

HPE Network Node Manager i Software

ソフトウェアバージョン: NNMi 10.20

HPE Network Node Manager i Software—HPE ArcSight Logger統合ガイド

ドキュメントのリリース日:2016年7月 ソフトウェアのリリース日:2016年7月

ご注意

保証

HPE製品とサービスの保証は、当該製品、およびサービスに付随する明示的な保証文によってのみ規定されるものとします。 ここに記載された情報は追加の保証をなすものではありません。HPEでは、ここに記載されている技術的、または編集上の不 正確さや脱漏については責任を負いません。

ここに記載されている情報は予告なく変更されることがあります。

制限付き権利

機密性のあるコンピューターソフトウェアです。これらを所有、使用、または複製するには、HPEが提供する有効なライセンス が必要です。FAR 12.211および12.212に準拠し、商用コンピューターソフトウェア、コンピューターソフトウェアドキュメント、お よび商用アイテムの技術データは、ベンダーの標準商用ライセンスの下、米国政府にライセンスされています。

著作権

© Copyright 2016 Hewlett Packard Enterprise Development LP

商標について

Adobe®は、Adobe Systems Incorporatedの商標です。

Appleは、米国および他の国々で登録されたApple Computer, Inc.の商標です。

AMDは、Advanced Micro Devices, Inc.の商標です。

Google™は、Google Inc.の登録商標です。

Intel®、Intel® Itanium®、Intel® Xeon®、Itanium®は、米国およびその他の国におけるIntel Corporationの商標です。

Linux®は、米国およびその他の国におけるLinus Torvalds氏の登録商標です。

Internet Explorer、Lync、Microsoft、Windows、Windows Serverは、米国および/またはその他の国におけるMicrosoft Corporationの登録商標または商標です。

OracleおよびJavaは、Oracleおよびその関連会社の登録商標です。

Red Hat® Enterprise Linux Certifiedは、米国およびその他の国におけるRed Hat, Inc.の登録商標です。

sFlowは、InMon Corpの登録商標です。

UNIX®はThe Open Groupの登録商標です。

この製品には、Apache Software Foundation (http://www.apache.org)によって開発されたソフトウェアが含まれています。

この製品には、Visigoth Software Society (http://www.visigoths.org/) によって開発されたソフトウェアが含まれています。

マニュアル更新

このドキュメントのタイトルページには、次の識別情報が含まれています。

ソフトウェアーバージョン番号。ソフトウェアーのバージョンを示します。

ドキュメントリリース日。ドキュメントが更新されるたびに変更されます。

ソフトウェアリリース日。ソフトウェアのこのバージョンのリリース日を示します。

最近の更新を確認するか、ドキュメントの最新版を使用していることを確認するには、

https://softwaresupport.hpe.com/group/softwaresupport/search-result?keyword=を参照してください。

このサイトでは、HPパスポートのアカウントが必要です。HPパスポートのアカウントがない場合は、HPパスポートのサインインページで [**アカウントを作成してください**] ボタンをクリックしてください。

サポート

HPEソフトウェアサポートWebサイトには、次のアドレスからアクセスしてください。https://softwaresupport.hpe.com

このWebサイトでは、製品、サービス、およびHPEソフトウェアが提供するサポートに関する詳細と連絡先の情報を提供します。

HPEソフトウェアサポートでは、お客様にセルフソルブ機能を提供しています。すばやく効率的な方法で、お客様のビジネス管理に必要な対話型テクニカルサポートツールにアクセスできます。サポートの大切なお客様として、サポートWebサイトで次の操作が可能です。

- 興味のあるナレッジドキュメントの検索
- サポート事例と改善要求の送信と追跡
- ソフトウェアーパッチのダウンロード
- サポート契約の管理
- HPEサポートの問合せ先の検索
- 利用可能なサービスに関する情報のレビュー
- 他のソフトウェアーユーザーとの情報交換
- ソフトウェアートレーニングの調査と登録

ほとんどのサポートエリアでは、HPパスポートのユーザーとして登録してサインインする必要があります。また、多くのエリアでは サポート契約も必要です。HPパスポートのIDを登録するには、https://softwaresupport.hpe.com にアクセスし、[HPパス ポートに登録]をクリックしてください。

アクセスレベルの詳細については、次のURLにアクセスしてください。 https://softwaresupport.hpe.com/web/softwaresupport/access-levels

目次

HPE ArcSight Logger	. 5
HPE NNMi - HPE ArcSight Logger統合	5
HPE NNMi – HPE ArcSight Loggerについて	. 5
值	. 5
統合製品	. 6
HPE ArcSight Loggerフィルターのカスタマイズ	. 6
ドキュメント	. 6
HPE NNMi - HPE ArcSight Logger統合の有効化	. 7
前提条件	. 7
HPE NNMi - HPE ArcSight Logger統合を有効にする手順	7
HPE NNMi - HPE ArcSight Logger統合の変更	. 15
受信 Syslogメッセージ数の管理	. 15
HPE NNMi - HPE ArcSight Logger統合の使用法	. 17
NNMiコンソールからHPE ArcSight Loggerを開く	17
ArcSightEvent SNMPトラップおよびArcSightEvent SNMPトラップ設定の表示	. 17
NNMiコンソールの [アクション] メニューの変更	. 18
[インシデントの管理] ワークスペース	18
[トポロジマップ] ワークスペース	. 19
[モニタリング] ワークスペース	.20
[トラブルシューティング] ワークスペース	.20
[インベントリ] ワークスペース	20
[インシデントの参照] ワークスペース	20
HPE NNMi - HPE ArcSight Logger統合の無効化	. 20
問題および解決策	. 21
ドキュメントのフィード バックを送信	.22

HPE ArcSight Logger



HPE ArcSight Loggerは、あらゆるタイプの企業ログデータの検索、レポート、警告、分析を統合する汎用ログ 管理ソリューションであり、最新のネットワークで生成される大量のデータを収集、分析、保存する固有の機能 が備えられています。

