

# HA8000V シリーズ/RV3000

ユーザーズガイド  
Log Monitor 機能

## FASTFIND LINKS

[ドキュメント構成](#)

[お問い合わせ先](#)

[目次](#)

Hitachi, Ltd.

## ソフトウェア使用上の注意

お客様各位

株式会社 日立製作所

このたびは日立アドバンストサーバ **HA8000V** シリーズ、**RV3000** をお買い上げいただき、誠にありがとうございます。

下記の「ソフトウェアの使用条件」を必ずお読みいただきご了解いただきますようお願いいたします。ソフトウェアの使用条件

### 1. ソフトウェアの使用

このソフトウェアは、特定の1台の日立アドバンストサーバ **HA8000V** シリーズ、**RV3000** でのみ使用することができます。

### 2. 複製

お客様は、このソフトウェアの一部または全部の複製を行わないでください。ただし、下記に該当する場合に限り複製することができます。

お客様がご自身のバックアップ用、保守用として、1項に定める1台の日立アドバンストサーバ **HA8000V** シリーズ、**RV3000** で使用する場合に限り複製することができます。

### 3. 改造・変更

お客様によるこのソフトウェアの改造・変更は行わないでください。万一、お客様によりこのソフトウェアの改造・変更が行われた場合、弊社は該当ソフトウェアについてのいかなる責任も負いません。

### 4. 第三者の使用

このソフトウェアを譲渡、貸出、移転その他の方法で、第三者に使用させないでください。

### 5. 保証の範囲

(1) 万一、媒体不良のために、ご購入時に正常に機能しない場合には、無償で交換いたします。

(2) このソフトウェアの使用により、万一お客様に損害が生じたとしても、弊社は責任を負いません。あらかじめご了承ください。

以上



# 目次

目次.....	iii
お使いになる前に.....	v
重要なお知らせ.....	vi
登録商標・商標.....	vi
発行.....	vi
著作権について.....	vii
文書来歴.....	viii
ドキュメント構成.....	ix
凡例.....	x
お問い合わせ先.....	xi
安全にお使いいただくために.....	xiii
Log Monitor の概要.....	1
概要.....	2
機能.....	2
適用機器.....	6
サポート OS/仮想環境.....	6
要求リソース.....	7
前提ソフトウェア.....	9
検知対象障害.....	12
制限事項.....	12
Log Monitor の導入.....	15
インストール前の準備.....	16
インストール.....	17
アンインストール.....	20
アップグレード.....	21
バージョンの確認.....	22

<b>VMware 版 Log Monitor(ゲスト方式)の導入 .....</b>	<b>23</b>
Hypervisor の設定.....	26
監視対象のゲスト OS 設定.....	30
Log Monitor をインストールするゲスト OS 設定 .....	31
Log Monitor のインストール .....	36
アンインストール .....	37
アップグレード.....	39
バージョンの確認 .....	40
<b>VMware 版 Log Monitor(CIM 方式)の導入 .....</b>	<b>41</b>
Hypervisor の設定.....	43
CIM モジュールのインストール .....	44
DirectPath I/O を設定するゲスト OS の設定.....	45
ゲストモジュールのインストール.....	47
管理モジュールをインストールする OS の設定.....	47
管理モジュールのインストール .....	48
管理モジュールの設定.....	52
動作確認.....	55
アンインストール .....	55
アップグレード.....	57
バージョンの確認 .....	59
<b>Log Monitor の操作 .....</b>	<b>61</b>
起動と停止方法.....	62
障害解析結果コード(RC)の参照 .....	63
動作検証.....	66
監視対象 syslog ファイルの変更 (Linux のみ) .....	69
<b>付録.....</b>	<b>71</b>
メッセージ一覧.....	72
Windows 版のイベントローガー一覧.....	72
Linux 版の syslog メッセージ一覧.....	74
VMware 版 Log Monitor の syslog メッセージ一覧.....	76
インストールフォルダ構成.....	78
<b>頭字語と略語 .....</b>	<b>81</b>

# お使いになる前に

このマニュアルは、弊社サーバ製品を使用する前に、知っておいていただきたい内容について説明しています。製品を使用する前に、安全上の指示をよく読み十分理解してください。このマニュアルは、いつでも参照できるよう、手近な所に保管してください。

この章の内容は以下の通りとなっています：

- [重要なお知らせ](#)
- [規制・対策などについて](#)
- [登録商標・商標](#)
- [発行](#)
- [著作権について](#)
- [文書来歴](#)
- [ドキュメント構成](#)
- [凡例](#)
- [お問い合わせ先](#)
- [安全にお使いいただくために](#)



弊社サーバ製品の使用は、弊社とのお客様の契約の条件によって決定されます。

---

## 重要なお知らせ

- 本書の内容の一部、または全部を無断で転載すること、複製することは固くお断わりします。
- 本書の内容について、改良のため予告なしに変更することがあります。
- 本書の内容については万全を期しておりますが、万一ご不審な点や誤りなど、お気づきのことがありましたら、お買い求め先へご一報くださいますようお願いいたします。
- 本書に準じないで本製品を運用した結果については責任を負いません。あらかじめご了承ください。

## 規制・対策などについて

### 輸出規制について

本製品を輸出される場合には、外国為替及び外国貿易法並びに米国の輸出管理関連法規などの規制をご確認の上、必要な手続きをお取りください。なお、ご不明の場合は弊社担当営業にお問い合わせください。

### 海外での使用について

本製品は日本国内専用です。国外では使用しないでください。なお、他国には各々の国で必要となる法律、規格等が定められており、本製品は適合していません。

## 登録商標・商標

- Microsoft、Windows、Windows Server、Hyper-V は米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
- Linux は、Linus Torvalds 氏の日本およびその他の国における登録商標または商標です。
- Red Hat は、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。
- VMware、VMware vSphere は、米国およびその他の地域における VMware, Inc. の登録商標または商標です。
- その他、本マニュアル中の製品名および会社名は、各社の商標または登録商標です。

## 発行

2024年9月（第12版）

## 著作権について

このマニュアルの内容はすべて著作権に保護されています。  
このマニュアルの内容の一部または全部を、無断で記載することは禁じられています。

Copyright© Hitachi, Ltd. 2018-2024. All rights reserved.

## 文書来歴

改訂	年月日	説明
4071-1J-101	2018年1月	初版
4071-1J-101-10	2018年9月	RV3000 に対応
4071-1J-101-20	2018年12月	RV3000 Log Monitor VMware 版のサポート
4771-1J-101-30	2019年4月	<ul style="list-style-type: none"><li>・ Log Monitor の起動、停止方法に関する記載を追加</li><li>・ rsyslog の設定値に関する記載を追加</li><li>・ エラーメッセージの誤記を修正</li></ul>
4771-1J-101-40	2019年6月	<ul style="list-style-type: none"><li>・ 技術情報、アップデートプログラムに関する誤記を訂正</li></ul>
4771-1J-101-50	2020年1月	<ul style="list-style-type: none"><li>・ Standalone ESXCLI に関する記載を追加</li><li>・ XFS ファイルシステムに関する制限事項を見直し</li></ul>
4771-1J-101-60	2020年7月	<ul style="list-style-type: none"><li>・ Red Hat Enterprise Linux 8 のサポートに伴う、バージョンの記載を修正</li><li>・ VMware vSphere のバージョンに関する記載を修正</li></ul>
4771-1J-101-70	2021年2月	<ul style="list-style-type: none"><li>・ RV3000 A2 に対応</li><li>・ 32G Fibre Channel ボード[日立製]に対応</li><li>・ VMware 版 CIM 方式をサポート</li></ul>
4771-1J-101-80	2021年6月	<ul style="list-style-type: none"><li>・ VMware 版 CIM 方式の誤記訂正</li></ul>
4771-1J-101-90	2023年5月	<ul style="list-style-type: none"><li>・ RV3000 A2 Windows 版のサポート</li></ul>
4771-1J-101-A0	2024年3月	<ul style="list-style-type: none"><li>・ 誤記訂正</li></ul>
4771-1J-101-B0	2024年9月	<ul style="list-style-type: none"><li>・ RV3000 A3 に対応</li><li>・ RHEL9 対応</li></ul>



# ドキュメント構成

## 本ドキュメントの構成

このドキュメントの内容と構成の概要を下記表に示します。各章のタイトルをクリックすることで、各章を参照することができます





章	説明
Chapter 1, <a href="#">Log Monitor の概要</a>	この章では Log Monitor の概要について説明します。
Chapter 2, <a href="#">Log Monitor の導入</a>	この章では、Log Monitor のインストール方法およびアンインストール方法について説明します。
Chapter 3, <a href="#">VMware 版 Log Monitor(ゲスト方式)の導入</a>	この章では、VMware 版 Log Monitor(ゲスト方式)のインストール方法およびアンインストール方法について説明します。
Chapter 4, <a href="#">VMware 版 Log Monitor(CIM 方式)の導入</a>	この章では、VMware 版 Log Monitor(CIM 方式)のインストール方法およびアンインストール方法について説明します。
Chapter 5, <a href="#">Log Monitor の操作</a>	この章では、Log Monitor の操作について説明します。
Chapter 6, <a href="#">付録</a>	この章では、Log Monitor に関する補足情報を記載します。

## 凡例

弊社サーバ製品の用語は特に明記がない場合、弊社サーバ製品すべてのモデルで使用されています。このドキュメントで使用されている記号は以下の通りです。

記号	説明
太字	メニュー、オプション、ボタン、フィールドおよびラベルを含めて、ウィンドウ・タイトル以外に表示される内容を示します。 例: Click <b>OK</b> .
イタリック体	ユーザまたはシステムによって提供される変数を示します。 例: copy source-file target-file <b>通知:</b> "<>" も変数を示すために使用されます。
画面/コマンドライン	画面に表示またはユーザによって入力する内容を示します。 例: # pairdisplay -g ora <b>d</b>
< >	ユーザまたはシステムによって提供される変数を示します。 例: # pairdisplay -g <group> <b>通知:</b> イタリック体のフォントも変数を示すために使用されます。
[ ]	オプションの値を示します。 例: [ a   b ] a、b または入力なしのどれかを選択することを示します。
{ }	必要な値あるいは予期された値を示します。 例: { a   b } a または b のどちらかを選択することを示します。
	2 つ以上のオプションあるいは引数から選択できることを示します。 例: [ a   b ] a、b または入力なしのどれかを選択することを示します。 { a   b } a または b のどちらかを選択することを示します。
アンダーライン	デフォルト値を示します。例: [ <u>a</u>   b ]

このドキュメントは、注意すべき情報に対して次のアイコンを使用しています:

アイコン	意味	記述
 <b>警告</b>	警告	死亡または重大な傷害を引き起こすおそれのある潜在的な危険の存在を示すのに用います。
 <b>注意</b>	注意	軽度の傷害、あるいは中程度の傷害を引き起こすおそれのある潜在的な危険の存在を示すのに用います。
<b>通知</b>	通知	人身傷害とは関係のない損害を引き起こすおそれのある場合に用います。
 <b>制限</b>	制限	本製品の故障や障害の発生を防止し、正常に動作させるための事項を示します。
 <b>補足</b>	補足	本製品を活用するためのアドバイスを示します。

# お問い合わせ先

## 技術情報、アップデートプログラムについて

HA8000V シリーズ/RV3000 ホームページで、技術情報、ドライバやユーティリティ、BIOS/EFI、ファームウェアなどのアップデートプログラムを提供しております。本ユーティリティでアップデートに対応していない場合やトラブルシューティングが必要となります。[ダウンロード]をクリックしてください。

- HA8000V シリーズホームページアドレス：  
<https://www.hitachi.co.jp/products/it/ha8000v/index.html>
- RV3000 ホームページアドレス：  
<https://www.hitachi.co.jp/products/it/rv3000/index.html>


各アップデートプログラムの適用はお客様責任にて実施していただきますが、システム装置を安全にご使用いただくためにも、定期的にホームページにアクセスして、本ユーティリティを使用して最新のドライバやユーティリティ、BIOS/EFI、ファームウェアへ更新していただくことをお勧めいたします。

障害等の保守作業で部品を交換した場合、交換した部品の BIOS/EFI、ファームウェアは原則として最新のものが適用されます。また保守作業時、交換していない部品の BIOS/EFI、ファームウェアも最新のものへ更新する場合があります。

## 操作や使いこなしについて

本製品のハードウェアについての機能や操作方法に関するお問い合わせは、HCA センター（Hitachi カスタマ・アンサ・センター）でご回答いたしますので、次のフリーダイヤルにおかけください。受付担当がお問い合わせ内容を承り、専門エンジニアが折り返し電話でお答えするコールバック方式をとらせていただきます。

### HCA センター（Hitachi カスタマ・アンサ・センター）

 0120-2580-12

受付時間

9:00～12:00/13:00～17:00（土・日・祝日、年末年始を除く）

お願い

- お問い合わせになる際に次の内容をメモし、お伝えください。お問い合わせ内容の確認をスムーズに行うため、ご協力をお願いいたします。

形名（TYPE）／製造番号（S/N）／インストール OS／サービス ID（SID）

「形名」、「製造番号」および「サービス ID」は、システム装置前面に貼り付けられている機器ラベルにてご確認ください。

- 質問内容を FAX でお送りいただくこともありますので、ご協力をお願いいたします。

- Hitachi カスタマ・アンサ・センターでお答えできるのは、製品のハードウェアの機能や操作方法などです。ハードウェアに関する技術支援や、OS や各言語によるユーザープログラムの技術支援は除きます。


ハードウェアや OS の技術的なお問い合わせについては有償サポートサービスにて承ります。詳細は、「[技術支援サービスについて](#)」(P.xii)をご参照ください。

- 明らかにハードウェア障害と思われる場合は、販売会社または保守会社にご連絡ください。

## 欠品・初期不良・故障について

本製品の納入時の欠品や初期不良および修理に関するお問い合わせは日立コールセンタにご連絡ください。

日立コールセンタ

 0120-921-789

受付時間

9:00～18:00（土・日・祝日、年末年始を除く）

お願い

- お電話の際には、製品同梱の保証書をご用意ください。

## 技術支援サービスについて

ハードウェアやソフトウェアの技術的なお問い合わせについては、技術支援サービスによる有償サポートとなります。

### 日立統合サポートサービス「日立サポート 360」

ハードウェアと、Windows や Linux などの OS を一体化したサポートサービスをご提供いたします。

詳細は次の URL で紹介しています。

- ホームページアドレス：  
<https://www.hitachi.co.jp/Prod/comp/soft1/support360/index.html>

インストールや運用時のお問い合わせや問題解決など、システムの円滑な運用のためにサービスのご契約をお勧めします。

運用時の問題解決をスムーズに行うためにサービスのご契約をお勧めします。

## 安全にお使いいただくために

安全に関する注意事項は、下に示す見出しによって表示されます。これは安全警告記号と「警告」、「注意」および「通知」という見出し語を組み合わせたものです。



これは、安全警告記号です。人への危害を引き起こす潜在的な危険に注意を喚起するために用います。起こりうる傷害または死を回避するために、このシンボルのあとに続く安全に関するメッセージに従ってください。



**警告** これは、死亡または重大な傷害を引き起こすおそれのある潜在的な危険の存在を示すのに用います。



**注意** これは、軽度の傷害、あるいは中程度の傷害を引き起こすおそれのある潜在的な危険の存在を示すのに用います。



**通知** これは、人身傷害とは関係のない損害を引き起こすおそれのある場合に用います。



【表記例1】感電注意

「△」の図記号は注意していただきたいことを示し、「△」の中に「感電注意」などの注意事項の絵が描かれています。



【表記例2】分解禁止

「⊗」の図記号は行ってはいけないことを示し、「⊗」の中に「分解禁止」などの禁止事項の絵が描かれています。

なお、「⊗」の中に絵がないものは、一般的な禁止事項を示します。



【表記例3】電源プラグをコンセントから抜け

「○」の図記号は行っていただきたいことを示し、「○」の中に「電源プラグをコンセントから抜け」などの強制事項の絵が描かれています。

なお、「○」は一般的に行っていただきたい事項を示します。

## 安全に関する共通的な注意について

次に述べられている安全上の説明をよく読み、十分理解してください。

- 操作は、このマニュアル内の指示、手順に従って行ってください。
- 本製品やマニュアルに表示されている注意事項は必ず守ってください。
- 本ソフトウェアをインストールするシステム装置のマニュアルを参照し、記載されている注意事項は必ず守ってください。

これを怠ると、人身上の傷害やシステムを含む財産の破損を引き起こすおそれがあります。

## 操作や動作は

マニュアルに記載されている以外の操作や動作は行わないでください。  
本製品について何か問題がある場合は、お買い求め先にご連絡ください。

## 自分自身でもご注意を

本製品やマニュアルに表示されている注意事項は、十分検討されたものです。それでも、予測を超えた事態が起こることが考えられます。操作に当たっては、指示に従うだけでなく、常に自分自身でも注意するようにしてください。

## 製品の損害を防ぐための注意

本製品の取り扱いにあたり次の注意事項を常に守ってください。



### 本製品のインストールについて

本製品は、本製品の動作をサポートしているシステム装置でご使用ください。それ以外のシステム装置にインストールすると、システム装置の仕様の違いにより故障の原因となります。サポート有無については、システム装置のマニュアルなどをご確認ください。

### 本マニュアル内の警告表示

#### 警告

本マニュアル内にはありません。

#### 注意

本マニュアル内にはありません。

### 通知

本マニュアル内にはありません。

本ページは空白ページです。





# Log Monitor の概要

この章では Log Monitor の概要について説明します。

- [概要](#)
- [機能](#)
- [適用機器](#)
- [サポート OS/仮想環境](#)
- [要求リソース](#)
- [前提ソフトウェア](#)
- [検知対象障害](#)
- [制限事項](#)

## 概要

Log Monitor は、OS 上のログ情報から Fibre Channel ボード[日立製]の障害情報を収集・解析します。

Log Monitor を導入することで、Fibre Channel ボード[日立製]の迅速な障害復旧が可能となり、システム装置の稼働率向上を実現します。

さらに保守会社の障害通報サービス（障害発生時に障害情報を保守会社に自動送信）と連携することで、障害発生時の初動対応における人的な時間のロスを抑えることができます。



