



物理ホスト アップグレード ガイド

バージョン 10.6.6.xから11.2



Copyright © 1994-2019 Dell Inc. or its subsidiaries. All rights Reserved.

連絡先情報

RSA Link(<https://community.rsa.com>)では、よくある質問への回答や、既知の問題の解決方法を含むナレッジベースを公開しています。また、製品ドキュメント、コミュニティ ディスカッション、ケース管理なども公開されています。

商標

RSAの商標のリストについては、japan.emc.com/legal/emc-corporation-trademarks.htm#rsaを参照してください。

使用許諾契約

本ソフトウェアと関連ドキュメントは、Dellが著作権を保有しており、使用許諾契約に従って提供されます。本ソフトウェアと関連ドキュメントの使用と複製は、使用許諾契約の条項に従い、上記の著作権を侵害しない場合のみ許諾されます。本ソフトウェアと関連ドキュメント、およびその複製物を他人に提供することは一切認められません。

本使用許諾契約によって、本ソフトウェアと関連ドキュメントの所有権およびその他の知的財産権が譲渡されることはありません。本ソフトウェアと関連ドキュメントを不正に使用または複製した場合、民事および刑事上の責任が課せられる可能性があります。

本ソフトウェアは予告なく変更されることがありますので、あらかじめご承知おきください。

サードパーティライセンス

この製品にはRSA以外のサードパーティによって開発されたソフトウェアが含まれます。本製品内のサードパーティ製ソフトウェアに適用される使用許諾契約の内容については、RSA Linkの製品ドキュメント ページで確認できます。本製品を使用することにより、本製品のユーザは、これらの使用許諾契約の条項に同意したものとみなされます。

暗号技術に関する注意

本製品には、暗号技術が組み込まれています。これらの暗号技術の使用、輸入、輸出は、各国の法律で禁止または制限されています。本製品を使用、輸入、輸出する場合は、各国における使用または輸出入に関する法律に従わなければなりません。

配布

この資料に記載される情報は、発行日時点で正確であるとみなされます。この情報は予告なく変更されることがあります。

2月 2019

目次

概要	7
CentOS6からCentOS7へのアップグレード	7
RSA NetWitness® Platform 11.2のアップグレード パス	8
サポートされるホストのアップグレード パス	8
11.2でサポートされないハードウェア、導入形態、サービス、機能	8
ESA(Event Stream Analysis) のアップグレードに関する考慮事項	9
アップグレードのフェーズ分け	9
フェーズ1	9
フェーズ2	10
混在モードでの調査	11
アップグレードのワークフロー	14
カスタマー サポートへのお問い合わせ	14
アップグレード準備タスク	15
グローバル	15
タスク1: コア ポートを確認してファイアウォール ポートを開く	15
タスク2: 10.6.6.xのadmin userのパスワードの記録	16
タスク3: /etc/fstab ファイルのバックアップの作成	16
タスク4: 10.6.6.xでパスワードの強度設定のチェックボックスがオンになっていることを確認	16
Respond	17
タスク5: 「Domain」または「Domain for Suspected C&C」を使用した統合ルール的一致条件を確認	17
タスク6: データ保存の実行間隔を24時間以上に設定	18
Reporting Engine	19
(オプション) タスク7: 外部ストレージのリンク解除	19
Warehouse Connector	20
(オプション) タスク8: 他のディレクトリに格納されているkeytabファイルをrootディレクトリまたはetcディレクトリへコピー	20
ハードウェア	20
タスク9: アップグレード前のBAD-INDEX BIOSエラーの確認	20
バックアップ手順	21
タスク1: ファイルをバックアップするための外部ホストのセットアップ	22
タスク2: バックアップするホストのリストの作成	24
トラブルシューティング情報	25
タスク3: バックアップ ホストとターゲット ホストの間での認証の設定	27
タスク4: 特定のタイプのホストのバックアップ要件の確認	27
すべてのホスト タイプ	27

MongoデータベースのあるESAホスト	28
Decoder、Concentrator、Brokerホスト：データ収集と集計の停止	28
LC(Log Collector)とVLC(Virtual Log Collector)：prepare-for-migrate.shの実行	28
Web Threat Detectionとの統合、Archer Cyber Incident & Breach ResponseまたはNetWitness Endpointとの統合：RabbitMQユーザ名とパスワードの一覧表示	29
Bluecoat イベント ソース	30
タスク5：バックアップ用のディスク容量のチェック	30
タスク6：ホスト システムのバックアップ	31
バックアップ後のタスク	34
タスク1：all-systemsファイルとバックアップtarファイルのコピーの保存	34
タスク2：必要なバックアップ ファイルの生成の確認	34
タスク3：(オプション)複数のESAホストがある場合は、mongodb tar ファイルをESAプライマリホスト にコピー	35
タスク4：必要なすべてのバックアップ ファイルが各ホスト上にあることを確認	35
アップグレード タスク	38
フェーズ1：SA Server、Event Stream Analysis、Malware Analysisホスト、BrokerまたはConcentratorの アップグレード	38
タスク1：10.6.6.x SA Serverの11.2 NW Serverへのアップグレード	38
タスク2：10.6.6.x ESAの11.2へのアップグレード	38
タスク3：10.6.6.x Malware Analysisの11.2へのアップグレード	39
タスク4：10.6.6.x Brokerまたは10.6.6.x Concentratorの11.2へのアップグレード	39
フェーズ2：その他すべてのホストのアップグレード	39
DecoderホストおよびConcentratorホスト	39
Log Decoderホスト	39
Virtual Log Collectorホスト	39
他のすべての10.6.6.xホストを11.2にする	41
10.6.6.x SA Serverホストを11.2 NW Serverホストにアップグレード	41
10.6.6.x 非SA Serverホストの11.2へのアップグレード	49
Legacy Windows収集の更新またはインストール	57
アップグレード後のタスク	58
全般	58
タスク1：ポート15671が正しく設定されていることを確認	58
(オプション)タスク2：カスタムAnalystsロールのリストア	58
NW Server	59
タスク3：AD(Active Directory)の移行	59
タスク4：移行したAD構成の変更と証明書のアップロード	59
タスク5：11.2でのPAM(Pluggable Authentication Module)の再構成	59
タスク6：NTPサーバのリストア	60
タスク7：FlexNet Operations-On Demandを使用しない環境でのライセンスのリストア	60
(オプション)タスク8：標準ファイアウォール構成を無効化した場合、カスタムiptablesを追加	60
(オプション)タスク9：信頼接続を設定していない場合、SSLポートを指定	60

タスク10:(オプション)Logstash出力構成ファイルで更新されていない監査ログテンプレートの修正	61
RSA NetWitness® Endpoint	62
タスク11:メッセージパス経由のEndpointアラートの再構成	62
タスク12:Javaバージョンの変更により、レガシーEndpointからの定期実行Feedを再構成	62
RSA NetWitness® Endpoint Insights	62
(オプション)タスク13:Endpoint HybridまたはEndpoint Log Hybridのインストール	62
Event Stream Analysisタスク	63
タスク14:ESAの自動脅威検出の再構成	63
タスク15:Web Threat Detection、Archer Cyber Incident & Breach ResponseまたはNetWitness Endpointとの統合のためのSSL相互認証の構成	63
タスク16:Threat - Malware Indicatorsダッシュボードの有効化	64
Investigate	64
タスク17:カスタマイズしたユーザロールにイベント分析にアクセスするInvestigate-server権限があることを確認	64
ログ収集	65
タスク18:アップグレード後のLog CollectorのStable System Valueのリセット	65
(オプション:FIPSが有効な10.6.6.xのLog Collector、Log Decoder、Network Decoderをアップグレードした場合)タスク19:FIPSモードの有効化	65
DecoderおよびLog Decoder	66
(オプション)タスク20:GeoIP2 Parserのメタデータの有効化	66
Reporting Engine	66
(オプション)タスク21:外部SyslogサーバのCA証明書をReporting Engineにリストア	66
(オプション)タスク22:Reporting Engineの外部ストレージのリストア	66
Respond	67
タスク23:Respondサービスのカスタムキーのリストア	67
タスク24:Respondサービスのカスタム正規化スクリプトのリストア	67
タスク25:カスタムロールに対応の通知設定の権限を追加する	68
タスク26:対応の通知設定を手動で構成	68
タスク27:デフォルトのインシデントルールのGroup By値の更新	69
タスク28:インシデントルールへの[Group By]フィールドの追加	69
タスク29:アップグレード準備タスクで特定した一致条件で「Domain」を使用するインシデントルールの更新	71
RSA Archer Cyber Incident & Breach Response	73
タスク30:RSA Archer Cyber Incident & Breach Response統合の再構成	73
RSA NetWitness® UEBA	73
タスク31:NetWitness UEBAのインストール	73
Warehouse Connector	73
タスク32:keytabファイルのリストア、NFSのマウント、サービスのインストール	73
タスク33:Warehouse Connector Lockboxの更新とストリームの開始	74
バックアップ	74
タスク34:ホストのローカルディレクトリからバックアップ関連ファイルを削除	74

付録A: トラブルシューティング	75
セクション1: 一般的なトラブルシューティングの情報	75
CLI(コマンド ライン インタフェース)	76
バックアップ(nw-backupスクリプト)	77
Event Stream Analysis	79
Log Collectorサービス(nwlogcollector)	80
NW Server	82
Orchestration	82
Reporting Engineサービス	83
NetWitness UEBA	84
セクション2: ハードウェアに関するトラブルシューティングの情報	85
付録B: データ収集と集計の停止と再開	89
データ収集と集計の停止	89
データ収集と集計の開始	91
付録C: DVD ISOイメージでのiDRACの使用	92
NFSサーバの構成	92
iDRACでのNFSとブートの構成	93
付録D: 外部リポジトリの作成	94
改訂履歴	96

概要

このガイドの手順は、物理ホストをRSA NetWitness® Platform 11.2にアップグレードする場合にのみ適用できます。仮想ホストを11.2にアップグレードする手順は、『*NetWitness Platform 仮想ホスト アップグレード ガイド (10.6.6から11.2)*』を参照してください。

NetWitness Platform 11.2は、NetWitness Platformのすべての製品に影響を与えるメジャーリリースです。NetWitness Platformのコンポーネントは、NetWitness Server(Admin Server、Config Server、Integration Server、Investigate Server、Orchestration Server、Respond Server、Security Server、Source Server)、Archiver、Broker、Concentrator、Context Hub、Decoder、Endpoint Hybrid、Endpoint Log Hybrid、ESAプライマリ、ESAセカンダリ、Log Collector、Log Decoder、Malware Analysis、Reporting Engine、UEBA、Warehouse Connector、Workbenchで構成されます。

11.xのユーザ インタフェースに関する主要な変更については、『*NetWitness Platform スタート ガイド*』を参照してください。11.xのプラットフォームに関する主要な変更については、『*NetWitness Platform 導入 ガイド*』を参照してください。

NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

注 : Reporting EngineはNW Serverホストにインストールされ、WorkbenchはArchiverホストにインストールされ、Warehouse ConnectorはDecoderまたはLog Decoderホストにインストールすることができます。

CentOS6からCentOS7へのアップグレード

NetWitness Platform 11.2は、オペレーティングシステムの新しいバージョンへのアップグレード (CentOS6からCentOS7) を伴うメジャーリリースです。さらに、11.2プラットフォーム環境は大幅に強化され、現在および将来の物理環境および仮想環境に対応します。これらの変更を適用するには、新しい環境へのアップグレードと機能のアップグレードが必要です。

