/SM Common Component
- 6.Alert Manager Socket(R) Service(*)
- 7.ESMPRO/SM Base Service
- 8.Dmi Event Watcher(*)
- 9.ESM Alert Service
- 10.ESM Command Service

■サービス開始順序

- 1.Alert Manager WMI Service
- 2.Alert Manager HTTPS Service(*)
- 3.ESM Base Service
- 4.ESM Remote Map Service
- 5.ESM Command Service
- 6.ESM Alert Service
- 7.Dmi Event Watcher(*)
- 8.ESMPRO/SM Base Service
- 9.Alert Manager Socket(R) Service(*)
- 10.ESMPRO/SM Common Component

11.ESM Remote Map Service	11.ESMPRO/SM Base AlertListener
12.ESM Base Service	12.ESMPRO/SM Event Manager
13.Alert Manager HTTPS Service(*)	13.ESMPRO/SM Web Container
14.Alert Manager WMI Service	14.DianaScope ModemAgent

* 設定によりサービスが停止している場合があります。

サービスが停止している場合、サービスを開始する必要はありません。

ESMPRO/ServerAgentService側のMACアドレスを変更されるとき(ネットワークボードの交換など)

- ・ ESMPRO/ServerAgentService 側の設定を変更する項目
設定を変更する項目はありません。
- ・ ESMPRO/ServerManager 側の設定を変更する項目
システム管理(SNMP)にて、リモートウェイクアップ機能を使用している場合、リモートウェイクアップ設定画面にて、MAC アドレスと IP ブロードキャストアドレスを変更してください。

ESMPRO/ServerManager側のMACアドレスを変更されるとき(ネットワークボードの交換など)

- ・ ESMPRO/ServerAgentService 側の設定を変更する項目
設定を変更する項目はありません。
- ・ ESMPRO/ServerManager 側の設定を変更する項目
設定を変更する項目はありません。

SNMPのコミュニティ名を変更されるとき

- ・ ESMPRO/ServerAgentService 側の設定を変更する手順
 - 1) SNMP 設定ファイル(snmpd.conf)を編集して、コミュニティ名を変更する。
 - 2) コントロールパネル(ESMagntconf)の「SNMP Trap」の「SNMP Community」にて、コミュニティ名を変更する。
 - 3) snmpd サービスと ESMPRO/ServerAgentService または OS を再起動する。
- ・ ESMPRO/ServerManager 側の設定を変更する手順
設定を変更する項目はありません。

ESMPRO/ServerAgentService Ver.2
ユーザーズガイド(Linux 編)

日 本 電 気 株 式 会 社
東京都港区芝五丁目 7 番 1 号
TEL (03) 3454-1111 (大代表)

©NEC Corporation 2018

日本電気株式会社の許可なく複製・改変などを行うことはできません。