HA8000V シリーズ/RV3000 の Log Monitor は、Fibre Channel ボード[日立製]の障害検知専用であり、Fibre Channel ボード[日立製]を含まない構成の場合、Log Monitor は不要です。なお、Fibre Channel ボード[日立製]の障害は iLO で検知できません。

なお、(株)日立システムズ(保守会社)が提供する障害通報サービス（プラットフォーム通報サービス）では Fibre Channel ボード[日立製]の通報機能を標準サポートしていません。障害通報するためには担当営業もしくは(株)日立システムズの保守員に Fibre Channel ボード[日立製]が搭載される構成であり Fibre Channel ボード[日立製]のプラットフォーム通報サービスの導入が必要なことをお伝え願います。

HA8000V シリーズ/RV3000 は、Fibre Channel ボード[日立製]の有無に関係なく、プラットフォーム通報サービスを導入する場合は iLO の設定が必要です。

## 機能

Log Monitor の機能について説明します。

### ハードウェアの障害・保守情報を収集・解析

Windows 版、Linux 版の Log Monitor は、OS ログ（Linux: syslog メッセージ）を監視し、障害イベントを検知すると障害イベントコードを生成します。

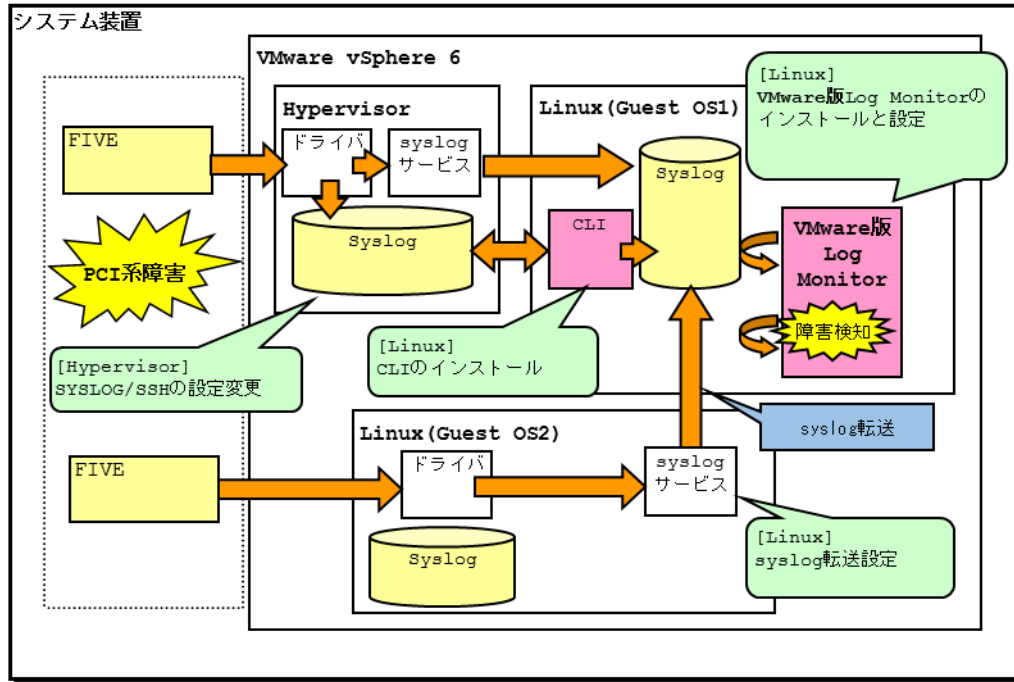
VMware 版 Log Monitor は、以下の 3 種類の syslog を監視することで、障害イベントの検知をし、障害イベントコードを生成します。

- Hypervisor の syslog
- Log Monitor をインストールしたゲスト OS の syslog
- VMware vSphere DirectPath I/O を設定したゲスト OS の syslog

なお、VMware vSphere DirectPath I/O を設定していない、ゲスト OS の syslog については Hypervisor の syslog 経由で監視されません。

VMware 版 Log Monitor は、ゲスト OS 上に Log Monitor をインストールして、監視対象の syslog を Log Monitor をインストールしたゲスト OS に転送して障害イベントを検知する方式（以下、ゲスト方式と略す）と ESXi ホストに CIM プロバイダ対応版の Log Monitor をインストールして障害イベントを検知する方式（以下、CIM 方式と略す）の 2 種類があります。

ゲスト方式の Log Monitor を導入した、システム装置の構成例は以下になります。



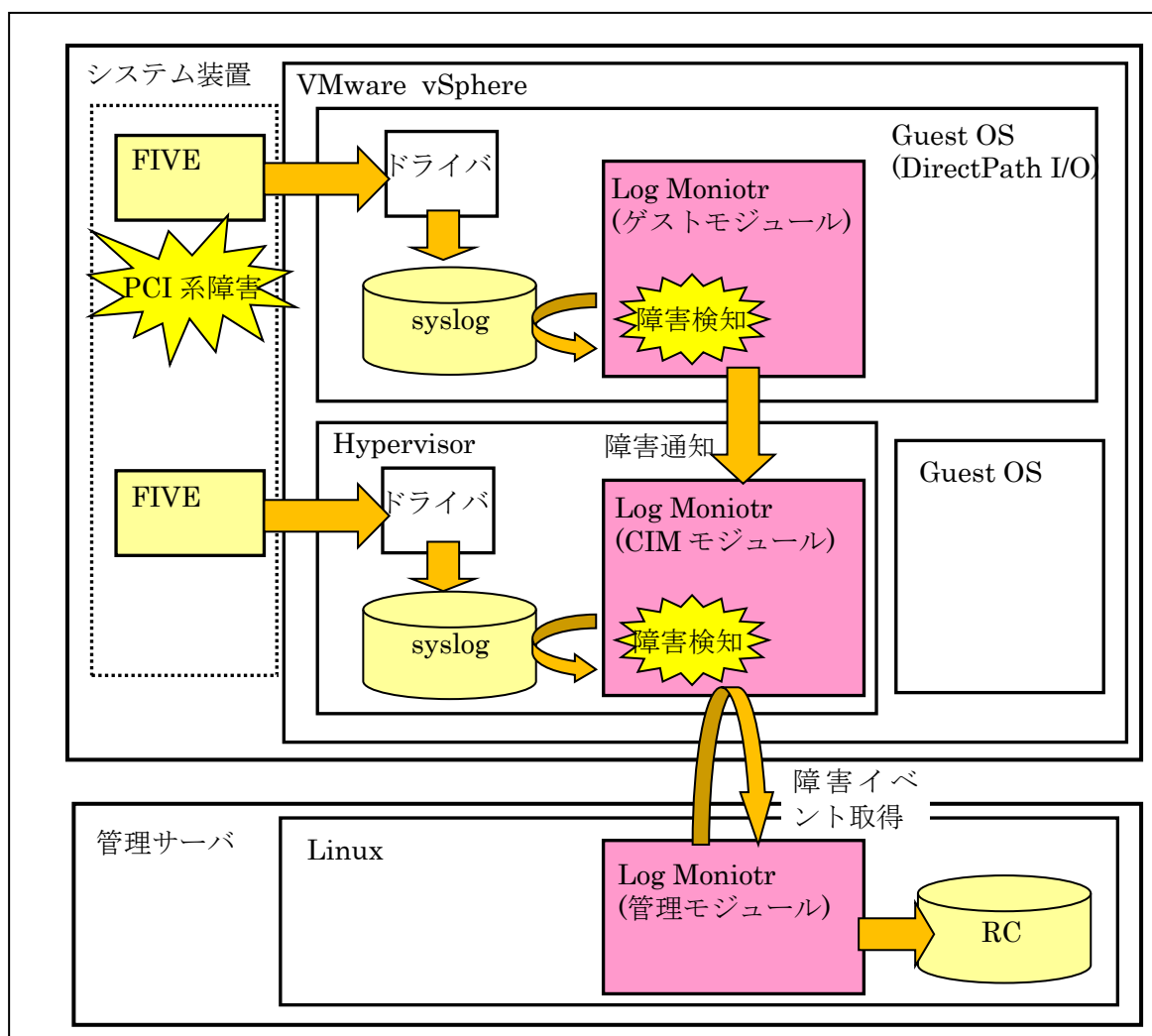
VMware 版 Log Monitor はシステム装置上のゲスト OS の内、1 つのゲスト OS に対してインストールを行います。Log Monitor をインストールしたゲスト OS は、syslog 転送により Hypervisor の syslog と VMware vSphere DirectPath I/O を設定したゲスト OS の syslog を取得します。これにより、Hypervisor と VMware vSphere DirectPath I/O を設定したゲスト OS の障害監視を実現します。また、Log Monitor が動作していないときに発生した障害は、Log Monitor 起動時に、Hypervisor および VMware vSphere DirectPath I/O を設定しているゲストに接続して syslog を採取します。

CIM 方式の Log Monitor は、下記の 3 つのモジュールで構成されます。

モジュール	機能
CIM モジュール	Hypervisor の syslog を監視して障害イベントを検知します。ゲストモジュールで検知した障害イベントも取得して、システム装置で発生した障害イベントを全て管理します。管理モジュールからのポーリングに対して、発生した障害イベントを通知します。

モジュール	機能
ゲストモジュール	DirectPath I/O を設定したゲスト OS の syslog を監視して障害イベントを検知します。検出した障害イベントは、CIM モジュールに通知します。
管理モジュール	監視対象のシステム装置上の CIM モジュールをポーリングして、システム装置で発生した障害イベントを取得します。 障害解析結果コード(RC)の生成と保守会社の通報サービスとの連携は本モジュールが行います。

CIM 方式の Log Monitor を導入した、システム装置の構成例は以下になります。



CIM モジュールは、ESXi 上で常時動作し、Hypervisor の syslog から障害イベントを検知します。ゲストモジュールは、DirectPath I/O を設定しているゲスト OS 上で動作し、ゲスト OS の syslog から検知した障害イベントを CIM モジュールに通知します。管理モジュールは、管理サーバ上で動作し、CIM モジュールを定期的に監視して障害イベントを取得します。取得した障害イベントを解析して、障害解析結果コード(RC)を生成し、障害解析結果コード(RC)の内容に応じて保守会社の通報サービスと連携します。

## 障害解析結果コード(RC)の生成

HA8000V シリーズ/RV3000 では、障害イベントコードを元に障害解析結果コード(RC)を生成します。障害解析結果コードは保守対応時に現象の把握と障害部位特定に利用されます。

## 通報サービスとの連携

保守会社の通報サービスと連携し、障害情報（障害解析結果コードなど）を自動送信することができます。

## 適用機器

Log Monitor がサポートする機器は次の通りです。  
なお Log Monitor のバージョンにより適用可能なシリーズ／モデルが異なります。

シリーズ		モデル	Log Monitor バージョン	対応 OS
HA8000V	Gen10 モデル	DL360 Gen10, DL380 Gen10, DL580 Gen10	47-xx	Linux
RV3000	A1 モデル	RV3000 A1	07-03 以降	Windows
			47-02 以降	Linux
			97-xx(ゲスト方式)	VMware
			98-xx(CIM 方式)	
	A2 モデル	RV3000 A2	07-06 以降	Windows
			47-10 以降	Linux
			98-xx(CIM 方式)	VMware
A3 モデル	RV3000 A3	47-13 以降	Linux	

## サポート OS/仮想環境

### サポート OS

Log Monitor がサポートする OS は以下の通りです。詳細なバージョンにつきましては、動作するシステム機器がサポートする OS を確認してください。

- Windows
- Red Hat Enterprise Linux

### サポート仮想環境

以下の仮想環境をサポートします。詳細なバージョンにつきましては、動作するシステム機器がサポートする OS を確認してください。

- VMware vSphere(サポートするゲスト OS は「サポート OS」の Linux OS となります)

## 要求リソース

Log Monitor は常駐型アプリケーションです。以下に、無負荷時、障害検知時における要求リソースの目安を表記します。

項目	無負荷時	障害検知時
CPU 負荷率	1%以下	10～30%
メモリ使用量	約 7MB	約 15MB
ディスク使用量 (*1)	約 7MB	約 200MB
ディスク使用量(syslog 転送用)(*2)	約 600MB	

\*1 : Log Monitor のインストールフォルダについては、「付録. [インストールフォルダ構成](#)」 P.78 を参照してください。

\*2 : 1 日あたりの syslog 転送量が 200MB 以内を想定しています。それ以上の syslog 転送量が発生する場合に、ディスクの空き領域を確保いただくか、ESXi(Hypervisor)上の syslog 発生量の削減をお願いいたします

Log Monitor は以下のサービスが常駐します。

OS 種別	サービス名称	常駐プロセス
Windows	SMAL2_MainteAgtSvc	C:\Program Files(x86)\HITACHI\miacat\Program\SMAL2Svc.exe C:\Program Files(x86)\HITACHI\miacat\Program\SMAL2MASvc.exe
Linux	smal2d	/opt/hitachi/miacat/Program/SMAL2MASvc
VMware	smal2d	/opt/hitachi/miacat/Program/SMAL2MASvc
	VmSyslogMAgtSrvd	/opt/hitachi/VmSyslogMAgtSrvd/bin/VmSyslogMAgtSrvd

Log Monitor は以下のポートを使用します。

ポート番号	サービス名称(*1)	説明
23141/tcp	core-linux	通報用機器との通信用ポート
23141/udp	—	通報用機器との疎通確認用ポート
31100/tcp	smal2_mainteregagt_port	Log Monitor の内部通信用ポート
31101/tcp	smal2_mainteagt_port	Log Monitor の内部通信用ポート
514/udp	syslog	Hypervisor の syslog メッセージ受信用ポート
443/tcp	https	esxcli コマンドの通信用ポート

他のプロセスにて既にポート番号が使用されている場合は、下記によりポート番号を変更することができます。

・通報用機器との通信用ポート (23141 ポート) は、(株)日立システムズ(保守会社)の作業が必要となりますので、(株)日立システムズに変更を依頼してください。

・上記以外のポートは、services ファイル(\*2)を編集することで使用するポート番号を変更することができます。

\*1 : Log Monitor インストール時、services ファイル(\*2)にサービス名称は追加されません。

\*2 : Linux:/etc/services



ファイアウォール機能でポート制限をしている場合は、**Log Monitor** で使用するポートを開放する必要があります。

---



## 前提ソフトウェア

Log Monitor の動作に必要なソフトウェアは次の通りです。

前提ソフトウェア	Windows 版	Linux 版	VMware 版 (ゲスト方式)	VMware 版(CIM 方式)			
				CIM モジュール	ゲストモジュール	管理モジュール(windows)	管理モジュール(Linux)
syslog サービス	—	○	○	—	○	—	○
32bit 実行環境ライブラリ	—	○	○(*1)	—	○(*1)	—	○
vSphere Client	—	—	○(*2)	—	○(*2)	—	—
esxcli	—	—	○(*1)	—	○(*1)	—	—
wbemcli	—	—	—	—	○	—	○
Fibre Channel ボード[日立製]用ユーティリティ(*3)	—	—	—	—	—	○	○
*1 : Log Monitor をインストールするゲスト OS にのみ必要 *2: 操作用の端末にインストール *3: Hitachi Gigabit Fibre Channel Adapter 対応ユーティリティ							

### syslog サービス

Log Monitor の OS ログ監視機能は、以下の設定を前提に動作します。OS に標準インストールされる syslog サービスの下記のフォーマットにのみ対応しています。

- syslogd の標準フォーマット  

```
Oct 31 00:00:00 localhost AppName[1234]: Message text ...
```
- syslogd の起動オプションに「-S または-SS」を指定した場合のフォーマット  

```
Oct 31 00:00:00 <syslog.info> localhost AppName[1234]: Message text ...
```
- rsyslogd の標準フォーマット（「\$ActionFileDefaultTemplate」ディレクティブで「RSYSLOG\_TraditionalFileFormat」を指定した場合）  

```
Oct 31 00:00:00 localhost AppName[1234]: Message text ...
```
- rsyslogd の「\$ActionFileDefaultTemplate」ディレクティブで「RSYSLOG\_FileFormat」を指定した場合のフォーマット  

```
2011-10-31T00:00:00.913136+09:00 localhost AppName[1234]: Message text ...
```

rsyslogd の「\$IncludeConfig」ディレクティブで設定ファイルの読み込み先を変更しないでください。変更すると Log Monitor の rsyslog 設定ファイルが読み込まれなくなります。

監視対象となる **syslog** ファイルは、**info** レベルを書き込む設定となっています。設定を変更しないでください。なお、監視対象となる **syslog** ファイルは、デフォルトパスに保存されているものを対象とします。監視対象となる **syslog** ファイルのデフォルトパスと、変更方法については「[監視対象 syslog ファイルの変更](#)」 P.69 をご覧ください。

## 32bit 実行環境ライブラリ

Linux OS には、次のライブラリがインストールされている必要があります。これらのパッケージは OS のインストール媒体に格納されています。

- glibc (32-bit x86)
- libstdc++ (32-bit x86)
- libgcc (32-bit x86)
- zlib (32-bit x86) ※VMware 版(CIM 方式)のみ必要

## vSphere Client

VMware 版 Log Monitor を導入する際の操作には vSphere Client を使用します。VMware 版 Log Monitor のインストールを行う前に vSphere Client で VMware システムを操作できる環境を用意してください。

## esxcli

VMware 版 Log Monitor を導入する際には esxcli のインストールが必要です。esxcli をインストールするには、VMware vSphere Command Line Interface もしくは Standalone ESXCLI をインストールする必要があります。Standalone ESXCLI をインストールする場合は、/usr/bin/に esxcli をインストールしてください。esxcli で hypervisor に接続する際、以下のメッセージが表示される場合は、Hypervisor への接続情報の設定で thumbprint を設定する必要があります。

```
Connect to xxx.xxx.xxx.xxx failed. Server SHA-1 thumbprint: thumbprint (not trusted)
```

## webmcli

VMware 版 Log Monitor(CIM 方式)を導入する際、ゲストモジュールと管理モジュール(Linux)は、次のライブラリがインストールされている必要があります。このパッケージは OS のインストール媒体に格納されています。

- sblim-wbemcli

### **Fibre Channel ボード[日立製]用ユーティリティ**

VMware 版 Log Monitor(CIM 方式)を導入する際には、管理サーバに Fibre Channel ボード [日立製]用ユーティリティの Hitachi Gigabit Fibre Channel Adapter 対応ユーティリティのインストールが必要です。保守会社の通報サービスとの連携の設定処理や障害時の保守対応で、本ユーティリティを使用します。

## 検知対象障害

Log Monitor は以下の障害を検知することができます。

ただし [前提ソフトウェア\(P.9\)](#) がインストールされ、正常に動作している必要があります。

No	部位(*7)		検知対象 (○:対象、-:対象外)					
			HA8000V シリーズ			RV3000		
			Windows	Linux	VMware	Windows	Linux	VMware
1	システム装置	FC コントローラ障害	-	○(*1)	-	○	○(*1)	○(*2)

\*1 : HA Logger Kit for Linux のログを検知する場合は、Log Monitor Ver.47-03 以降を使用してください。  
\*2 : VMware 版 Log Monitor(ゲスト方式)で Fibre Channel ボード[日立製]を VM DirectPath I/O モードで動作させる場合は、ゲスト OS 上の syslog に Fibre Channel ボードの障害ログが採取されます。Log Monitor がインストールされている OS へ syslog 転送する設定が必要になります。

## 制限事項

Log Monitor の制限事項を説明します。

- OS ログ (syslog メッセージ) が高頻度 (5 件/秒超) で記録されている状態では、その頻度・発生時間に比例して障害の検知が遅れることがあります。
- Log Monitor で障害監視を始める前に動作検証を実施してください。動作検証方法については「[3. Log Monitor の動作](#)」 - 「[動作検証](#)」 P.66 をご覧ください。
- Log Monitor はストレージの空き容量枯渇で継続動作が不可能となった場合、以下のメッセージを syslog に書き込み Log Monitor のサービスを停止します。

Log Monitor のサービスを再起動するためにはストレージの空き容量の確保が必要となります。

[ERROR] Stopped the log monitor. Because not enough available disk space.