RSA NetWitness® Platform 11.2のアップグレード パス

RSA NetWitness® Platform 11.2でサポートされているもっとも古いアップグレード パスはSecurity Analytics 10.6.6.xです。10.6.6.xよりも前のバージョンのNetWitness Platformを実行している場合は、10.6.6.xにアップグレードしてから11.2にアップグレードする必要があります。RSA Linkの『*RSA Security Analytics 10.6.6更新ガイド*』(<https://community.rsa.com/docs/DOC-85119>)を参照してください。

サポートされるホストのアップグレード パス

ホストは同じタイプのホストへアップグレードする必要があります。

- RSA物理アプライアンスは同じシリーズのRSA物理アプライアンスへ(すなわち、シリーズ4はシリーズ4へ、シリーズ5はシリーズ5へ)
11.2では、サードパーティの物理ホストをサポートしていません。
- オンプレミスの仮想アプライアンスからオンプレミスの仮想アプライアンスへ

注意: 11.2へのアップグレードでは、異なるプラットフォームへのアップグレードはサポートされません(たとえば、物理から仮想へのアップグレードはサポートされません)。

11.2でサポートされないハードウェア、導入形態、サービス、機能

次のハードウェア、導入形態、サービス、機能の11.2へのアップグレードはサポートされていません。

- RSA AIO(All in One) アプライアンス
- 複数のNetWitness Serverがある構成
- IPDBサービス
- SAサーバ上に共存するMalware Analysisサービス(Malware Analysis Enterpriseのアップグレードは11.2でサポートされます)。
- スタンドアロンWarehouse Connectorサービス(非スタンドアロンのWarehouse Connectorのアップグレードは11.2でサポートされます)。
- Context Hubサービスの10.6.xでのカスタムヘルスマニタポリシー
NetWitness 11.2にアップグレードした後、カスタムポリシーは表示されなくなります。その代わりに、バージョン11.2に固有の、標準提供の「Context Hub Serve Monitoring Policy」がユーザインタフェースに表示されます。
- DISA-STIG(米国国防情報システム局セキュリティ技術情報ガイド)のハードニングに対応した導入環境。
- Warehouse Analytics(データサイエンス)

ESA(Event Stream Analysis) のアップグレードに関する考慮事項

RSA NetWitness® Platform 11.2では、ESA関連ルールによるシステム生成のアラートを保存および送信する方法が変更されました。11.2では、ESAはすべてのアラートをセントラルアラートシステムに送信します。ESA 10.6.6.xのローカルMongoDBストレージは削除されました。

注意: 10.6.6.xでIncident Managementを使用していない場合は、バージョン11.2にアップグレードするかどうかを慎重に検討してください。

ESAホストを11.2にアップグレードするかどうかを判断する際に、次のガイドラインを参考にしてください。10.6.6.x導入環境の構成により異なります。

- 1つのESAホスト(Incident Managementが構成されているかどうかを問わず) の場合 : 11.2.にアップグレードします。
- 複数のESAホストがIncident Managementを使用するよう構成されている場合 : システムは引き続きアラートを一元的に統合します。10.6.6.xのシステムが正確にサイジングされ、想定どおり動作している場合、バージョン11.2にアップグレードできます。
- 複数のESAホストをIncident Managementなしで使用し、個々のESAホストに接続してアラートを表示している場合 : バージョン11.2にアップグレードしないでください。

注: 10.6.6.xでIncident Managementを使用していない場合は、移行スクリプトを実行しないと11.2 Respondコンポーネントで10.6.6.xのESAアラートを表示できません。ESAアラート移行スクリプトを使用して、11.2 Respondコンポーネントが表示できる場所に、これらのアラートを移行します。このスクリプトを実行する方法については、RSA Linkのナレッジベース記事「*ESA Alert Migration Instructions (ESAアラート移行手順)*」(<https://community.rsa.com/docs/DOC-84102>)を参照してください。

アップグレードのフェーズ分け

RSAは、このセクションの説明に従って、ホストのアップグレードを実行することを推奨します。CentOS7への更新と物理アクセスまたはiDRACアクセスの必要性により、11.2へのアップグレードは通常のアップグレードよりも時間がかかります。

注意: 時間差でアップグレードする場合は、次の点に注意してください。

- 最初にフェーズ1のホストを、表示されている順にアップグレードする必要があります。
- 導入環境全体をアップグレードするまで、一部の機能を使用できない可能性があります。
- 導入環境内のすべてのホストをアップグレードするまでサービス管理機能を利用できません。

フェーズ1

最初にフェーズ1のアップグレードを実行します。フェーズ1では、次の順序でホストをアップグレードする必要があります。

1. Security Analytics Serverホスト
2. Event Stream Analysisホスト
3. Malware Analysisホスト

4. Brokerホスト (Brokerがない場合は、Concentratorホストをアップグレード)
11.2 NW Serverの新しいInvestigate機能は10.6.6.xコア サービスと通信できません。このため、フェーズ1でBrokerまたはConcentratorのホストをアップグレードする必要があります。

フェーズ2

残りのホストをアップグレードします。

RSAでは、次のリスクを低減するため、フェーズ2に記載された順序に従うことを推奨します。

- 調査の一部機能の停止。
- ダウンタイムによる、ネットワークとログの収集停止。

注: ダウンストリームのイベント送信先を持つログ収集ホストを除き、フェーズ2に記載された順序でホストをアップグレードする技術上の理由はありません。

フェーズ2のホストは次の順序でアップグレードすることを推奨します。

1. Decoderホスト
2. Concentratorホスト
3. Archiverホスト
4. ログ収集ホスト: LD (Log Decoder) ホスト上のLog Collector、VLC (仮想Log Collector)、LWC (Legacy Windows Collector)
ログ収集ホストをアップグレードする前に、アップグレードの準備をする必要があります。この準備の過程でキューにイベント データが残っていないことを確認します。これを確認するには、イベント データのダウンストリームの送信先 (Log Collector、Virtual Log Collector、Log Decoder) が稼働し、正常に機能している必要があります。

Log Decoderにダウンストリームのイベント データ送信先がある場合、次の順序でLog Collectorを準備し、アップグレードする必要があります。

- a. 各LD (一度に1つのLD)
- b. VLCとLWC

Log Decoderにダウンストリームのイベント データ送信先がない場合は、複数のLD、VLC、LWCをまとめて準備してアップグレードできます。

5. その他のすべてのホスト

次の項目については、「*RSANetWitness Platform*ホストおよびサービス スタート ガイド」の「ホストおよびサービスの基本」で、「混在モードでの実行」を参照してください。

- 混在モードで発生する機能ギャップ
- 段階的アップグレードの例

NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

混在モードでの調査

混在モードは、一部のサービスが11.2にアップグレードされたが、一部がまだ11.0.0.xまたは10.6.6.xのまま残っている状態です。この状態は、段階的に11.2にアップグレードする場合に発生します。

注: 調査機能を完全に維持するためには、[アップグレードのフェーズ分け](#)に示す順序に従いホストをアップグレードする必要があります。SAサーバをアップグレードすると、11.2 Investigate Serverがインストールされますが、イベント分析ビューにアクセスするには、Brokerホストを11.2にアップグレードする必要があります。Brokerがアップグレードされていない場合、Brokerの横に警告アイコンが表示され、そのBrokerに集計されたデータは表示されません。

すべてのサービスを11.2にアップグレードした後、アナリストが調査を実施する場合、RBAC(ロールベースのアクセス制御)はダウンロード操作に対しても一貫して機能し、制限されたデータにはアクセスできません。

混在モード(一部のサービスが11.2にアップグレードされ、一部はまだ11.0.0.xまたは10.6.6.xの状態)で、アナリストが調査を行う場合、RBACは表示とダウンロードに同一に適用されません。

`sdk.packets`設定を10.6.6.xまたは11.0.0.xサービスで無効にしていない場合、イベントのコンテンツの表示および再構築を制限するSDKメタとロール権限を割り当てられたアナリストが、コンテンツ制限のあるイベントのPCAPをダウンロードできます。他のタイプのダウンロードができたように見える場合、その後、権限の不足によるエラーが生成され、データは保護されたままです。

段階的な更新中、10.6.6.xおよび11.0.x.xサービスで`sdk.packets`設定を無効にして、混在モードの間はすべてのPCAPまたはログをアナリストがダウンロードできないように制限できます。すべてのサービスを11.2に更新して`sdk.packets`を再度有効にした後、すべてのサービスでRBACが一貫して機能します。

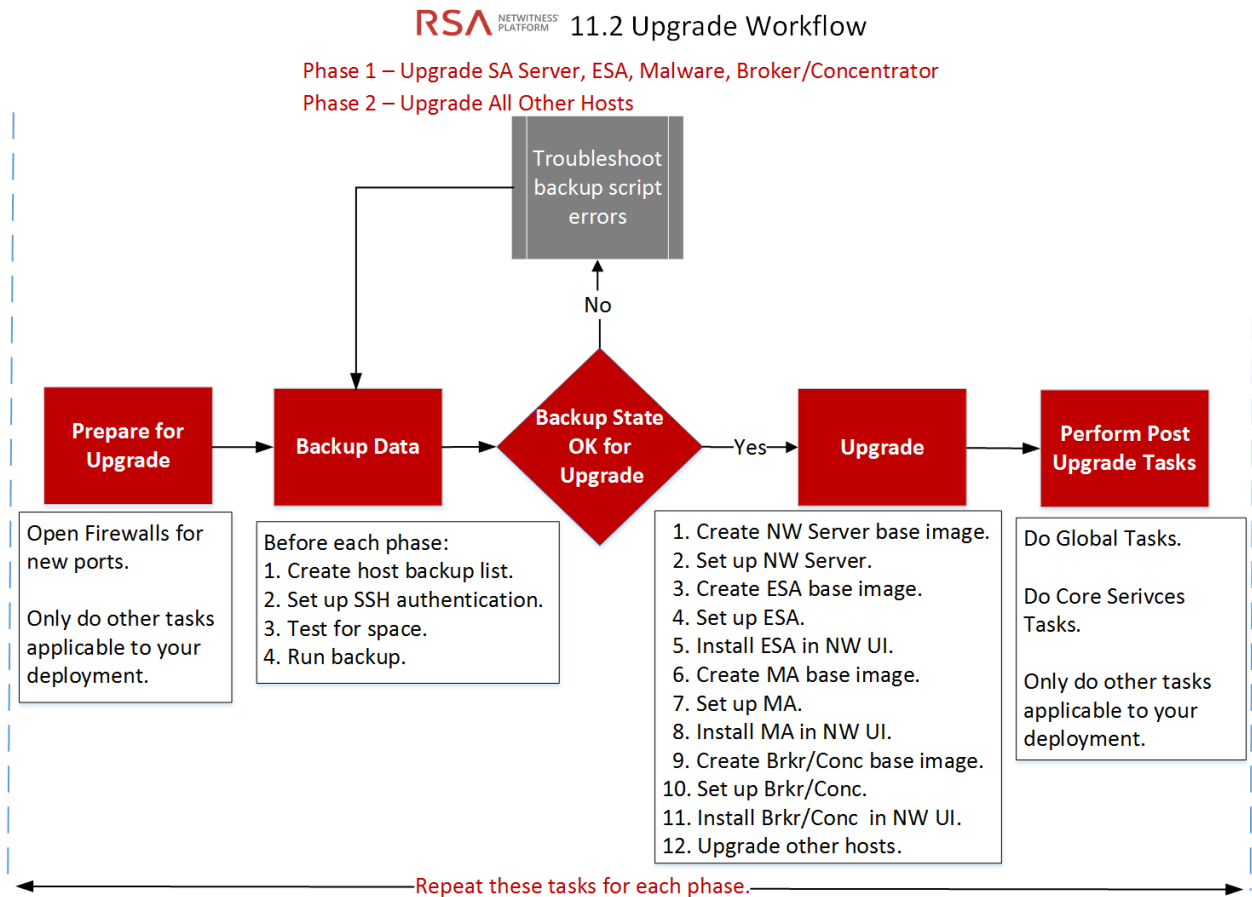
次の表は、バージョン11.2のNWサーバが以前のバージョンのサービスに接続する場合に、[調査]ビューで表示およびダウンロードできる対象を示します。

