HP Network Node Manager i Software

Windows®、HP-UX、Linux、および Solaris オペレーティングシステム用

ソフトウェアーバージョン : NNMi 9.20

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

ドキュメントリリース日 : 2012 年 5 月
ソフトウェアーリリース日 : 2012 年 5 月

ご注意

保証について

HP 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。ここでの記載で追加保証を意図するものは一切ありません。HP 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。

権利制限について

機密性のあるコンピューターソフトウェアーです。これらを所有、使用、または複製するには、HP 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ー、コンピューターソフトウェアードキュメント、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。

著作権について

商標に関する通知

Adobe® は Adobe Systems Incorporated の登録商標です。

HP 9000 コンピューター上の HP-UX リリース 10.20 以降および HP-UX リリース 11.00 以降 (32 ビットおよび 64 ビット両方の環境) は、すべて Open Group UNIX 95 製品です。

Microsoft® および Windows® は Microsoft Corporation の米国内での登録商標です。

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

UNIX® は The Open Group の登録商標です。

Oracle テクノロジの制限された権限に関する通知

国防省連邦調達規則補足 (DOD FAR Supplement) に従って提供されるプログラムは、「商用コンピューターソフトウェアー」であり、ドキュメントを含む同プログラムの使用、複製および開示は、該当する Oracle 社のライセンス契約に規定された制約を受けるものとします。それ以外の場合は、連邦調達規則に従って供給されたプログラムは、「制限されたコンピューターソフトウェアー」であり、関連文書を含むプログラムの使用、複製、および公開は、FAR 52.227-19、『商用コンピューターソフトウェアー - 制限された権限』(1987 年 6 月) に記載されている制限に従うものとします。Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

Oracle ライセンスの全文は、NNMi の製品 DVD にある license-agreements のディレクトリを参照してください。

謝辞

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

この製品には、Indiana University Extreme! Lab で開発されたソフトウェアーが含まれています。
(http://www.extreme.indiana.edu)

2012 年 5 月

使用可能な製品ドキュメント

このガイドに加え、次のドキュメントが NNMi について利用できます。

- HP Network Node Manager i Software ドキュメント一覧 - HP マニュアル Web サイト上にあります。このファイルを使用して、このバージョンの NNMi の NNMi ドキュメントセットにある追加や改訂を調べることができます。リンクをクリックして、HP マニュアル Web サイト上のドキュメントにアクセスします。
- HP Network Node Manager i Software インタラクティブインストールガイド - これは対話型ドキュメントで、NNMI 9.20 製品メディアで入手できます。
  詳細については、製品メディアの nnmi_interactive_installation_ja_README.txt ファイルを参照してください。
- HP Network Node Manager i Software アップグレードリファレンス - HP マニュアル Web サイトから入手できます。
- HP Network Node Manager i Software リリースノート - 製品メディアおよび NNMi 管理サーバーから入手できます。
- HP Network Node Manager i Software システムとデバイス対応マトリックス - 製品メディアおよび NNMi 管理サーバーから入手できます。
- HP Network Node Manager iSPI Network Engineering Toolset 計画とインストールガイド (HP Network Node Manager iSPI Network Engineering Toolset Planning and Installation Guide) - NNM iSPI NET 診断サーバー製品メディアにあります。

最近の更新を確認する場合、または最新のドキュメントを使用しているか確認する場合は、以下をご覧ください。

http://support.openview.hp.com/selfsolve/manuals

このサイトを利用するには、HP Passport への登録とサインインが必要です。HP Passport ID のご登録は、次の URL で行ってください。

http://h20229.www2.hp.com/passport-registration.html (英語サイト)

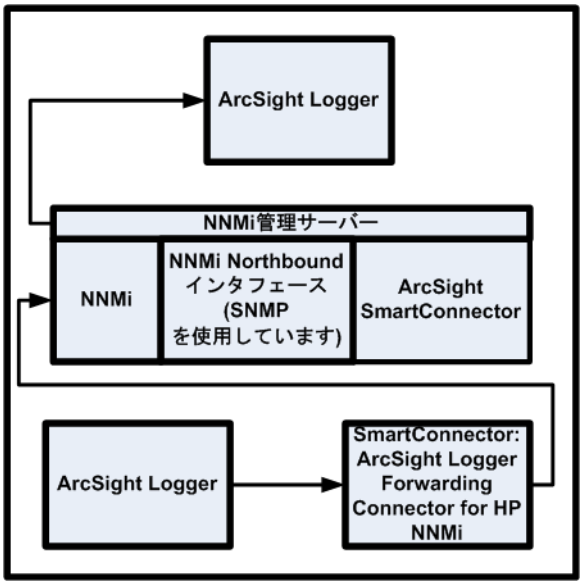
または、HP Passport のログインページの [**New users - please register**] リンクをクリックします。

製品のサポートサービスに登録すると、最新版を入手できます。詳細は HP 販売員にお尋ねください。

目次

HP NNMi-HP ArcSight Logger 統合 8
HP NNMi-HP ArcSight Logger について 8
値 8
統合製品 8
HP ArcSight Logger フィルターのカスタマイズ 8
ドキュメント 9
HP NNMi - HP ArcSight Logger 統合の有効化 9
必要条件 10
HP NNMi HP ArcSight Logger 統合を有効にする手順 10
HP NNMi - HP ArcSight Logger 統合の変更 17
受信 Syslog メッセージ数の管理 17
HP NNMi - HP ArcSight Logger 統合の使用法 19
NNMi コンソールから HP ArcSight Logger を開く 19
ArcSightEvent SNMP トラップおよび ArcSightEvent SNMP トラップ設定の表示 19
NNMi コンソールの [アクション] メニューの変更 20
[インシデントの管理] ワークスペース 20
[トポロジマップ] ワークスペース 22
[モニタリング] ワークスペース 24
[トラブルシューティング] ワークスペース 26
[インベントリ] ワークスペース 28
[インシデントの参照] ワークスペース 30
HP NNMi-HP ArcSight Logger 統合の無効化 31
問題および解決策 31

HP ArcSight Logger



HP 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。

HP 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。

このドキュメントでは、利用可能な以下の統合について説明します。

- HP NNMi-HP ArcSight Logger 統合
- HP NNMi - HP ArcSight Logger 統合の有効化
- HP NNMi - HP ArcSight Logger 統合の変更
- HP NNMi - HP ArcSight Logger 統合の使用法
- HP NNMi-HP ArcSight Logger 統合の無効化

HP NNMi-HP ArcSight Logger 統合

HP NNMi-HP ArcSight Logger について

この章の手順に従って ArcSightEvents を HP NNMi に転送するように HP 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

HP NNMi – HP ArcSight Logger 統合では Syslog 情報が HP NNMi に追加され、HP 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。

- HP ArcSight Logger
- SmartConnector: ArcSight HP Network Node Manager i SNMP
- SmartConnector: ArcSight Logger Forwarding Connector for HP NNMi

  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 システムおよびデバイスの対応マトリックスを参照してください。

- NNMi 9.20

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。

HP ArcSight Logger フィルターのカスタマイズ

HP ArcSight Logger フィルターを渡して HP NNMi に転送する Syslog メッセージがあります。HP ArcSight Logger フィルターを設定しないと、HP ArcSight Logger から大量の ArcSightEvents が HP NNMi に転送されます。このため、HP 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、HP ArcSight Logger から HP 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、HP ArcSight Logger から NNMi に転送されるメッセージを調整できます。

HP NNMi から HP 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、HP NNMi ユーザーが管理者権限で HP ArcSight Logger にアクセスすることが HP 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。HP 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

HP NNMi - HP 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。

- 『HP Network Node Manager i SNMP 用の SmartConnector 設定ガイド』(SmartConnector Configuration Guide for HP Network Node Manager i SNMP) (NNMi Northbound インタフェース)
  HP Network Node Manager i 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。
- 『ArcSight Logger Forwarding Connector for HP NNMi 用の SmartConnector 設定ガイド』(SmartConnector Configuration Guide for ArcSight Logger Forwarding Connector for HP NNMi)
  HP ArcSight Logger Forwarding Connector for HP NNMi は、Syslog メッセージを `ArcSightEvent` の形式で NNMi に転送します。
- 『Logger 管理者ガイド』(Logger Administrator's Guide)
  この統合では、HP ArcSight Logger は SNMP トラップを `ArcSightEvents` の形式で HP NNMi に転送します。

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

『SmartConnector 設定ガイド』(SmartConnector Configuration Guide) や『Logger 管理者ガイド』(Logger Administrator's Guide) などの HP 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
HP ArcSight 製品情報にアクセスするには、HP 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、HP 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、ブラウザーで以下の場所を指定します。
http://www.arcsight.com/products/products-logger HP ArcSight Logger でサポートされているシステム要件は、『Logger 管理者ガイド』(Logger Administrator's Guide) でも確認できます。