Log Monitor が必要とするファイル容量は、「[要求リソース](#)」(P.7)の項を参照してください。

- 以下のメッセージが syslog に記録されている場合、Log Monitor の起動時に内部障害が発生したため、サービス起動後に発生するイベントの監視を始めたことを意味します。

サービス起動以前に発生したイベントについては遡って検知しません。

[WARN] Master Config is initialized.

## Linux 環境での制限事項

- Linux の場合、syslog メッセージがデフォルトフォーマット以外で記録されると、障害を検知できない場合があります。障害検知可能な syslog メッセージのフォーマットについては「[syslog サービス](#)」P.9 をご覧ください。
- 監視対象となる syslog ファイルの保存位置をデフォルトパス以外に変更する場合、Log Monitor の設定変更が必要となります。監視対象となる syslog ファイルのデフォルトパスと、変更方法については「[監視対象 syslog ファイルの変更](#)」P.69 をご覧ください。
- バージョン 47-04 以前の Log Monitor は、inode64(i-node 番号が 2 の 32 乗を超えるファイルシステムをマウントする時に使用するオプション)でマウントした XFS ファイルシステムにインストールして使用できません。

## VMware 環境での制限事項

- VMware 版 Log Monitor(ゲスト方式)では、ゲスト OS のシャットダウン中に発生した障害は hypervisor がログとして保持しており、Log Monitor は次回の ゲスト OS 起動時に同ログを取得して障害検知しますが、hypervisor がログを保持できる容量に限りがあるため、ゲスト OS シャットダウン中に発生したすべての障害を検知できないことがあります。
- VMware vSphere DirectPath I/O で I/O 占有しているゲスト OS の監視は、最大 5 ゲストまでとなります。VMware vSphere DirectPath I/O を用いず、I/O を共有する場合はゲスト数に制限はありません。
- Log Monitor(ゲスト方式)を同一の Hypervisor 上で稼働する複数の Linux(ゲスト OS)に対して、インストールしないでください。正常に障害監視ができなくなります。
- バージョン 97-02 以前の Log Monitor は、inode64(i-node 番号が 2 の 32 乗を超えるファイルシステムをマウントする時に使用するオプション)でマウントした XFS ファイルシステムにインストールして使用できません。
- VMware 版 Log Monitor(CIM 方式)を適用する場合、ESXi のログインパスワードに '@' と ':' は使用できません。
- VMware 版 Log Monitor(CIM 方式)の管理モジュールに登録できる監視対象のシステム装置は 32 台までです。32 台以上を監視する場合は、管理サーバを追加して管理モジュールをインストールしてください。
- VMware 版 Log Monitor(CIM 方式)で監視対象のシステム装置を登録できるのは、1 台の管理モジュールだけです。同じシステム装置を複数の管理モジュールに登録しないでください。



## Log Monitor の導入

この章では、Windows 版及び Linux 版 Log Monitor の導入方法について説明します。VMware 版の Log Monitor の導入方法は [VMware 版 Log Monitor の導入](#) を参照してください。

- [インストール前の準備](#)
- [インストール](#)
- [アンインストール](#)
- [アップグレード](#)
- [バージョンの確認](#)

## インストール前の準備

インストール前の準備について説明します。

- [前提ソフトウェアのインストール](#) (P.16)
- [ファイアウォールの設定](#) (P.16)

### 前提ソフトウェアのインストール

Log Monitor のインストールの前に[前提ソフトウェア](#)(P.9)をインストールしてください。  
インストール方法については、各ソフトウェアのマニュアルを参照してください。

### ファイアウォールの設定

ファイアウォールによる通信制限を行っているシステムでは、HA8000V シリーズ/RV3000 で通報サービスとの連携を行う場合、23141/tcp と 23141/udp を外部通信許可に設定してください。



## インストール

Log Monitor のインストール方法について説明します。

- [Windows へのインストール](#) (P.18)
- [Linux へのインストール](#) (P.19)



Log Monitor のインストール/アップグレードによるシステム装置のリブートは必要ありません。

ただし[前提ソフトウェア\(P.9\)](#)のインストールでリブートが必要になる場合があります。  
(各ソフトウェアのマニュアルを参照してください)

---

## Windows へのインストール

### Windows 版 Log Monitor のインストール

Windows 版のインストール方法について説明します。

1. "Administrator" でログインします。
2. インストーラパッケージ内にある次のインストーラを実行します。

**MIACAT.exe**

最新のインストーラパッケージは、ダウンロードサイトから入手してください。

[RV3000]

<https://www.hitachi.co.jp/products/it/rv3000/index.html>

3. 以降は画面の指示にしたがってインストールしてください。  
(インストール中にカスタマイズ可能な設定はありません)

以上で Log Monitor のインストールは終了です。

インストールに失敗した場合、次のメッセージが表示されます。

メッセージ	意味と対処(必要な場合に記載)
Not support this OS version.	インストールしようとしている OS は、Log Monitor でサポートされていません。
You do not have access to make the required system configuration modifications. Stop the installation. Please rerun this installation from an administrators account.	システムの設定を変更する権利がありません。 対処: アドミニストレータ権限を持つユーザでインストールしてください。
Stop the installation. Remote Maintenance Option Setting Tool is running. Please start an installer after terminating Remote Maintenance Option Setting Tool.	ハードウェア保守登録プログラムが実行中です。 対処: ハードウェア保守登録プログラムを停止させてから、Log Monitor のインストールを実行してください。

## Linux へのインストール

### Linux 版 Log Monitor のインストール

Linux 版のインストール方法について説明します。

1. root 権限でログインします。
2. snvlnm\_47-xx\_linux.zip (Linux 版 Log Monitor) をインストールするシステム装置上に転送します。
3. 次のコマンドを実行し、snvlnm\_47-xx\_linux.zip (Linux 版 Log Monitor) を展開します。  
`# unzip snvlnm_47-xx_linux.zip`  
"x"(イタリック体) : バージョン番号等の英数字が入ります。
4. 次のコマンドを実行し、Linux 版 Log Monitor のインストールを行います。  
`# ./logmonsetup.sh -i`

最新のインストーラパッケージは、下記ダウンロードサイトから入手してください。

[HA8000V シリーズ]

<https://www.hitachi.co.jp/products/it/ha8000v/index.html>

[RV3000]

<https://www.hitachi.co.jp/products/it/rv3000/index.html>

以上で Log Monitor のインストールは終了です。インストールに失敗した場合、次のメッセージが表示されます。

メッセージ	意味と対処(必要な場合に記載)
MIACAT-xxxx-x is already installed.	【新規インストールのみ】 Log Monitor またはハードウェア保守エージェントが既にインストールされている。 対処：アップグレードを実施してください。
Failed. You are not root user.	実行ユーザが"root"ではありません。 対処：実行ユーザを"root"に切り替えてインストールしてください。
This machine is un-support model, or failed to read model code.	未サポートの機器に対してインストールしようとした。

## アンインストール

Log Monitor のアンインストール方法について説明します。

### Windows 版 Log Monitor のアンインストール

Windows 版のアンインストール方法について説明します。

1. "Administrator" でログインします。
2. Uninstall を起動します。

次のコマンドを実行します。

```
C:¥Program Files(x86)¥HITACHI¥miacat¥UNINST.EXE
```

以上で Log Monitor のアンインストールは終了です。

### Linux 版 Log Monitor のアンインストール

Linux 版のアンインストール方法について説明します。

1. root 権限でログインします。
2. snvlnm\_47-xx\_linux.zip (Linux 版 Log Monitor) をインストールするシステム装置上に転送します。
3. 次のコマンドを実行し、snvlnm\_47-xx\_linux.zip (Linux 版 Log Monitor) を展開します。

```
# unzip snvlnm_47-xx_linux.zip
```

4. 次のコマンドを実行します。

```
# ./logmonsetup.sh -e
```

以上で Log Monitor のアンインストールは終了です。

## アップグレード

Log Monitor のアップグレード方法について説明します。

- [Windows でのアップグレード](#) (P.21)
- [Linux でのアップグレード](#) (P.21)

## Windows でのアップグレード

### Windows 版 Log Monitor のアップグレード

新規インストールと同じ手順でインストールできます。(旧バージョンをアンインストールする必要はありません。またすべての設定が引き継がれます。)

インストール手順については、[Windows へのインストール](#) (P.18)を参照ください。

## Linux でのアップグレード

### Linux 版 Log Monitor のアップグレード

Linux 版 Log Monitor をアップグレードする方法について説明します。

アップグレードではすべての設定が引き継がれます。

1. root 権限でログインします。
2. `snvlnm_47-xx_linux.zip` (Linux 版 Log Monitor) をインストールするシステム装置上に転送します。
3. 次のコマンドを実行し、`snvlnm_47-xx_linux.zip` (Linux 版 Log Monitor) を展開します。  
`# unzip snvlnm_47-xx_linux.zip`  
"x"(イタリック体) : バージョン番号等の英数字が入ります。
4. 次のコマンドを実行し、Linux 版 Log Monitor のアップグレードを行います。

```
# ./logmonsetup.sh -i
```

最新のインストーラパッケージは、下記ダウンロードサイトから入手してください。

[HA8000V シリーズ]

<https://www.hitachi.co.jp/products/it/ha8000v/index.html>

[RV3000]

<https://www.hitachi.co.jp/products/it/rv3000/index.html>

以上で Log Monitor のアップグレードは終了です。

インストール失敗時に表示されたメッセージについては、[Linux へのインストール \(P.19\)](#)を参照ください。

## バージョンの確認

バージョンの確認方法について説明します。

### Windows 版 Log Monitor のバージョンの確認

Windows 版 Log Monitor のバージョンの確認方法について説明します。

1. "Administrator" でログインします。
2. コマンドプロンプト上で、次のコマンドを実行します。

```
sc qdescription SMAL2_MainteAgtSvc
```

3. Log Monitor の製品名とバージョンが表示されます。

以上で Log Monitor のバージョンの確認は終了です。

### Linux 版 Log Monitor のバージョンの確認

Linux 版 Log Monitor のバージョンの確認方法について説明します。

1. root 権限でログインします。
2. 次のコマンドを実行します。

```
rpm -qi MIACAT
```

3. 「Version」にバージョン番号が表示されます。

以上で Log Monitor のバージョンの確認は終了です。

## VMware 版 Log Monitor(ゲスト方式)の導入

この章では、VMware 版 Log Monitor (ゲスト方式)の導入方法について説明します。VMware 版 Log Monitor (CIM 方式)の導入方法については、「[VMware 版 Log Monitor\(CIM 方式\)の導入](#)」を参照してください。

### Log Monitor VMware 版 Log Monitor(ゲスト方式)での障害検知方法

VMware 版 Log Monitor(ゲスト方式)での障害検知の方法は、1つのゲストに Log Monitor をインストールし、そのゲスト OS にログ情報を転送することで障害を検知します。なお、正常に障害監視ができなくなりますので、Log Monitor を 2 ゲスト以上に対してインストールしないでください。

Log Monitor をインストールするゲスト OS と Log Monitor をインストールしないゲスト OS に対するログ情報を転送するための設定について、以下説明します。

VMware vSphere DirectPath I/O を適用しない場合に必要な設定は下記となります。

#### 【Log Monitor をインストールするゲスト OS】

下記の設定が必要となります。

- Hypervisor が検知したログ情報を syslog 転送するための出力先の設定
- Log Monitor が、動作していないときに発生した障害を検知するために、Log Monitor 起動時に、Hypervisor に接続してログ情報を採取するための設定

#### 【Log Monitor をインストールしないゲスト OS】

設定は不要です。

VMware vSphere DirectPath I/O を適用する場合に必要な設定は下記となります。

#### 【Log Monitor をインストールするゲスト OS】

下記の設定が必要となります。

- Hypervisor が検知したログ情報を syslog 転送するための出力先の設定

- VMware vSphere DirectPath I/O を設定しているゲスト OS が検知したログ情報を syslog 転送するための出力先の設定
- Log Monitor が、動作していないときに発生した障害を検知するために、Log Monitor 起動時に、Hypervisor および VMware vSphere DirectPath I/O を設定しているゲスト OS に接続してログ情報を採取するための設定

#### 【Log Monitor をインストールしないゲスト OS】

VMware vSphere DirectPath I/O を設定するゲスト OS には、OS が検知したログ情報を syslog 転送するための設定が必要となります。この、VMware vSphere Direct Path I/O を設定するゲスト OS を、これ以降「監視対象のゲスト OS」と呼びます。

Log Monitor のインストールや syslog 転送の設定をする際は、作業用のディレクトリを用意して頂き、そのディレクトリに Log Monitor のインストールファイルをコピーしてください。操作説明では設定値の例として以下の値を記載しています。お客様の環境に合わせて読み換えてください。

#### 【操作説明での設定値の例】

- Hypervisor の IP アドレス : 「192.168.100.2」  
Hypervisor の root 権限ユーザ ID : 「root」  
Hypervisor の root 権限ユーザパスワード : 「password」  
ゲスト OS(\*1)の IP アドレス(ゲスト 1) : 「192.168.100.10」  
ゲスト OS(\*2)の IP アドレス(ゲスト 2) : 「192.168.100.11」  
ゲスト OS(\*2)の IP アドレス(ゲスト 3) : 「192.168.100.12」
- (\*1) Log Monitor をインストールするゲスト OS
- (\*2)監視対象のゲスト OS

#### 【VMware 版 Log Monitor(ゲスト方式)の導入手順】

- [Hypervisor の設定](#)
- [監視対象のゲスト OS の設定](#)
- [Log Monitor をインストールするゲスト OS の設定](#)
- [Log Monitor のインストール](#)
- [アンインストール](#)
- [アップグレード](#)
- [バージョンの確認](#)



## 前提条件について

- Log Monitor をインストールするゲスト OS と監視対象のゲスト OS は同一の Hypervisor 上である必要があります。
- VMware ESXi のロックダウンモードを無効にしてください。ロックダウンモードが有効な場合、VMware 版 Log Monitor は障害を検知することができません。
- VMware vSphere DirectPath I/O で I/O 占有しているゲスト OS は、最大 5 ゲストまで監視することができます。VMware vSphere DirectPath I/O を用いず、I/O を共有する場合はゲスト数に制限はありません。

## Hypervisor の設定

- [Hypervisor の SSH 機能の有効化](#)
- [Hypervisor の syslog メッセージ転送の有効化](#)
- [VMware\(Hypervisor\)を再起動する](#)

### Hypervisor の SSH 機能の有効化

Hypervisor の SSH 機能を有効化します。

1. システム装置(Hypervisor)の起動画面で [F2] キーを押します。
2. Login 画面が表示されるので、root 権限ユーザでログインします。
3. [System Customization]画面が表示されるので、[Troubleshooting Options]を選択して、[Enter]キーを押します。
4. [Enable SSH]を選択して、[Enter]キーを押します。
5. [ESC]キーを数回押し、起動画面に戻ります。

以上で Hypervisor の SSH 機能の有効化は終了です。



- Hypervisor の設定で、SSH 機能の有効化にタイムアウトを設定されている場合、SSH 機能有効化後に設定された時間が経過すると自動的に SSH 機能が無効化されます。
  - Log Monitor をインストール後も Hypervisor の SSH 機能の有効化が必要です。
- 