接続するサービスのバージョン	影響するビュー	制限コンテンツのあるユーザーロール	参照可能	制限コンテンツのダウンロード(正常)	制限コンテンツのダウンロード(エラー)
11.2 Broker -> 10.6.6 x Concentrator -> 10.6.6 Network Decoder/Log Decoder	[イベント]ビュー	Analyst	RBACで許可されたアイテム	PCAP	ファイルアーカイブがダウンロードされますが解凍できません。
	[イベントの再構築]ビュー	Analyst	RBACで許可されたアイテム	PCAP	ファイルアーカイブがダウンロードされますが解凍できません。
	[イベント分析]ビュー	Analyst	RBACで許可されたアイテム	PCAP	サービスからのペイロード取得エラー(ペイロード、リクエストペイロード、レスポンスペイロード)
11.2 Broker -> 11.2 Concentrator -> 11.2 Decoder/Log Decoder	[イベントの再構築]ビュー	AnalystとData Privacy Officer	RBACで許可されたアイテム	PCAP	ファイルアーカイブがダウンロードされますが解凍できません。ダウンロードされたPCAPとログは、ゼロバイトです

接続するサービスのバージョン	影響するビュー	制限コンテンツのあるユーザーロール	参照可能	制限コンテンツのダウンロード (正常)	制限コンテンツのダウンロード(エラー)
11.2 Broker -> 11.0.0 x Concentrator -> 11.0.0 Network Decoder/Log Decoder	[イベント]ビュー	Analyst	RBACで許可されたアイテム	なし	ファイルアーカイブがダウンロードされませんが解凍できません。 ダウンロードされたPCAPとログは、ゼロバイトです
	[イベントの再構築]ビュー	Analyst	RBACで許可されたアイテム	なし	ファイルアーカイブがダウンロードされませんが解凍できません。 ダウンロードされたPCAPとログは、ゼロバイトです
	[イベント分析]ビュー	Analyst	RBACで許可されたアイテム	なし	サービスからのペイロード取得エラー (ペイロード、リクエストペイロード、レスポンスペイロード) ダウンロードされたPCAPとログは、ゼロバイトです

アップグレードのワークフロー

次の図は、RSA NetWitness® Platform 11.2にアップグレードするワークフローを示しています。



カスタマー サポート へのお問い合わせ

RSA NetWitness Platform 11.2に関する支援が必要な場合には、RSAカスタマー サポートにお問い合わせください。

アップグレード準備タスク

NetWitness Platform 11.2にアップグレードするには次のタスクを実行します。これらのタスクは、次のカテゴリに分類されます。

- [グローバル](#)
- [Reporting Engine](#)
- [Respond](#)
- [Warehouse Connector](#)
- [ハードウェア](#)

グローバル

NetWitness Platformを導入する方法や使用するコンポーネントに関係なく、これらのタスクを完了する必要があります。

タスク1: コアポートを確認してファイアウォールポートを開く

次の表は、11.2での新しいポートを示します。

注意: ポートに接続できないことが原因でアップグレードが失敗しないよう、新しいポートを開いたら、アップグレード前にテストしておいてください。

NW Serverホスト

ソースホスト	宛先ホスト	宛先ポート	コメント
NWホスト	NW Server	TCP 4505、4506	Saltマスターポート
NWホスト	NW Server	TCP 27017	MongoDB
管理ワークステーション	NW Server	TCP 15671	RabbitMQ管理UI
NWホスト	NW Server	TCP 15671	RabbitMQ管理UI

ESAホスト

ソースホスト	宛先ホスト	宛先ポート	コメント
NW Server、 NW Endpoint、 ESAセカンダリ	ESAプライマリ	TCP 27017	MongoDB

Endpoint HybridまたはEndpoint Log Hybrid

ソース ホスト	宛先ホスト	宛先ポート	コメント
Endpoint HybridまたはEndpoint Log Hybrid	NW Server	TCP 5672	メッセージ バス
Endpoint Server	NW Server	TCP 27017	MongoDB

NetWitness Platformのサービスとファイアウォールを再構成する場合は、すべてのNetWitness Platformコアポートを「RSA NetWitness® Platform 導入ガイド」の「ネットワークアーキテクチャとポート」のトピックで参照してください。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

タスク2: 10.6.6.xのadmin userのパスワードの記録

10.6.6.xのadmin userのパスワードを記録します。このパスワードは、アップグレードを完了するために必要です。

タスク3: /etc/fstab ファイルのバックアップの作成

/etc/fstabファイルをすべての物理ホストからローカルマシン(バックアップホストまたはリモートマシン)にコピーします。

注: このファイルは、物理ホストに外部ストレージを再マウントする際に必要です。

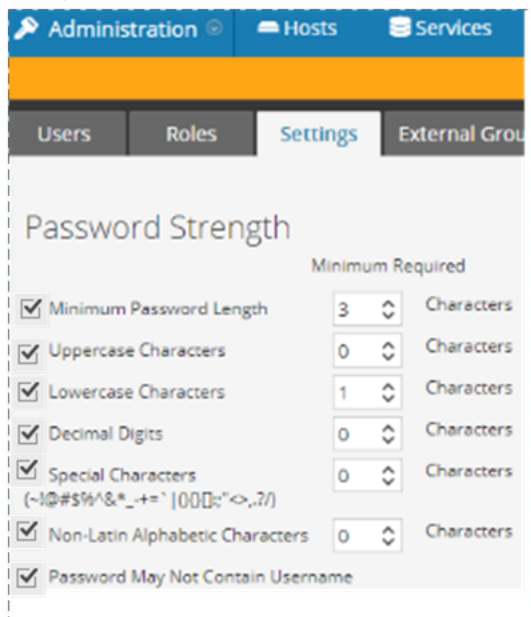
タスク4: 10.6.6.xでパスワードの強度設定のチェックボックスがオンになっていることを確認

10.6.6.xで[管理] > [セキュリティ] > [設定] タブの[パスワードの強度] セクションのチェックボックスをオンにしておく必要があります。オフの場合は、設定が11.2に移行されません。

次のタスクを実行し、10.6.6.xで[パスワードの強度] セクションのチェックボックスがオンになっていることを確認します。

1. Security Analytics 10.6.6.xで、[管理] > [セキュリティ] > [設定] タブの順に進みます。
2. [パスワードの強度] セクションの各設定の左側のチェックボックスがすべてオンになっていることを確認します。オンになっていない場合は、オンにして[適用]をクリックします。
次の例では、すべてのチェックボックスがオンになっています(11.2にアップグレードする前に10.6.6.xで

必須)。



Respond

タスク5: 「Domain」または「Domain for Suspected C&C」を使用した統合ルールの一 致条件を確認

ルールビルダのドロップダウン リストで、一致条件の中で「Domain」または「Domain for Suspected C&C」を使用したIncident Management統合ルールがないか確認します。11.2にアップグレードした後、「[アップグレード後のタスク](#)」の「Respond」セクションの説明に従い、これらの条件を再び追加する必要があります。

各統合ルールについてこのタスクを実行します。

1. Security Analytics 10.6.6.xで、[インシデント] > [構成] > [統合ルール] タブの順に進み、一致条件を表示するためにルールを編集します。

2. [一致条件] セクションで、条件のドロップダウン リストから [Domain] または [Domain for Suspected C&C] を選択しているものがないか探します。


The screenshot shows the configuration page for a rule in RSA Security Analytics. The rule name is "Verify Domain for Suspected C&C field". Under "Match Conditions", there are two conditions: "Domain is equal to" and "Domain for Suspected C&C is equal to". The "Action" is "Group into an Incident". Under "Grouping Options", "Group By" is set to "Domain" and "Domain for Suspected C&C". The "Time Window" is "1 Hours". The "Priority" is set to "High" (50) on a scale from 1 to 100. The interface also shows "Incident Options" and "Notifications" sections.

3. 該当する場合は、ルール名と、[Domain] または [Domain for Suspected C&C] を使用する条件の全体 (演算子や値を含む) を記録します。

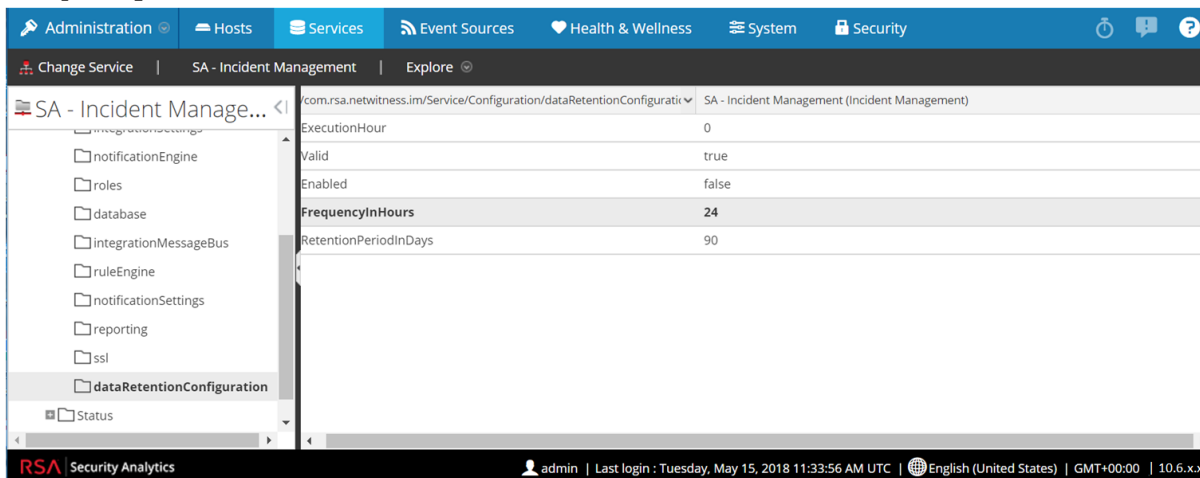
タスク6: データ保存の実行間隔を24時間以上に設定

Security Analytics 10.6.x では、データ保存の実行間隔の最小値はチェックされません。11.2 では、少なくとも24時間以上の間隔で実行するようチェックが追加されました。11.2 にアップグレードする際、この値が24時間未満の場合、Respond サービスは開始されません。

11.2 にアップグレードした後に Respond サービスが開始されるよう、次のタスクを完了します。

1. Security Analytics 10.6.6.x で、[管理] > [サービス] にアクセスします。
2. Incident Management サービスを選択し、 > [表示] > [エクスプローラ] を選択します。
3. Incident Management の [エクスプローラ] ビューで、[Service] > [Configuration] > [dataRetentionConfiguration] にアクセスします。

4. FrequencyInHoursパラメータが24以上であることを確認します。



Reporting Engine

(オプション) タスク7: 外部ストレージのリンク解除

Reporting Engineに外部ストレージ(SAN(Storage Area Network)またはNAS(Network Attached Storage)など)が接続されている場合は、次の手順を実行してストレージのリンクを解除します。