HP NNMi - HP ArcSight Logger 統合の有効化

HP NNMi Northbound インタフェースなどの既存の HP NNMi 機能を効果的に活用して、HP ArcSight Logger と HP NNMi 間でカスタム統合を設定することがあります。NNMi 9.20 をインストールする場合は、この HP NNMi - HP 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 9.20 で提供されるさらに堅牢な HP NNMi - HP ArcSight Logger 統合を有効にします。

必要条件

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

- NNMi 9.20 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.hp.com/selfsolve/manuals を指定して、インタラクティブバージョンの『HP Network Node Manager i インストールガイド』をダウンロードします。
- 『HP Network Node Manager i SNMP 用の SmartConnector 設定ガイド』(SmartConnector Configuration Guide for ArcSight Logger Forwarding Connector for HP NNMi) マニュアルの手順に従って、HP Network Node Manager i SNMP 用の SmartConnector をインストールします。
- 『ArcSight Logger Forwarding Connector for HP NNMi 用の SmartConnector 設定ガイド』(SmartConnector Configuration Guide for ArcSight Logger Forwarding Connector for HP NNMi) マニュアルの手順に従って、HP ArcSight Logger Forwarding Connector for HP NNMi をインストールします。

HP NNMi HP ArcSight Logger 統合を有効にする手順

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

タスク 1: NNMi 9.20 のインストール

タスク 2: HP ArcSight MIB についての理解

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

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

タスク 5: HP ArcSight Logger フィルターの設定

タスク 6: HP Network Node Manager i 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 HP ArcSight Logger に転送するための HP 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 9.20 のインストール

NNMi 9.20 を入手してインストールするには、以下の手順を実行します。

1 ブラウザーで http://support.openview.hp.com/selfsolve/patches を指定します。

2 お使いのオペレーティングシステム用の NNMi 9.20 を検索し、パッチをダウンロードします。

3 NNMi 9.20 のインストール手順に従って、パッチをインストールします。

タスク 2: HP ArcSight MIB についての理解

タスク 1 ～タスク 5 を実行すると、HP ArcSight Logger はフィルタリングされた `ArcSightEvent` の HP NNMi への転送を開始します。HP 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 9.20 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、HP 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: HP ArcSight Logger Forwarding Connector for HP NNMi の設定

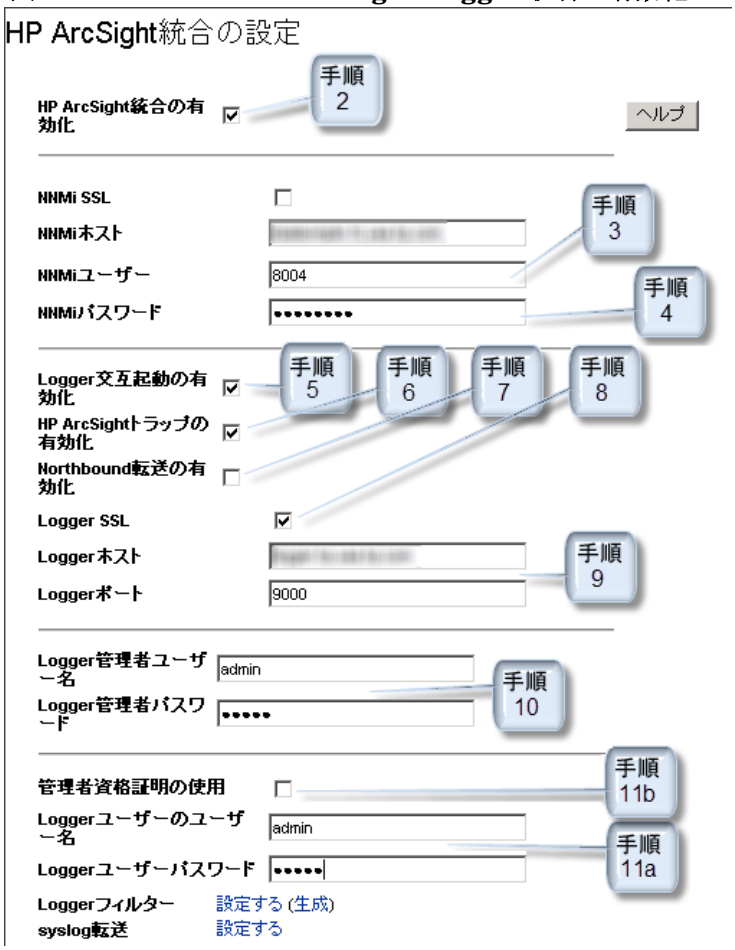
『ArcSight Logger Forwarding Connector for HP NNMi 用の SmartConnector 設定ガイド』(SmartConnector Configuration Guide for ArcSight Logger Forwarding Connector for HP NNMi) マニュアルの手順に従って、HP ArcSight Logger Forwarding Connector for HP NNMi を設定します。

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

HP NNMi - HP 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 HP ArcSight Logger を設定することにより、HP 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。HP NNMi - HP 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**] > [**HP ArcSight**] の順にクリックします。HP NNMi で、図 1 に示す [**ArcSight 統合の設定**] 画面が表示されます。HP NNMi - HP ArcSight Logger 統合の設定時に、図 1 を参照してください。

図 1　HP NNMi - HP ArcSight Logger 統合の有効化



2 [**ArcSight 統合の有効化**] を選択します。

3 以下の HP 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が含まれます。
- 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 [**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 HP NNMi インシデントを HP 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 HP 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 HP NNMi - HP ArcSight Logger 統合に含まれる HP 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。

SSL 用の Logger の設定については、『HP ArcSight Logger v5.1 管理者ガイド』(HP ArcSight Logger v5.1 Administrators Guide) を参照してください。

9 以下の HP 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 HP 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 手順 a を実行します。手順 b も実行できますが、手順 a 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。これらのの資格証明は、HP 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 HP ArcSight Logger で HP 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、手順 a 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 HP NNMi からサインアウトします。

b HP NNMi にサインインします。

タスク 4 を実行すると、フィルタリングされていない ArcSightEvent が HP ArcSight Logger によって HP NNMi に転送されます。HP 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 を実行して、HP ArcSight Logger から HP 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: HP ArcSight Logger フィルターの設定

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

管理不可能な数のトラップ受信を避けるため、タスク 4 の直後にタスク 5 を実行してください。

[**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、手順 1 ～手順 6 を実行します。

HP 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**] > [**HP ArcSight**] の順にクリックします。

2 [**Logger フィルター**] > [**(生成)**] の順にクリックします。HP 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 HP 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


フィルターを有効にしました
次のsyslogが有効です。それ以外の着信syslogメッセージはすべて破棄されます。用意されているフィルターを使用してLoggerを設定することを強くお勧めします