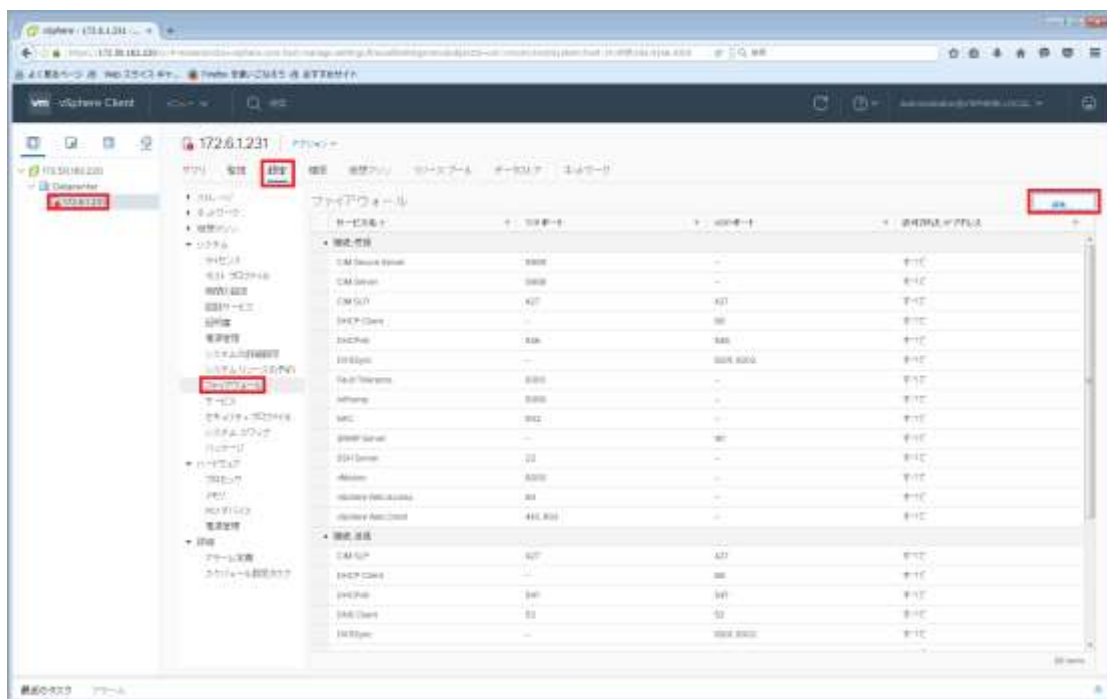
### Hypervisor の syslog メッセージ転送の有効化

Hypervisor の syslog 設定の変更方法について説明します。

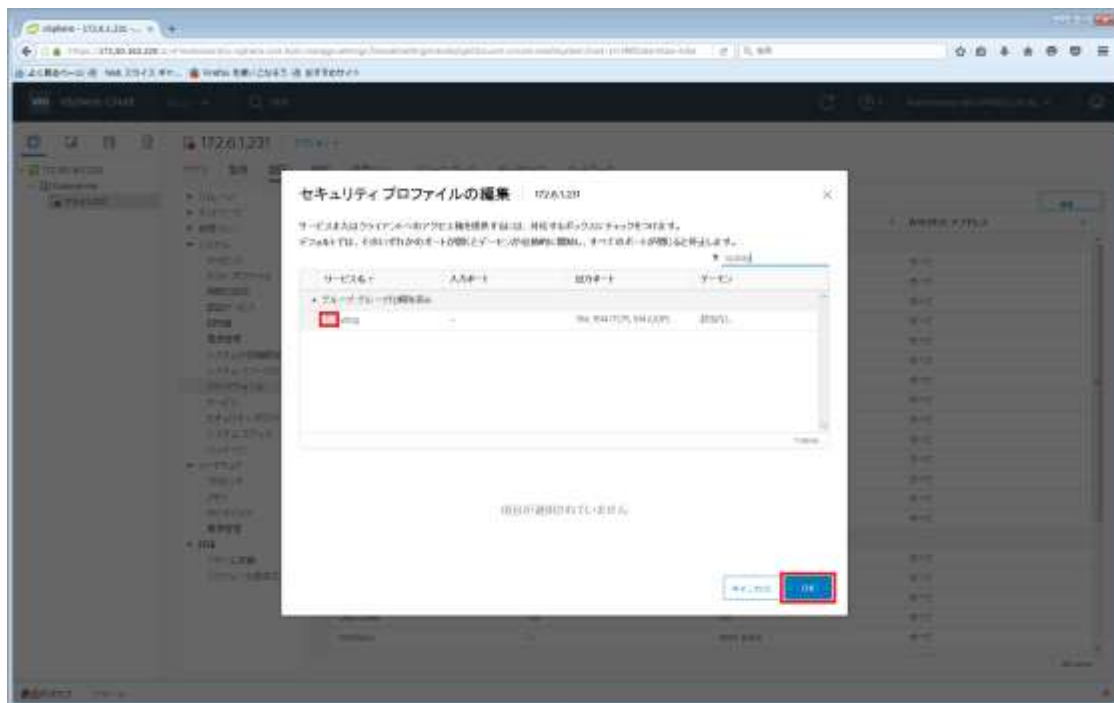


- 本書は、vSphere Client(HTML5)を使用した操作を前提にしているため、VMware Host Client を使用した操作手順については記載していません。
-

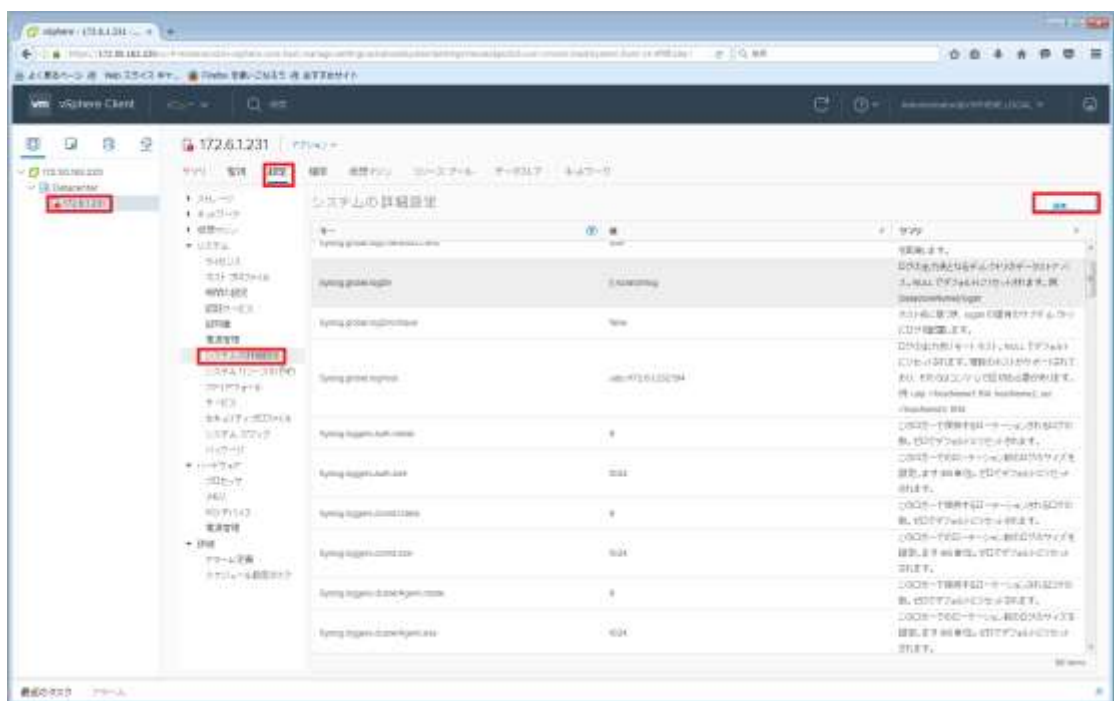
1. vSphere Client の Hypervisor の「設定」タブを開き、「システム」-「ファイアウォール」を選択します。「ファイアウォール」が表示されたら、「編集」ボタンをクリックします。



2. 「セキュリティプロファイルの編集」が開くので、「syslog」のチェックボックスにチェックを入れ、OKを押します。



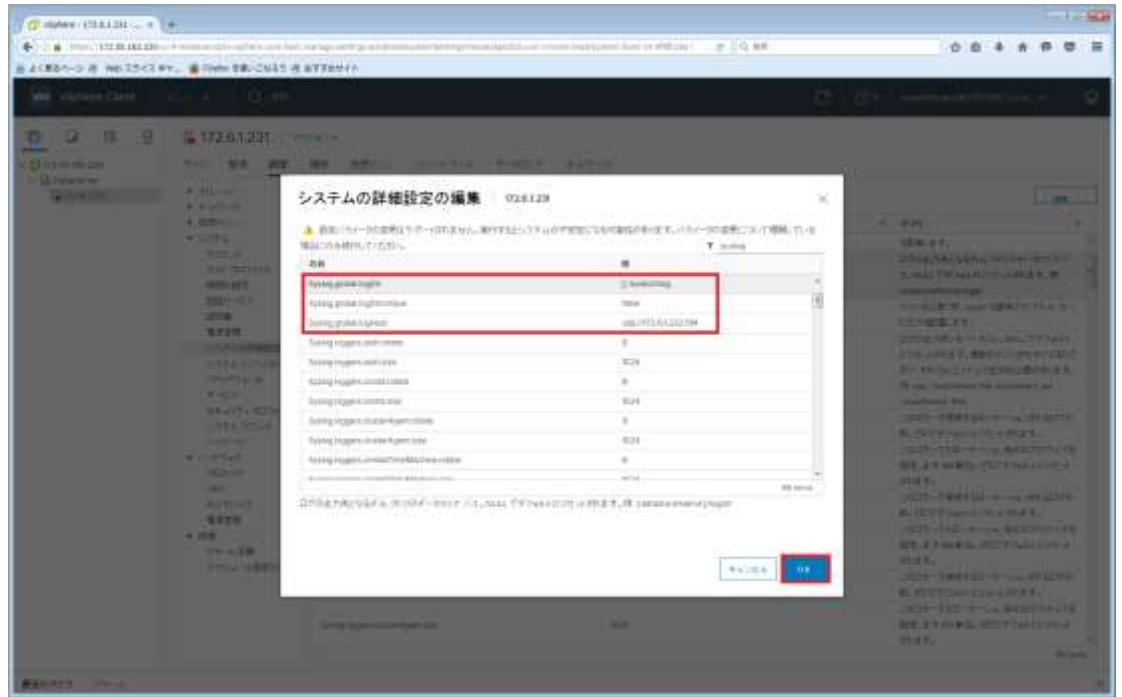
3. vSphere Client の Hypervisor の「設定」タブを開き、「システムの詳細設定」をクリックします。「システムの詳細設定」が表示されたら、「編集」ボタンをクリックします。



システムの詳細設定の編集で設定を下記のように変更して OK を押します。

- Syslog.global.logDir : "[ ] /scratch/log"
- Syslog.global.logDirUnique : "いいえ"を選択する
- Syslog.global.logHost : "udp://IP アドレス (\*1):514"  
(例 "udp://192.168.100.10:514")

(\*1) Log Monitor をインストールするゲスト OS の IP アドレスを設定する。



以上で syslog 設定は終了です。

## VMware(Hypervisor)を再起動する

必ず VMware(Hypervisor)の再起動を行ってください。

再起動を行わなかった場合、Log Monitor のインストールに失敗します。

## 監視対象のゲスト OS 設定

### Syslog 転送設定をする

監視対象のゲスト OS に対して、Syslog 転送設定を行います。

1. vSphere Client からゲスト OS のコンソールを開きます。(root ユーザでログインしてください)
2. snvlnm\_97-xx\_vm.zip (VMware 版 Log Monitor) を監視対象のゲスト OS に転送します。
3. 次のコマンドを実行し、ファイルを展開します。xxxx はバージョンを示す数字となります。

```
# unzip snvlnm_xx-xx_vm.zip
# tar pxzvf miacat_syslog_xxxx.tar.gz
```

4. 次のコマンドを実行し、syslog 転送の設定をコピーします。

```
#cd miacat_syslog/rsyslog_conf
#cp rsyslog_conf_vm_guest_for_miacat.conf /etc/rsyslog.d/
```

5. コピーした syslog 転送の設定を変更します。設定ファイルの設定内容について、**ゲスト OS の IP アドレス**に Log Monitor をインストールするゲスト OS の IP アドレスを設定してください。また、**UDP のポート番号**には syslog サービスで使用する UDP のポート番号を設定してください。デフォルトのポート番号は 514 で、ポート番号を変更した場合は設定を変更してください。

設定ファイル名 : `/etc/rsyslog.d/rsyslog_conf_vm_guest_for_miacat.conf`

設定内容 :

\*.\* @**ゲスト OS の IP アドレス: UDP のポート番号 (\*1)(\*2)**

(\*1) Log Monitor をインストールするゲスト OS の IP アドレスを設定してください。

(\*2) UDP のポート番号 : syslog サービスの UDP のポート番号(デフォルト:514)

### ゲスト OS を再起動する

必ず Log Monitor の監視対象となる全てのゲスト OS の再起動を行ってください。再起動を行わなかった場合、Log Monitor のインストールに失敗します。

## Log Monitor をインストールするゲスト OS 設定

Log Monitor をインストールするゲスト OS の設定変更の方法について説明します。Log Monitor をインストールするゲスト OS は必ず 1 つである必要があります。

### 【操作の流れ】

- [前提ソフトウェアのインストール](#)
- [ファイアウォールの設定](#)
- [Hypervisor への接続確認](#)
- [Log Monitor CLI のインストール](#)
- [Hypervisor 及びゲスト OS への接続情報の設定](#)
- [Syslog の出力先の設定をする](#)

### 前提ソフトウェアのインストール

Log Monitor のインストールの前に[前提ソフトウェア](#)(P.9)をインストールしてください。インストール方法については、各ソフトウェアのマニュアルを参照してください。

### ファイアウォールの設定

ファイアウォールによる通信制限を行っているシステムでは、RV3000 で通報サービスとの連携を行う場合、23141/tcp と 23141/udp を外部通信許可に設定してください。

### Hypervisor への接続確認

作業前に Hypervisor への接続状態を確認します。

1. 下記のコマンドで Hypervisor に接続可能かを確認します。**IP アドレス**は Hypervisor の IP アドレスを指定してください。接続できない場合は、メッセージに表示される thumbprint を記録してください、

```
# esxcli -s IP アドレス
```

以下に接続できない場合の実行例を示します。

```
# esxcli -s xxx.xxx.xxx.xxx
Certificate error: Server SHA-1 thumbprint:
C7:45:29:9B:70:41:FC:5E:42:A9:C4:8A:99:5C:0E:70:E1:8D:94:DA (not trusted)
↑ thumbprint
```

## Log Monitor CLI のインストール

Hypervisor 及び監視対象のゲスト OS への接続設定をするための Log Monitor CLI をインストールします。

1. vSphere Client から Log Monitor をインストールするゲスト OS のコンソールを開きます。(root ユーザでログインしてください)
2. 次のコマンドを実行し、ファイルを展開します。

```
#unzip snvIm_xx-xx_vm.zip  
#tar pxzvf logmoncli.tar.gz
```

3. 次のコマンドを実行し、Log Monitor CLI をインストールします。

```
#cd logmoncli  
#./logmoncli_setup.sh
```

以上で Log Monitor CLI のインストールは終了です。

## Hypervisor 及びゲスト OS への接続情報の設定

Log Monitor をインストールするゲスト OS から、Hypervisor 及び監視対象のゲスト OS への接続情報の設定の手順について説明します。

1. 下記コマンドで Hypervisor への接続情報の設定をします。

```
# /opt/hitachi/tools/miacat/logmoncli -t esxi <パラメータ>
```

以下に設定するパラメータを示します。

パラメータ	省略可否	説明
-i IP アドレス	必須	Hypervisor の IP アドレス
-u user 名	必須	ログインユーザ名。root 権限があること
-d thumbprint	省略可	esxcli の実行に必要なサムプリントを指定する。(注 1)
password	必須	ログインパスワード。 コマンド実行後に表示される入力プロンプトに入力してください。

注 1 : Hypervisor への接続確認で接続できなかった場合は、記録した thumbprint を指定してください。

以下に実行例を示します。

```
# /opt/hitachi/tools/miacat/logmoncli -t esxi -i IP アドレス -u User 名  
password:  
INFO: Configuration has been saved.
```





Hypervisor への接続情報を設定した後、thumbprint が変更された場合は、変更された thumbprint を指定して Hypervisor への接続情報を再設定してください。

2. 接続情報が正しく設定できているか確認してください。確認方法は設定ファイルである、`/opt/hitachi/tools/miacat/data/esxihost.ini` を参照してください。

```
[Esxihost]
ipaddress=192.168.100.2
username=root
password=
thumbprint=
:
```

3. 下記コマンドで監視対象のゲスト OS への接続設定をします。なお、Log Monitor をインストールするゲスト OS への接続情報は不要です。**IP アドレス**は監視対象のゲスト OS の IP アドレス、**User 名**は root、**ゲスト OS 上の syslog パス**は監視対象のゲスト OS 上の syslog パス(`/var/log/messages` など)を指定してください。

```
# /opt/hitachi/tools/miacat/logmoncli -t vm -i IP アドレス -u User 名 -s ゲスト OS 上の syslog パス
password:
INFO: Configuration has been saved.
```

4. 接続情報が正しく設定できているか確認してください。確認方法は設定ファイルである、`/opt/hitachi/tools/miacat/data/vminfo.ini` を参照してください。

```
[Server0]
ipaddress:192.168.1.11
username:root
password:
thumbprint:
[Server1]
ipaddress:192.168.1.12
username:root
password:
thumbprint:
```

## Syslog の出力先の設定をする

監視対象のゲスト OS から転送されてきた Syslog の出力先の設定を行います。

1. vSphere Client から Log Monitor をインストールするゲスト OS のコンソールを開きます。  
(root ユーザでログインしてください)
2. 次のコマンドを実行し、イベント管理ツールをインストールします。miacat-vel-install-xxxx.sh の xxxx はバージョンを示す数字となります。

```
# tar pxzvf miacat_syslog_xxxx.tar.gz
```

```
# cd miacat_syslog/miacat-vel
# ./miacat-vel-install-xxxx.sh
```

### 3. syslog の設定ファイルの変更を行います。

Hypervisor 及び監視対象のゲスト OS から転送されてきた syslog の出力先の設定をします。デフォルトでは、Log Monitor がインストールされているゲスト OS と Hypervisor のみを監視する設定です。監視対象のゲスト OS を追加するには、次の設定ファイルの変更をしてください。