注:ここに示す手順では次のことが前提となっています。

/home/rsasoc/rsa/soc/reporting-engine/は、Reporting Engineのホーム ディレクトリです。
/externalStorage/は、外部ストレージのマウント ポイントです。

1. Reporting EngineのホストにSSHで接続し、root の認証情報でログインします。
2. Reporting Engineサービスを停止します。
`stop rsasoc_re`
3. rsasocユーザに切り替えます。
`su rsasoc`
4. Reporting Engineのホーム ディレクトリに移動します。
`cd /home/rsasoc/rsa/soc/reporting-engine/`
5. 外部ストレージをマウントしたresultstoreディレクトリのリンクを解除します。
`unlink /externalStorage/resultstore`
6. 外部ストレージをマウントしたformattedReportsディレクトリのリンクを解除します。
`unlink /externalStorage/formattedReports`

Warehouse Connector

(オプション) タスク8: 他のディレクトリに格納されているkeytabファイルをrootディレクトリまたはetcディレクトリへコピー

keytabファイルが別のディレクトリに格納されている場合は、rootディレクトリまたはetcディレクトリにコピーするため、次のタスクを実行します。

1. NFSマウント ディレクトリとkeytabファイルの絶対パスを記録します。
アップグレード後に、この情報を[Warehouse Connector](#)にリストアする必要があります。
2. NFSディレクトリをアンマウントします。
 - a. Warehouse ConnectorにSSHで接続し、rootの認証情報でログインします。
 - b. 次のコマンドを実行して、NFSディレクトリをアンマウントします。
`umount <NFS-absolute-path>`

ハードウェア

タスク9: アップグレード前のBAD-INDEX BIOSエラーの確認

11.2にアップグレードする前にBAD-INDEX BIOSエラーがないか確認するため、次の手順を実行します。

1. 各ホスト アプライアンスにSSHで接続します。
2. 次のコマンドを実行します。
`dmidecode`
3. BAD-INDEXエラーが出力された場合は、RSAカスタマー サービスまでお問い合わせください。

バックアップ手順

Security Analytics 10.6.6.xからNetWitness Platform 11.2にアップグレードする最初のステップは、10.6.6.xのすべてのホストの構成データをバックアップすることです。

注: 1.) カスタム証明書ファイルおよびその他すべてのCA(認証局)ファイルを`/root/customcerts`フォルダに配置して、これらの証明書ファイルが確実にバックアップされるようにしてください。このディレクトリに配置されているカスタム証明書ファイルは、アップグレード中に自動的にリストアされます。11.2にアップグレードした後、カスタム証明書ファイルは`/etc/pki/nw/trust/import`に配置されます。これらのファイルタイプのバックアップの詳細については、「すべてのホスト タイプ」のステップ1を参照してください。2.) バックアップを開始する前に、PKI(公開鍵基盤)の設定を無効にします。

注意: 次のサービスは、10.6.6.xのバックアップおよびアップグレード プロセスではサポートされません。

- IPDB
- All in Oneサーバ
- Security Analyticsサーバ上に共存するMalware Analysis
- スタンドアロンのWarehouse Connector
- Warehouse Analytics(Datascience)

次のタイプのホストは、バックアップして、アップグレード中に自動的にリストアすることができます。

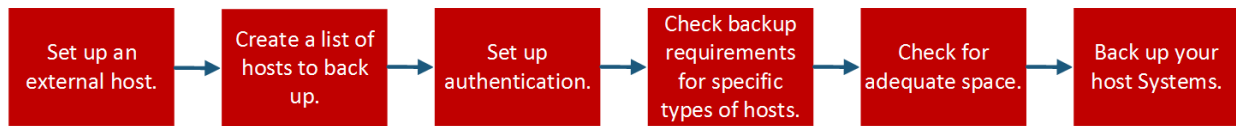
- Security Analytics Admin Server
- Malware Analysis(スタンドアロン)
- Archiver
- Broker
- Event Stream Analysis(Context HubとIncident Managementデータベースを含む)
- Concentrator
- Log Decoder(ローカルLogCollectorとWarehouse Connector(インストールされている場合)を含む)
- Log Hybrid
- Network Decoder(インストールされている場合は、Warehouse Connectorを含む)
- Network Hybrid
- Virtual Log Collector

次のタイプのファイルは、自動的にバックアップされますが、アップグレード後に手動でリストアする必要があります。

- PAM構成ファイル: PAM構成ファイルをリストアする方法については、「アップグレード後のタスク」の「グローバル」セクションにある「タスク5: 11.2でのPAM(Pluggable Authentication Module) の再構成」を参照してください。
- `/etc/pfring/mtu.conf`および`/etc/init.d/pf_ring`: これらのファイルをリストアするには、手動でファイルを取得する必要があります。`/etc/pfring/mtu.conf`ファイルは`/var/netwitness/database/nw-backup/restore/etc/pfring/mtu.conf`に、`/etc/init.d/pf_ring`ファイルは`/var/netwitness/database/nw-backup/restore/etc/init.d/pf_ring`に配置されます。これらのファイルをリストアする方法につ

いては、「アップグレード後のタスク」の「ハードウェア関連タスク」セクションにある「(オプション) タスク 2: 10G Decoderのファイルのリストアップ」を参照してください。

次の図は、ホストのバックアップを実行するタスクのフローの概要を示しています。



次のセクションで、これらのタスクについて説明します。

- タスク1: ファイルをバックアップするための外部ホストのセットアップ
- タスク2: バックアップするホストのリストの作成
- タスク3: バックアップホストとターゲットホストの間での認証の設定
- タスク4: 特定のタイプのホストのバックアップ要件の確認
- タスク5: バックアップ用のディスク容量のチェック
- タスク6: ホストシステムのバックアップ
- バックアップ後のタスク

タスク1: ファイルをバックアップするための外部ホストのセットアップ

ファイルのバックアップに使用する外部ホストをセットアップする必要があります。このホストはCentOS 6を実行し、Security Analyticsの各ホストにSSHで接続する必要があります。

注: ファイルのバックアップに外部ホストを使用できない場合は、RSAカスタマーサポートにお問い合わせください。

外部ホストからバックアップ対象のシステムのホスト名を、DNSまたは/etc/hostsファイルにより解決できることを確認します。

注: バックアップスクリプトは、CentOS 6でのみ実行するよう設計されています。バックアップスクリプトは、CentOS 6のマシンで実行する必要があります。

バックアップ中にいくつかのスクリプトが実行されます。RSA Link(<https://community.rsa.com/docs/DOC-81514>) から、スクリプト (nw-backup-v4.1.zip以降) を含むzipファイルをダウンロードし、CentOS 6のバックアップシステムにコピーする必要があります。zipファイルを解凍して、スクリプトにアクセスします。次のスクリプトが含まれます。

- `get-all-systems.sh`: `all-systems`ファイルを作成します。このファイルには、バックアップするすべてのSecurity Analyticsサーバとホストシステムの一覧が含まれます。

注意: 混在モードでアップグレードを実行する場合は、導入環境のすべてのホストを11.2にアップグレードするまで、`all-systems`ファイルのマスターコピーを保存しておきます。混在モードでは、最初にNW Serverをアップグレードする必要がありますが、アップグレード後のNW ServerのオペレーティングシステムはCentOS71になるため、`get-all-systems.sh`を再度実行することはできません。

- `ssh-propagate.sh`: バックアップ対象のシステムとバックアップ ホスト システム間のキー共有を自動化し、パスワードの入力プロンプトが何度も表示されないようにします。
- `nw-backup.sh`: ホストのバックアップを実行します。
- `azure-mac-retention.ps1`: Azureを使用している場合にのみ必要です。詳細については、「[Azure 導入ガイド](#)」を参照してください。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

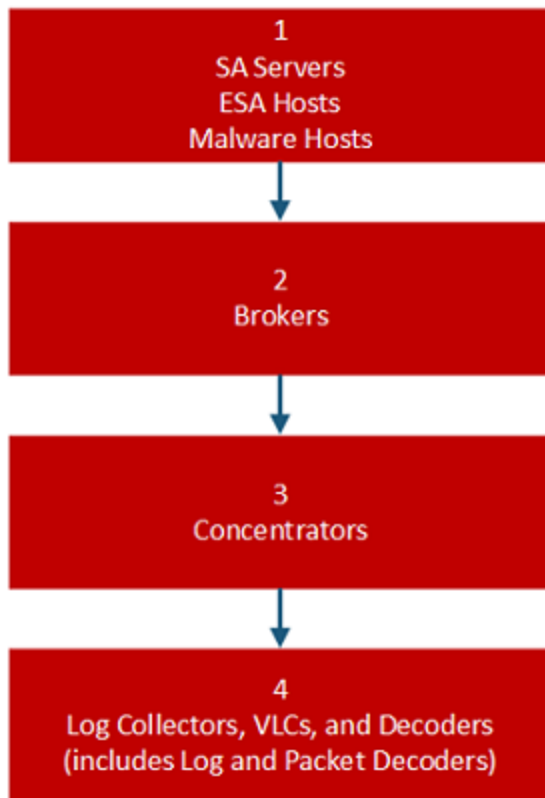
注: 10.6.6ホストで、バージョン10.6.xのバックアップとリストアスクリプトを既に使用している場合でも、ここにリストされているすべてのスクリプトを実行する必要があります。

注: 通常のバックアップでは`nw-backup-v4.1.zip`ファイルのスクリプトを使用しないでください。これらのスクリプトは、10.6.6.xから11.2へのアップグレード専用設計されています。

注: バックアップスクリプトは、STIGのハードニングが適用されたホストのデータバックアップをサポートしません。

タスク2: バックアップするホストのリストの作成

ファイルをバックアップするために使用するスクリプトは、`all-systems`ファイルと`all-systems-master-copy`ファイルを参照します。これらのファイルには、バックアップするホストのリストが含まれます。`all-systems-master-copy`ファイルには、すべてのホストのリストが含まれています。`all-systems`ファイルは、バックアップセッションごとに使用され、特定のセッションでバックアップするホストのみが含まれます。これらのファイルは`get-all-systems.sh`スクリプトを実行して生成します。RSAでは、一度にすべてのホストをバックアップするのではなく、グループに分けてバックアップすることを推奨します。バックアップセッションで推奨されるホストの順序とグループを、次の図に示します。



各バックアップセッションではホストを5台に制限し、バックアップファイル用のディスク領域が不足しないようにします。`all-systems-master-copy`ファイルを参照しながら、バックアップセッション用の`all-systems`ファイルを作成します。`all-systems`ファイルを手動で編集し、対象のホストが含まれるようにします。

`all-systems`ファイルおよび`all-systems-master-copy`ファイルを生成するには、次の手順を実行します。

1. バックアップを実行するホストで、次のコマンドを実行し、`get-all-systems.sh`スクリプトを実行可能にします。
`chmod u+x get-all-systems.sh`
2. `root`レベルで、`get-all-systems.sh`スクリプトを次のように実行します。
`./get-all-systems.sh <IP-Address-of-SA-Admin-Server>`
 ホストごとに1回、ホストシステムのパスワードの入力を求められます。
 このスクリプトが`all-systems`ファイルと`all-systems-master-copy`ファイルを
`/var/netwitness/database/nw-backup/`に保存します。