HPE ArcSight Loggerの購入の詳細については、ブラウザーでhttp://www.arcsight.com/productsを指定してください。

HPE NNMi - HPE ArcSight Logger統合

HPE NNMi – HPE ArcSight Loggerについて

この章の手順に従ってArcSightEventsをNNMiに転送するようにHPE ArcSight Loggerを設定すれば、ネット ワーク運用スタッフはNNMiコンソールでSyslogインシデントを表示できます。

値

HPE NNMi-HPE ArcSight Logger統合ではSyslog情報がNNMiに追加され、NNMiユーザーがこれらのSyslog メッセージを表示して潜在的な問題を調査できます。

統合製品

この章の情報は、以下の製品に当てはまります。

- HPE ArcSight Logger
- SmartConnector: ArcSight HPE NNMi SNMP
- SmartConnector:ArcSight Logger Forwarding Connector for NNMi

ヒント: サポートされているLoggerバージョンのリストについては、NNMiシステムとデバイス対応マトリックスを参照してください。

• NNMi 10.20

サポートされているハード ウェアプラットフォームおよびオペレーティングシステムの最新情報については、両方の製品の対応マトリックスを参照してください。

HPE ArcSight Loggerフィルターのカスタマイズ

HPE ArcSight Loggerフィルターを渡してNNMiに転送するSyslogメッセージがあります。HPE ArcSight Logger フィルターを設定しないと、HPE ArcSight Loggerから大量のArcSightEventsがNNMiに転送されます。このた め、NNMiのパフォーマンスに悪影響を及ぼす可能性があります。このフィルターを速やかに設定して、HPE ArcSight LoggerからNNMiに流れるArcSightEventsの量を制限することが非常に重要です。NNMiコンソール から、Loggerフィルターの設定ページに移動できます。このページでLoggerフィルターを追加し、HPE ArcSight LoggerからNNMiに転送されるメッセージを調整できます。

NNMiからHPE ArcSight Loggerを開く場合、管理者以外(検索のみ)の資格証明を指定することをお勧めしま す。管理者資格証明を入力すると、NNMiユーザーが管理者権限でHPE ArcSight Loggerにアクセスすること がHPE ArcSight Loggerで許可され、フィルター設定の変更が可能になります。HPE ArcSight Logger設定に変 更を加える必要がない場合は、管理者以外の資格証明を入力します。

ドキュメント

HPE NNMi - HPE ArcSight Logger統合のインストールと設定の準備を行うため、以下のマニュアルを入手してお読みください。

- 『SmartConnector Configuration Guide for HPE NNMi SNMP』(NNMi Northboundインタフェース) HPE NNMi SNMP用のSmartConnectorは、NNMiインシデントおよび他の情報をLoggerに転送します。
- 『SmartConnector Configuration Guide for ArcSight Logger Forwarding Connector for HPE NNMi』 HPE ArcSight Logger Forwarding Connector for NNMiは、SyslogメッセージをArcSightEventsの形式で NNMiに転送します。
- 『Logger Administrator's Guide』
 この統合では、HPE ArcSight LoggerはSNMPトラップをArcSightEventsの形式でNNMiに転送します。

『Logger Administrator's Guide』に加え、HPE ArcSight Loggerの統合オンラインヘルプにも『Logger Administrator's Guide』とほぼ同等の情報が含まれています。

『SmartConnector Configuration Guides』や『Logger Administrator's Guide』などのHPE ArcSightマニュアルのコ ピーを入手するには、ブラウザーで以下の場所を指定します。

https://protect724.arcsight.com

HPE ArcSight製品情報にアクセスするには、HPE ArcSightのお客様である(ユーザー資格証明を入力できる) 必要があります。 オペレーティングシステムやブラウザーなどの、HPE ArcSight Loggerでサポートされているシステム要件を表示するには、ブラウザーで

http://www.arcsight.com/products/products-loggerを指定します。HPE ArcSight Loggerでサポートされている システム要件は、『Logger Administrator's Guide』でも確認できます。

HPE NNMi - HPE ArcSight Logger統合の有効化

NNMi Northboundインタフェースなどの既存のNNMi機能を効果的に活用して、HPE ArcSight LoggerとNNMi間でカスタム統合を設定した可能性もあります。NNMi 10.20をインストールする場合は、このHPE NNMi - HPE ArcSight Loggerカスタム統合を無効にする必要があります。このカスタム統合を無効にした後、このセクションのタスクを実行してNNMi 10.20で提供されるさらに堅牢なHPE NNMi - HPE ArcSight Logger統合を有効にします。

前提条件

HPE NNMi - HPE ArcSight Logger統合を有効にする前に、以下を実行します。

- NNMi 10.20をインストールします。このタスクをサポートするため、ブラウザーで http://support.openview.hpe.com/selfsolve/manualsを指定して、 インタラクティブバージョンの『Network Node Manager iインストールガイド』をダウンロードします。
- 『SmartConnector Configuration Guide for HPE Network Node Manager i SNMP』マニュアルの手順に従って、HPE NNMi SNMP用のSmartConnectorをインストールします。
- 『SmartConnector Configuration Guide for ArcSight Logger Forwarding Connector for HPE NNMi』マニュア ルの手順に従って、HPE ArcSight Logger Forwarding Connector for HPE NNMiをインストールします。

HPE NNMi - HPE ArcSight Logger統合を有効にする手順

以下のタスクを実行して、HPE NNMi - HPE ArcSight Logger統合を有効にします。

「タスク1: NNMi 10.20のインストール」

「タスク2: HPE ArcSightのMIBの理解」

「タスク3: HPE ArcSight Logger Forwarding Connector for NNMiの設定」

「タスク4: HPE NNMi - HPE ArcSight Logger統合の設定」

「タスク5: HPE ArcSight Loggerフィルターの設定」

「タスク6: HPE NNMi SNMP用のSmartConnectorの設定 (Northboundインタフェース用のコネクター、オプションのタスク)」

「タスク7: SNMPv1、v2、v3トラップインシデントをHPE ArcSight Loggerに転送するためのNNMiの設定 (Northboundインタフェース、オプションのタスク)」