設定ファイル名 : `/etc/rsyslog.d/rsyslog_conf_for_miacat.conf`

- 以下の設定値の変更と追加を行います。監視対象の OS の IP アドレスはゲスト数に応じて追加をしてください。以下は 2 つのゲスト OS を監視する場合の設定です。  
:fromhost-ip, **isequal**, "**Hypervisor の IP アドレス**" /var/log/esxi-syslog\_for\_miacat.log;RSYSLOG\_FileFormat (\*1)  
& ~ (\*2)  
:fromhost-ip, isequal, " **ゲスト OS の IP アドレス(ゲスト 2)**" /var/log/vmquest-syslog\_for\_miacat\_server0.log;RSYSLOG\_FileFormat (\*3)  
& ~ (\*2)  
:fromhost-ip, isequal, " **ゲスト OS の IP アドレス(ゲスト 3)**" /var/log/vmquest-syslog\_for\_miacat\_server1.log;RSYSLOG\_FileFormat (\*3)  
& ~ (\*2)

(\*1) デフォルトでは、転送されてきた syslog を Hypervisor の syslog として出力する設定になっています。監視対象のゲスト OS を追加する場合は、上記のように、Hypervisor の IP アドレスを指定して、/var/log/esxi-syslog\_for\_miacat.log へ書き込む設定に変更してください。isequal は等しい場合、!isequal は等しくない場合を表します。Hypervisor に関する設定のデフォルトの値は、!isequal となっています。Hypervisor の IP アドレスを指定して監視する場合は"!"を削除するようにしてください。

(\*2) 直前の条件に合致したログを破棄する設定です。二重にログが出力されるのを防止します。

(\*3) syslog の転送元が、IP アドレスと等しい場合に vmquest-syslog\_for\_miacat\_serverX.log(X は 0 から 4 の数字)へ書き込む設定です。監視対象のゲスト OS 毎に vmquest-syslog\_for\_miacat\_serverX.log の X の値を変更してください。X の値は、[Hypervisor 及びゲスト OS への接続情報の設定](#) で作成した /opt/hitachi/tools/miacat/data/vminfo.ini を参照し、[ServerX](X は数字)の値に合わせてください。

## ゲスト OS を再起動する

必ずゲスト OS の再起動を行ってください。

再起動を行わなかった場合、Log Monitor のインストールに失敗します。

## Syslog メッセージ転送の動作を確認する

Log Monitor をインストールするゲスト OS 上に以下のファイルがあることを確認してください。

- /var/log/esxi-syslog\_for\_miacat.log  
(Hypervisor から転送される syslog メッセージのファイル)
  - 「[Hypervisor の syslog メッセージ転送の有効化](#)」の「Syslog.global.logHost」の設定
- /var/log/vmquest-syslog\_for\_miacat\_serverX(X は 0 から 4 の数字)  
(監視対象のゲスト OS から転送される syslog メッセージのファイル)
  - 「[Hypervisor 及びゲスト OS への接続情報の設定](#)」の /opt/hitachi/tools/miacat/data/vminfo.ini の設定

## Log Monitor のインストール

VMware 版 Log Monitor のインストール方法について説明します。

1. vSphere Client から Log Monitor をインストールするゲスト OS のコンソールを開きます。(root ユーザでログインしてください)
2. インストールファイルを展開した作業ディレクトリで次のコマンドを実行し、VMware 版 Log Monitor のインストールを行います。

```
# ./logmonsetup.sh -i
```

3. 次のコマンドを実行し、「Version」にバージョン番号が表示されることを確認します。

```
#rpm -qi MIACAT_HAVRHEL
```

最新のインストーラパッケージは、下記ダウンロードサイトから入手してください。  
[RV3000]

<https://www.hitachi.co.jp/products/it/rv3000/index.html>

以上で VMware 版 Log Monitor のインストールは終了です。

インストールに失敗した場合、次のメッセージが表示されます。

メッセージ	意味と対処(必要な場合に記載)
package MIACAT_XXXXX-XXXX-X is already installed	Log Monitor が既にインストールされている。 アップグレードインストールを行ってください。
Failed. You are not root user.	実行ユーザが"root"ではありません。 対処：実行ユーザを"root"に切り替えてインストールしてください。



Hypervisor への接続情報の設定で thumbprint の設定が漏れていた場合、インストール時に ESXi から装置情報が取得できないためインストールに失敗する場合があります。[Log Monitor をインストールするゲスト OS 設定](#)の Hypervisor への接続確認で thumbprint の設定が必要かを確認してください。

### Log Monitor の動作確認

Log Monitor をインストールしたゲスト OS 上にある、「/var/opt/hitachi/VmSyslogMAgtSrvd/vmkernel.log」ファイル (Log Monitor 起動時に取得した Hypervisor 上の vmkernel.log) の更新日時が、Log Monitor のインストール後の日時になっていることを確認してください。  
更新されていない場合、次の操作を見直してください。

- 「[Hypervisor の syslog メッセージ転送の有効化](#)」の「Syslog.global.logDir」と「Syslog.global.logDirUnique」の設定

動作確認後は、「[障害解析結果コード\(RC\)の参照](#)」及び「[動作検証](#)」を実施してください。

## アンインストール

VMware 版 Log Monitor のアンインストール方法について説明します。VMware 版は Log Monitor のアンインストール、Syslog 転送設定のアンインストール、CLI のアンインストールが必要です。

### Log Monitor のアンインストール

1. vSphere Client から Log Monitor をインストールするゲスト OS のコンソールを開きます。(root ユーザでログインしてください)
2. 次のコマンドを実行し、ファイルを展開します。

```
# unzip snvIm_XX-XX_vm.zip
```

"x"(イタリック体) : バージョン番号等の英数字が入ります。

3. 次のコマンドを実行します。

```
# ./logmonsetup.sh -e
```

以上で VMware 版 Log Monitor のアンインストールは終了です。

### Syslog 転送設定のアンインストール

Syslog 転送設定のアンインストール方法について説明します。

1. root 権限でログインします。
2. 次のコマンドを実行し、syslog 転送設定のファイルを削除します。

[Log Monitor をインストールしたゲスト OS]

```
# rm /etc/rsyslog.d/rsyslog_conf_for_miacat.conf
```

[監視対象のゲスト OS]

```
# rm /etc/rsyslog.d/rsyslog_conf_vm_guest_for_miacat.conf
```

3. rsyslog の再起動を行います。

```
# systemctl restart rsyslog
```

以上で Syslog 転送設定のアンインストールは終了です。

## Log Monitor CLI のアンインストール

Log Monitor CLI のアンインストール方法について説明します。

1. Log Monitor をインストールしたゲスト OS に **root** 権限でログインします。
2. 次のコマンドを実行し、ファイルを展開します。

```
#unzip snvIm_xx-xx_vm.zip  
#tar pxzvf logmoncli.tar.gz
```

3. 次のコマンドを実行し、CLI をアンインストールします。

```
#cd logmoncli  
#./logmoncli_setup.sh -e
```

以上で Log Monitor CLI のアンインストールは終了です。

## アップグレード

VMware 版 Log Monitor のアップグレード方法について説明します。

1. vSphere Client から Log Monitor をインストールしたゲスト OS のコンソールを開きます。(root ユーザでログインしてください)
2. 次のコマンドを実行し、VMware 版 Log Monitor のアップグレードインストールを行います。

(1) 次のコマンドを実行し、ファイルを展開します。

```
# unzip snvIm_XX-XX_vm.zip
```

"X"(イタリック体) : バージョン番号等の英数字が入ります。

(2) 次のコマンドを実行し、VMware 版 Log Monitor のインストールを行います。

```
# ./logmonsetup.sh -i
```

インストール失敗時に表示されたメッセージについては、[Log Monitor のインストール](#)を参照ください。

3. VMware 版 Log Monitor の動作を確認します。  
動作確認手順については、[Log Monitor の動作確認](#)を参照ください。

以上で VMware 版 Log Monitor のアップグレードは終了です。

## バージョンの確認

VMware 版 Log Monitor のバージョンの確認方法について説明します。

1. vSphere Client から Log Monitor がインストールされているゲスト OS のコンソールを開きます。(root ユーザでログインしてください)
2. 次のコマンドを実行します。

```
# rpm -qi MIACAT_HAVRHEL
```
3. 「Version」にバージョン番号が表示されます。

以上で VMware 版 Log Monitor のバージョンの確認は終了です。



## VMware 版 Log Monitor(CIM 方式)の導入

この章では、VMware 版 Log Monitor (CIM 方式)の導入方法について説明します。VMware 版 Log Monitor (ゲスト方式)の導入方法については、「[VMware 版 Log Monitor \(ゲスト方式\)の導入](#)」を参照してください。

### Log Monitor VMware 版 Log Monitor(CIM 方式)での障害検知方法

CIM 方式の Log Monitor は、下記の 3つのモジュールで構成されます。それぞれのインストール先と検知する障害の内容について示します。

モジュール	インストール先と検知する障害
CIM モジュール	ESXi にインストールし、Hypervisor の syslog を監視して障害イベントを検知します。
ゲストモジュール	DirectPath I/O を設定するゲスト OS にインストールし、OS の syslog を監視して障害イベントを検知します。検出した障害イベントは、CIM モジュールに通知します。
管理モジュール	管理サーバにインストールし、システム装置上の CIM モジュールをポーリングして、システム装置で発生した障害イベントを取得します。

CIM モジュールは、Hypervisor の syslog から障害イベントを検知します。ゲストモジュールは、DirectPath I/O を設定しているゲスト OS の syslog から障害イベントを検知します。DirectPath I/O を設定している全てにゲスト OS にゲストモジュールをインストールする必要があります。検知した障害イベントは、CIM モジュールに通知します。管理モジュールは、CIM モジュールを定期的に監視して障害イベントを取得します。

#### 【VMware 版 Log Monitor(CIM 方式)の導入手順】

- [Hypervisor の設定](#)
- [CIM モジュールのインストール](#)
- [DirectPath I/O を設定するゲスト OS の設定](#)
- [ゲストモジュールのインストール](#)
- [管理モジュールをインストールする OS の設定](#)

- [管理モジュールのインストール](#)
- [管理モジュールの設定変更](#)
- [Fibre Channel ボード\[日立製\]用ユーティリティの動作確認](#)
- [Log Monitor の動作確認](#)
- [アンインストール](#)
- [アップグレード](#)
- [バージョンの確認](#)

最新のインストーラパッケージは、下記ダウンロードサイトから入手してください。

[RV3000]

<https://www.hitachi.co.jp/products/it/rv3000/index.html>

#### 前提条件について

- VMware vSphere DirectPath I/O で I/O 占有しているゲスト OS は、最大 5 ゲストまで監視することができます。VMware vSphere DirectPath I/O を用いず、I/O を共有する場合はゲスト数に制限はありません。

## Hypervisor の設定

### Hypervisor の SSH 機能の有効化

Hypervisor の SSH 機能を有効化します。

1. システム装置(Hypervisor)の起動画面で [F2] キーを押します。
2. Login 画面が表示されるので、root 権限ユーザでログインします。
3. [System Customization]画面が表示されるので、[Troubleshooting Options]を選択して、[Enter]キーを押します。
4. [Enable SSH]を選択して、[Enter]キーを押します。
5. [ESC]キーを数回押し、起動画面に戻ります。

以上で Hypervisor の SSH 機能の有効化は終了です。



- Hypervisor の設定で、SSH 機能の有効化にタイムアウトを設定されている場合、SSH 機能有効化後に設定された時間が経過すると自動的に SSH 機能が無効化されます。
- Log Monitor をインストール後も Hypervisor の SSH 機能の有効化が必要です。

### CIM オブジェクトマネージャの起動確認

CIM オブジェクトマネージャの設定を確認し、停止している場合は起動します。

1. 下記のコマンドで CIM オブジェクトマネージャの設定を確認します。Enabled が false の場合、true に変更してください。CIM オブジェクトマネージャが起動します。

```
# esxcli system wbem get
```

以下に Enabled を false から true に変更する場合の実行例を示します。

```
#esxcli system wbem get
Authorization Model: password
Enabled: false          ←true に変容要
Loglevel: warning
Port: 5989
WSManagement Service: true

#esxcli system wbem set --enable=true
```

## CIM モジュールのインストール

CIM モジュールのインストール方法について説明します。既にインストールされている場合はアップグレードの手順を実施してください。

1. CIM モジュールのパッケージ(コンポーネントファイル)を ESXi に転送します。
2. ESXi の acceptance level を確認します。acceptance level は、VMwareAccepted に設定してください。

```
# esxcli software acceptance get
```

以下に実行例を示します。

```
# esxcli software acceptance get
VmwareCertified

# esxcli software acceptance set --level=VMwareAccepted
Host acceptance level changed to 'VMwareAccepted'.
```

3. esxcli コマンドで ESXi にインストールします。

```
# esxcli software component apply -d <コンポーネントファイル名(絶対パス)>
```

以下に実行例を示します。

```
# esxcli software component apply -d /vmfs/volumes/datastore1/
VMW-esx-7.0.0-HTI-logmonitor-1.0-0.0.0000.zip
Installation Result
  Components Installed: HTI-logmonitor_1.0-0.0.0000
  Components Removed:
  Components Skipped:
  Message: Operation finished successfully.
  Reboot Required: false ← リブートは不要
```

4. CIM モジュールが動作していることを確認します。

```
# esxcli software component list | grep logmonitor
```

以下に実行例を示します。HTI-logmonitor が表示されることを確認してください。

```
# esxcli software component list | grep logmonitor
  HTI-logmonitor          Log Monitor For VMware          1.0-0.0.0000          1.0 - Build 0000
Hitachi                   12-25-2020          VMwareAccepted
```

## DirectPath I/O を設定するゲスト OS の設定

DirectPath I/O を設定するゲスト OS には、ゲストモジュールをインストールする必要があります。ゲストモジュールをインストールするための設定変更の方法について説明します。DirectPath I/O を設定するゲスト OS の全てにゲストモジュールをインストールしてください。

### 前提ソフトウェアのインストール

ゲストモジュールのインストールの前に[前提ソフトウェア\(P.9\)](#)をインストールしてください。インストール方法については、各ソフトウェアのマニュアルを参照してください。

### Hypervisor への接続確認

作業前に Hypervisor への接続状態を確認します。

1. 下記のコマンドで Hypervisor に接続可能かを確認します。**IP アドレス**は Hypervisor の IP アドレスを指定してください。接続できない場合は、メッセージに表示される thumbprint を記録してください、

```
# esxcli -s IP アドレス
```

以下に接続できない場合の実行例を示します。

```
# esxcli -s xxx.xxx.xxx.xxx
Certificate error. Server SHA-1 thumbprint:
C7:45:29:9B:70:41:FC:5E:42:A9:C4:8A:99:5C:0E:70:E1:8D:94:DA (not trusted)
      ↑ thumbprint
```

### Log Monitor CLI のインストール

Hypervisor への接続設定をするための Log Monitor CLI をインストールします。

1. vSphere Client から Log Monitor をインストールするゲスト OS のコンソールを開きます。(root ユーザでログインしてください)
2. snvIm\_xx-xx\_vm.zip (ゲストモジュール) を監視対象のゲスト OS に転送します。
3. 次のコマンドを実行し、ファイルを展開します。

```
#unzip snvIm_xx-xx_vm.zip
#tar pxzvf logmoncli.tar.gz
```

4. 次のコマンドを実行し、Log Monitor CLI をインストールします。

```
#cd logmoncli
```

```
#!/logmoncli_setup.sh
```

## Hypervisor への接続情報の設定

ゲストモジュールをインストールしたゲスト OS から、Hypervisor への接続情報の設定の手順について説明します。

1. 下記コマンドで Hypervisor への接続情報の設定をします。

```
# /opt/hitachi/tools/miacat/logmoncli -t esxi <パラメータ>
```

以下に設定するパラメータを示します。

パラメータ	省略可否	説明
-i IP アドレス	必須	Hypervisor の IP アドレス
-u user 名	必須	ログインユーザ名。root 権限があること
-d thumbprint	省略可	esxcli の実行に必要なサムプリントを指定する。(注 1)
password	必須	ログインパスワード。 コマンド実行後に表示される入力プロンプトに入力してください。

注 1 : Hypervisor への接続確認で接続できなかった場合は、記録した thumbprint を指定してください。

以下に実行例を示します。

```
# /opt/hitachi/tools/miacat/logmoncli -t esxi -i IP アドレス -u User 名  
password:  
INFO: Configuration has been saved.
```

2. 接続情報が正しく設定できているか確認してください。確認方法は設定ファイルである、`/opt/hitachi/tools/miacat/data/esxihost.ini` を参照してください。

```
[Esxihost0]  
ipaddress=192.168.100.2  
username=root  
password=  
thumbprint=  
:
```



Hypervisor への接続情報を設定した後、接続先の IP アドレスを変更する場合は、下記コマンドで登録した接続情報を削除してから、新たな接続情報を設定してください。

また、ESXi へ接続時の thumbprint が変更された場合も同様の手順で変更してください。

```
# /opt/hitachi/tools/miacat/logmoncli -t esxi -x IP アドレス
```

## ゲストモジュールのインストール

ゲストモジュールのインストール方法について説明します。

1. vSphere Client から Log Monitor をインストールするゲスト OS のコンソールを開きます。(root ユーザでログインしてください)
2. インストールファイルをコピーした作業ディレクトリで次のコマンドを実行し、VMware 版 Log Monitor のインストールを行います。

```
# ./logmonsetup.sh -i
```

3. 次のコマンドを実行し、「Version」にバージョン番号が表示されることを確認します。

```
#rpm -qi MIACAT_HAVRHEL
```

インストールに失敗した場合、次のメッセージが表示されます。

メッセージ	意味と対処(必要な場合に記載)
package MIACAT_XXXXX-XXXX-X is already installed	Log Monitor が既にインストールされている。 アップグレードインストールを行ってください。
Failed. You are not root user.	実行ユーザが"root"ではありません。 対処：実行ユーザを"root"に切り替えてインストールしてください。