3. `all-systems`ファイルと`all-systems-master-copy`ファイルに、正しいホストが含まれていることを確認します。
4. バックアップしたいシステムのみが含まれるよう、`all-systems`ファイルを編集します。`all-systems-master-copy`ファイルを参照しながら、`all-systems`ファイルをエディタ(`vi`など)で開き、バックアップしたいシステムのみを含むように変更します。バックアップしないホストはコメントアウトすることを推奨します(バックアップしないホストの行の先頭にシャープ記号(`#`)を追加)。次の例では、10.6.6 Security Analyticsサーバをコメントアウトしています。
`loghybrid,loghyb,172.16.0.1,45fe9de1-1a82-49d7-9bb1-7ac5fa1d18d8,10.6.6.0`
`#nwserver,nwserver106,172.31.255.23,67a9a0eb-1300-4fba-838f-`
`7be4d8cf5e65,10.6.6.0`

注: `vi`を使用する場合は、`all-systems`ファイルへのパスを必ず指定してください。

`all-systems-master-copy`ファイルの例を以下に示します。

```
nwserver,my-nw-server,10.0.0.1,af922b9f-cd61-49cd-afdc-a48e558cec3e,10.6.6.0
archiver,my-nw-archiver,10.0.0.2,a65c1236-5e46-4117-8529-8ea837074bd0,10.6.6.0
concentrator,my-nw-concentrator,10.0.0.3,dc620e94-bcf5-4d51-83fe-
c003cdfcd7a6,10.6.6.0
esa,my-nw-esa,10.0.0.4,8b608c0d-a7f9-40c0-baee-8407dec774ab,10.6.6.0
logdecoder,my-nw-logdecoder,10.0.0.5,c8be5d45-e19e-4a8d-90ce-
1cb2fe60077a,10.6.6.0
malwareanalysis,my-nw-malwareanalysis,10.0.0.6,2edc9585-7081-48c3-8f8c-
e0d02aa0a2fd,10.6.6.0
packetdecoder,my-nw-packetdecoder,10.0.0.7,a8f2f574-3dd0-4b65-9cf7-
d8141b78a192,10.6.6.0
vlc,my-nw-vlc,10.0.0.8,3ffefc4e-0b31-4951-bb77-dea5869fa98c,10.6.6.0
broker,my-nw-broker,10.0.0.9,0b65e7ce-61d5-4177-9647-c56ccfb0f737,10.6.6.0
```

以下は、最初のバックアップセッションで使用する`all-systems`ファイルの例で、Security Analyticsサーバ、ESAホスト、Malware Analysisホストのみがバックアップされます。

```
nwserver,my-nw-server,10.0.0.1,af922b9f-cd61-49cd-afdc-a48e558cec3e,10.6.6.0
#archiver,my-nw-archiver,10.0.0.2,a65c1236-5e46-4117-8529-
8ea837074bd0,10.6.6.0
#concentrator,my-nw-concentrator,10.0.0.3,dc620e94-bcf5-4d51-83fe-
c003cdfcd7a6,10.6.6.0
esa,my-nw-esa,10.0.0.4,8b608c0d-a7f9-40c0-baee-8407dec774ab,10.6.6.0
#logdecoder,my-nw-logdecoder,10.0.0.5,c8be5d45-e19e-4a8d-90ce-
1cb2fe60077a,10.6.6.0
malwareanalysis,my-nw-malwareanalysis,10.0.0.6,2edc9585-7081-48c3-8f8c-
e0d02aa0a2fd,10.6.6.0
#packetdecoder,my-nw-packetdecoder,10.0.0.7,a8f2f574-3dd0-4b65-9cf7-
d8141b78a192,10.6.6.0
#vlc,my-nw-vlc,10.0.0.8,3ffefc4e-0b31-4951-bb77-dea5869fa98c,10.6.6.0
#broker,my-nw-broker,10.0.0.9,0b65e7ce-61d5-4177-9647-c56ccfb0f737,10.6.6.0
```

トラブルシューティング情報

- `all-systems`ファイルと`all-systems-master-copy`ファイルのコピーを安全な場所に保存しておきます。以下の推奨事項に従ってください。

- `all-systems-master-copy`ファイルは編集しないでください。
- `all-systems`ファイルを複数バージョン作成する場合(複数のバックアップセッションを使用する場合など)、現在バックアップするホストのみをリストに追加し、その他のホストはコメントアウトするようにします。詳細については、「[バックアップ後のタスク](#)」を参照してください。
- `get-all-systems.sh`スクリプトを実行中にダウンしているホスト システムがある場合、スクリプトは、情報が見つからないホストのリストを作成します。スクリプトが完了し、`all-systems`ファイルが作成されたら、`all-systems`ファイルを手動で編集し、不足しているホストの情報を追加する必要があります。
- `get-all-systems.sh`スクリプトは、Security Analyticsユーザ インタフェースに定義されたホストのリストを生成します。すべてのホストとサービスが正常にシステムに追加されていることを確認します。正常にシステムに追加されていないホストやサービスがある場合、それらはバックアップされません。RSAでは、ホストおよびサービスをSecurity Analyticsシステムに追加するときには、正常に追加されるよう、Security Analyticsユーザ インタフェースを使用して追加することを推奨しています。ただし、ユーザ インタフェースに定義されていないホストまたはサービスがある場合は、手動で`all-systems`ファイルに追加する必要があります。
- `get-all-systems.sh`スクリプトは、最後に、Security Analyticsサーバのリストに含まれるシステムと、必要な情報を取得できたシステムとの相違を確認します。情報を取得できないノードIDまたはシステム名のリストが表示された場合は、それらのシステムが存在すること、それらのサービスがすべて実行中であること、Security Analyticsサーバと正しく通信していることを確認します。(Windows Legacy CollectorまたはAWSクラウド Collectorは`all-systems`ファイルに追加されないため、不一致の原因となる可能性があります。これらは、手動で`all-systems`ファイルに追加しないでください。)
- `all-systems`ファイルの構文が正しくない場合、スクリプトは失敗します。たとえば、ホスト エントリーの前後に余分なスペースがある場合、スクリプトは失敗します。

タスク3: バックアップ ホストとターゲット ホストの間での認証の設定

RSAでは、`ssh-propagate.sh`スクリプトを実行し、バックアップ ホストとホスト システムの間のキー共有を自動化することを推奨します。

注: パスフレーズで保護されるSSHキーがある場合、`ssh-agent`を使用して時間を節約できます。詳細については、`ssh-agent`のマニュアル ページを参照してください。

次のタスクを実行して、バックアップ ホストとターゲット ホスト間の認証を設定します。

1. バックアップ用の外部ホスト システムで、次のコマンドを実行して`ssh-propagate.sh`スクリプトを実行可能にします。
`chmod u+x ssh-propagate.sh`
2. ルート ディレクトリで次のコマンドを実行します。<path-to-all-systems-file>は`all-systems`ファイルが保存されているディレクトリへのパスです。
`ssh-propagate.sh <path-to-all-systems-file>`
3. ホストごとに1回、パスワード入力を求められますが、バックアップ中に繰り返し入力する必要はありません。

タスク4: 特定のタイプのホストのバックアップ要件の確認

バックアップに使用する`all-systems`ファイルを作成した後、バックアップを実行する前に、ファイルに記載されたホストのいずれかに固有の要件がないか確認する必要があります。

すべてのホスト タイプ

すべてのホスト タイプで、次の手順を実行します。

1. Security Analyticsサーバ上で、カスタム証明書ファイルと他のすべてのCA(認証局)ファイルを `/root/customcerts` フォルダに配置し、これらの証明書ファイルが確実にバックアップされるようにします。このディレクトリに配置されているカスタム証明書ファイルは、アップグレード中に自動的にリストアされます。11.2へのアップグレード後、カスタム証明書ファイルは`/etc/pki/nw/trust/import`に配置されます。

CA証明書とキーは、特定のタイプのサーバまたはソフトウェアとの互換性を維持するため、OpenSSLを使用してさまざまな形式に変換できます。たとえば、Apacheで使用するPEMファイルをPFX(PKCS#12)ファイルに変換し、TomcatやIISで使用できます。ファイルを変換するには、SSHでSecurity Analyticsサーバに接続し、変換のタイプに応じて次のコマンドを実行します。

DERファイル(.crt .cer .der)をPEMに変換

```
openssl x509 -inform der -in certificate.cer -out certificate.pem
```

PEMファイルをDERに変換

```
openssl x509 -outform der -in certificate.pem -out certificate.der
```

PEM証明書ファイルと秘密キーをPKCS#12(.pfx .p12)に変換

```
openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -in certificate.crt -certfile CACert.crt
```

秘密キーと証明書を含むPKCS#12ファイル(.pfx .p12)をPEMに変換

```
openssl pkcs12 -in keyStore.pfx -out keyStore.pem -nodes
```

注: 次のパラメータをコマンドに追加します。
 -nocertsは、秘密キーのみを変換します。
 -nokeysは、証明書のみを変換します。

- CentOS 7に更新後にリストアするために、CentOS 6で行ったすべてのカスタム構成(例: ドライバのカスタマイズ)を手動で記録します。CentOS 6へのカスタム構成は、自動的にバックアップもリストアもされません。

MongoデータベースのあるESAホスト

デフォルトの10.6.x Mongoデータベースのパスワードはnetwitnessです。このパスワードを変更した場合、バックアップスクリプトの実行中にエラーが発生する可能性があります。バックアップでカスタムMongoデータベースパスワードを使用するか、または、パスワードをnetwitnessに戻してからnw-backup.shスクリプトを実行できます。

- Mongoデータベースパスワードがnetwitnessであるか、または変更されているかを確認します。
- 変更されている場合、netwitnessに戻すか、または変更されたパスワードを把握しておき、バックアップ中に入力できるようにします。

Decoder、Concentrator、Brokerホスト: データ収集と集計の停止

「すべてのホストタイプ」で説明するタスクに加え、Decoderホスト、Concentratorホスト、Brokerホストについては、バックアップするすべてのシステムでデータ収集と集計を停止します。手順については、「付録B: データ収集と集計の停止と再開」を参照してください。

LC(Log Collector) とVLC(Virtual Log Collector) : prepare-for-migrate.shの実行

注意: このタスクはログ収集を停止するため、収集できないイベントを最小限にするようアップグレードの直前に実行する必要があります。このガイドに記載されているバックアップとアップグレードのタスクに従って、このタスクを完了します。

前提条件

LCとVLCのアップグレードの準備をする前に、次の情報が必要です。

- LockboxがLCとVLCで初期化されている場合、Lockboxのパスワードを把握しておく必要があります。アップグレード後に、Lockboxを再構成する必要があります。
- RabbitMQのlogcollectorユーザのパスワードを設定した場合は、アップグレード後に再度設定するためにパスワードを把握しておく必要があります。

アップグレードのためのLCとVLCの準備

次のタスクを実行して、アップグレードするLog CollectorとVirtual Log Collectorを準備します。

- Log CollectorにSSHでログインします。
- 次のコマンドを実行します。

```
# /opt/rsa/nwlogcollector/nwtools/prepare-for-migrate.sh --prepare
```

このコマンドは次の処理を行います。

- Puppet Agentサービスを停止します。
- Log Collectorにログ ファイルをアップロードするために使用するファイル収集アカウント(「sftp」ユーザと「upload」グループのすべてのユーザ)を無効化します。ログ ファイルは、Log Collectorが11.2にアップグレードされるまで、イベント ソースに蓄積されます。
- Log Collectorサービス上ですべての収集プロトコルを停止します。
- プラグイン アカウントとRabbitMQアカウント のリストを保存します。
- 新しいイベントが発行されないよう、RabbitMQサーバを構成します。シヨベルやLog Decoder Event Processorなどの、キューに溜まったイベントのconsumerは、動作を継続します。
- Log Collectorのキューが空になるまで待機します。
- Log Collectorサービスを停止します。
- Log Collectorが正常にアップグレード の準備ができたことを示すマーカー ファイルを作成します。