タスク1: NNMi 10.20のインストール

タスク2: HPE ArcSightのMIBの理解

「タスク1: NNMi 10.20のインストール」~「タスク5: HPE ArcSight Loggerフィルターの設定」を実行すると、HPE ArcSight LoggerはフィルタリングされたArcSightEventのNNMiへの転送を開始します。NNMiは、インタフェース とノードを、ArcSightEventに含まれるソースオブジェクトに解決します。NNMi 10.20のインストール中、hparcsight.mib MIBがインストールされ、NNMi管理サーバーにロードされます。ArcSightEventに存在するOID に関する理解を深めるには、NNMiの [ノードアクション] > [MIB情報] 機能を使用してください。

タスク3: HPE ArcSight Logger Forwarding Connector for NNMiの設定

『SmartConnector Configuration Guide for ArcSight Logger Forwarding Connector for HPE NNMi』マニュアルの 手順に従って、HPE ArcSight Logger Forwarding Connector for NNMiを設定します。

タスク4: HPE NNMi - HPE ArcSight Logger統合の設定

HPE NNMi - HPE ArcSight Logger統合とArcSightEventを有効にし、ArcSightEvents形式のSNMPトラップ を転送するようHPE ArcSight Loggerを設定することにより、NNMiで各ArcSightEventの内容を評価し、それを SNMPトラップまたはSyslogメッセージとして表示できます。HPE NNMi - HPE ArcSight Logger統合を有効にす るには、以下の手順を実行します。

 NNMiコンソールで、[統合モジュールの設定] > [HPE ArcSight] をクリックします。NNMiで、「図1 HPE NNMi-HPE ArcSight Logger統合の有効化」に示す [ArcSight統合の設定] 画面が表示されます。 HPE NNMi - HPE ArcSight Logger統合の設定時に、「図1 HPE NNMi-HPE ArcSight Logger統合の有 効化」を参照してください。

Configure HP	E ArcSight Integration	0
Enable HPE ArcSight Integration	● 手順 2	
NNMI SSL		
NNMi Host	autosuse.Rc./speciala.net	手順
NNMi User	system	
NNMi Password	•••••	手順
Enable Logger Cross- Launch	✓ 手順 5 手順	
Enable HPE ArcSight Trap	6 手順	
Enable Northbound Forwarding		手順
Logger SSL		0
Logger Host	autosuse.Rrc.hposwiab.net	手順
Logger Port	9000	9
Logger Admin Username	admin	手順
Logger Admin Password	•••••	10
Use Administrator Credentials		手順
Logger User Username	nonadmin	115
Logger User Password	•••••	手順 11a
Logger Filters	Configure (Generate)	
Syslog Forwarding	Configure	
Submit		Cancel

図1 HPE NNMi-HPE ArcSight Logger統合の有効化

- 2. [HPE ArcSight統合の有効化]を選択します。
- 3. 以下のNNMi統合情報を追加または確認します。
 - NNMiホスト: このフィールドには、NNMi管理サーバーの完全修飾ドメイン名を入力します。
 - NNMiポート: このフィールドには、NNMiのアクセスに使用するHTTPポート番号が含まれます。詳細については、『NNMiデプロイメントリファレンス』を参照してください。
 - NNMiユーザー: NNMi管理者ユーザーグループにマッピングするNNMiユーザー名を入力します。
- 4. NNMiパスワード: ユーザー名 のパスワードを入力します。

- 5. [Logger交互起動の有効化]を選択します。
- 6. [HPE ArcSightトラップの有効化]を選択します。

以下の手順を実行して、ArcSightトラップを有効にすることもできます。

- a. NNMiコンソールで、[設定] > [インシデント] > [SNMPトラップの設定]の順にクリックします。
- b. [ArcSightEvent] > [開く] の順にクリックします。
- c. [有効にする]を選択します。
- d. [保存して閉じる]をクリックします。
- 7. NNMiインシデントをHPE ArcSight Loggerに転送する場合は、[Northbound転送の有効化]を選択します。
- すべてのHPE ArcSight LoggerアプリケーションがSSLを使用するように設定されているわけではありません。 このHPE NNMi - HPE ArcSight Logger統合に含まれるHPE ArcSight LoggerアプリケーションがSSLを使用するように設定されている場合は、[Logger SSL]を選択します。

注: SSL用のLoggerの設定については、『HPE ArcSight Logger v5.1 Administrators Guide』を参照してください。

- 9. 以下のHPE ArcSight Logger統合情報を追加します。
 - Loggerホスト (Logger Hostの完全修飾ドメイン名)
 - Loggerポート
- 10. HPE ArcSight Loggerの以下の管理者資格証明を追加します。
 - Logger管理者ユーザー名
 - Logger管理者パスワード
- 11. 「NNMiコンソールで、[設定]>[インシデント]>[SNMPトラップの設定]の順にクリックします。」を実行しま す。「[管理者資格証明の使用]を選択します。これにより、[Loggerユーザーのユーザー名]および[Logger ユーザーパスワード]フィールドに管理者資格証明が適用されます。これは一部のアプリケーションには便 利ですが、このオプションを選択してもHPE ArcSight LoggerでNNMiレベル1オペレーターに完全な管理者 権限が付与されるわけではありません。セキュリティの理由により、「読み取り専用の交互起動に対して、 以下のユーザー資格証明を追加します。これらの資格証明は、HPE ArcSight Logger内で読み取り専用 ユーザーを使用する場合のみ設定します。」が推奨される方法です。」も実行できますが、「読み取り専 用の交互起動に対して、以下のユーザー資格証明を追加します。これらの資格証明は、HPE ArcSight Logger内で読み取り専用ユーザーを使用する場合のみ設定します。」が推奨される方法です。
 - a. 読み取り専用の交互起動に対して、以下のユーザー資格証明を追加します。これらの資格証明 は、HPE ArcSight Logger内で読み取り専用ユーザーを使用する場合のみ設定します。
 - Loggerユーザーのユーザー名
 - Loggerユーザーのパスワード
 - b. [管理者資格証明の使用]を選択します。これにより、[Loggerユーザーのユーザー名]および[Logger ユーザーパスワード]フィールドに管理者資格証明が適用されます。これは一部のアプリケーションには 便利ですが、このオプションを選択してもHPE ArcSight LoggerでNNMiレベル1オペレーターに完全な 管理者権限が付与されるわけではありません。セキュリティの理由により、「読み取り専用の交互起 動に対して、以下のユーザー資格証明を追加します。これらの資格証明は、HPE ArcSight Logger 内で読み取り専用ユーザーを使用する場合のみ設定します。」が推奨される方法です。
- 12. [送信]をクリックして変更内容を保存します。
- 13. 交互起動に加えた変更をNNMiコンソールで表示するには、以下の手順を実行します。