Hypervisor への接続情報の設定で thumbprint の設定が漏れていた場合、インストール時に ESXi から装置情報が取得できないためインストールに失敗する場合があります。[DirectPath I/Oを設定するゲストOSの設定](#)の Hypervisor への接続確認で thumbprint の設定が必要かを確認してください。

## 管理モジュールをインストールする OS の設定

監視対象のシステム装置上の CIM モジュールが検出した障害イベントを解析して保守会社の通報サービスと連携するには、管理サーバに管理モジュールをインストールする必要があります。管理モジュールをインストールするための管理サーバの設定変更の方法について説明します。管理モジュールは、複数の CIM モジュールを監視することができます。監視対象のシステム装置を追加する場合は、「[管理モジュールの設定変更](#)」を実施してください。CIM モジュールと管理モジュールのバージョンが異なる場合は、VMware 版 Log Monitor(CIM 方式)のアップグレードを実施してください。



(株)日立システムズ(保守会社)が提供する ASSIST 中継エージェント (ハードウェア障害を保守会社へ通知するために、お客様のサーバと ASSIST センタとの通信を中継するソフトウェア) と同一の OS に管理モジュールをインストールすることも可能です。

## 前提ソフトウェアのインストール

管理モジュールのインストールの前に[前提ソフトウェア\(P.9\)](#)をインストールしてください。インストール方法については、各ソフトウェアのマニュアルを参照してください。

## ファイアウォールの設定

ファイアウォールによる通信制限を行っているシステムでは、RV3000 で通報サービスとの連携を行う場合、23141/tcp と 23141/udp を外部通信許可に設定してください。

## 管理モジュールのインストール

管理モジュールのインストール方法について説明します。

### Windows へのインストール

Windows 版の管理モジュールを新規にインストールする方法について説明します。

#### Log Monitor(管理モジュール)のインストール

1. "Administrator" でログインします。
2. インストーラパッケージ内にある次のインストーラを実行します。

**MIACAT.exe**

3. 以降は画面の指示にしたがってインストールしてください。  
(インストール中にカスタマイズ可能な設定はありません)

インストールに失敗した場合、次のメッセージが表示されます。



メッセージ	意味と対処(必要な場合に記載)
Not support this OS version.	インストールしようとしている OS は、Log Monitor でサポートされていません。
You do not have access to make the required system configuration modifications. Stop the installation. Please rerun this installation from an administrators account.	システムの設定を変更する権利がありません。 対処: アドミニストレータ権限を持つユーザでインストールしてください。
Stop the installation. Remote Maintenance Option Setting Tool is running. Please start an installer after terminating Remote Maintenance Option Setting Tool.	ハードウェア保守登録プログラムが実行中です。 対処: ハードウェア保守登録プログラムを停止させてから、Log Monitor のインストールを実行してください。

## 監視対象のシステム装置の設定

コマンドプロンプトを「管理者として実行」で開いて、下記コマンドで監視対象のシステム装置の ESXi への接続情報の設定をします。

```
"C:\Program Files(x86)\HITACHI\miacat\toolsData\logmoncli.exe" -t esxi <パラメータ>
```

以下に設定するパラメータを示します。

パラメータ	省略可否	説明
-i IP アドレス	必須	監視対象の ESXi の IP アドレス (注1)
-u user 名	必須	監視対象の ESXi のログインユーザ名。root 権限があること
-v ポーリング間隔	省略可	CIM モジュールに対して監視を行う際のポーリング間隔を指定する。 設定範囲は 2~60 (単位: 秒)。省略すると 5。
password	必須	監視対象の ESXi のログインパスワード。 コマンド実行後に表示される入力プロンプトに入力してください。
注1: 登録済の ESXi の IP アドレスを指定した場合は、設定情報を変更します。 登録できる ESXi の IP アドレス数は、32 台までです。		

以下に実行例を示します。

```
"C:\Program Files(x86)\HITACHI\miacat\toolsData\logmoncli.exe" -t esxi -i xxx.xxx.xxx.xxx -u XXXXXX -v 10  
password:  
INFO: Configuration has been saved.
```

## Log Monitor サービスの設定と起動

- "Administrator" でログインします。
- サービスを開いて、SMAL2\_MainteAgtSvc を右クリックし、プロパティ → ログオン タブを開きます。

3. アカウントを選択し、管理者権限があるアカウントとパスワードを設定し、[適用]ボタンを押します。
4. 全般 タブを開いて、[開始(S)]ボタンを押します。

## Linux へのインストール

Linux 版の管理モジュールを新規にインストールする方法について説明します。

### Log Monitor CLI のインストール

監視対象の ESXi への接続設定をするための Log Monitor CLI をインストールします。

1. root 権限でログインします。
2. lm\_mng\_xx-xx\_linux.zip (管理モジュール) をインストールするシステム装置上に転送します。
3. 次のコマンドを実行し、lm\_mng\_xx-xx\_linux.zip (Linux 版管理モジュール) を展開します。

```
# unzip lm_mng_xx-xx_linux.zip
```

"x"(イタリック体) : バージョン番号等の英数字が入ります。

4. 次のコマンドを実行し、logmoncli.tar.gz (Log Monitor CLI) を展開します。

```
# tar pxzvf logmoncli.tar.gz
```

5. 次のコマンドを実行し、Log Monitor CLI をインストールします。

```
#cd logmoncli
#./logmoncli_setup.sh
```

### 監視対象のシステム装置の設定

下記コマンドで監視対象のシステム装置の ESXi への接続情報の設定をします。

```
# /opt/hitachi/tools/miacat/logmoncli -t esxi <パラメータ>
```

以下に設定するパラメータを示します。

パラメータ	省略可否	説明
-i IP アドレス	必須	監視対象の ESXi の IP アドレス (注1)
-u user 名	必須	監視対象の ESXi のログインユーザ名。root 権限があること
-v ポーリング間隔	省略可	CIM モジュールに対して監視を行う際のポーリング間隔を指定する。設定範囲は 2~60 (単位: 秒)。省略すると 5。

パラメータ	省略可否	説明
password	必須	監視対象の ESXi のログインパスワード。 コマンド実行後に表示される入力プロンプトに入力してください。
注 1 : 登録済の ESXi の IP アドレスを指定した場合は、設定情報を変更します。 登録できる ESXi の IP アドレス数は、32 台までです。		

以下に実行例を示します。

```
# /opt/hitachi/tools/miacat/logmoncli -t esxi -i xxx.xxx.xxx.xxx -u XXXXXXXXX -v 10
password:
INFO: Configuration has been saved.
```

## Log Monitor(管理モジュール)のインストール

1. root 権限でログインします。
2. インストールファイルを展開した作業ディレクトリで次のコマンドを実行し、Linux 版管理モジュールのインストールを行います。

```
# ./logmonsetup.sh -i
```

インストールに失敗した場合、次のメッセージが表示されます。

メッセージ	意味と対処(必要な場合に記載)
package MIACAT_XXXXX-XXXX-X is already installed	Log Monitor が既にインストールされている。 アップグレードインストールを行ってください。
Failed. You are not root user.	実行ユーザが"root"ではありません。 対処：実行ユーザを"root"に切り替えてインストールしてください。

## Fibre Channel ボード[日立製]用ユーティリティの動作確認

[Fibre Channel ボード\[日立製\]用ユーティリティの動作確認](#)を実行して、Hitachi Gigabit Fibre Channel Adapter 対応ユーティリティが動作することを確認してください。



Hitachi Gigabit Fibre Channel Adapter 対応ユーティリティは、保守会社の通報サービスとの連携用の設定処理や障害時の保守対応で使用されるツールです。必ず動作することを確認してください。

以上で VMware 版 Log Monitor(CIM 方式)のインストールは終了です。

## 管理モジュールの設定変更

管理モジュールに監視対象のシステム装置を追加や接続情報を変更する方法、および監視対象のシステム装置を削除する方法について説明します。

Windows は "Administrator" で、Linux は root 権限でログインして、下記の設定変更を実施してください。

### 監視対象のシステム装置情報の追加・変更

管理モジュールに監視対象のシステム装置を追加する場合や、登録済の ESXi への接続情報を変更する場合、下記コマンドで設定します。

#### Windows の場合:

コマンドプロンプトを「管理者として実行」で開いて、下記コマンドで監視対象のシステム装置の ESXi への接続情報の設定をします。

```
"C:\Program Files(x86)\HITACHI\miacat\toolsData\logmoncli.exe" -t esxi <パラメータ>
```

#### Linux の場合:

```
# /opt/hitachi/tools/miacat/logmoncli -t esxi <パラメータ>
```

以下に設定するパラメータを示します。

パラメータ	省略可否	説明
-i IP アドレス	必須	監視対象の ESXi の IP アドレス (注 1)
-u user 名	必須	監視対象の ESXi のログインユーザ名。root 権限があること
-v ポーリング間隔	省略可	CIM モジュールに対して監視を行う際のポーリング間隔を指定する。 設定範囲は 2~60 (単位: 秒)。 省略すると 5、変更時も 5 となります。
password	必須	監視対象の ESXi のログインパスワード。 コマンド実行後に表示される入力プロンプトに入力してください。

注 1 : 登録済の ESXi の IP アドレスを指定した場合は、設定情報を変更します。

登録できる ESXi の IP アドレス数は、32 台までです。

以下に Linux 版の実行例を示します。

```
# /opt/hitachi/tools/miacat/logmoncli -t esxi -i xxx.xxx.xxx.xxx -u XXXXXXXXX -v 10  
password:
```

```
INFO: Configuration has been saved.
```

設定変更を反映させるために、管理モジュールを再起動させます。再起動方法は、[停止方法と起動方法](#)を参照ください

## 監視対象のシステム装置の削除

登録済の監視対象のシステム装置の情報を削除する場合は、下記コマンドを実行します。**IP アドレス**は削除するシステム装置の ESXi の IP アドレスを指定してください。

### Windows の場合:

コマンドプロンプトを「管理者として実行」で開いて、下記コマンドを実行します。

```
"C:\Program Files(x86)\HITACHI\miacat\toolsData\logmoncli.exe" -t esxi -x IP アドレス
```

### Linux の場合:

```
# /opt/hitachi/tools/miacat/logmoncli -t esxi -x IP アドレス
```

設定変更を反映させるために、管理モジュールを再起動させます。再起動方法は、[停止方法と起動方法](#)を参照ください。

## Fibre Channel ボード[日立製]用ユーティリティの動作確認

監視対象のシステム装置を追加した場合は、[Fibre Channel ボード\[日立製\]用ユーティリティの動作確認](#)を実行して、Hitachi Gigabit Fibre Channel Adapter 対応ユーティリティが動作することを確認してください。

## Fibre Channel ボード[日立製]用ユーティリティの動作確認

下記コマンドを実行して、Hitachi Gigabit Fibre Channel Adapter 対応ユーティリティが動作することを確認してください。**IP アドレス**は設定したシステム装置の ESXi の IP アドレス、**User 名 / Password** はログインユーザ名とパスワードを指定してください。

### Windows の場合:

コマンドプロンプトを開いて、下記コマンドを実行してください。

[16G Fibre Channel ボード[日立製]]

```
hfcvmutil IP アドレス User 名 Password yes -g
```

[32G Fibre Channel ボード[日立製]]

```
hfcvmutil2 IP アドレス User 名 Password yes -g
```

#### Linux の場合:

[16G Fibre Channel ボード[日立製]]

```
# /opt/hitachi/drivers/hba/hfcvmutil.sh IP アドレス User 名 Password yes -g
```

[32G Fibre Channel ボード[日立製]]

```
# /opt/hitachi/drivers/hba2/hfcvmutil2.sh IP アドレス User 名 Password yes -g
```

以下に 16G Fibre Channel ボード[日立製]の実行例を示します。

```
# /opt/hitachi/drivers/hba/hfcvmutil.sh xxx.xxx.xxx.xxx XXXXXXXX P P P P P P P P yes -g
Time:2020/12/28 05:28:05
Connecting...
Connect OK
--- Host Information -----
Host Name : localhost
Build Number : VMware ESXi 7.0.0 build-15843807
CIM Client Version : 1.42.19-100a

--- Adapter Information -----
Vender ID : 1054
Device ID : 3070
Manufacturer ID : Hitachi Corporation
Parts number : 3HAC92xxx-A
EC level : A
Model name : HFCE1602
Driver : HITACHI FC HBA Driver hfcndd 10.48.22.204
Firmware : c400103
CIM Provider : HITACHI CMPI HBA CIM Provider 4.48.20-126
ECID : 00000000 00000000 00000000 00000000 00000000 00000002 04000000 00000008
      00000000 00000000 00000000 00000000 ca000000 226f5060 70e708c0 4010a180
--- Port Information -----
vmhba1 (hfcndd0) WWPN:50000870005b4080 Location:16:00:00 Status:LinkDown
SFP Part Number : FTLF8528P2BCV-HD
  Serial Number : PGQ3CUP
  Date Code    : 091211
  Transceiver Replacement : not replaceable
--- Port Information -----
vmhba2 (hfcndd1) WWPN:50000870005b4082 Location:16:00:01 Status:LinkDown
SFP Part Number : FTLF8528P2BCV-HD
  Serial Number : PGQ3DGJ
  Date Code    : 091211
  Transceiver Replacement : not replaceable
```



Hitachi Gigabit Fibre Channel Adapter 対応ユーティリティは、保守会社の通報サービスとの連携用の設定処理や障害時の保守対応で使用するツールです。必ず動作することを確認してください。

## Log Monitor の動作確認

VMware 版 Log Monitor(CIM 方式)のインストールが完了した後、「[障害解析結果コード\(RC\)の参照](#)」及び「[動作検証](#)」を実施してください。

## アンインストール

VMware 版 Log Monitor(CIM 方式)のアンインストール方法について説明します。

ゲストモジュールを適用している場合は、全てのゲストモジュールをアンインストールしてから CIM モジュールをアンインストールしてください。

### ゲストモジュールのアンインストール

1. vSphere Client から Log Monitor をインストールするゲスト OS のコンソールを開きます。(root ユーザでログインしてください)

2. 次のコマンドを実行し、ファイルを展開します。

```
# unzip snvIm_XX-XX_vm.zip
```

"x"(イタリック体) : バージョン番号等の英数字が入ります。

3. 次のコマンドを実行し、ゲストモジュールをアンインストールします。

```
# ./logmonsetup.sh -e
```

4. 次のコマンドを実行し、ファイルを展開します。

```
#tar pxzvf logmoncli.tar.gz
```

5. 次のコマンドを実行し、Log Monitor CLI をアンインストールします。

```
#cd logmoncli  
#./logmoncli_setup.sh -e
```

### CIM モジュールのアンインストール

1. CIM モジュールがインストールされていることを確認します。

```
# esxcli software component get | grep logmonitor
```

以下に実行例を示します。

```
# esxcli software component get | grep logmonitor
HTI-logmonitor_1.0-0.0.0000
Name: HTI-logmonitor
VIBs: HTI_bootbank_logmonitor_0001-0000
Summary: logmonitor:Log Monitor For VMware
```

2. 次のコマンドを実行し、CIM モジュールをアンインストールします。

```
# esxcli software component remove -n HTI-logmonitor
```

## Windows 版管理モジュールのアンインストール

1. "Administrator" でログインします。
2. Uninstall を起動します。  
次のコマンドを実行します。

```
C:¥Program Files(x86)¥HITACHI¥miacat¥UNINST.EXE
```

## Linux 版管理モジュールのアンインストール

1. root 権限でログインします。
2. lm\_mng\_xx-xx\_linux.zip (Linux 版管理モジュール) をインストールするシステム装置上に転送します。
3. 次のコマンドを実行し、lm\_mng\_xx-xx\_linux.zip を展開します。  

```
# unzip lm_mng_xx-xx_linux.zip
```
4. 次のコマンドを実行し、管理モジュールをアンインストールします。  

```
# ./logmonsetup.sh -e
```
5. 次のコマンドを実行し、ファイルを展開します。  

```
#tar pxzvf logmoncli.tar.gz
```
6. 次のコマンドを実行し、Log Monitor CLI をアンインストールします。

```
#cd logmoncli
#./logmoncli_setup.sh -e
```

以上で VMware 版 Log Monitor(CIM 方式)のアンインストールは終了です。



## アップグレード

VMware 版 Log Monitor(CIM 方式)のアップグレード方法について説明します。

アップグレードを行う場合は、適用している全ての VMware 版 Log Monitor(CIM 方式)をアップグレードしてください。

### CIM モジュールのアップグレード

1. CIM モジュールのパッケージ(コンポーネントファイル)を ESXi に転送します。
2. esxcli コマンドで ESXi にインストールします。

```
# esxcli software component apply -d <コンポーネントファイル名(絶対パス)>
```

以下に実行例を示します。

```
# esxcli software component apply -d /vmfs/volumes/datastore1/
VMW-esx-7.0.0-HTI-logmonitor-1.0-0.0.0000.zip
Installation Result
  Components Installed: HTI-logmonitor_1.0-0.0.0000
  Components Removed:
  Components Skipped:
  Message: Operation finished successfully.
  Reboot Required: true ← リブートが必要
```

3. ESXi をリブートしてください。ESXi が起動したら CIM モジュールが動作していることを確認します。

```
# esxcli software component list | grep logmonitor
```

以下に実行例を示します。HTI-logmonitor が表示されることを確認してください。

```
# esxcli software component list | grep logmonitor
  HTI-logmonitor      Log Monitor For VMware      1.0-0.0.0000      1.0 - Build 0000
Hitachi              12-25-2020    VMwareAccepted
```

### ゲストモジュールのアップグレード

1. vSphere Client から Log Monitor をインストールするゲスト OS のコンソールを開きます。(root ユーザでログインしてください)
2. 次のコマンドを実行し、ファイルを展開します。

```
# unzip snvIm_XX-XX_vm.zip
```