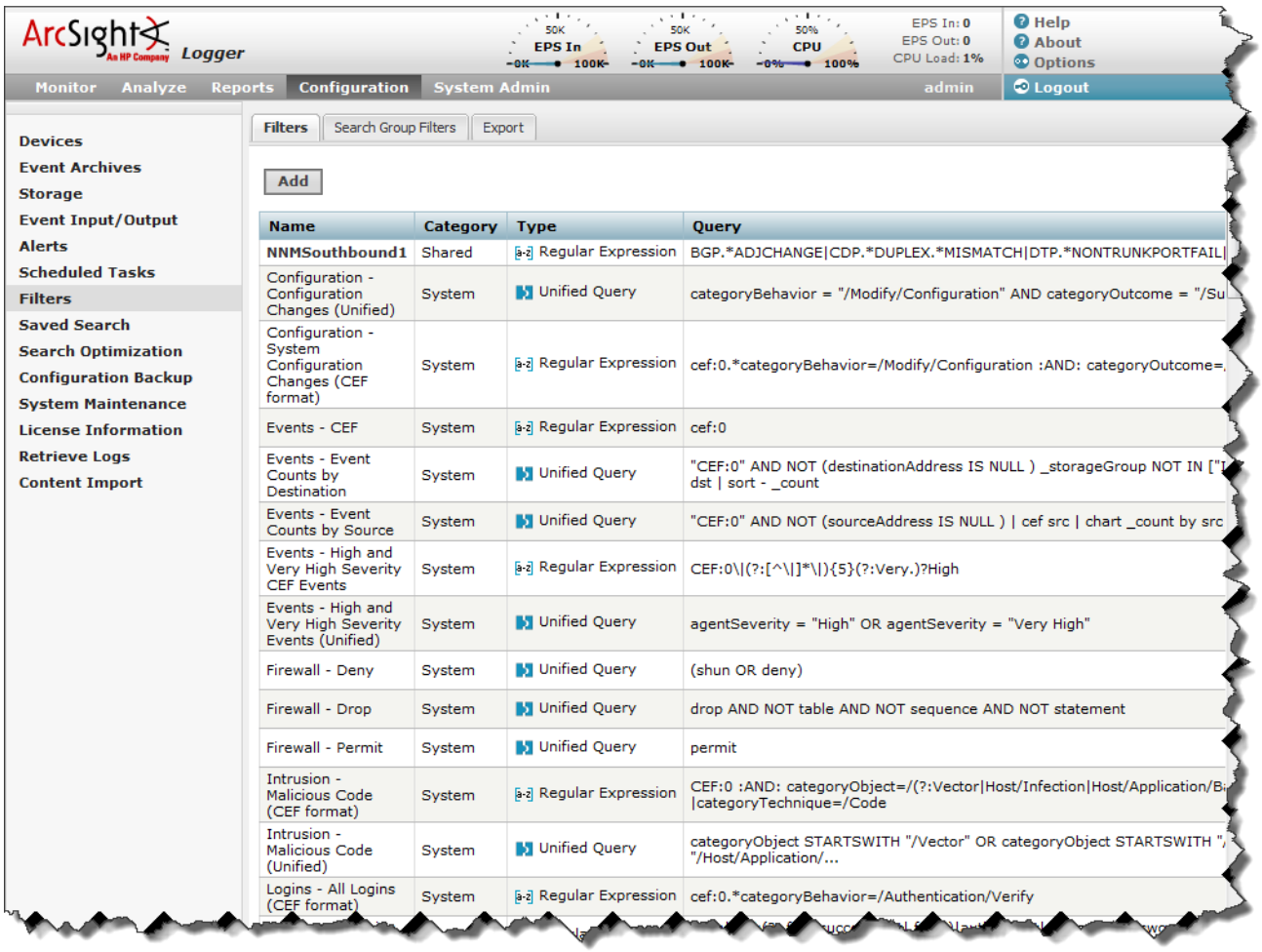
SYS.*PKTBUFBAD|BGP.*ADJCHANGE|CDP.*DUPLEX.*MISMATCH|DTP.*NONTRUNKPORTFAIL|DTP.*TRUNKPORTFAIL|DTP.*NONTRUNKPORTON|DTP.*TRUNKPORTON|DTP.*TRUNKPORTCHG|FR.*DLCICHANGE|ARP.*ARP.*DUPVRRPIP|LINK.*UPDOWN|LINK.*ERROR|LINEPROTO.*UPDOWN|OSPF.*ADJCHG|PAGP.*PORTTOSTP|PAGP.*PORTFROMSTP|PORT.*SECURITY.*PSECURE.*VIOLATION.*VLAN|SNMP.*MODULETRAP|SPANTREE.*PORTLISTEN|SPANTREE.*ROOTCHANGE|SPANTREE.*PORTFWD|SPANTREE.*PORTLISTEN|STACKMGR.*MASTER.*ELECTED|STACKMGR.*MASTER.*READY|STACKMGR.*STACK.*LINK.*CHANGE|STANDBY.*DUPADDR|STANDBY.*STATECHANGE|SYS.*MOD.*CFGMISMATCH.*|SYS.*MOD.*CFGMISMATCH.*|SYS.*MOD.*CFGMISMATCH.*|SYS.*MOD.*CFGMISMATCH.*|SYS.*PORT.*COLL|SYS.*PORT.*COLLDIS|SYS.*PORT.*IN.*ERRORS|SYS.*PORT.*RUNTS|SYS.*SYS.*LCPERR.*|SYS.*SYS.*LCPERR.*|SYS.*MOD.*INSERT|SYS.*MOD.*OK|SYS.*RELOAD|SYS.*MOD.*REMOVE|SYS.*MOD.*RESET|SYS.*RESTART|RMON.*PMGR.*PORT.*UP|RMON.*CHASSIS.*FAN.*STATUS|RMON.*STP.*NEW.*ROOT|RMON.*LACP.*DYNAMIC.*TRUNK.*OFF.*LINE|RMON.*LACP.*DYNAMIC.*TRUNK.*ON.*LINE|RMON.*LACP.*ERROR.*CONDITION.*BLOCK|RMON.*POEMGR.*PD.*DENIED.*POWER|RMON.*POEMGR.*PD.*OVERCURRENT|RMON.*POEMGR.*INTERNAL.*V.*FAULT|RMON.*BOOT.*CRASH.*RECORD.*|RMON.*BOOT.*CRASH.*RECORD.*|RMON.*BOOT.*NO.*CRASH.*RECORD|RMON.*BOOT.*SELFTEST.*FAILURE|RMON.*SSH.*DISABLED|RMON.*SSH.*ENABLED|RMON.*CHASSIS.*POWER.*STATUS|RMON.*CHASSIS.*HEARTBEAT.*FAILURE|CFM.*CFM.*SAVECONFIG.*SUCCESSFULLY|NTP.*NTP.*SOURCE.*LOST|DEV.*FAN.*FAILED|DEV.*FAN.*RECOVERED|OSPF.*OSPF.*NBR.*CHG|DEVM.*BOARD.*REMOVED|DEVM.*BOARD.*STATE.*FAULT|VRRP.*VRRP.*STATUS.*CHANGE|DEV.*POWER.*FAILED|DEV.*POWER.*RECOVERED|MSTP.*MSTP.*BPDU.*RECEIVE.*EXPIRY|OPTMOD.*MODULE.*OUT|OPTMOD.*MODULE.*IN|OSPF.*OSPF.*LAST.*NBR.*DOWN|ARP.*ROUTECONFLICT|BFD.*BFD.*CHANGE.*FSM|BGP.*BGP.*RECHED.*THRESHOLD|DEV.*BOARD.*LOADING|DEV.*LOAD.*FINISHED|DEVM.*POWER.*FAILED|DEVM.*POWER.*RECOVERED|DEVM.*RPS.*ABSENT|DEVM.*RPS.*NORMAL|DEVM.*SYSTEM.*REBOOT|DEV.*POWER.*ABSENT|DEV.*SYSTEM.*REBOOT|LDP.*LDP.*SESSION.*DOWN|OPTMOD.*CHKSUM.*ERR|OPTMOD.*IO.*ERR|OPTMOD.*MOD.*ALM.*ON|OPTMOD.*MOD.*ALM.*OFF|OPTMOD.*TYPE.*ERR|PIM.*PIM.*NBR.*DOWN|STM.*STM.*LINK.*STATUS.*DOWN|STM.*STM.*LINK.*STATUS.*UP|STM.*LINK.*STATUS.*CHANGE

有効にされたインシデントの表示

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 HP 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。**15 ページの図 3** に示す HP ArcSight Logger の [**設定**] ページにビューが表示されます。

図 3　HP 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、HP 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。

HP 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　HP 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　内容を手順 3 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。

HP 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 HP NNMi に転送する Syslog メッセージを特定するために HP 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 内容を手順 3 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、HP ArcSight Logger により目的の Syslog メッセージのみが HP NNMi に転送されるようになりました。

タスク 6: HP Network Node Manager i 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)

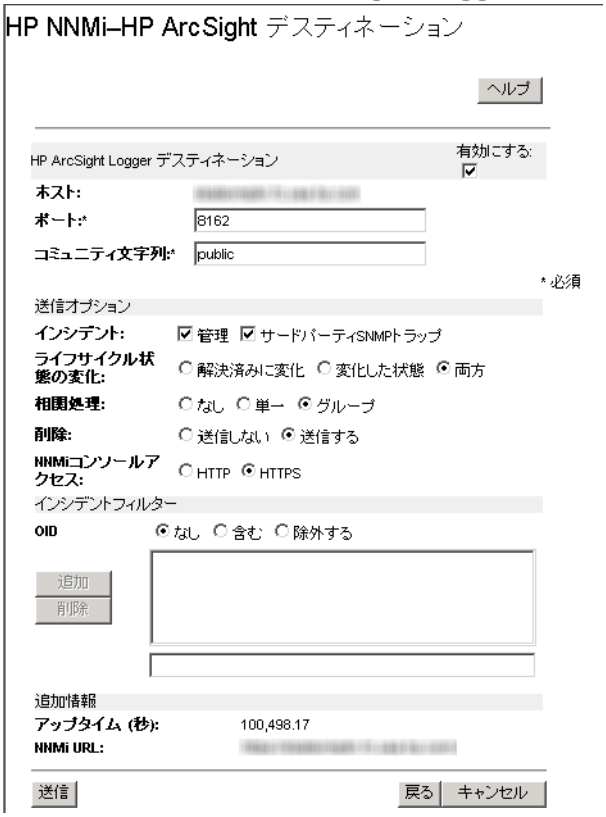
『HP Network Node Manager i SNMP 用の SmartConnector 設定ガイド』(SmartConnector Configuration Guide for HP Network Node Manager i SNMP)マニュアルの手順に従って、HP Network Node Manager i SNMP 用の SmartConnector を設定します。

タスク 7: SNMPv1、v2、v3 トラップインシデントを HP ArcSight Logger に転送するための HP 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**] > [**HP ArcSight**] の順にクリックします。