- a. NNMiからサインアウトします。
- b. NNMiにサインインします。

「タスク4: HPE NNMi - HPE ArcSight Logger統合の設定」を実行すると、フィルタリングされていない ArcSightEventがHPE ArcSight LoggerによってNNMiに転送されます。NNMiでArcSightEventの内容が評価 され、それがSNMPトラップまたはSyslogメッセージとして表示されます。

この後ですぐに「タスク5: HPE ArcSight Loggerフィルターの設定」を実行して、HPE ArcSight LoggerからNNMiに 転送するSyslogメッセージのみを特定し、設定します。

タスク5: HPE ArcSight Loggerフィルターの設定

「タスク5: HPE ArcSight Loggerフィルターの設定」では、HPE ArcSight Loggerフィルターを設定してNNMiに転送するSyslogメッセージを指定します。

注: 管理不可能な数のトラップ受信を避けるため、「タスク4: HPE NNMi - HPE ArcSight Logger統合の設定」の直後に「タスク5: HPE ArcSight Loggerフィルターの設定」を実行してください。

注:[設定]>[Syslogメッセージの設定]の順にクリックしてSyslogメッセージの有効化または無効化などの 変更を行うたびに、「NNMiコンソールで、[統合モジュールの設定]>[HPE ArcSight]をクリックします。」~ 「以下のいずれかの操作を実行して、NNMiに転送するSyslogメッセージを特定するフィルターを設定しま す。」を実行します。

HPE ArcSight Loggerの設定にアクセスして新しいフィルターの内容を追加するには、以下の手順を実行します。

- 1. NNMiコンソールで、[統合モジュールの設定] > [HPE ArcSight] をクリックします。
- [>Loggerフィルター] > [(生成)] の順にクリックします。NNMiにより、[設定] > [Syslogメッセージの設定] に 表示されるEnabled SyslogメッセージがHPE ArcSight Loggerフィルターで使用できる形式に変換され、こ れらの変換が[フィルターを有効にしました] ページに表示されます。

図2 [フィルターを有効にしました] ページ

Enabled Filters The following SysLogs are enabled: all other incoming syslog messages will be dropped. It is strongly recommended that you configure Logger with the provided filter
BGP.*ADJCHANGE[CDP.*DUPLEX.*MISMATCH DTP.*NONTRUNKPORTFAIL] DTP.*TRUNKPORTFAIL DTP.*NONTRUNKPORTON DTP.*TRUNKPORTON DT P.*TRUNKPORTGH]SYS.*PORT.*COLLDISJFR.*DLCICHANGE]LINK.*UPDOW N LINK.*ERRORLINEPROTO.*UPDOWN OSPF.*ADJCHGIPAGP.*PORTTOSTP PAGP.*PORTFROMSTP PORT.*SECURITY.*PSECURE.*/IOLATION.*/LANJS NMP.*MODULETRAP]SPANTREE.*PORTLISTEN SPANTREE.*ROOTCHANGE] SPANTREE.*PORTFWD]SPANTREE.*PORTLISTEN SPANTREE.*ROOTCHANGE] STANDBY.*DUPADDR]STANDBY.*STATECHANGE[SYS.*MOD.*CFGMISMATC H.*]SYS.*MOD.*CFGMISMATCH.*]SYS.*MOD.*CFGMISMATCH.*]SYS.*MOD.*C FGMISMATCH.*]SYS.*PKTBUFBAD]SYS.*PORT.*COLLISYS.*PORT.*IN.*ERRO- RSJSYS.*PORT.*RUNTSJSYS.*SYS.*LCPERR.*]SYS.*NOD.*CFGMISMATC H.*]SYS.*MOD.*CFGMISMATCH.*]SYS.*NOD.*CFGMISMATCH.*]SYS.*MOD.*C FGMISMATCH.*]SYS.*PKTBUFBAD]SYS.*PORT.*COLLISYS.*PORT.*IN.*ERRO- RSJSYS.*PORT.*RUNTSJSYS.*SYS.*LCPERR.*]SYS.*LCPERR.*]SYS.*MOD.*C FGMISMATCH.*]SYS.*MOD.*CKJSYS.*RELOAD]SYS.*MOD.*REMOVE]SYS.*MOD. *RESET]SYS.*NESTARTIRMON.*PMGR.*PORT.*UPIRMON.*CHASIS.*FAN.*S TATUSIRMON.*STP.*NEW.*ROOT RMON.*LACP.*DYNAMIC.*TRUNK.*OFF.*L INEJRMON.*LACP.*DYNAMIC.*TRUNK.*ON.*LINEJRMON.*LACP.*ERROR.*CON DITION.*BLOCKJRMON.*POEMGR.*PD.*DENIED.*POWERJRMON.*BOOT.* CRASH.*RECORD.*JRMON.*BOOT.*CRASH.*RECORD.*JRMON.*BOOT.* CRASH.*RECORD.*JRMON.*BOOT.*CASSH.*RECORD.*JRMON.*BOOT.* CRASH.*RECORD.*JRMON.*BOOT.*CASSH.*RECORD.*JRMON.*BOOT.* CRASH.*RECORD.*JDDEV.*FAN.*FAILUED]DEV.*FAN.*RECOVEREDIOSPF .*OSPF.*NBR.*CHGJDEV.M.*BOARD.*REMOVED]DEV.*FAN.*RECOVEREDIOSPF .*OSPF.*NBR.*CHGJDEV.M.*BOARD.*REMOVED]DEV.*FAN.*RECOVEREDIOSPF .*OSPF.*NBR.*CHGJDEV.M.*BOARD.*REMOVED]DEV.*FAN.*RECOVEREDIOSPF .*OSPF.*NBR.*CHGJDEV.M.*BOARD.*REMOVED]DEV.*FAN.*RECOVEREDIOSPF .*OSPF.*NBR.*CHGJDEV.M.*BOARD.*REMOVED]DEV.*FAN.*RECOVEREDIOSPF .*OSPF.*NBR.*CHGJDEV.M.*BOARD.*REMOVED]DEV.*FAN.*RECOVEREDIOSPF .*OSPF.*NBR.*CHGJDEV.M.*BOARD.*REMOVED]DEV.*FAN.*RECOVEREDIOSPF .*OSPF.*NBR.*CHGJDEV.M.*BOARD.*REMOVED]DEV.*FAN.*RECOVEREDIOSPF .*OSPF.*NBR.*CHGJDEV.M.*BOARD.*REMOVED]DEV.*FAN.*RECOVEREDIOSPF .*OSPF.*NBR.*CHGJDEV.M.*BOARD.*REMOVED]DEV.*FAN.*RECOVEREDIOSF
Show Enabled Incidents