"x"(イタリック体) : バージョン番号等の英数字が入ります。

3. 次のコマンドを実行し、ゲストモジュールをインストールします。

```
# ./logmonsetup.sh -i
```

4. 次のコマンドを実行し、ファイルを展開します。

```
#tar pxzvf logmoncli.tar.gz
```

5. 次のコマンドを実行し、Log Monitor CLI をインストールします。

```
#cd logmoncli  
#./logmoncli_setup.sh -i
```

## Windows 版管理モジュールのアップグレード

1. "Administrator" でログインします。
2. インストーラパッケージ内にある次のインストーラを実行します。  

```
MIACAT.exe
```
3. 以降は画面の指示にしたがってインストールしてください。  
(インストール中にカスタマイズ可能な設定はありません)
4. サービスを開いて、SMAL2\_MainteAgtSvc を右クリックし、プロパティ → ログオン タブを開きます。
5. アカウントを選択し、管理者権限があるアカウントとパスワードを設定し、[適用]ボタンを押します。
6. 全般 タブを開いて、[開始(S)]ボタンを押します。

## Linux 版管理モジュールのアップグレード

1. root 権限でログインします。
2. lm\_mng\_xx-xx\_linux.zip (Linux 版管理モジュール) をインストールするシステム装置上に転送します。
3. 次のコマンドを実行し、lm\_mng\_xx-xx\_linux.zip (Linux 版管理モジュール) を展開します。  

```
# unzip lm_mng_xx-xx_linux.zip
```
4. 次のコマンドを実行し、管理モジュールをインストールします。  

```
# ./logmonsetup.sh -i
```

5. 次のコマンドを実行し、ファイルを展開します。

```
#tar pxzvf logmoncli.tar.gz
```

6. 次のコマンドを実行し、Log Monitor CLI をインストールします。

```
#cd logmoncli  
#./logmoncli_setup.sh -i
```

以上で VMware 版 Log Monitor(CIM 方式)のアップグレードは終了です。

## バージョンの確認

VMware 版 Log Monitor(CIM 方式)のバージョンの確認方法について説明します。

### CIM モジュールのバージョンの確認

1. ESXi にログインします。
2. 次のコマンドを実行することで、ESXi 上で動作している CIM プロバイダのバージョンを確認することができます。

```
# esxcli software component list
```

以下に実行例を示します。

```
# esxcli software component list | grep logmonitor  
HTI-logmonitor      Log Monitor For VMware      1.0-0.0.0001      ....  
                        ↑ バージョン
```

### ゲストモジュールのバージョンの確認

1. vSphere Client から Log Monitor がインストールされているゲスト OS のコンソールを開きます。(root ユーザでログインしてください)
2. 次のコマンドを実行します。

```
# rpm -qi MIACAT_HAVRHEL
```
3. 「Version」にバージョン番号が表示されます。

### Windows 版管理モジュールのバージョンの確認

1. "Administrator" でログインします。

2. コマンドプロンプト上で、次のコマンドを実行します。

```
sc qdescription SMAL2_MainteAgtSvc
```

3. Log Monitor の製品名とバージョンが表示されます。

### Linux 版管理モジュールのバージョンの確認

1. root 権限でログインします。

2. 次のコマンドを実行します。

```
# rpm -qi MIACAT_MANAGER
```

3. 「Version」にバージョン番号が表示されます。

以上で VMware 版 Log Monitor(CIM 方式)のバージョンの確認は終了です。

## Log Monitor の操作

この章では、Log Monitor の操作方法について説明します。

- [起動と停止方法](#)
- [障害解析結果コード\(RC\)の参照](#)
- [動作検証](#)
- [監視対象 syslog ファイルの変更](#)

## 起動と停止方法

Log Monitor の起動方法、停止方法と状態の確認方法について説明します。なお、Log Monitor インストール後は自動で Log Monitor が起動します。

### 起動方法

#### Windows 及び VMware(CIM 方式)の管理モジュール(Windows)の場合:

SMAL2\_MainteAgtSvc サービスを開始することで起動できます。サービスを開き、SMAL2\_MainteAgtSvc を右クリックし、開始を選択します。

#### Linux/VMware(ゲスト方式)の場合[RHEL6]:

```
# service smal2d start  
# service VmSyslogMAgtSrvd start (VMware(ゲスト方式)のみ)
```

#### Linux 及び VMware(CIM 方式)のゲストモジュール/管理モジュール(Linux)の場合 [RHEL7 以降]:

```
# systemctl start smal2d
```

#### VMware(ゲスト方式)の場合[RHEL7, 8]:

```
# systemctl start smal2d  
# systemctl start VmSyslogMAgtSrvd
```

### 停止方法

#### Windows 及び VMware(CIM 方式)の管理モジュール(Windows)の場合:

SMAL2\_MainteAgtSvc サービスを停止することで停止できます。サービスを開き、SMAL2\_MainteAgtSvc を右クリックし、停止を選択します。

#### Linux/VMware の場合[RHEL6]:

```
# service smal2d stop  
# service VmSyslogMAgtSrvd stop (VMware のみ)
```

#### Linux 及び VMware(CIM 方式)のゲストモジュール/管理モジュール(Linux)の場合 [RHEL7 以降]:

```
# systemctl stop smal2d
```

**VMware(ゲスト方式)の場合[RHEL7, 8]:**

```
# systemctl stop smal2d  
# systemctl stop VmSyslogMAgtSrvd
```

## 状態の確認方法

**Windows 及び VMware(CIM 方式)の管理モジュール(Windows)の場合:**

サービスを開き、SMAL2\_MainteAgtSvc の状態を参照してください。

**Linux/VMware の場合[RHEL6]:**

```
# service smal2d status  
# service VmSyslogMAgtSrvd status (VMware のみ)
```

**Linux 及び VMware(CIM 方式)のゲストモジュール/管理モジュール(Linux)の場合 [RHEL7 以降]:**

```
# systemctl status smal2d
```

**VMware(ゲスト方式)の場合[RHEL7, 8]:**

```
# systemctl status smal2d  
# systemctl status VmSyslogMAgtSrvd (VMware のみ)
```

## 障害解析結果コード(RC)の参照

障害解析結果コード(RC)を参照する方法について説明します。



発生したハードウェア障害の事象を保守会社に障害連絡していただく際に、障害解析結果コード (RC) も併せて連絡していただくと、対策時間の短縮を図ることができます。

保守会社への障害連絡には「障害状況連絡シート」(\*1)をご利用ください。障害解析結果コード (RC) を記載する欄があります。

\*1: 「障害状況連絡シート」は、『ユーザーズガイド』メディア (システム装置に添付) に電子データとして格納されています。

1. 管理者権限でログインします。VMware(CIM 方式)は、管理モジュールにログインします。  
Windows の場合 : "Administrator"  
Linux/VMware の場合 : "root"

2. RC Viewer を起動します。

Windows/VMware(CIM 方式):管理モジュール(Windows)の場合 :

```
C:¥Program Files(x86)¥HITACHI¥miacat¥Program¥ASSIST¥ccp.exe
```

Linux/VMware(ゲスト方式)/VMware(CIM 方式):管理モジュール(Linux)の場合 :

```
/opt/hitachi/miacat/Program/ASSIST/ccp
```

3. 障害解析結果コード(RC)が表示されます。

Linux/Windows/VMware(ゲスト方式)の場合

```
MODEL CODE : N/A / PRODUCT No. : N/A
MODEL NAME : HA8000V/DL360,DL380,DL580
MODEL FRU : HA8000V/DL380
RC DICT : xp_dl380xp/xP-00-09

date/time      Lv RE UID  EC Failure  Additional
-----
12/08/01 15:24:33  ** 10 E400 10 19006500 65000000
12/08/01 15:23:35   10 0100 E2 1F22FFFF 6F06FFFF
12/08/01 15:23:33   10 2000 E0 09370BF1 0BA1FFFF
12/08/01 15:23:33   10 2000 AC 042F0BF1 0BA1FFFF
  発生日時      障害解析結果コード(RC)
-- (q:quit) --
```

VMware(CIM 方式 : 管理モジュール)の場合

```
No. ESXi IP address  host name      Model name      Model code      MFG No.
-----
  1 xxx.xxx.xxx.xxx host1          RV3000/A2
  2 xxx.xxx.xxx.xxx host2          RV3000/A1
> Select No. :      ←表示するシステム装置の番号(No.)を入力

MODEL CODE : N/A / PRODUCT No. : N/A
MODEL NAME : RV3000/A1
MODEL FRU : RV3000 A1
RC DICT : rv_rv3000a1/rV-00-10

date/time      Lv RE UID  EC Failure  Additional
-----
12/08/01 15:24:33  ** 10 E400 10 19006500 65000000
12/08/01 15:23:35   10 0100 E2 1F22FFFF 6F06FFFF
12/08/01 15:23:33   10 2000 E0 09370BF1 0BA1FFFF
12/08/01 15:23:33   10 2000 AC 042F0BF1 0BA1FFFF
  発生日時      障害解析結果コード(RC)
-- (q:quit) --
```

4. 「q」を入力して RC Viewer を終了します。



以上で障害解析結果コード(RC)の参照は終了です。

## 動作検証

Log Monitor を動作検証する方法について説明します。

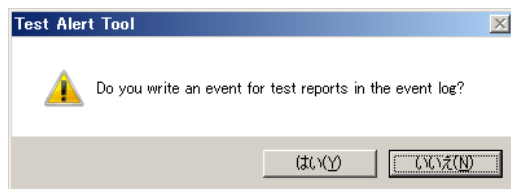
1. 管理者権限でログインします。  
Windows の場合 : "Administrator"  
Linux/VMware の場合 : "root"
2. テストアラート実行ツールを起動します。

Windows の場合 :

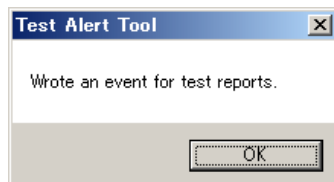
コマンドプロンプトを開き、次のコマンドを実行します。

```
C:¥Program Files(x86)¥HITACHI¥miacat¥Program¥ASSIST¥testalt.wsf
```

コマンドを実行すると「Test Alert Tool」画面が表示されるので、[はい] ボタンをクリックします。



テストアラート実行を示す画面が表示されるので、[OK] ボタンをクリックして終了です。



Linux/VMware(ゲスト方式)/VMware(CIM方式: ゲストモジュール)の場合 :  
次のコマンドを実行します。

```
#!/opt/hitachi/miacat/Program/ASSIST/testalt.sh
```

コマンドを実行すると実行確認のメッセージが表示されるので、[yes] を入力します。

```
# /opt/hitachi/miacat/Program/ASSIST/testalt.sh
==== TEST ALERT TOOL ====
Do you write a message for test reports in the syslog?
(yes|no[no]): yes
```

テストアラート実行を示すメッセージ("Wrote a message for test reports.")が表示されて終了です。

```
# /opt/hitachi/miacat/Program/ASSIST/testalt.sh
==== TEST ALERT TOOL ====
Do you write a message for test reports in the syslog?
(yes|no[no]): yes
Wrote a message for test reports.
```

VMware(CIM 方式 : CIM モジュール)の場合 :  
ESXi にログインして、次のコマンドを実行します。

```
#sh /opt/hitachi/logmonitor/Tool/testalt.sh
```

テストアラート実行はこれで終了です。

3. 3分程度待った後 RC Viewer を起動します。

Windows の場合 :

コマンドプロンプトを開き、次のコマンドを実行します。

```
C:¥Program Files(x86)¥HITACHI¥miacat¥Program¥ASSIST¥ccp.exe
```

Linux/VMware の場合 :

次のコマンドを実行します。VMware(CIM 方式)の場合は、管理モジュールで実行してください。

```
# /opt/hitachi/miacat/Program/ASSIST/ccp
```

4. 障害解析結果コード(RC)が表示されますので、下記に示す RC が表示されることを確認してください。

確認する RC : 10 Ex00 FA D0F0yy01 yyyyyyyy

"x"(イタリック体) : 0,3,4 の何れかが入ります。

"y"(イタリック体) : 任意の数値(16進数)が入ります。

Linux/Windows/VMware(ゲスト方式)の場合 :

```
MODEL CODE : N/A / PRODUCT No. : N/A
MODEL NAME : HA8000V/DL360, DL380, DL580
MODEL FRU : HA8000V/DL380
RC DICT : xp_dl380xp/xP-00-09
```

date/time	Lv	RE	UID	EG	Failure	Additional
12/08/01 15:24:33	10	<i>E</i>	<i>x00</i>	<i>FA</i>	<i>D0F0yy01</i>	<i>yyyyyyyy</i>
12/08/01 15:23:35	10	0100	E2	1F22FFFF	6F06FFFF	
12/08/01 15:23:33	10	2000	E0	09370BF1	OBA1FFFF	
12/08/01 15:23:33	10	2000	AC	042F0BF1	OBA1FFFF	

発生日時                      障害解析結果コード(RC)  
— (q:quit) —

VMware(CIM 方式)の場合 :

No.	ESXi IP address	host name	Model name	Model code	MFG No.
1	xxx.xxx.xxx.xxx	rv3000host2	RV3000/A1		
2	xxx.xxx.xxx.xxx	rv3000host2	RV3000/A1	TX-CNx-CC7Fxx	1234
>Select No. : ←表示するシステム装置の No. を入力					
MODEL CODE : N/A / PRODUCT No. : N/A					
MODEL NAME : HA8000V/DL360, DL380, DL580					
MODEL FRU : HA8000V/DL380					
RC DICT : xp_d1380xp/xP-00-09					
date/time		Lv	RE	UID	EC Failure Additional
12/08/01 15:24:33		10	E	X00	FA D0F0yy01 yyyyyyyy
12/08/01 15:23:35		10	0100	E2	1F22FFFF 6F06FFFF
12/08/01 15:23:33		10	2000	E0	09370BF1 0BA1FFFF
12/08/01 15:23:33		10	2000	AC	042F0BF1 0BA1FFFF
発生日時		障害解析結果コード (RC)			
— (q:quit) —					

なお、OS インストール直後は、表示されない場合があります。その際は、「2.テストアラート実行ツールを起動」から再度実行してください。

5. 「q」を入力して RC Viewer を終了します。

以上で Log Monitor の動作検証は終了です。

## 監視対象 **syslog** ファイルの変更 (Linux のみ)

監視対象となる **syslog** ファイルは、デフォルトパス(/var/log/messages)に保存されているものを対象とします。デフォルトパスから変更する場合は、下記ファイル内の設定を変更後、**Log Monitor** を再起動してください。

ファイル名 : `/opt/hitachi/miacat/MainteData/smal2.conf`

`[SOFTWARE¥HITACHI¥miacat¥Maintenance Agent Service¥LogWatch]`

`MessagesFileName=/var/log/messages (SYSLOG ファイルの完全パスを設定する。)`

(例)

SYSLOG ファイルパスを/data/log/Messages に変更する場合

`[SOFTWARE¥HITACHI¥miacat¥Maintenance Agent Service¥LogWatch]`

`MessagesFileName=/data/log/messages`



# 6

## 付録

この章では、Log Monitor に関する補足情報を記載しています。

- [メッセージ一覧](#)
- [インストールフォルダ構成](#)

## メッセージ一覧

Log Monitor が出力するメッセージ一覧について説明します。

- [Windows 版のイベントローグ一覧 \(P.72\)](#)
- [Linux 版の syslog メッセージ一覧 \(P.74\)](#)
- [VMware 版の syslog メッセージ一覧 \(P.76\)](#)

## Windows 版のイベントローグ一覧

Windows 版 Log Monitor が出力するイベントログのメッセージ一覧について説明します。

イベントログのログ内容一覧を以下に表記します。

イベントソース名称：「SMAL2\_MainteAgtSvc」

EventID	メッセージ ( )内は英語	意味と対処(必要な場合に記載)
4	メールサーバへ送信しました。 (Transmitted to the email server.)	SMTP 通信でお客様登録情報を送信した。
5	メールサーバへ送信しました。 (Transmitted to the email server.)	SMTP 通信で装置登録情報を送信した。
11	メールサーバへ送信しました。 (Transmitted to the email server.)	SMTP 通信で障害通報を送信した。
12	統合監視装置へ送信しました。 (Transmitted to the ASSIST agent.)	保守会社設置の統合監視装置に障害通報を送信した。
13	統合監視装置からログ収集要求を受信しました。 (Received a log collection demand from the ASSIST agent.)	保守会社設置の統合監視装置よりログ収集要求を受信した。
14	統合監視装置へログ情報を送信しました。 (Transmitted log information to the ASSIST agent.)	保守会社設置の統合監視装置にログ情報を送信した。
15 *1	統合監視装置から設定登録要求を受信しました。 (Received a setting registration demand from the ASSIST agent.)	保守会社設置の統合監視装置から設定情報の登録要求を受信した。
16 *2	BMC に SEL を出力しました。 (SEL was written in BMC.)	BMC に SEL を出力した。
100	ログ監視を開始しました。 (Started log monitoring.)	Log Monitor を開始した。
101	アライブチェック機能を開始しました。 (Started alive-check.)	アライブチェック機能を開始した。
102	統合監視装置からアライブチェック機能の停止要求を受信したため、アライブチェック機能を停止しました。 (Stopped alive-check, because received the stop demand from the ASSIST agent.)	アライブチェック機能を停止した。