トラブルシューティング情報

prepare-for-migrate.sh スクリプトは、次の処理を行います。

- 情報、警告、エラー メッセージをコンソールに送信します。
- セッション ログを/var/log/backup/ ディレクトリに保存します。

次のエラーが発生した場合は、エラーを修正し、準備を再開する必要があります。支援が必要な場合は、RSAカスタマー サポートにお問い合わせください。

- Log Collectorのキューにイベントが残っているのに、Consumerが見つからない。
- Puppet Agentサービスを停止できない。
- Log Collectorサービスの収集プロトコルを停止できない。
- RabbitMQサーバへのイベント公開をブロックできない。
- キューに登録されたイベントを処理できないか、処理に時間がかかりすぎている。スクリプトはイベントの処理の完了確認を30回まで試行します。毎回の試行の後、30秒間スリープします。
- Log Collectorサービスを停止できない。

トラブルシューティングの詳細については、「付録A:トラブルシューティング」を参照してください。

Web Threat Detectionとの統合、Archer Cyber Incident & Breach ResponseまたはNetWitness Endpointとの統合 : RabbitMQユーザ名 とパスワードの一覧表示

11.2.へのアップグレード後にRabbitMQのユーザアカウントをリストアできるように、10.6.6.xのSecurity Analyticsサーバホストで、RabbitMQのすべてのユーザ名とパスワードのリストを取得する必要があります。

RabbitMQのユーザ名とパスワードのリストを取得するには、次のコマンドを実行します。

```
rabbitmqctl list_users >> /root/rabbitmq_users.txt
```

RabbitMQのユーザアカウントをリストアするには、「アップグレード後のタスク」の「タスク2: Web Threat Detection、NetWitness SecOps ManagerまたはNetWitness Endpointとの統合のためのSSL相互認証の構成」を参照してください。

Bluecoat イベント ソース

Bluecoat ProxySG イベント ソースでは、FTPS プロトコルを使用して、ログ ファイルを LC (Log Collector) および VLC (Virtual Log Collector) にアップロードします。イベント ソースに関するドキュメントには、LC および VLC 上で VSFTPD サービスを構成する手順が記載されています。

- キー要素が `10.6.6.x` の `/root/vsftpd/` ディレクトリに存在する場合、バックアップおよびリストアされます。キー要素が別の場所にある場合、手動でバックアップおよびリストアする必要があります。
- `/etc/vsftpd/vsftpd.conf` ファイルが `10.6.6.x` に存在する場合、ファイルはバックアップおよびリストアされます。

タスク5: バックアップ用のディスク容量のチェック

「[テスト オプション](#)」に記載されている `-t` オプションを指定してバックアップ スクリプトを実行すると、バックアップに必要なディスク容量を確認できます。スクリプトは、実際にファイルをバックアップしたり、すべてのサービスを停止することなく実行できます。RSA では、すべてのデータを収集できるように、この手順を実行してバックアップ用に十分なディスク容量があることを確認することを推奨します。

次のタスクを実行して、十分なディスク容量があることを確認します。

1. 次のコマンドを実行して、バックアップ スクリプトを実行可能にします。

```
chmod u+x nw-backup.sh
```

2. ルート ディレクトリレベルで次のコマンドを実行します。

```
./nw-backup.sh -t
```

出力には、バックアップに必要なディスク容量が表示されます。

注: デフォルトでは、`./nw-backup.sh -t` コマンドは `-d` オプションで実行されます。ただし、より正確なディスク容量を知りたい場合は、`-D` を指定し、`-d` オプションを上書きできます。`-D` オプションを指定すると、バックアップに必要なディスク容量がホストごとに表示されます。ただし、現在使用可能なディスク容量は表示されません。使用可能な容量が足りない場合、`-D` オプションはエラーを返します。外部ホスト上の使用可能な容量を知りたい場合は、`df -h` コマンドを実行します。

次の図は、`-t` オプションを使用した出力の例を示しています。

```

***** NW-BACKUP SCRIPT - TEST MODE *****
* * RSA nw-backup script is running in test mode where in it will only verify the disk space required for successful backup.
-----
CONTENT options currently selected:
-----
Backup IPDB? 'no' Backup Yum Repo? 'no'
Backup Malware Analysis repository? 'no' Backup SA Colo MA? 'no'
Backup Reporting Engine repository? 'no' Backup /var/log? 'no'
Backup ESA DB? 'yes' Backup Context Hub? 'yes'
Backup SMS RRD? 'yes'
-----
Checking that the environment is configured for proper execution of script...
Backup path configured... [ OK ] Backup path has been set to /var/netwitness/database/nw-backup
Backup path existence... [ OK ]
Check for all-systems file... [ OK ]
Dated backup dir... [ OK ] Backup directory: /var/netwitness/database/nw-backup/2017-09-18
Logging to /var/netwitness/database/nw-backup/rsa-nw-backup-2017-09-18.log

Testing SSH connectivity to saserver
SSH connectivity... [ OK ]
Calculating size of backup for saserver
Disk space required for saserver backup is 1.91GB
Check Backup Storage Space @ lab-cos6-RF:/var/netwitness/database/nw-backup
Space Required 1.91GB vs. Space Available 11.66GB
Backup Storage Space... [ OK ]
Total Execution Time : 0 d 0 h 0 m 19 s

Disk space check test completed with no errors.
[root@lab-cos6-RF ~]# █

```

タスク6: ホスト システムのバックアップ

バックアップ スクリプトを実行して実際にバックアップする前に、十分なディスク容量があることを確認します。ホストをバックアップするには、`-u` オプションを指定して `nw-backup.sh` スクリプトを実行します。このオプションは、11.2へのアップグレードに必須です。

注: スクリプトは、実行時にサービスを停止します。ただし、必要な場合は、スクリプトを実行する前に手動でサービスを停止できます。

バックアップ スクリプトの実行時に、次のセクションで説明するオプションを指定できます。

使用方法

```
./nw-backup.sh [-u -t -d -D -l -x -e] <external-mnt> -b <backup file path>
```

一般オプション

`-u` : This option is required for upgrading to 11.2. Enables the upgrade flag to run backup for upgrading to 11.2. It also enables disk space check (`-d`), backing up reporting engine reports (`-r`) and stores backup content locally (`-l`). Default: (no)

`-d` : enables disk space check in 'fast' mode (quick estimate of space using uncompressed data). Default: (no)

`-D` : enables disk space check in 'full' mode (estimate of space using compressed data, ~10X slower). Default: (no)

`-l` : stores backup content locally on each host (automatically set if `-u` is used). Default: (no)

`-e` <path to mount point> : copies backup files of all devices onto an external mount point. Default: (/mnt/external_backup)

`-x` : move all backup files to an external mount point. Default: (no) - COPY

-b <path to write backups> : path to the location for storing backup files on a backup server. For upgrading to 11.2, please use the default location!
Default: (/var/netwitness/database/nw-backup)

注: アップグレード (-u) モードでは、バックアップ パスを変更しないでください。

注: -u オプションでバックアップを実行すると、すべてのサービスが停止します。バックアップの実行後も引き続き10.6.xマシンを使用する必要がある場合は、10.6.xホストをリブートし、サービスを再起動します。

詳細なコンテンツ選択オプション

-c : back up Colocated Malware Analysis on SA servers. Default: (no)
-i : back up IPDB data (/var/netwitness/ipdbextractor). Default: (no)
-m : back up Malware Analysis File Repository. Default: (no)
-r : back up Reporting Engine Report Repository (automatically set if -u is used). Default: (no)
-v : back up system logs (/var/log). Default: (no)
-y : back up YUM Web Server & RPM Repository. Default: (no)
-S : If set: DISABLES back up of SMS RRD files. Default: (not-set)
-C : If set: DISABLES back up of Context-Hub configuration and database. Default: (not-set)
-E : If set: DISABLES back up of ESA Mongo database. Default: (not-set)

テスト オプション

-t : performs script test run for disk space check only. Services are not stopped and excludes execution of backup. Can be combined with (-d) or (-D) and other flags. Default: (-t)

コマンドの例:

```
./nw-backup.sh
```

このコマンドは、スクリプト自身のヘッダーに設定されているオプションを使用してバックアップを実行します。

コマンドの例:

```
./nw-backup.sh -ue /mnt/external_backup
```

このコマンドは、スクリプトに指定したバックアップパスを使用し、次のオプションを使用して通常のバックアップを実行します。

-u : enables the upgrade flag to run backup for upgrading to 11.2. It also enables disk space check (-d), backing up reporting engine reports (-r) and stores backup content locally (-l). Default: (no)

-e : Copy the backup files to external mount point, mounted on /mnt/external_backup

For Help: ./nw-backup.sh -h

スクリプトの実行時に、次のテキストがスクリプトの上部に表示されます。

注意: RSA `nw-backup` スクリプトは、スクリプトに指定されたオプションに基づいて、構成ファイル、データ、およびログをバックアップします。バックアップ ファイルをバックアップ サーバに保存したり、マウント ポイント (USB/NFS/SMB) 上の外部ストレージに移動またはコピーしたり、ターゲット ホストに安全にコピーするためのオプションを使用して、コンテンツを作成します。

このバックアップ スクリプトは、次のバージョンの Security Analytics で検証されています。

10.6.6.x

このスクリプトを他のバージョンで使用した場合、想定した結果が得られない可能性があります。また、RSA カスタマー サポートではサポートできない可能性があります。

注: RSA が提供していないすべてのカスタム ファイル、スクリプト、cron ジョブ、およびその他の重要なファイルをバックアップに含めるには、`/root`、`/home/'user'`、または `/etc` に配置する必要があります。

ホストをバックアップするには、次のタスクを実行します。

1. `all-systems` ファイルにバックアップするホストのみが含まれていることを確認します。詳細については、「[タスク2: バックアップするホストのリストの作成](#)」を参照してください。
2. 次のコマンドを実行して、バックアップ スクリプトを実行可能にします。
`chmod u+x nw-backup.sh`
3. ルート ディレクトリレベルで次のコマンドを実行して、バックアップ プロセスを開始します。
`./nw-backup.sh -u`

注: 11.2 へのアップグレード中にファイルが正しくリストアップされるよう、`-u` オプションを使用する必要があります。アップグレードでは規定のパスを使用し、規定の場所にデータを格納する必要があるため、バックアップ スクリプトのヘッダーでバックアップ パスを変更しないでください。

「Backup completed with no errors」が表示されれば、バックアップは正常に完了しています。

次のような名前のログ ファイルがバックアップ ディレクトリに作成され、バックアップされたファイルに関する情報が提供されます。

`rsa-nw-backup-2018-03-15.log`

4. バックアップが完了したら、目的のファイルがバックアップされたことを確認するために、次のコマンドを実行してバックアップされたすべてのファイルのリストを参照します。

`tar -tzvf hostname-ip-address-backup.tar.gz`

次のアーカイブ ファイルが作成されます。

すべてのホスト:

<hostname-IPaddress>-root.tar.gz

<hostname-IPaddress>-backup.tar.gz

tar checksum **ファイル**

<hostname-IPaddress>-network.info.txt

Security Analytics サーバ:

<hostname-IPaddress>-root.tar.gz

<hostname-IPaddress>-backup.tar.gz

<hostname-IPaddress>-mongodb.tar.gz

tar checksum **ファイル**

<hostname-IPaddress>-network.info.txt

ESA ホスト:

<hostname-IPaddress>-root.tar.gz

<hostname-IPaddress>-backup.tar.gz

<hostname-IPaddress>-mongodb.tar.gz

```
<hostname-IPaddress>-controldata-mongodb.tar.gz
tar checksumファイル
<hostname-IPaddress>-network.info.txt
```