- 3. [フィルターを有効にしました] ページでフィルターの内容を選択します。この内容をコピーし、後の手順でHPE ArcSight Logger内のフィルターに貼り付けます。 ウィンドウを閉じます。
- 4. [Loggerフィルター] > [設定] の順にクリックします。「図3 HPE ArcSight Loggerの [設定] ページ」に示す HPE ArcSight Loggerの [設定] ページにビューが表示されます。

旜 ArcSight Logger Summary Analyze 🗸 🛛 Dashboards Reports 🗸 Configuration 🐱 System Admin Take me to... (Alt Filters Type of Filter All \mathbf{v} Add Name Ouerv Category Type 8-3 Regular Expression BGP.*ADJCHANGEICDP.*DUPLEX.*MISMATCHIDTP.*NONTRUNKPORTFAILIDTP.*TRUNKPORTFAILIDTP NNMi_filters Shared Configuration -Configuration System 🛃 Unified Query categoryBehavior = "/Modify/Configuration" AND categoryOutcome = "/Success" Changes (Unified) Configuration -System Configuration System B-a Regular Expression cef:0.*categoryBehavior-/Modify/Configuration:AND: categoryOutcome-/Success Changes (CEF format) Events - CEF System Regular Expression cef:0 Events - Event "CEF:0" AND NOT (destinationAddress IS NULL) _storageGroup NOT IN ["Internal Event Storage Group Counts by System 🛃 Unified Query dst | sort - _count Destination Events - Event Counts by "CEF:0" AND NOT (sourceAddress IS NULL) | cef src | chart _count by src | sort - _count System 🛛 🛃 Unified Overv Source Events - High and Very High sion_CEF:(\\/2.fA\\]!\$\/5\/2.Varv.)2High_ ular Expr

図3 HPE ArcSight Loggerの[設定] ページ

- 5. [フィルター]をクリックし、フィルターのリストがロードされるのを待ちます。
- 6. 以下のいずれかの操作を実行して、NNMiに転送するSyslogメッセージを特定するフィルターを設定します。

NNMiに転送するSyslogメッセージを特定するフィルターを初めて作成する場合は、以下の手順を実行します。

- a. [追加]をクリックします。
- b. HPE ArcSight Loggerで [フィルターの追加] フォームが表示されたら、フィルター名を追加し、フィルターのタイプに [Regexクエリー] を選択して、[次へ] をクリックします。
- c. 内容を「[フィルターを有効にしました] ページでフィルターの内容を選択します。この内容をコピーし、後の手順でHPE ArcSight Logger内のフィルターに貼り付けます。ウィンドウを閉じます。」から [Query] フィールドにコピーします。
- d. 作業内容を保存します。

NNMiに転送するSyslogメッセージを特定する既存のフィルターを変更する場合は、以下の手順を実行します。

- a. NNMiに転送するSyslogメッセージを特定するためにHPE ArcSight Loggerで使用する既存のフィル ターを編集します。
- b. 既存のフィルターの内容をクリアします。
- c. 内容を「[フィルターを有効にしました] ページでフィルターの内容を選択します。この内容をコピーし、後の手順でHPE ArcSight Logger内のフィルターに貼り付けます。ウィンドウを閉じます。」から [Query] フィールドにコピーします。
- d. 作業内容を保存します。

これで、HPE ArcSight Loggerにより目的のSyslogメッセージのみがNNMiに転送されるようになりました。

タスク6: HPE NNMi SNMP用のSmartConnectorの設定 (Northboundインタフェース用のコネクター、オプションのタスク)

『SmartConnector Configuration Guide for HPE NNMi SNMP』マニュアルの手順に従って、HPE NNMi SNMP 用のSmartConnectorを設定します。

タスク7: SNMPv1、v2、v3トラップインシデントをHPE ArcSight Loggerに転送するためのNNMiの設定 (Northboundインタフェース、オプションのタスク)

- 1. NNMiコンソールで、[統合モジュールの設定] > [HPE ArcSight] をクリックします。
- [syslog転送]>[設定] の順にクリックします。[NNMi Loggerデスティネーション] ページにビューが表示されます。このタスクの手順の実行時に「図4 HPE NNMi HPE ArcSight Loggerデスティネーションの設定」を参照してください。

図4 HPE NNMi - HPE ArcSight Loggerデスティネーションの設定

P ArcSight Logger	Destination	Enabled: 🗸
lost:		_
'ort:*	8162	_
ommunity String:*	public	
		* Required
ending Options	Management 1 Zard Deaters	NMD Tree
ncidents:	Management Std Party s	ымме тгар
ifecycle State 'hanges:	 Enhanced Closed State 0 Both 	Changed
orrelations:	🔍 None 🔍 Single 🖲 Group	
eletions:	Dont Send Send	
INMi Console Access:	○ НТТР ◉ НТТРЅ	
ncident Filters		
)IDs 💿	None 🔍 Include 🔍 Exclude	
Add Remove		~
dditional Information	on	
Jptime (seconds):	46,606.69	