EventID	メッセージ ( )内は英語	意味と対処(必要な場合に記載)
103	ログ監視を停止しました。 (Stopped log monitoring.)	Log Monitor を停止した。
500	テスト通報を発生させます。 (The test report is generated.)	テスト通報契機メッセージ送信する。
1002, 1003, 1007	通信制御でエラーが発生しました。 (An error occurred at communication control.)	SMTP 通信でエラーが発生した。 対処: RV3000 と SMTP サーバとの通信経路を確認してください。
1008	通信制御でエラーが発生しました。 (An error occurred at communication control.)	保守会社設置の統合監視装置に障害通報を送信中にエラーが発生した。 対処:RV3000 と統合監視装置との通信経路を確認してください。
1011	IPMI ツールがインストールされていません。 (IPMI tool is not installed.)	IPMI ツールが存在しないため SEL 出力が失敗した。 対処:前提ソフトウェアのインストール状況を確認してください。
1012	IPMI ツールの実行に失敗しました。 (Failed to executing IPMI tool.)	IPMI ツールがエラー終了したため SEL 出力が失敗した。 対処:前提ソフトウェアの動作状況を確認し Log Monitor を再起動してください。
2001	Master Config is initialized.	設定ファイルを初期化してサービス起動した。 説明: 設定ファイルに異常があったため、初期化してから障害監視を開始します。Log Monitor の前回終了時から今回起動時までに発生したイベントは破棄されます。 ※Log Monitor インストール後の初回起動時には必ず採取されますが、異常ではありません。
2001	Master Config is recovered from backup config.	設定ファイルをバックアップファイルから回復してサービス起動した。 説明: 設定ファイルに異常があったため、バックアップファイルから回復しました。過去の障害を検知・通報することがあります。
2001	Backup Config is recovered from master config.	設定ファイルをバックアップファイルへコピーしサービス起動した。 説明: バックアップファイルに異常があったため、設定ファイルから回復しました。通常の障害監視を開始します。
2001	Stopped the log monitor. Because the master Config reading fails.	設定ファイルの読み込みに失敗し、サービス停止した。 対処:メモリ、ハードディスク等のリソースに空きがない可能性があります。リソース解放後 Log Monitor を再起動してください。
2001	Stopped the log monitor. Because the master Config writing fails.	設定ファイルの書き込みに失敗し、サービス停止した。 対処:メモリ、ハードディスク等のリソースに空きがない可能性があります。リソース解放後 Log Monitor を再起動してください。

EventID	メッセージ ( )内は英語	意味と対処(必要な場合に記載)
2001	Stopped the log monitor. Because cannot get disk space info.	ハードディスク空き容量の取得に失敗し、サービス停止した。 対処: メモリ、ハードディスク等のリソースに空きがない可能性があります。リソース解放後 Log Monitor を再起動してください。
2001	Stopped the log monitor. Because not enough available disk space.	ハードディスクに十分な空き容量がなく、サービス停止した。 対処: ハードディスクに十分な空き容量がありません。ハードディスクの空き容量を確保した後、Log Monitor を再起動してください。
2100	サービスの初期化に失敗しました。 (Failed in the initialization.)	ネットワークリソースの競合等により Log Monitor が終了した。 対処: Log Monitor で使用しているポート番号が競合していないか確認してください。
2101	アライブチェック機能を開始できませんでした。 統合監視装置との設定が不一致です。 (Failed to start of alive-check. The setting has not adjusted to the ASSIST agent.)	機器型名、製造番号等の設定情報が保守会社設置の統合監視装置の設定と一致していないため、アライブチェック機能を開始できない。 対処: 設定情報を確認してください。

## Linux 版の syslog メッセージ一覧

Linux版/Wmware版Log Monitorがsyslogに出力するメッセージ一覧について説明します。

Log Monitor のメッセージはタグ名称が「SMAL2\_MainteAgtSvc」で出力されます。

Aug 2 16:38:07 RHEL6264 SMAL2\_MainteAgtSvc[4026]: [INFO] (メッセージ)

メッセージの一覧を以下に表記します。

メッセージ	意味と対処(必要な場合に記載)
[INFO] Transmitted to the ASSIST agent.	保守会社設置の統合監視装置に障害通報を送信した。
[INFO] Received a log collection demand from the ASSIST agent.	保守会社設置の統合監視装置よりログ収集要求を受信した。
[INFO] Sent a log collection demand to the ASSIST agent.	保守会社設置の統合監視装置にログ情報を送信した。
[INFO] Received a setting registration demand from the ASSIST agent.	保守会社設置の統合監視装置から設定情報の登録要求を受信した。*1
[INFO] Started log monitoring.	Log Monitor を開始した。
[INFO] Started alive-check.	アライブチェック機能を開始した。
[INFO] Stopped alive check, because received the stop demand from the ASSIST agent.	アライブチェック機能を停止した。
[INFO] Stopped log monitoring.	Log Monitor を停止した。
[INFO] The test report is generated.	テスト通報開始メッセージ。

メッセージ	意味と対処(必要な場合に記載)
[WARN] An error occurred at communication control.	保守会社設置の統合監視装置に障害通報を送信中にエラーが発生した。 対処：HA8000V シリーズ/RV3000 と統合監視装置との間のネットワークを確認してください。
[WARN] Master Config is initialized.	設定ファイルを初期化してサービス起動した。 説明：設定ファイルに異常があったため、初期化してから障害監視を開始します。Log Monitor の前回終了時から今回起動時まで発生したイベントは破棄されます。
[WARN] Master Config is recovered from backup config.	設定ファイルをバックアップファイルから回復してサービス起動した。 説明：設定ファイルに異常があったため、バックアップファイルから回復しました。過去の障害を検知・通報することがあります。
[WARN] Backup Config is recovered from master config.	設定ファイルをバックアップファイルへコピーしサービス起動した。 説明：バックアップファイルに異常があったため、設定ファイルから回復しました。通常の障害監視を開始します。
[ERROR] Stopped the log monitor. Because the master Config reading fails.	設定ファイルの読み込みに失敗し、サービス停止した。 対処：メモリ、ハードディスク等のリソースに空きがない可能性があります。リソース解放後 Log Monitor を再起動してください。
[ERROR] Stopped the log monitor. Because the master Config writing fails.	設定ファイルの書き込みに失敗し、サービス停止した。 対処：メモリ、ハードディスク等のリソースに空きがない可能性があります。リソース解放後 Log Monitor を再起動してください。
[ERROR] Stopped the log monitor. Because cannot get disk space info.	ハードディスク空き容量の取得に失敗し、サービス停止した。 対処：メモリ、ハードディスク等のリソースに空きがない可能性があります。リソース解放後 Log Monitor を再起動してください。
[ERROR] Stopped the log monitor. Because not enough available disk space.	ハードディスクに十分な空き容量がなく、サービス停止した。 対処：ハードディスクに十分な空き容量がありません。ハードディスクの空き容量を確保した後、Log Monitor を再起動してください。
[ERROR] Failed in the initialization.	設定情報の不整合、ネットワークリソースの競合等により Log Monitor が終了した。 対処：Log Monitor で使用しているポート番号が競合していないか確認してください。
[ERROR] Failed to start of alive-check. The setting has not adjusted to the ASSIST agent.	機器型名、製造番号等の設定情報が保守会社設置の統合監視装置の設定と一致していないため、アライブチェック機能を開始できない。 対処：設定情報を確認してください。

## VMware 版 Log Monitor の syslog メッセージ一覧

VMware 版 Log Monitor が syslog に出力するメッセージ一覧について説明します。

Log Monitor のメッセージはタグ名称が「SMAL2\_MainteAgtSvc」で出力されます。

Aug 2 16:38:07 localhost SMAL2\_MainteAgtSvc[xxxx]: (メッセージ)

メッセージの一覧を以下に表記します。

メッセージ	意味と対処(必要な場合に記載)
[INFO] Transmitted to the ASSIST agent.	保守会社設置の統合監視装置に障害通報を送信した。
[INFO] Received a log collection demand from the ASSIST agent.	保守会社設置の統合監視装置よりログ収集要求を受信した。
[INFO] Sent a log collection demand to the ASSIST agent.	保守会社設置の統合監視装置にログ情報を送信した。
[INFO] Received a setting registration demand from the ASSIST agent.	保守会社設置の統合監視装置から設定情報の登録要求を受信した。(*1)
[INFO] Started log monitoring.	Log Monitor を開始した。
[INFO] Started alive-check.	アライブチェック機能を開始した。
[INFO] Stopped alive check, because received the stop demand from the ASSIST agent.	アライブチェック機能を停止した。
[INFO] Stopped log monitoring.	Log Monitor を停止した。
[INFO] The test report is generated.	テスト通報開始メッセージ。
[INFO] SEL was written in BMC.	BMC に SEL を出力した。 (*2)
[WARN] An error occurred at communication control.	保守会社設置の統合監視装置に障害通報を送信中にエラーが発生した。 対処:RV3000 と統合監視装置との間のネットワークを確認してください。
[WARN] Master Config is initialized. (*5)	設定ファイルを初期化してサービス起動した。 説明: 設定ファイルに異常があったため、初期化してから障害監視を開始します。Log Monitor の前回終了時から今回起動時まで発生したイベントは破棄されます。
[WARN] Master Config is recovered from backup config.	設定ファイルをバックアップファイルから回復してサービス起動した。 説明: 設定ファイルに異常があったため、バックアップファイルから回復しました。過去の障害を検知・通報することがあります。
[WARN] Backup Config is recovered from master config.	設定ファイルをバックアップファイルへコピーしサービス起動した。 説明: バックアップファイルに異常があったため、設定ファイルから回復しました。通常の障害監視を開始します。
[ERROR] Stopped the log monitor. Because the master Config reading fails.	設定ファイルの読み込みに失敗し、サービス停止した。 対処: メモリ、ハードディスク等のリソースに空きがない可能性があります。リソース解放後 Log Monitor を再起動してください。

メッセージ	意味と対処(必要な場合に記載)
[ERROR] Stopped the log monitor. Because the master Config writing fails.	設定ファイルの書き込みに失敗し、サービス停止した。 対処：メモリ、ハードディスク等のリソースに空きがない可能性があります。リソース解放後 <b>Log Monitor</b> を再起動してください。
[ERROR] Stopped the log monitor. Because cannot get disk space info.	ハードディスク空き容量の取得に失敗し、サービス停止した。 対処：メモリ、ハードディスク等のリソースに空きがない可能性があります。リソース解放後 <b>Log Monitor</b> を再起動してください。
[ERROR] Stopped the log monitor. Because not enough available disk space.	ハードディスクに十分な空き容量がなく、サービス停止した。 対処：ハードディスクに十分な空き容量がありません。ハードディスクの空き容量を確保した後、 <b>Log Monitor</b> を再起動してください。
[ERROR] Failed in the initialization.	設定情報の不整合、ネットワークリソースの競合等により <b>Log Monitor</b> が終了した。 対処： <b>Log Monitor</b> で使用しているポート番号が競合していないか確認してください。
[ERROR] Failed to start of alive-check. The setting has not adjusted to the ASSIST agent.	機器型名、製造番号等の設定情報が保守会社設置の統合監視装置の設定と一致していないため、アライブチェック機能を開始できない。 対処：設定情報を確認してください。
[ERROR] Stopped the log monitor, Because failed to connect to hypervisor, invalid username or password.(-23)	hypervisor との認証に失敗した。 対処：hypervisor のユーザ名・パスワードが変更された可能性があるため、以下の操作を実施してください。 (1)hypervisor でアカウントロック状態を解除してください。 (*3) (2)ESXi ホスト情報を hypervisor の現在のユーザ名・パスワードに再設定してください。 (3)Linux(ゲスト OS)を再起動してください。
[WARN] Failed in syslog reading. Because the record is Unexpected Date and Time Format.	受信した <b>syslog</b> メッセージの時刻形式が期待したものではありませんでした、(期待値: yyyy-mm-ddThh:mm:ss) 対処：イベント管理ツールがアップグレードされていない可能性があります。イベント管理ツールをアップグレードしてください。
[WARN] Failed in syslog reading. Because the record is Invalid Date and Time Value.	受信した <b>syslog</b> メッセージの時刻データに不正な値がありました。

## インストールフォルダ構成

Log Monitor のフォルダ構成について説明します。

### Windows 版のフォルダ構成

Windows 版 Log Monitor のフォルダ構成について説明します。

C:\Program Files(x86)\	
└ HITACHI\miacat\	
└ Log	← 実行ログ格納フォルダ (本フォルダ下のファイルは実行中に作成・変更・削除されます)
└ LogCollector	← ログ採取プログラムフォルダ (固定ファイル)
└ MainteTool	← サブプログラムフォルダ (固定ファイル)
└ MainteData	← 定義・設定格納フォルダ (設定変更時にファイルが変更されます)
└ Program	← サービスプログラムフォルダ (固定ファイル)
└ Temp	← 一時ファイル格納フォルダ (本フォルダ下のファイルは実行中に作成・変更・削除されます)

### Linux 版のフォルダ構成

Linux 版 Log Monitor のフォルダ構成について説明します。

/opt/	
└ hitachi/miacat/	
└ LogCollector	← ログ採取プログラムフォルダ (固定ファイル)
└ MainteTool	← サブプログラムフォルダ (固定ファイル)
└ MainteData	← 定義・設定格納フォルダ (設定変更時にファイルが変更されます)
└ Program	← サービスプログラムフォルダ (固定ファイル)
/var/	
└ opt/hitachi/miacat	
└ Log	← 実行ログ格納フォルダ (本フォルダ下のファイルは実行中に作成・変更・削除されます)
└ Temp	← 一時ファイル格納フォルダ (本フォルダ下のファイルは実行中に作成・変更・削除されます)

### VMware 版(ゲスト方式)のフォルダ構成

VMware 版 Log Monitor(ゲスト方式)のフォルダ構成について説明します。

/opt/hitachi/miacat	
└ LogCollector	← ログ採取プログラムフォルダ (固定ファイル)
└ MainteTool	← サブプログラムフォルダ (固定ファイル)
└ MainteData	← 定義・設定格納フォルダ (設定変更時にファイルが変更されます)
└ Program	← サービスプログラムフォルダ (固定ファイル)
/opt/hitachi/VmSyslogMAgtSrvd	
└ bin	← サブプログラムフォルダ (固定ファイル)
└ data	← サブプログラム定義・設定格納フォルダ (固定ファイル)
/opt/hitachi/tools/miacat/	
└ data	← CLI 設定データフォルダ (本フォルダ下のファイルは実行中に作成・変更・削除されます)
/var/opt/hitachi/miacat	
└ Log	← 実行ログ格納フォルダ (本フォルダ下のファイルは実行中に作成・変更・削除されます)
└ Temp	← 一時ファイル格納フォルダ (本フォルダ下のファイルは実行中に作成・変更・削除されます)
/var/opt/hitachi/VmSyslogMAgtSrvd	
└ log	← 実行ログ格納フォルダ (本フォルダ下のファイルは実行中に作成・変更・削除されます)
└ temp	← 一時ファイル格納フォルダ (本フォルダ下のファイルは実行中に作成・変更・削除されます)

## VMware 版(CIM 方式)のフォルダ構成

VMware 版 Log Monitor(CIM 方式)のフォルダ構成について説明します。

### ・ ゲストモジュール

/opt/hitachi/miacat	
└ LogCollector	← ログ採取プログラムフォルダ (固定ファイル)
└ MainteTool	← サブプログラムフォルダ (固定ファイル)
└ MainteData	← 定義・設定格納フォルダ (設定変更時にファイルが変更されます)
└ Program	← サービスプログラムフォルダ (固定ファイル)
/opt/hitachi/VmSyslogMAgtSrvd	
└ bin	← サブプログラムフォルダ (固定ファイル)
└ data	← サブプログラム定義・設定格納フォルダ (固定ファイル)
/opt/hitachi/tools/miacat/	
└ data	← CLI 設定データフォルダ (本フォルダ下のファイルは実行中に作成・変更・削除されます)
/var/opt/hitachi/miacat	
└ Log	← 実行ログ格納フォルダ (本フォルダ下のファイルは実行中に作成・変更・削除されます)
└ Temp	← 一時ファイル格納フォルダ (本フォルダ下のファイルは実行中に作成・変更・削除されます)
/var/opt/hitachi/VmSyslogMAgtSrvd	
└ log	← 実行ログ格納フォルダ (本フォルダ下のファイルは実行中に作成・変更・削除されます)
└ temp	← 一時ファイル格納フォルダ (本フォルダ下のファイルは実行中に作成・変更・削除されます)

### ・ 管理モジュール(Linux)


/opt/	
└ hitachi/miacat/	
└ LogCollector	← ログ採取プログラムフォルダ (固定ファイル)
└ MainteTool	← サブプログラムフォルダ (固定ファイル)
└ MainteData	← 定義・設定格納フォルダ (設定変更時にファイルが変更されます)
└ Program	← サービスプログラムフォルダ (固定ファイル)
/opt/hitachi/tools/miacat/	
└ data	← CLI 設定データフォルダ (本フォルダ下のファイルは実行中に作成・変更・削除されます)
/var/opt/hitachi/miacat	
└ Log	← 実行ログ格納フォルダ (本フォルダ下のファイルは実行中に作成・変更・削除されます)
└ Temp	← 一時ファイル格納フォルダ (本フォルダ下のファイルは実行中に作成・変更・削除されます)

### ・ 管理モジュール(Windows)

C:¥Program Files(x86)¥	
└ HITACHI¥miacat¥	
└ Log	← 実行ログ格納フォルダ (本フォルダ下のファイルは実行中に作成・変更・削除されます)
└ LogCollector	← ログ採取プログラムフォルダ (固定ファイル)
└ MainteTool	← サブプログラムフォルダ (固定ファイル)
└ MainteData	← 定義・設定格納フォルダ (設定変更時にファイルが変更されます)
└ Program	← サービスプログラムフォルダ (固定ファイル)
└ toolsdata	← CLI 設定データフォルダ (本フォルダ下のファイルは実行中に作成・変更・削除されます)
└ Data	← 監視対象装置情報 (本フォルダ下のファイルは実行中に作成・変更・削除されます)
└ Temp	← 一時ファイル格納フォルダ (本フォルダ下のファイルは実行中に作成・変更・削除されます)







## 頭字語と略語

BMC	Baseboard management controller
FC	Fiber Channel
GB	gigabyte
GUI	Graphical User Interface
Hz	Hertz
IPMI	Intelligent Platform Management Interface
KB	Kilobyte
LAN	local area network
OS	operating system
RAID	Redundant Arrays of Inexpensive Disks
SAS	Serial Attached SCSI
SEL	System Event Log
URL	Uniform Resource Locator
VGA	video graphics array
VM	virtual machine

---

 株式会社 日立製作所

〒100-8280 東京都千代田区丸の内一丁目6番6号

---

<https://www.hitachi.co.jp>

4071-1J-101-B0