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 を参照してください。

図 4 HP NNMi - HP 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。HP 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、HP 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 HP NNMi で設定エラーがテストされます。送信に成功するまで、エラーを修正して手順 7 を繰り返します。

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

HP NNMi - HP ArcSight Logger 統合の変更

ここでは、有効化した HP NNMi - HP 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

HP NNMi-HP ArcSight Logger 統合では、HP 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、HP 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。

- HP 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 HP 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、HP 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

  ニーズに合わせて、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。

- HP 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>
  UNIX 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。

定義する特定の Syslog メッセージが表示されない場合は、HP 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。13 ページの HP ArcSight Logger フィルターの設定を参照してください。

HP 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、サポート担当者に連絡してください。

2 手順 1 で取得したリストを使用して、HP 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。

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ーを探します。以下のようなエントリーが見つかります。

```
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 HP NNMi で使用されます。HP NNMi の名前フィールドで使用できない文字はすべて「_」(アンダースコアー) に置き換えられます。この例では、手順 7 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 手順 4 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。

英数字、スペース、および _ (アンダースコアー)、: (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ー (_) 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 手順 1 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手順 1 ～手順 9 を繰り返します。

HP NNMi が常に高いパフォーマンスを発揮するように、HP NNMi は一定数の SNMP トラップをデータベースに保存すると、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。

HP NNMi - HP ArcSight Logger 統合の使用法

ここでは、有効化した HP NNMi - HP ArcSight Logger 統合を使用する方法と、ニーズに合わせて変更する方法を説明します。

NNMi コンソールから HP ArcSight Logger を開く

NNMi コンソールから HP ArcSight Logger を起動するとき、交互起動を開始する前に、HP 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。

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。

HP NNMi - HP ArcSight Logger 統合を有効にすると、HP ArcSight Logger から HP 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。

HP ArcSight Logger から NNMi 9.20 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 HP 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

HP NNMi - HP 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 [**重要な未解決インシデント**] をクリックします。

NNMi コンソールを使用して、インシデントから HP ArcSight Logger アプリケーションを開きます。これを行うには、[**インシデントの管理**] ワークスペースの使用中にインシデントを選択し、図 5 に示すように NNMi コンソールの [**アクション**] メニューを使用して HP ArcSight Logger アプリケーションを開きます。

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