3. [ArcSight Loggerデスティネーション] > [有効にする]の順に選択します。

- 4. [ポート] フィールドの値に8162を追加します。NNMiにより、NNMi管理サーバーにインストールされたコネク ターが転送されます。ポートは、コネクターのデフォルトとして自動的に設定されます。
- 5. Loggerホストの[コミュニティ文字列]を入力します。 コミュニティ文字列を指定しないと、統合モジュールは空のコミュニティ文字列を使用しようとします。
- 6. [送信オプション] で選択を行います。これらの値を変更しないと、NNMiによりすべてが転送されます。
- 7. [送信]をクリックします。
- 8. NNMiで設定エラーがテストされます。送信に成功するまで、エラーを修正して「[送信]をクリックします。」を 繰り返します。

これで、NNMilによりSNMPv1、v2、v3トラップインシデントがHPE ArcSight Loggerに転送されるようになりました。

HPE NNMi - HPE ArcSight Logger統合の変更

ここでは、有効化したHPE NNMi - HPE ArcSight Logger統合を変更および改善する方法について説明します。

受信Syslogメッセージ数の管理

HPE NNMi – HPE ArcSight Logger統合では、HPE ArcSight LoggerでサポートされているすべてのベンダーからのSyslogメッセージに対応しています。

サポートされているベンダーに対して、NNMiでSyslogメッセージインシデントが設定されていない場合があります。未定義のSyslogメッセージに対してSyslog設定を作成する場合は、以下の手順をガイドラインとして使用してください。

- 1. 定義する未定義 Syslogメッセージリストを取得します。
 - NNMiのインストールでトラップの着信率が低い場合は、nnmtrapdump.ovplスクリプトを実行して、指定時間内にNNMiで保存されたすべてのトラップを表示します。以下の例は、NNMiによる過去10分間のトラップをすべて表示します。

nnmtrapdump.ovpl -last 10

注:必要に応じて、nnmtrapdump.ovp1スクリプトのオプションを調整します。使用可能なオプションの詳細については、nnmtrapdump.ovplのリファレンスページ、またはUNIXのマンページを参照してください。

NNMiのインストールでトラップ着信率が高い場合は、以下のファイルをExcelスプレッドシートにインポートします。

Windowsの場合:%NNM_DATA%\log\nnm\trap.csv.<compression> Linuxの場合:\$NNM_DATA/log/nnm/trap.csv.<compression>

trap.csv.<compression>ファイルの詳細については、『NNMiデプロイメントリファレンス』を参照してください。

注: 定義する特定のSyslogメッセージが表示されない場合は、NNMiに転送するSyslogメッセージの 再設定が必要な場合があります。「タスク5: HPE ArcSight Loggerフィルターの設定」を参照してください。 HPE ArcSight Loggerフィルターを設定しても定義する特定のSyslogメッセージが表示されない場合 は、HPE ArcSightサポート (https://softwaresupport.hpe.com/)で問い合わせてください。

- 「定義する未定義 Syslogメッセージリストを取得します。」で取得したリストを使用して、NNMiで定義する 最初のSyslogメッセージをリスト内で見つけます。 たとえば、インタフェースFastEthernet0/3でLINK-3-UPDOWNなどの特定のテキストを含むCiscoデバイスの メッセージを探しているとします。
- 3. リストを検索して、特定のメッセージ名を見つけます。

たとえば、Syslogメッセージのリストを検索すると、以下のCisco Syslogメッセージが見つかります。

.1.3.6.1.4.1.11937.1.16 Apr 6 01:08:30 10.10.10.10 49349:16w3d:%LINK-3-UPDOWN:Interface FastEthernet0/3, changed state to up

この例では、LINK-3-UPDOWNがメッセージ名になります。

注: 各メッセージ名は、ベンダー固有です。Ciscoメッセージでは通常、メッセージ名がパーセント(%) 記号の直後に配置されます。

4. 次に、メッセージ名に関連付けられたOIDを見つけます。OID .1.3.6.1.4.1.11937.1.42.1.3.1に関連付けられている値を探します。

この例では、LINK-3-UPDOWNという名前を含むログエントリを探します。以下のようなエントリが見つかります。

state=HAS_VALUE type=OCTET STRING oid=.1.3.6.1.4.1.11937.1.42.1.1.1 value=mnemonic state=HAS_VALUE type=OCTET STRING oid=.1.3.6.1.4.1.11937.1.42.1.3.1 value=LINK-3-UPDOWN

OID値を示すテキスト文字列をメモします。この値は、Syslogメッセージインシデントのそれぞれの設定を検索するためにNNMiで使用されます。NNMiの名前フィールドで使用できない文字はすべて「_」(アンダースコア)に置き換えられます。この例では、「「次に、メッセージ名に関連付けられたOIDを見つけます。OID .1.3.6.1.4.1.11937.1.42.1.3.1に関連付けられている値を探します。この例では、LINK-3-UPDOWNという名前を含むログエントリを探します。以下のようなエントリが見つかります。」で取得したOIDテキスト文字列の値を、定義する未定義Syslogメッセージ名として追加します。この例では、OID .1.3.6.1.4.1.11937.1.42.1.3.1の値はLINK-3-UPDOWNです。」で定義するときに、OID .1.3.6.1.4.1.11937.1.42.1.3.1に割り当てられたテキスト文字列の値をSyslogメッセージ名として使用します。この例では、値がLINK-3-UPDOWNに設定されています。

- 5. NNMiコンソールで、[設定] ワークスペースにある [Syslogメッセージの設定] をクリックします。
- 6. [新規作成]をクリックして、フォームを開きます。未定義のSyslogメッセージに対して新しいSyslog設定を 作成する場合は、このフォームを使用します。
- 7. 「次に、メッセージ名に関連付けられたOIDを見つけます。OID .1.3.6.1.4.1.11937.1.42.1.3.1に関連付け られている値を探します。この例では、LINK-3-UPDOWNという名前を含むログエントリを探します。以下 のようなエントリが見つかります。」で取得したOIDテキスト文字列の値を、定義する未定義Syslogメッセー ジ名として追加します。

