Hewlett Packard Enterprise

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

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。

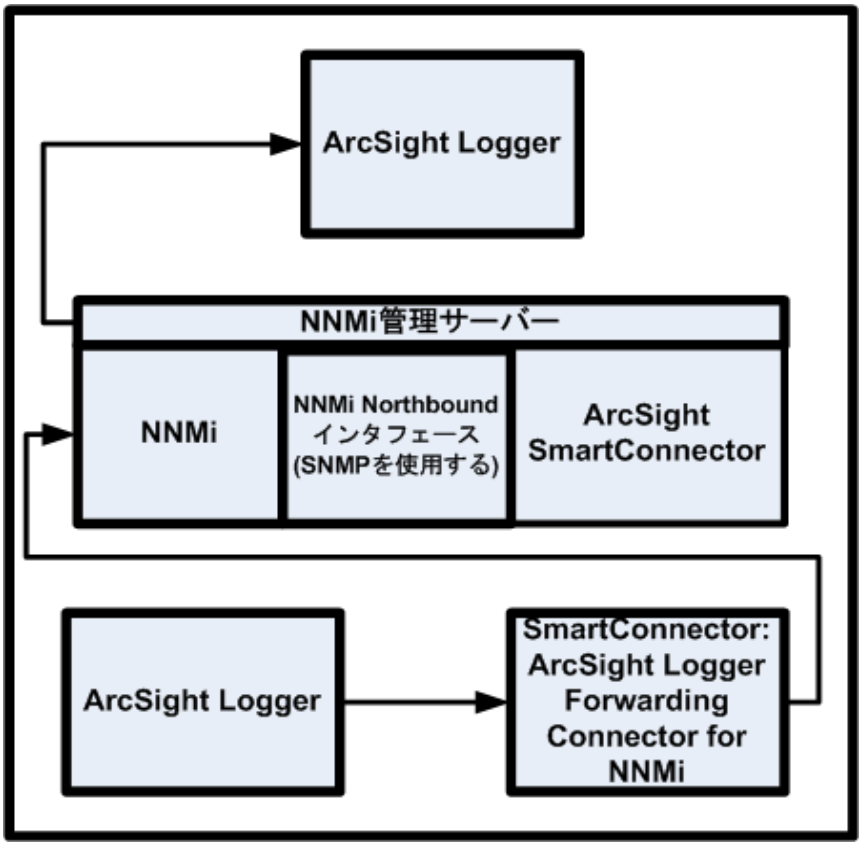
- 興味のあるナレッジドキュメントの検索
- サポート事例と改善要求の送信と追跡
- ソフトウェアーパッチのダウンロード
- サポート契約の管理
- HPEサポートの問合せ先の検索
- 利用可能なサービスに関する情報のレビュー
- 他のソフトウェアーユーザーとの情報交換
- ソフトウェアートレーニングの調査と登録

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



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、**`hp-arcsight.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