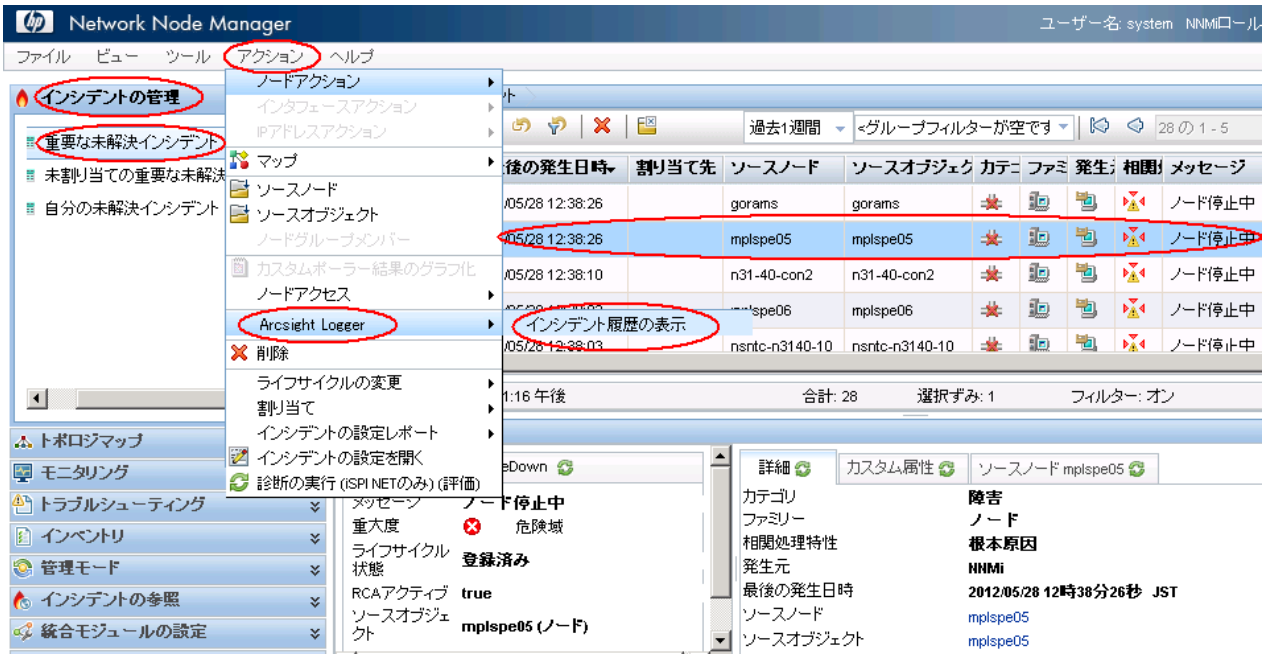
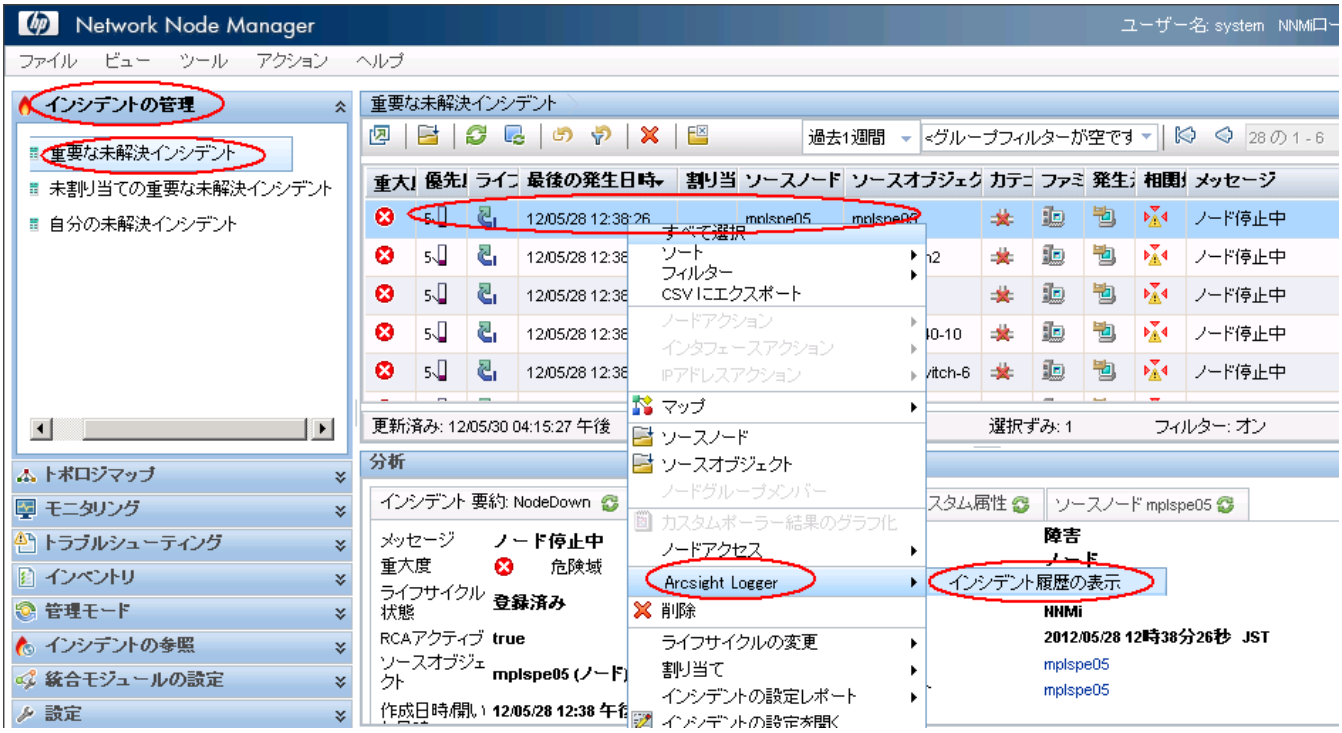


図 6 に示すように、インシデントを右クリックしてから、メニューを使用して HP ArcSight Logger アプリケーションを開くこともできます。

図 6　[インシデントの管理] ワークスペースでインシデントを右クリックして HP 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 [**ネットワークの概要**] をクリックします。

NNMi コンソールを使用して、ノードから HP ArcSight Logger アプリケーションを開きます。開くには、[**トポロジマップ**] ワークスペースでノードを選択し、次に NNMi コンソールの [**アクション**] メニューを使って HP ArcSight Logger アプリケーションを開きます (図 7)。

図 7　[トポロジマップ] ワークスペースでノードから HP ArcSight Logger を開く

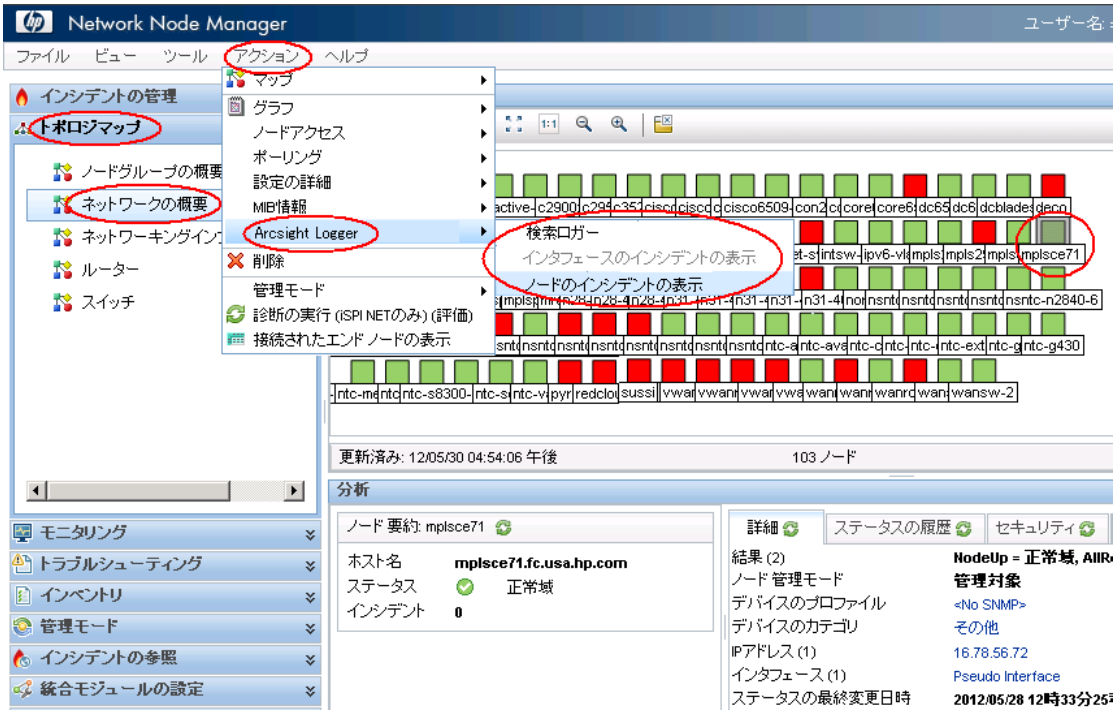
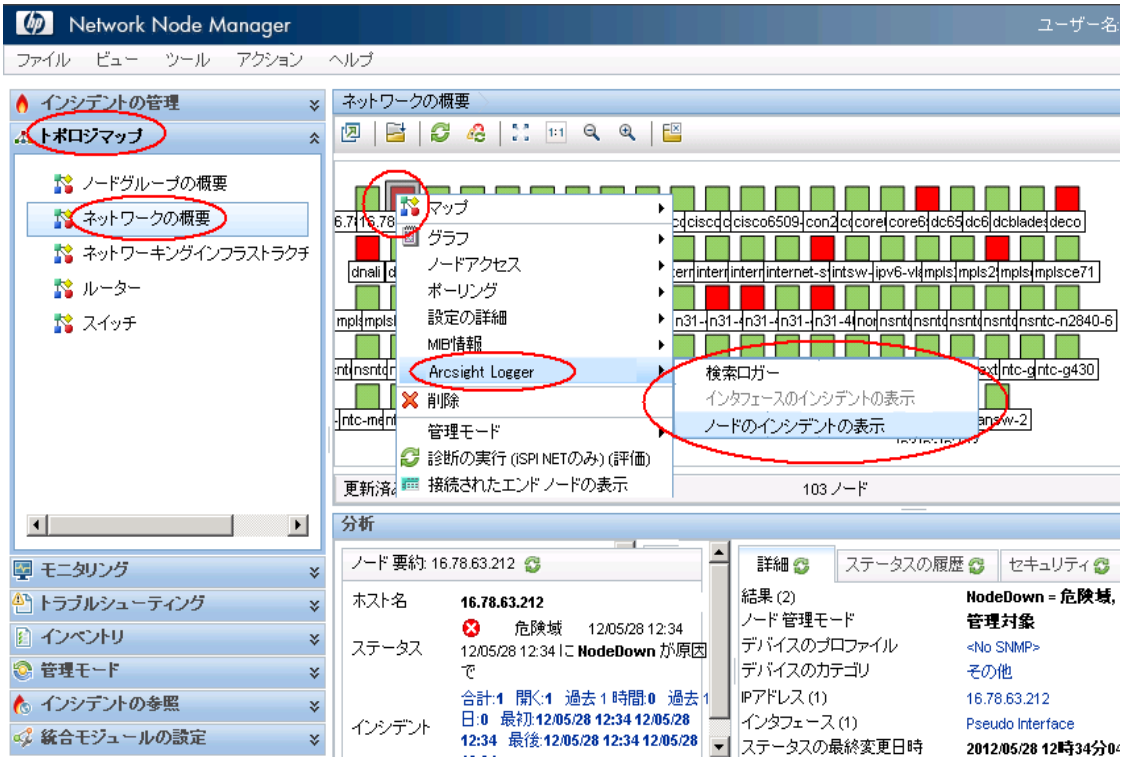


図 8 に示すように、ノードを右クリックしてから、メニューを使用して HP ArcSight Logger アプリケーションを開くこともできます。

図 8 [トポロジマップ] ワークスペースでノードを右クリックして HP 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、[**正常域にないノード**] をクリックします。

NNMi コンソールを使用して、ノードまたはインタフェースから HP ArcSight Logger アプリケーションを開きます。開くには、[**モニタリング**] ワークスペースでノードまたはインタフェースを選択し、次に NNMi コンソールの [**アクション**] メニューを使って HP ArcSight Logger アプリケーションを開きます (図 9)。

図 9　[モニタリング] ワークスペースでノードから HP ArcSight Logger を開く

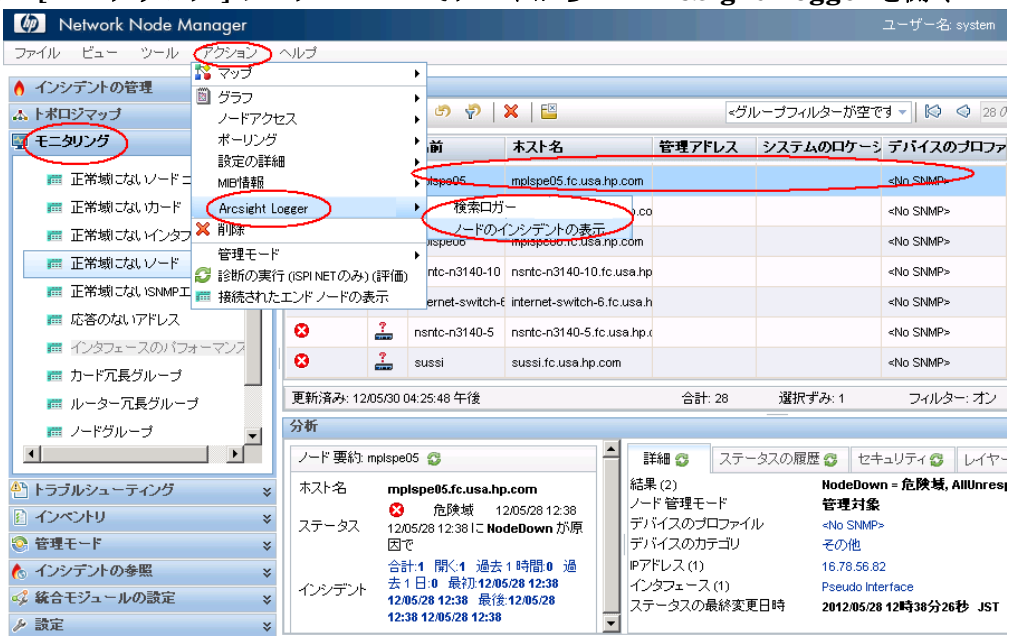
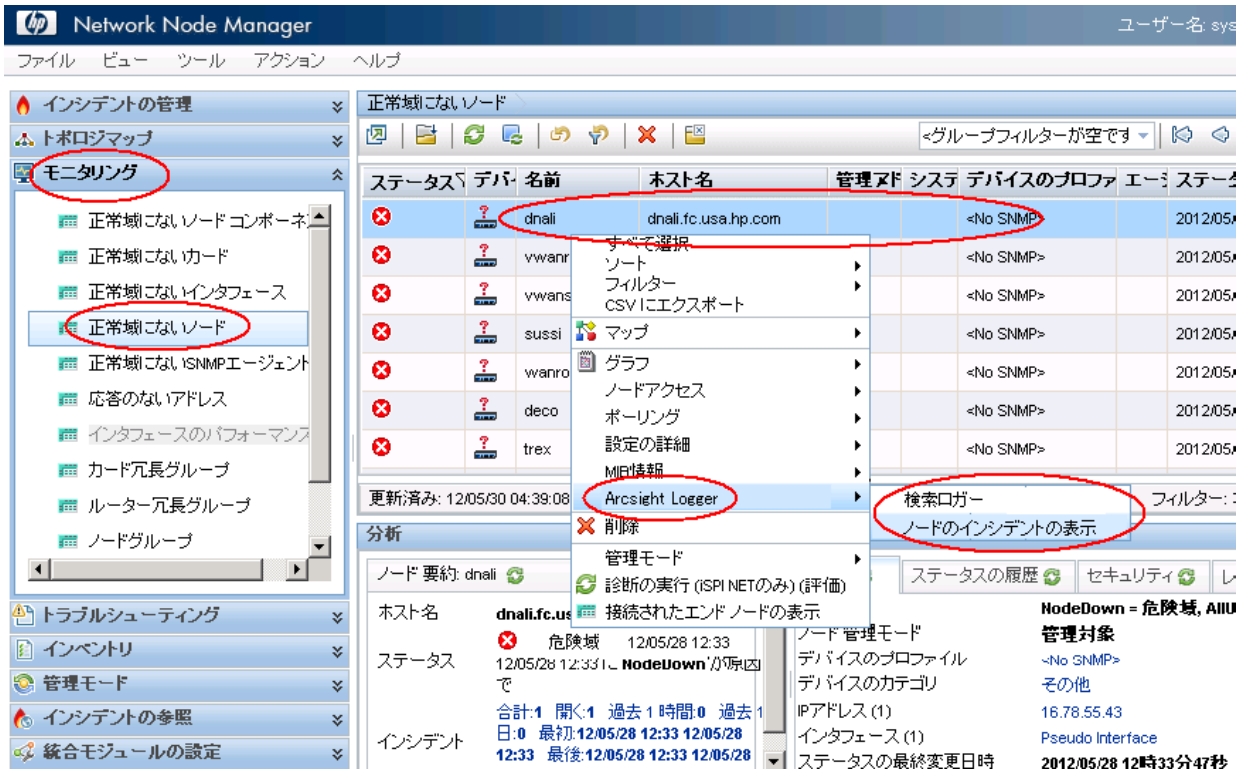


図 10 に示すように、[**モニタリング**] ワークスペースでノードを右クリックしてから、メニューを使用して HP ArcSight Logger アプリケーションを開くこともできます。

図 10 [モニタリング] ワークスペースでノードを右クリックして HP ArcSight Logger を開く



[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、[**レイヤー 2 の近隣接続ビュー**] を開きます。