この例では、OID.1.3.6.1.4.1.11937.1.42.1.3.1の値はLINK-3-UPDOWNです。

注: 英数字、スペース、_(アンダースコア)、: (コロン)、- (ダッシュ)、/ (スラッシュ) の各特殊文字が有効 です。 サポートされていない文字がニーモニック値に含まれる場合は、各文字をアンダースコア(_)またはスペースに置き換えます。

- 8. この新しいSyslog設定に対して、残りのフィールドを設定します。
- 9. [保存して閉じる] アイコンをクリックします。
- 「定義する未定義 Syslogメッセージリストを取得します。」で取得したリストを使用して、NNMiで定義する 残りのSyslogメッセージについて「定義する未定義 Syslogメッセージリストを取得します。」~「[保存して閉 じる] アイコンをクリックします。」を繰り返します。

ヒント: NNMiが常に高いパフォーマンスを発揮するように、NNMiはデータベース内に一定数のSNMPトラップを保存した後に着信SNMPトラップ (Syslogメッセージを含む)をドロップします。

最も古いSNMPトラップインシデントの自動削除機能を使用して、この数値を調整できます。詳細については、『NNMiデプロイメントリファレンス』を参照してください。

HPE NNMi - HPE ArcSight Logger統合の使用法

ここでは、有効化したHPE NNMi - HPE ArcSight Logger統合を使用する方法と、必要に応じて変更する方法を説明します。

NNMiコンソールからHPE ArcSight Loggerを開く

NNMiコンソールからHPE ArcSight Loggerを起動するとき、交互起動を開始する前に、HPE ArcSight Logger を信頼するようブラウザーから要求されることがあります。

注: 信頼されていないサイトにアプリケーションからリダイレクトしようとすると、リダイレクトを実行する前に、サイトを信頼するよう要求されます。

ArcSightEvent SNMPト ラップおよびArcSightEvent SNMPト ラップ設定の表示

ArcSightEvent SNMPトラップを表示するには、[インシデントの参照] ワークスペースで [SNMPトラップ] をクリック します。ArcSightEvent Syslogメッセージを表示するには、[インシデントの参照] ワークスペースで [Syslogメッ セージ] をクリックします。

HPE NNMi - HPE ArcSight Logger統合を有効にすると、HPE ArcSight LoggerからNNMiに転送される ArcSightEventが、SNMPトラップと同じように構造化されます。ArcSightEvent SNMPトラップ設定を表示する には、以下の手順を実行します。

- 1. NNMiコンソールで、[設定] > [インシデント] > [SNMPトラップの設定] に移動します。
- 2. [ArcSightEvent]トラップ定義を開きます。

HPE ArcSight LoggerからNNMi 10.20に転送される実際のSyslogメッセージであるArcSightEventsを表示するには、以下の手順を実行します。

- 1. NNMiコンソールで、[設定] > [インシデント] > [Syslogメッセージの設定] に移動します。
- 2. NNMilにより、Syslogメッセージの設定の現在のリストが表示されます。

NNMiコンソールの [アクション] メニューの変更

HPE NNMi - HPE ArcSight Logger統合を有効にすると、NNMiコンソールにより以下の新機能がNNMi管理 サーバーに表示されます。

[インシデントの管理] ワークスペース

[インシデントの管理] ワークスペースで、NNMiコンソールを使用してHPE ArcSight Loggerアプリケーションをインシデントから開きます。

インシデントビューで、インシデントを選択します。次に、「図5 [インシデントの管理] ワークスペースでNNMiイン シデントからHPE ArcSight Loggerを開く」に示すように、NNMiコンソールの [アクション] メニューで、[HPE ArcSight Logger] > [インシデント履歴の表示] をクリックします。

または、インシデントを右クリックしてから、[HPE ArcSight Logger] > [インシデント履歴の表示]をクリックします。

図5 [インシデントの管理] ワークスペースでNNMiインシデントからHPE ArcSight Loggerを開く

<u>F</u> il	e	<u>V</u> ie	w	<u>T</u> ools	Ac	tions		H	elp										
_				_		Node	Ac	ctio	ons					•					
Open Key Incidents 🗶					Interfa	face	e A	ction	15				1						
			0	1		IP Add	lare	ess	Actio	ons					-				
6	1		0	1	8	<u>M</u> aps	ŝ							•					
Sev	Pric	Life	▼ Las	t Occurre		Source	ce N	Noc	de						ı Or	i <u>e</u> Co	r Ten	ant	Manager
8	5 📱	5	8/1/1	6 4:20:05		Source	ce (Obj	ject						1	<u>ه</u>	Defa	ult	Local
8	5	ح .	8/1/1	6 3:33:55	5	Node	Gr	rou	p Me	mbe	ers					⊳ <u>⊼</u> ∢	Defa	ult	Local
8	5 📮	5	8/1/1	6 2:49:11		Graph	h C	Cust	tom F	Polle	er Resu	ults			1	₩ ×	Defa	ult	Local
8	5 📮	5	7/30/:	16 2:52:0	3	<u>N</u> ode	e Ac	cce	SS					•	1	١ <u>×</u>	Defa	ult	Local
$\mathbf{\Delta}$	5 📱	2,	7/26/3	16 11:46	:	HPE A	Arc	cSig	ght Lo	ogge	er			•	1		Defa	ult	Local
۲	5 📮	5	7/26/3	16 9:11:0		Enterp	pri	ise	Unifi	ied C	Comm	unicati	ions Ma	p 🕨	1	١ <u>×</u>	Defa	ult	Local
					Ê	Delete	e												
						C <u>h</u> ang	ge	Life	ecycl	le				•					
						<u>A</u> ssigr	ļn							•					
						Incide	ent	t Co	onfigu	urati	ion <u>R</u> e	eports		•					
						Open	i In	ncide	ent C	Confi	igurat	tion							
					0	Run D	Dia	agno	ostics	s (Ev	valuat	ion)							
						Hyper	:r <u>v</u> i:	isor	r					•					