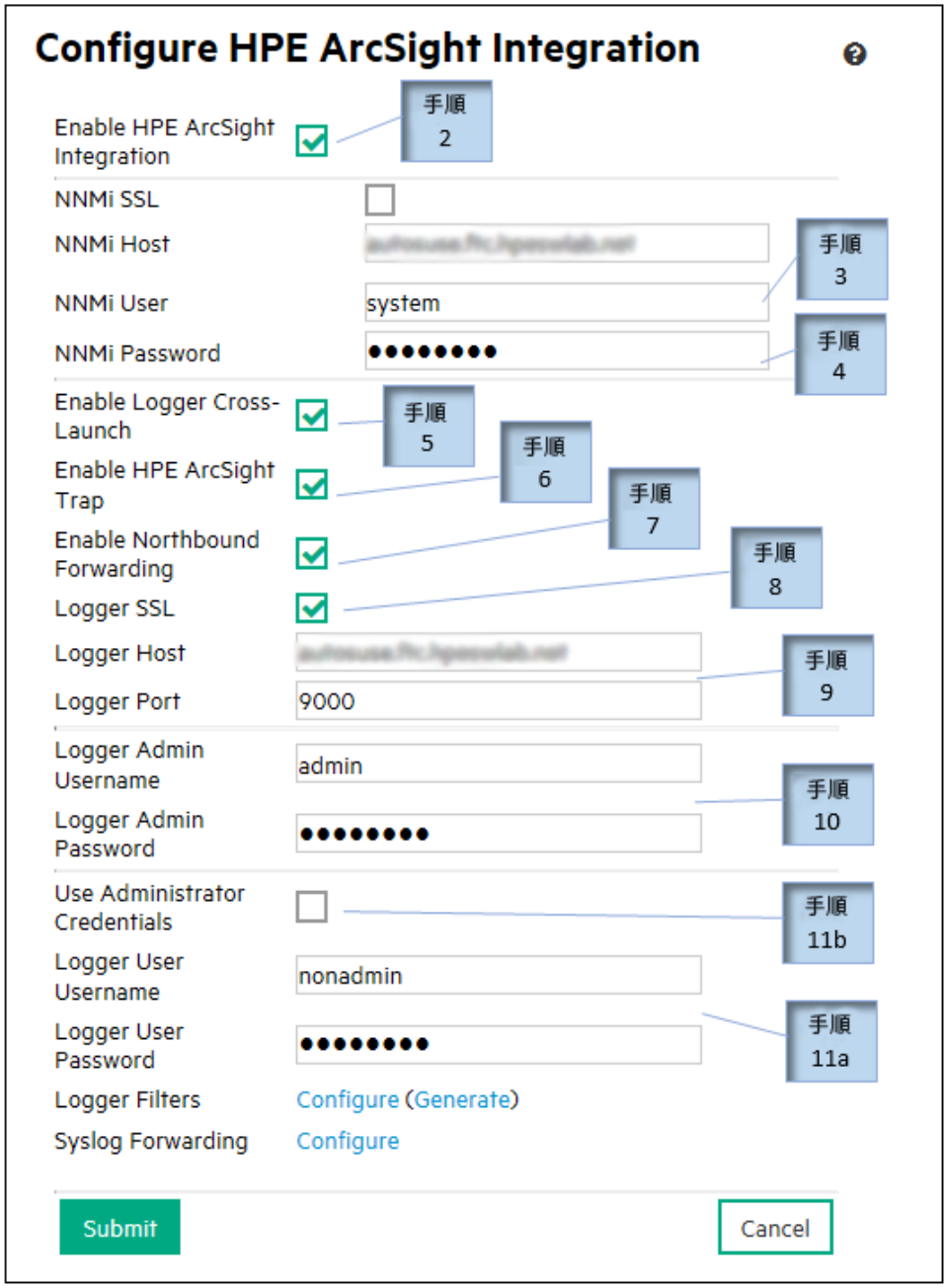
『SmartConnector Configuration Guide for ArcSight Logger Forwarding Connector for HPE NNMi』マニュアルの手 順 に従 って、HPE ArcSight Logger Forwarding Connector for NNMiを設 定 します。

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。

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。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。

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。
8. 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。