NNMi コンソールを使用して、ノードから HP ArcSight Logger アプリケーションを開きます。これを行うには、[**トラブルシューティング**] ワークスペースの使用中にノードを選択し、図 11 に示すように NNMi コンソールの [**アクション**] メニューを使用して HP ArcSight Logger アプリケーションを開きます。

図 11 [トラブルシューティング] ワークスペースでノードから HP ArcSight Logger を開く

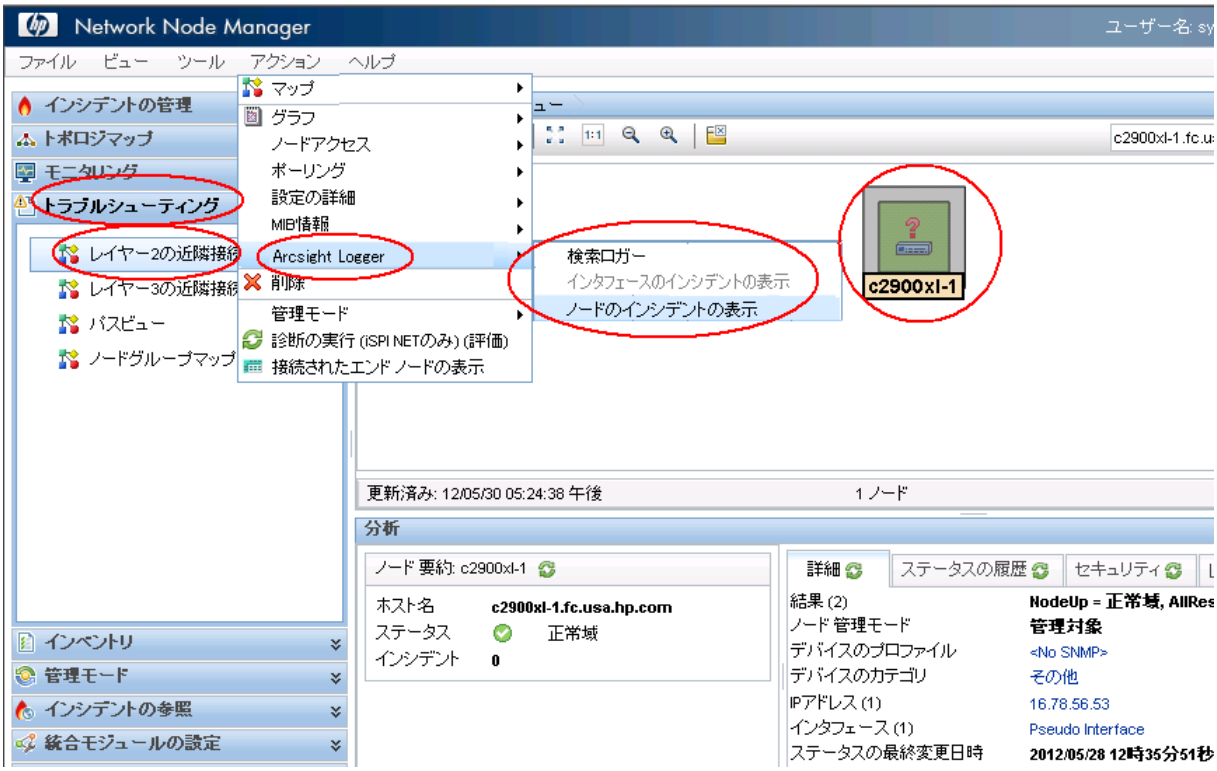
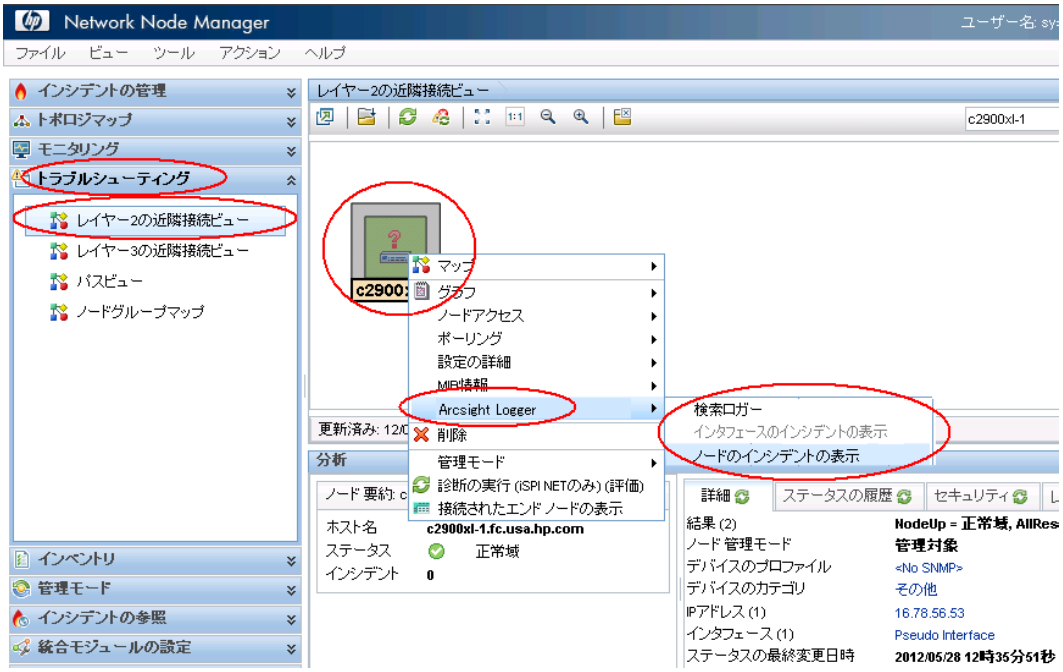


図 12 に示すように、[**トラブルシューティング**] ワークスペースでノードを右クリックしてから、メニューを使用して HP ArcSight Logger アプリケーションを開くこともできます。

図 12 [トラブルシューティング] ワークスペースでノードを右クリックして HP ArcSight Logger を開く



[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、[**ノード**] をクリックします。

NNMi コンソールを使用して、ノードまたはインタフェースから HP ArcSight Logger アプリケーションを開きます。これを行うには、[**インベントリ**] ワークスペースの使用中にノードまたはインタフェースを選択し、図 **13** に示すように NNMi コンソールのメニューを使用して HP ArcSight Logger アプリケーションを開きます。

図 13 [インベントリ] ワークスペースでノードまたはインタフェースから HP ArcSight Logger を開く

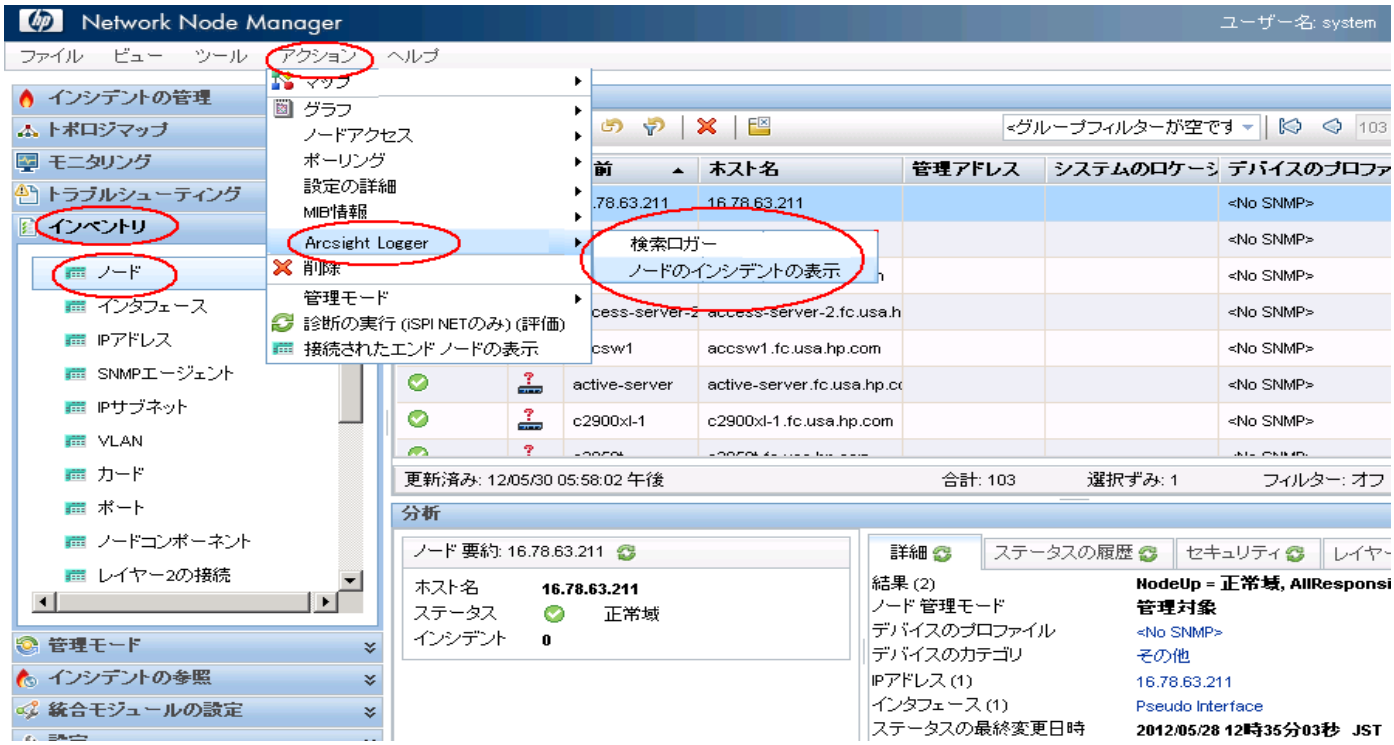
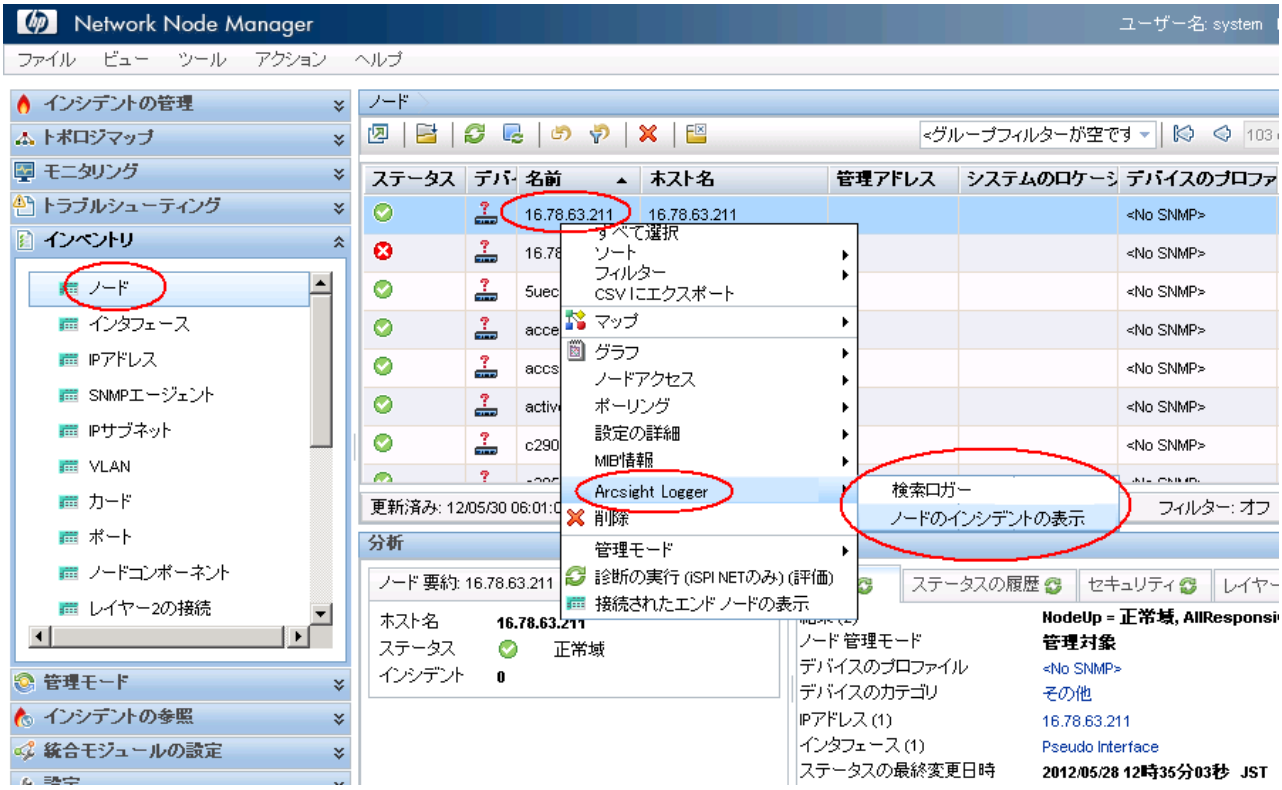


図 14 に示すように、[**インベントリ**] ワークスペースでノードを右クリックしてから、メニューを使用して HP ArcSight Logger アプリケーションを開くこともできます。

図 14 [インベントリ] ワークスペースでノードまたはインタフェースを右クリックして HP ArcSight Logger を開く

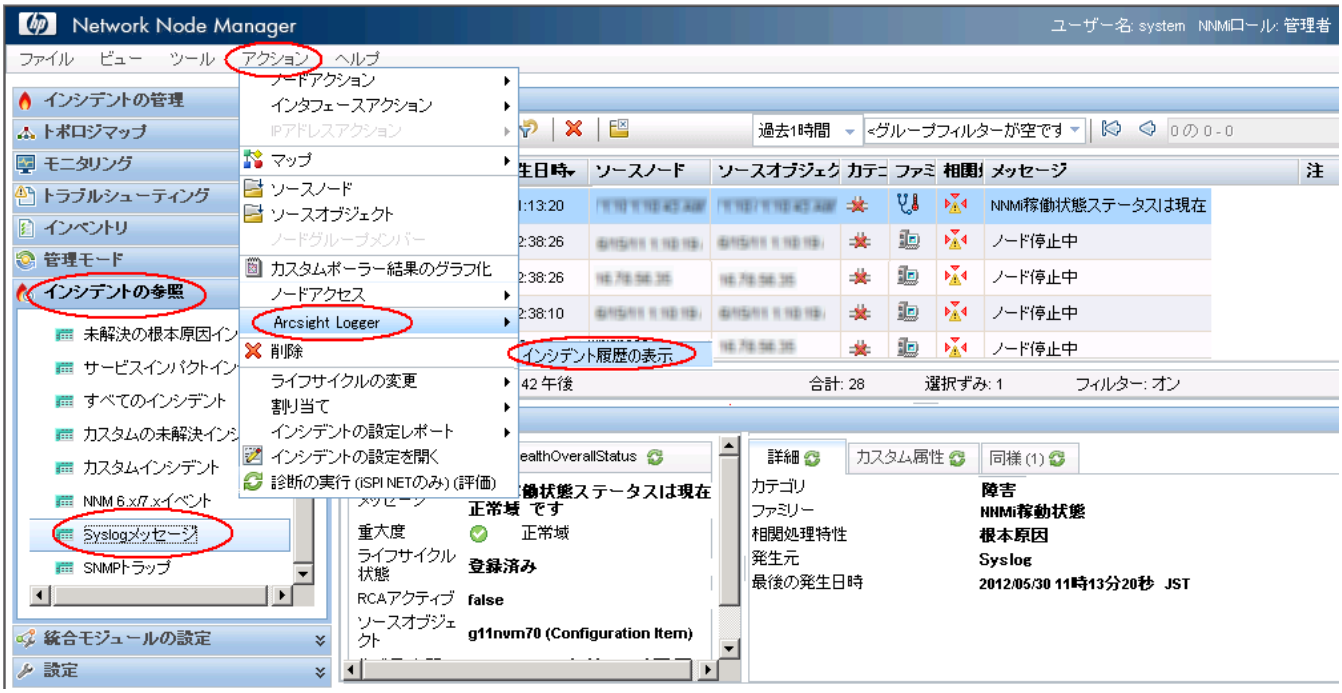


[インシデントの参照] ワークスペース

[**インシデントの参照**] ワークスペースで [**Syslog メッセージの設定**] をクリックして、HP ArcSight Logger から HP NNMi に転送する ArcSightEvents を表示します。

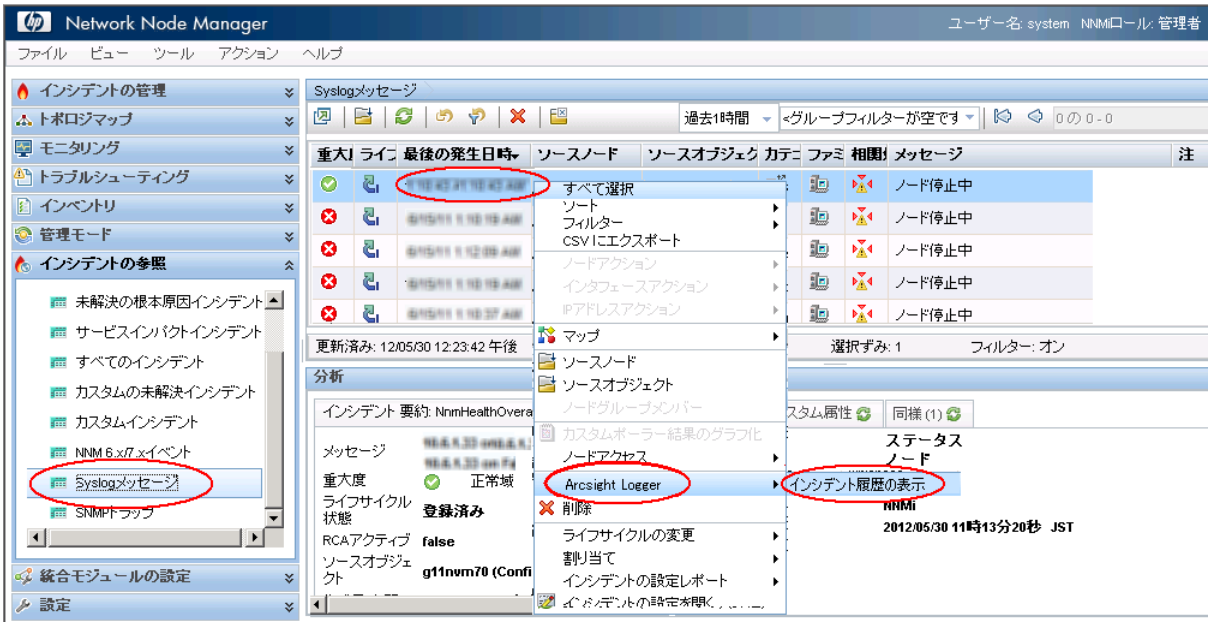
NNMi コンソールを使用して、HP NNMi インシデントから HP ArcSight Logger アプリケーションを開きます。これを行うには、[**インシデントの参照**] ワークスペースの使用中にインシデントを選択し、図 15 に示すように NNMi コンソールのメニューを使用してインシデント履歴を表示します。

図 15 [アクション] メニューを使用してインシデント履歴を表示する