[トポロジマップ] ワークスペース

[トポロジマップ] ワークスペースで、NNMiコンソールを使用してHPE ArcSight Loggerアプリケーションをノードから 開きます。

マップビューで、ノードまたはインタフェースを選択します。次に、「図6 [トポロジマップ] ワークスペースでノードから HPE ArcSight Loggerを開く」に示すように、NNMiコンソールの [**アクション**] メニューで [**HPE ArcSight Logger**] をクリックし、使用可能ないずれかのオプションをクリックします。

あるいは、ノードまたはインタフェースを右クリックし、[HPE ArcSight Logger] をクリックして、使用可能ないずれかのオプションをクリックします。

図6 [トポロジマップ] ワークスペースでノード からHPE ArcSight Loggerを開く

<u>F</u> ile	<u>V</u> iew	<u>T</u> ools	Actions <u>H</u> elp	
_		_	<mark>™</mark> aps	•
Netwo	ork Overvie	w x	 Graphs Node Access Polling Configuration Details MIB Information Node Group Membership Custom Attributes Sample Node Action HPE ArcSight Logger 	 > ><
			Delete	
IF	2		Management Mode External Map Tests FrameRelay Map All DLCIs FrameRelay Map Selected DLCIs Run Baseline Diagnostics (Unlicensed Show Attached End Nodes Hyper <u>v</u> isor	, , , , , , , , , , , , , , , , , , ,
		÷.		

[モニタリング] ワークスペース

[モニタリング] ワークスペースで、NNMiコンソールを使用してHPE ArcSight Loggerアプリケーションをノードまたは インタフェースから開きます。モニタリングビューで、ノードまたはインタフェースを選択します。次に、NNMiコンソー ルの [アクション] メニューで [HPE ArcSight Logger] をクリックし、使用可能ないずれかのオプションをクリックしま す。

あるいは、ノードまたはインシデントを右クリックし、[HPE ArcSight Logger] をクリックして、使用可能ないずれかのオプションをクリックします。

[トラブルシューティング] ワークスペース

[トラブルシューティング] ワークスペースで、NNMiコンソールを使用してHPE ArcSight Loggerアプリケーションを ノードまたはインタフェースから開きます。トラブルシューティングビューで、ノードまたはインタフェースを選択しま す。次に、NNMiコンソールの[アクション] メニューで [HPE ArcSight Logger] をクリックし、使用可能ないずれか のオプションをクリックします。

あるいは、ノードまたはインタフェースを右クリックし、[HPE ArcSight Logger] をクリックして、使用可能ないずれかのオプションをクリックします。

[インベントリ] ワークスペース

[インベントリ] ワークスペースで、NNMiコンソールを使用してHPE ArcSight Loggerアプリケーションをノードまたは インタフェースから開きます。

インベントリビューで、ノードまたはインタフェースを選択します。次に、NNMiコンソールの[**アクション**] メニューで [HPE ArcSight Logger] をクリックし、使用可能ないずれかのオプションをクリックします。

あるいは、ノードまたはインタフェースを右クリックし、[HPE ArcSight Logger] をクリックして、使用可能ないずれかのオプションをクリックします。

[インシデントの参照] ワークスペース

[インシデントの参照] ワークスペースで、NNMiコンソールを使用してHPE ArcSight Loggerアプリケーションをインシデントから開きます。

インシデントビューで、インシデントを選択します。次に、NNMiコンソールの[**アクション**] メニューで、[HPE ArcSight Logger] > [インシデント履歴の表示] をクリックします。

または、インシデントを右クリックしてから、[HPE ArcSight Logger] > [インシデント履歴の表示]をクリックします。

HPE NNMi - HPE ArcSight Logger統合の無効化

統合を無効にするには、以下の手順を実行します。

- 1. NNMiコンソールで、[統合モジュールの設定] > [HPE ArcSight] をクリックします。
- 2. [ArcSight統合の有効化]の選択を解除します。
- 3. [送信]をクリックします。

問題および解決策

問題:ポートデータを含むインシデントを選択してNNMiコンソールからHPE ArcSight Loggerアプリケーションを開くと、NNMiはインシデントをHPE ArcSight Loggerで見つけられません。

解決方法:これは、NNMiがソースオブジェクトをポートではなくインタフェースに解決する一方で、HPE ArcSight Loggerのデータベースにはsyslogメッセージに関連付けられたインタフェースデータがないためです。これを解決す るには、以下のいずれかを実行してください。

- インタフェースに関連付けられたインシデントを選択してHPE ArcSight Loggerを開くのではなく、NNMiコン ソールからインタフェースを選択してHPE ArcSight Loggerを開きます。HPE ArcSight Loggerが開いたら、 HPE ArcSight Loggerのクエリーを変更し、インタフェースに関連付けられているポート名を含めます。
- syslogメッセージを選択し、HPE ArcSight Loggerクエリーを使用して情報を表示します。この方法を使った 手順の例を以下に示します。
 - a. NNMiコンソールからインタフェースを選択してHPE ArcSight Loggerを開き、[インシデント履歴の表示]を クリックします。
 - b. HPE ArcSight Loggerが開いたら、そのインシデントでHPE ArcSight Loggerのクエリーを変更し、インタフェースに関連付けられているポート名を含めます。
 - c. 変更したHPE ArcSight Loggerクエリーを実行し、HPE ArcSight Loggerでインシデントを検索します。

ドキュメントのフィードバックを送信

このドキュメントに関するご意見については、電子メールでドキュメントチームまでご連絡ください。このシステムで 電子メールクライアントが設定されていれば、このリンクをクリックすることで、以下の情報が件名に記入された電 子メールウィンドウが開きます。

HPE Network Node Manager i Software—HPE ArcSight Logger統合ガイドに関するフィードバック (Network Node Manager i Software NNMi 10.20)

電子メールの本文にご意見、ご感想を記入の上、[送信]をクリックしてください。

電子メールクライアントが利用できない場合は、上記の情報をコピーしてWebメールクライアントの新規メッセージに貼り付け、network-management-doc-feedback@hpe.comにお送りください。

フィード バックをお寄 せください