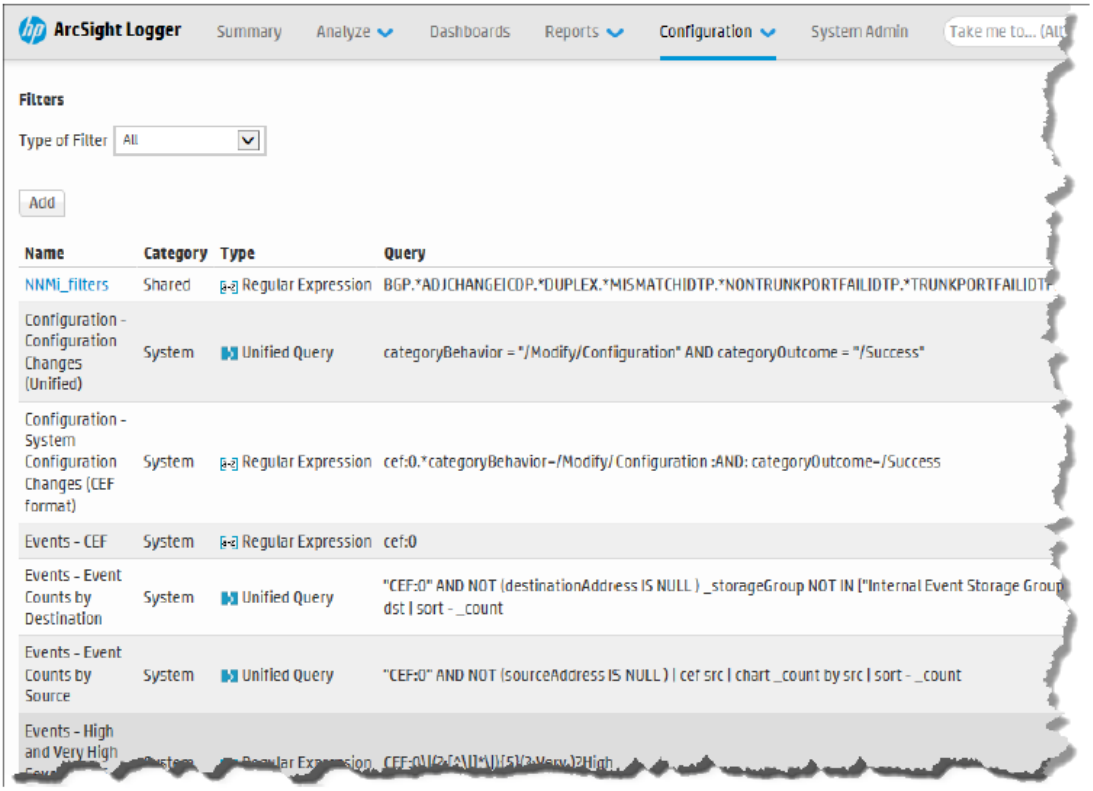
HPE ArcSight Loggerの設定にアクセスして新しいフィルターの内容を追加するには、以下の手順を実行します。

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。
2. [**>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

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。

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。

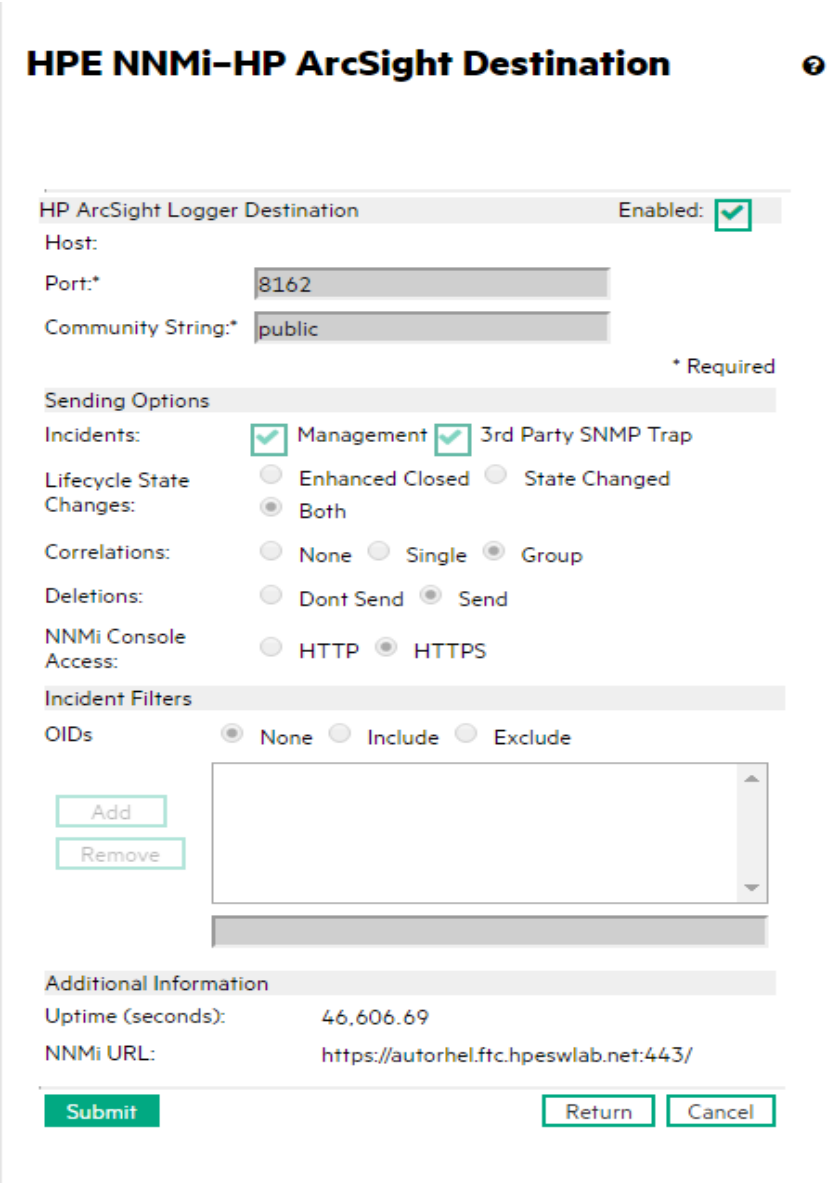
タスク6: HPE NNMi SNMP用 のSmartConnectorの設 定 (Northboundインタフェース用 のコネクター、オプションのタスク)