アーカイブされたファイルは、/var/netwitness/database/nw-backupディレクトリに保存されます。tarファイルのいずれかが予想よりも小さい場合は、ファイルを開いて正しくバックアップされているか確認します。

バックアップ後のタスク

タスク1: all-systemsファイルとバックアップtarファイルのコピーの保存

all-systemsファイル、all-systems-master-copyファイル、バックアップtarファイルのコピーを作成し、コピーを安全な場所に保存します。Security Analyticsサーバ(具体的には、Adminサービス)を11.2にアップグレードした後は、これらのファイルは再生成できません。

タスク2: 必要なバックアップファイルの生成の確認

バックアップスクリプトを実行した後、いくつかのファイルが生成されます。これらのファイルは、11.2へのアップグレードに必要です。アップグレードを開始する前に、アップグレードするホスト上に必要なバックアップファイルを配置する必要があります。

バックアップスクリプトによって、すべてのホストに次のファイルが生成されます。

- all-systems
- all-systems-master-copy
- appliance_info
- service_info
- <hostname>-<host-IP-address>-backup.tar.gz
- <hostname>-<host-IP-address>-backup.tar.gz.sha256
- <hostname>-<host-IP-address>-root.tar.gz
- <hostname>-<host-IP-address>-root.tar.gz.sha256
- <hostname>-<host-IP-address>-network.info.txt

上記のファイルに加えて、Security AnalyticsサーバホストとESAホストには次のファイルが生成されません。

- <hostname>-<host IP address>-mongodb.tar.gz
- <hostname>-<host IP address>-mongodb.tar.gz.sha256

バックアップスクリプトは、次の controldata-mongodb.tar.gzファイルも生成します。

注: バックアップスクリプトは、次のファイルを、すべてのESAホストからSecurity Analyticsサーバホストのバックアップパスにコピーします。

- <esa hostname>-<esa hostip>-controldata-mongodb.tar.gz
- <esa hostname>-<esa hostip>-controldata-mongodb.tar.gz.sha256

タスク3: (オプション) 複数のESAホストがある場合は、mongodb tar ファイルをESAプライマリホストにコピー

導入環境に複数のESAホストがある場合、次の2つのファイルを、各ESAホストからESAプライマリホスト (Context Hubサービスが実行されているホスト) の/opt/rsa/database/nw-backup/ディレクトリにコピーします。

- <hostname>-<host-IP-address>-mongodb.tar.gz
- <hostname>-<host-IP-address>-mongodb.tar.gz.sha256

タスク4: 必要なすべてのバックアップファイルが各ホスト上にあることを確認

11.2にアップグレードする前に、アップグレードするホストに、次のリストに示すファイルが存在することを確認します。

注: バックアップファイルのデフォルトパスは次の通りです。

- Security Analyticsサーバ: /var/netwitness/database/nw-backup
- ESAホスト: /opt/rsa/database/nw-backup
- Malwareホスト: /var/lib/rsamalware/nw-backup

NetWitness Serverに必要なファイル

- all-systems-master-copy
- <hostname>-<host-IP-address>-backup.tar.gz
- <hostname>-<host-IP-address>-backup.tar.gz.sha256
- <hostname>-<host-IP-address>-root.tar.gz
- <hostname>-<host-IP-address>-root.tar.gz.sha256
- <hostname>-<host-IP-address>-network.info.txt
- <hostname>-<host-IP-address>-mongodb.tar.gz
- <hostname>-<host-IP-address>-mongodb.tar.gz.sha256
- <esa-hostname>-<esa-host-IP-address>-controldata-mongodb.tar.gz
- <esa-hostname>-<esa-host-IP-address>-controldata-mongodb.tar.gz.sha256

ESAホストに必要なファイル

- all-systems-master-copy
- <hostname>-<host-IP-address>-backup.tar.gz
- <hostname>-<host-IP-address>-backup.tar.gz.sha256
- <hostname>-<host-IP-address>-root.tar.gz

- <hostname>-<host-IP-address>-root.tar.gz.sha256
- <hostname>-<host-IP-address>-network.info.txt
- <hostname>-<host-IP-address>-mongodb.tar.gz
- <hostname>-<host-IP-address>-mongodb.tar.gz.sha256

その他のすべてのホストに必要なファイル

- all-systems-master-copy
- <hostname>-<host-IP-address>-backup.tar.gz
- <hostname>-<host-IP-address>-backup.tar.gz.sha256
- <hostname>-<host-IP-address>-root.tar.gz
- <hostname>-<host-IP-address>-root.tar.gz.sha256
- <hostname>-<host-IP-address>-network.info.txt

注: 次のファイルは、すべてのホストの<hostname>-<host-IP-address>-backup.tar.gz tarに含まれます。

```
appliance_info  
service_info
```

注: iptable、NAT構成、ユーザアカウント、crontabエントリーのバックアップファイルとリストアファイルの場所は、次のとおりです。

バックアップパス:

BUPATH=/opt/rsa/database/nw-backup(ESA関連エンジン)

BUPATH=/var/lib/rsamalware/nw-backup(マルウェア サービス)

BUPATH=/var/netwitness/database/nw-backup(その他のすべてのサービス)

リストアの場所:

BUPATH/restore/etc/sysconfig(iptableルール)

BUPATH/restore/etc/sysconfig(NAT構成)

BUPATH/restore/etc(crontabエントリー)

BUPATH/restore/etc(ユーザアカウント。ユーザは passwdファイルに存在し、グループはgroupファイルに存在します。これらはアップグレード プロセスではリストアされませんが、手動でリストアできます)。

BUPATH/restore/etc/ntp.conf(NTP構成。NetWitness Platform UIを使用してリストアする必要があります)

アップグレード タスク

このトピックでは、Security Analyticsバージョン10.6.6.xをNetWitness Platform 11.2にアップグレードするために必要なタスクについて説明します。

注意: 1.) NetWitness Platform 11.2へのアップグレードを開始する前に、Security Analytics 10.6.6.xデータをバックアップしたことを確認します。
2.) 古いデータのリストアを避けるため、各フェーズのホストをアップグレードする直前に、バックアップを実行します。
3.) このガイドは、物理ホストのアップグレードにのみ適用されます。導入環境に物理ホストと仮想ホストがある場合、仮想ホストをアップグレードする手順については、『RSA NetWitness® Platform 11.2 仮想ホスト アップグレード ガイド』を参照してください。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

次の2つのフェーズを順番に実行します。

- **フェーズ1: SA Server、ESA(Event Stream Analysis)、Malware Analysisホストのアップグレード**

注: 10.6.6.xのEvent Stream AnalysisでC2モジュールを有効化していた場合、Event Stream Analysisサービスを11.2にアップグレードすると、C2モジュールがウォームアップを始め、ウォームアップが完了するまで使用できなくなります。

- **フェーズ2: その他すべてのホストのアップグレード**

フェーズ1: SA Server、Event Stream Analysis、Malware Analysisホスト、BrokerまたはConcentratorのアップグレード

タスク1: 10.6.6.x SA Serverの11.2 NW Serverへのアップグレード

「[10.6.6.x SA Serverホストの11.2 NW Serverホストへのアップグレード](#)」の手順に従います。

タスク2: 10.6.6.x ESAの11.2へのアップグレード

注意: 10.6.6.xでC2モジュールを有効化していた場合、Event Stream Analysisサービスを11.2にアップグレードすると、C2モジュールがウォームアップを始め、ウォームアップが完了するまで使用できなくなります。

「[10.6.6.x 非SA Serverホストの11.2へのアップグレード](#)」の手順に従い、ESAホストをアップグレードします。10.6.6.x ESAを11.2にアップグレードする場合は、次の手順を実行します。

1. プライマリESAホストにベースイメージを作成し、セットアッププログラムを実行してセットアップし、ユーザインタフェースの[管理]>[ホスト]ビューを使用して、ホスト上にESAプライマリをインストールします。

注: 導入環境に複数のESAホストがある場合は、ESAセカンダリホストをアップグレードする前に、ESAプライマリホストを最初にアップグレードする必要があります。プライマリホストにはすべてのmongodb(MongoDBデータベース) のバックアップのtarファイルが保存されています。

2. (オプション) ESAセカンダリホストがある場合、ESAセカンダリホストにベースイメージを作成し、セットアッププログラムを実行してセットアップし、ユーザインタフェースの[管理]>[ホスト]ビューを使用して、ホスト上にESAセカンダリをインストールします。

タスク3: 10.6.6.x Malware Analysisの11.2へのアップグレード

「10.6.6.x 非SA Serverホストの11.2へのアップグレード」の手順に従います。

タスク4: 10.6.6.x Brokerまたは10.6.6.x Concentratorの11.2へのアップグレード

「10.6.6.x 非SA Serverホストの11.2へのアップグレード」の手順に従います。

注: Brokerがない場合は、Concentratorホストをアップグレードします。11.2 NW Serverの新しいInvestigate機能は10.6.6.xコア サービスと通信できません。このため、フェーズ1でBrokerまたはConcentratorのホストをアップグレードする必要があります。

フェーズ2: その他すべてのホストのアップグレード

Decoder、Concentrator、Log Collectorのホストをアップグレードする場合の、データ収集および集計の停止と再開の手順については、「[付録B: データ収集と集計の停止と再開](#)」を参照してください。

DecoderホストおよびConcentratorホスト

1. データ収集と集計を停止します。
2. 「[非NW Serverホストの11.2へのアップグレード](#)」の手順を実行します。
3. データ収集と集計を再開します。

Log Decoderホスト

1. Log Collectorの準備が完了したことを確認します。「[バックアップ手順](#)」の「LC(Log Collector)とVLC(Virtual Log Collector): prepare-for-migrate.shの実行」を参照してください。
2. Log Decoder上でデータ収集を停止します。
3. 「[非NW Serverホストの11.2へのアップグレード](#)」の手順を実行します。
4. Log Decoder上でデータ収集を再開します。

注: アップグレードした後、ログ収集を再開する前に、アップグレード後のタスクの、[タスク29: アップグレード準備タスクで特定した一致条件で「Domain」を使用するインシデント ルールの更新](#)」を完了します。

Virtual Log Collectorホスト

1. Virtual Log Collectorの準備が完了したことを確認します。「[バックアップ手順](#)」の「LC(Log Collector)とVLC(Virtual Log Collector): prepare-for-migrate.shの実行」を参照してください。
2. バックアップを実行するホストでall-systemsファイルを編集し、10.6.6.x VLCをバックアップします。

- a. このステップを実行する前に、all-systemsファイルの内容に、次の情報が含まれていることを確認します。


```
vlc, <host-name>, <IP-address>, <UUID>, 10.6.6.x
```
- b. 次のコマンドを実行して、バックアップを作成します。


```
./nw-backup.sh -u
```

 ホストをバックアップする詳細な手順については、「[バックアップ手順](#)」を参照してください。
3. バックアップ ホストに、次の形式で、VLCのバックアップが作成されていることを確認します。


```
<hostname>-<IPaddress>-root.tar.gz
<hostname>-<IPaddress>-root.tar.gz.sha256
<hostname>-<IPaddress>-backup.tar.gz
<hostname>-<IPaddress>-backup.tar.gz.sha256
<hostname-IPaddress>-network.info.txt
all-systems-master-copy
```
4. 新しい11.2仮想マシンが同じネットワーク構成を使用できるように、10.6.6.x VLCをパワーオフします。
5. 11.2 NetWitness Platform ovaを使用して、NetWitness 11.2の非NW Serverホストを新規に導入します。
6. 新しいVLCの仮想マシンのコンソールに接続します。
7. 10.6.6.x VLCと同じになるように、ネットワーク構成を更新します。
この情報は、10.6.6.x VLCバックアップの<hostname-IPaddress>-network.info.txt ファイルに保存されています。