インシデントを右クリックし、[**ArcSight ロガー**] > [**インシデント履歴の表示**] を使用して、HP NNMi インシデントから HP ArcSight Logger アプリケーションを開くこともできます。

図 16 Syslog メッセージを右クリックしてインシデント履歴を表示する



HP NNMi-HP 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**] > [**HP ArcSight**] の順にクリックします。

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

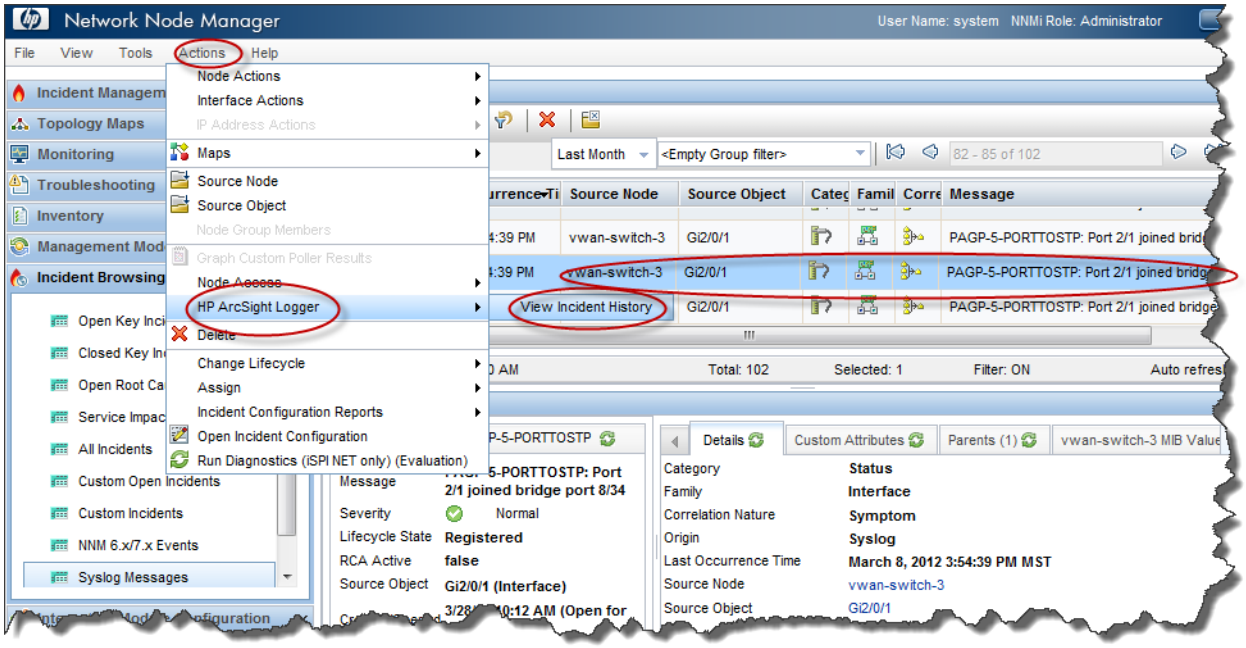
問題 : NNMi コンソールからポートデータを含むインシデントを選択して HP ArcSight Logger アプリケーションを開くと、HP NNMi はインシデントを HP ArcSight Logger で見つけられません。

解決方法 : これは、HP 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、HP 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 HP 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 HP ArcSight Logger を開きます。HP ArcSight Logger が開いたら、HP ArcSight Logger のクエリを変更し、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、HP ArcSight Logger クエリ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 HP ArcSight Logger を開き、[**インシデント履歴の表示**] をクリックします。

図 17 インタフェースを選択して [インシデント履歴の表示] を開く



  b HP ArcSight Logger が開いたら、そのインシデントで HP ArcSight Logger のクエリを変更し、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 HP ArcSight Logger クエリを実行し、HP ArcSight Logger でインシデントを検索します。

フィードバックをお待ちしております。

ご使用のシステムに電子メールクライアントが設定されている場合は、デフォルトで、ここをクリックすると電子メールウィンドウが開きます。

使用可能な電子メールクライアントがない場合は、Web メールクライアントの新規メッセージに以下の情報をコピーして、**ovdoc-nsm@hp.com** にこのメッセージを送信してください。

製品名およびバージョン : NNMi 9.20

ドキュメントタイトル : HP Network Node Manager i Software - HP ArcSight Logger 統合ガイド

フィードバック :


Java™
COMPATIBLE