『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。
2. [**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



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、NNMi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.ovpl`**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。

2. 「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。
10. 「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. NNMi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。

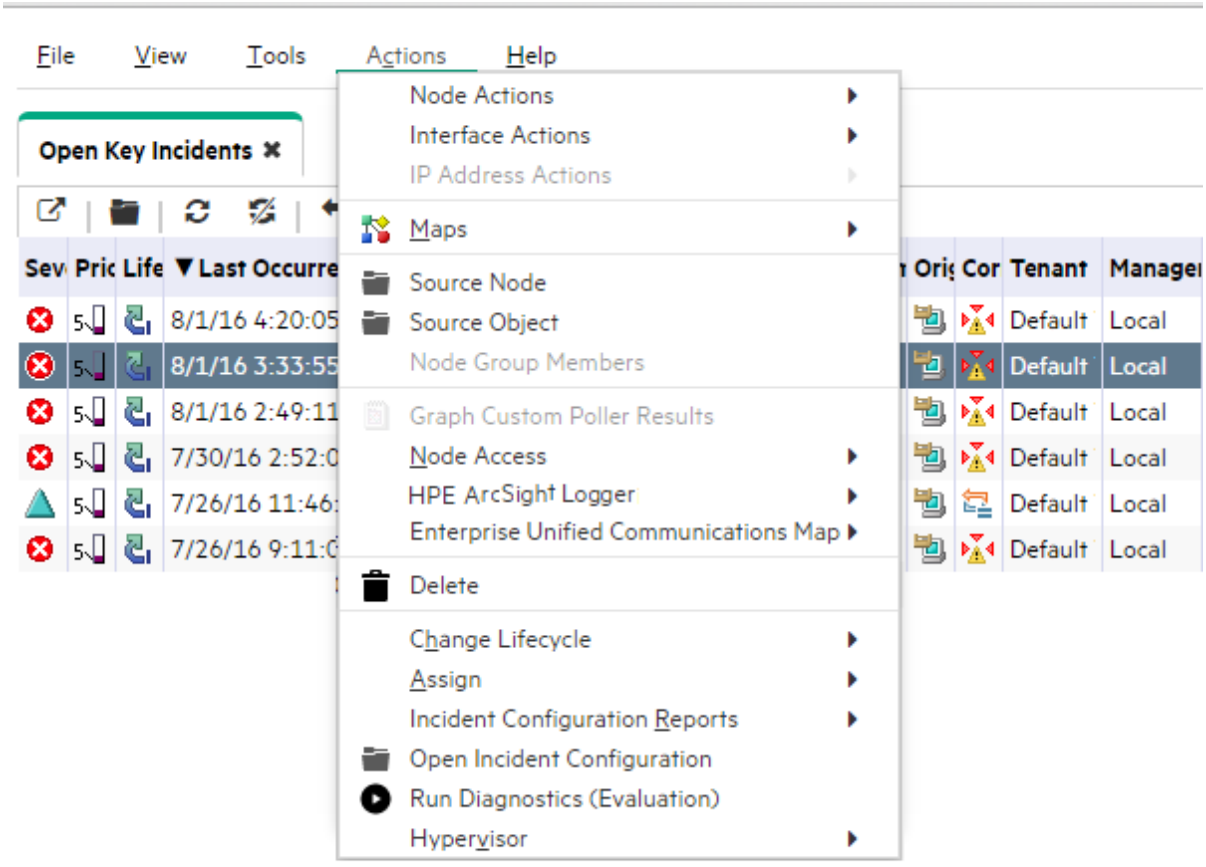
[インシデント の管 理] ワークスペース

[**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



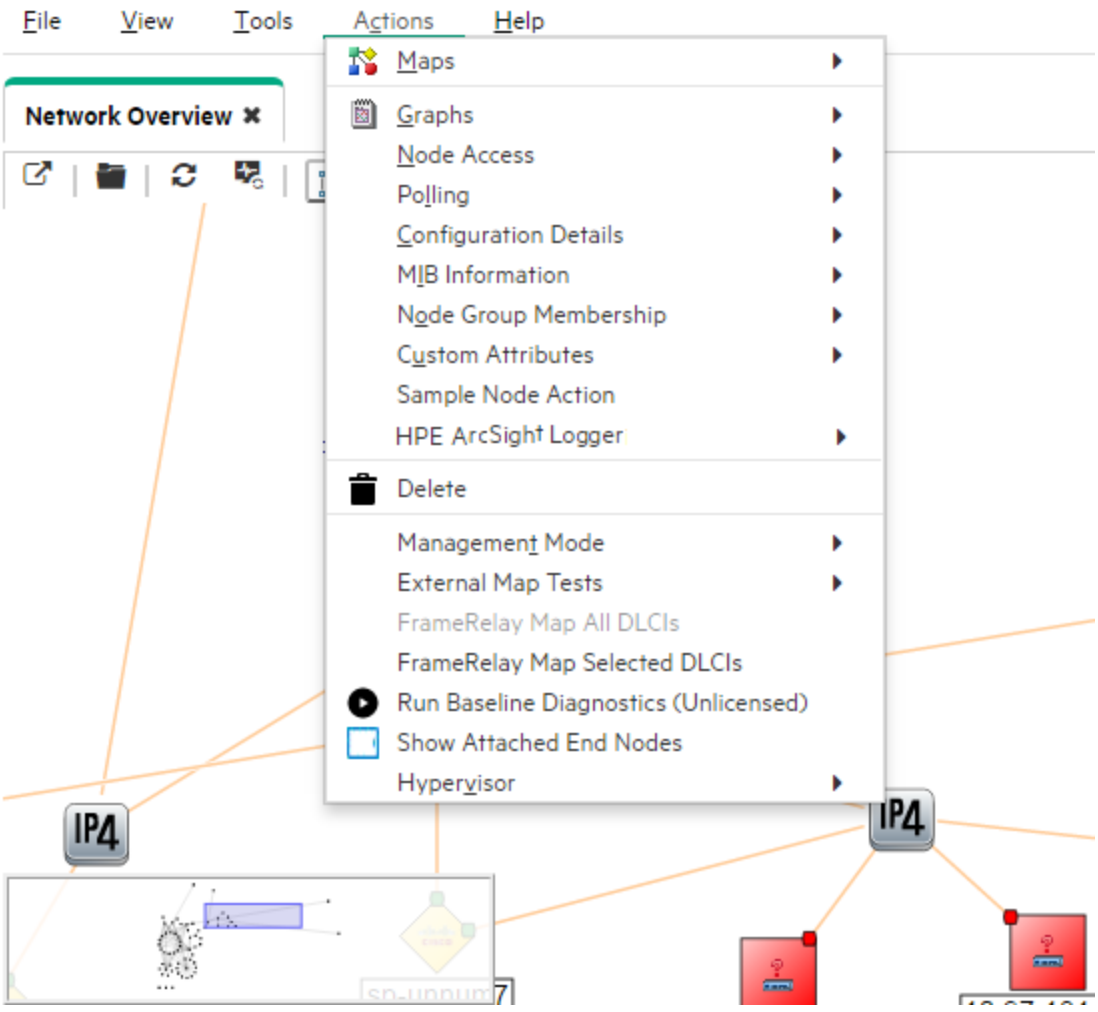
[トポロジマップ] ワークスペース

[**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



[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