注: IPv6が無効化されていることを確認します。

- a. /etc/sysconfig/network-scripts/ifcfg-eth0ファイルを編集し、設定を更新します。
ifcfg-eth0 の内容を次のように編集する必要があります。


```
TYPE=Ethernet
DEFROUTE=yes
NAME=eth0
UUID=<uuid>
DEVICE=eth0
DNS1=<nameserver from <hostname>-<ipaddress>-network-info.txt>
DNS2=<nameserver from <hostname>-<ipaddress>-network-info.txt>
BOOTPROTO=static
IPADDR=<ipaddress from <hostname>-<ipaddress>-network-info.txt>
NETMASK=<netmask from <hostname>-<ipaddress>-network-info.txt>
GATEWAY=<gateway from <hostname>-<ipaddress>-network-info.txt>
NM_CONTROLLED=no
ONBOOT=yes
```
- b. 次のコマンドを実行します。


```
systemctl restart network.service
```
8. バックアップ ディレクトリを作成します。


```
# mkdir -p /var/netwitness/database/nw-backup/
```


9. バックアップ ホストの/var/netwitness/database/nw-backupから新しいVLCの/var/netwitness/database/nw-backupディレクトリに、バックアップをコピーします。
10. 「[10.6.6.x 非SA Serverホストの11.2へのアップグレード](#)」のステップ2～12を実行します。ステップ12では、サービスとしてLog Collectorを選択します。

他のすべての10.6.6.xホストを11.2にする

「[10.6.6.x 非SA Serverホストの11.2へのアップグレード](#)」の手順に従います。

10.6.6.x SA Serverホストを11.2 NW Serverホストにアップグレード

SA Serverホストの10.6.6.xデータを必ずバックアップします。ホストをバックアップするには、「[バックアップ手順](#)」の手順に従う必要があります。

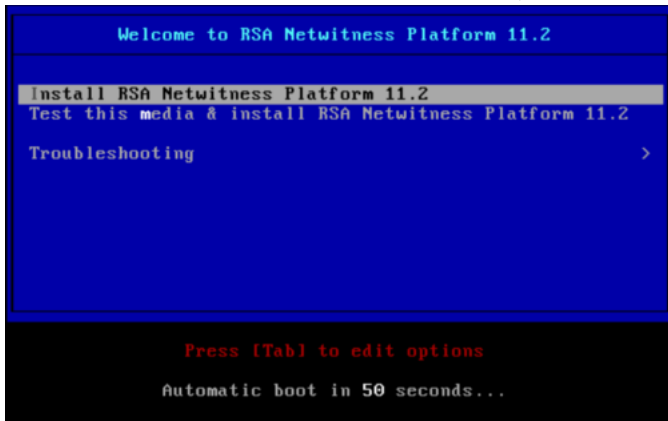
注意: データができる限り最新になるよう、SA Serverを11.2にアップグレードする直前にバックアップを実行してください。SA Serverをアップグレードする前にall-systemsファイルを作成する必要があります。このファイルは、SA Serverが11.2にアップグレードされた後は作成できません。

10.6.6.x SA Serverホストを11.2 NW Serverホストにアップグレードするには、次の手順を実行します。

1. ホストで、ベース イメージを作成します。
 - a. ホストにメディア(ビルド スティックなどISOファイルを含むメディア)を接続します。**「OEMDRV」というラベルのビルド スティックを使用する必要があります。**詳細については、「[RSA NetWitness Platformビルド スティックの作成手順](#)」を参照してください。
 - ハイパーバイザーのインストール: ISOイメージを使用します。
 - 物理メディア: ISOファイルを使用し、Universal Netboot Installer(UNetbootin)または他の適切なイメージングツールを使用して起動可能なフラッシュドライブ メディアを作成します。ISOファイルからビルド スティックを作成する方法の詳細については、「[RSA NetWitness® Platformビルド スティックの作成手順](#)」を参照してください。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。
 - iDRACのインストール: 仮想メディア タイプは、次の通りです。
 - 仮想フロッピー(フラッシュドライブをマッピングする場合)。
 - 仮想CD(光学メディア デバイスまたはISOファイルをマッピングする場合)。
 - b. ホストにログインし、リブートします。

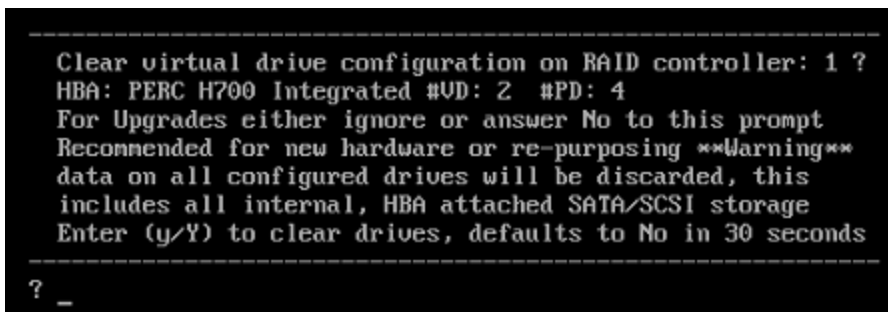
```
login: root
Password:
Last login: Tue Sep 19 13:27:15 on tty1
[root@saserver ~]# reboot
```
 - c. 再起動中にF11(起動メニュー)を選択し、ブート デバイスを選択して、接続されているメディアから起動します。起動時のシステム チェックの後、[Welcome to RSA NetWitness® Platform 11.2]インストールメニューが表示されます。物理USBフラッシュメディアを使用する場合、メニュー画面の表示は多少異なります。

- d. [Install RSA Netwitness Platform 11.2] (デフォルトの選択) を選択し、Enterキーを押します。



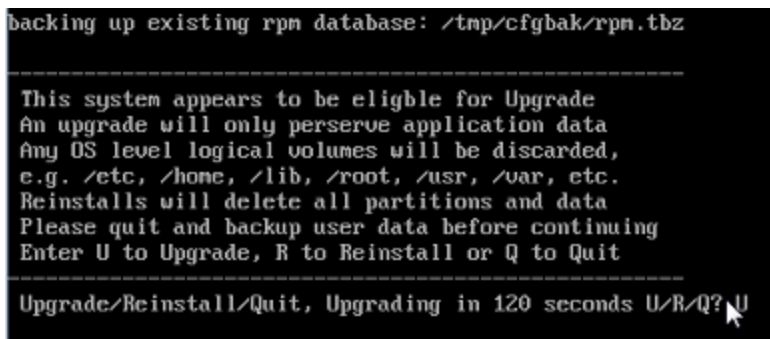
オペレーティングシステムのインストールが実行され、[Enter (y/Y) to clear drives] プロンプトで停止します。

- e. 「n」(No) を入力します。
デフォルトのアクションは「No」となっているため、プロンプトを無視すると、30秒後に「No」が選択され、ドライブはクリアされません。



[Upgrade/Reinstall/Quit(U/Q/R)?] プロンプトが表示されます。

- f. 「U」を入力すると、ホストをアップグレードします。
メッセージを無視した場合は、120秒後に「U」が選択されます。



CentOS7コンポーネントのインストールには数分かかります。インストールプログラムにより、インストール中のコンポーネントが表示されます。表示されるコンポーネントはアプライアンスによって異なります。CentOS7のインストールが完了すると、[Continue (Y/N)?] プロンプトが表示されます。

- g. 「Y」を入力し、Enterキーを押して、このホストをアップグレードすることを確認します。

```
-----
Steps to be executed listed below.  Warning:
this is irreversible.
-----
luremove -f /dev/VolGroup00/rabmq
luremove -f /dev/VolGroup00/root
luremove -f /dev/VolGroup00/swap
luremove -f /dev/VolGroup00/tmp
luremove -f /dev/VolGroup00/usrhome
luremove -f /dev/VolGroup00/var
luremove -f /dev/VolGroup00/vartmp
luremove -f /dev/napper/VolGroup01-uax
luremove -f /dev/napper/VolGroup01-rsasoc
ugrename VolGroup00 netwitness_ug00
ugchange -a n VolGroup01
ugmerge netwitness_ug00 VolGroup01
ugchange -a y netwitness_ug00
Continue (Y/N)? Y
```

[The old operating system is about to be removed. Continue (Y/N)?]の警告が表示されま
す。

- h. 「Y」を入力し、Enterキーを押して、オペレーティングシステムを更新することを確認します。

```
Warning: The old operating system is about to be removed. Continue (Y/N)?
```

ホストをCentOS7にアップグレードすると、ホストは自動的に再起動され、ログインプロンプトが表示されます。

注意: 接続されたメディア(ビルドスティックなどISOファイルを含むメディア)から再起動しないでください。

- i. root 認証情報を使用してホストにログオンします。

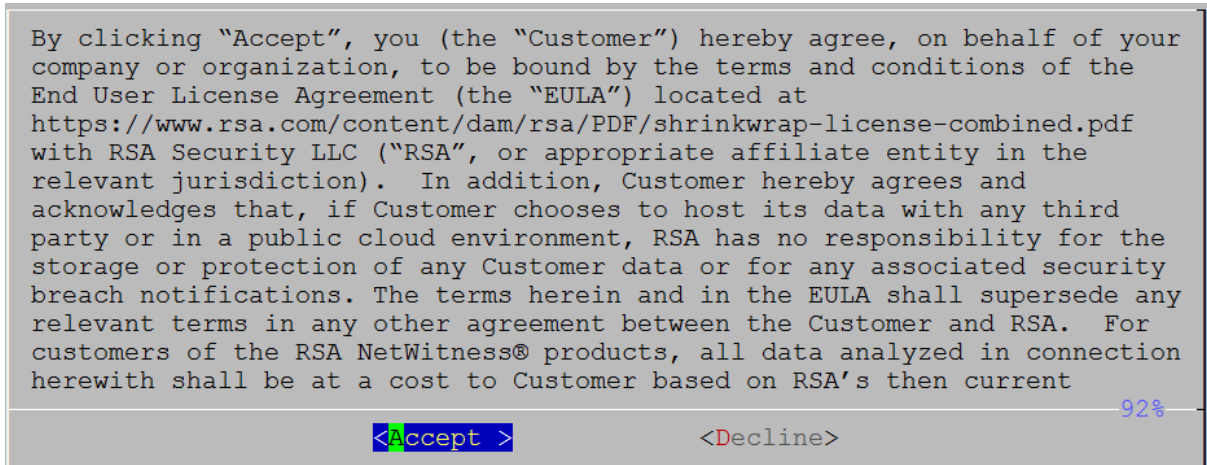
```
CentOS Linux 7 (Core)
Kernel 3.10.0-514.26.1.el7.x86_64 on an x86_64

NWAPPLIANCE9240 login: root
Password:
[root@NWAPPLIANCE9240 ~]#
```

2. nwsetup-tuiコマンドを実行し、ホストをセットアップします。
nwsetup-tui(セットアッププログラム)が開始され、EULAが表示されます。

注: 1.) セットアッププログラムのプロンプト間を移動する場合、フィールド間の移動には下向き矢印と上向き矢印を使用し、コマンド間(<Yes>、<No>、<OK>、<Cancel>など)の移動にはTabキーを使用します。コマンドの選択を確定し、次のプロンプトに移動するには、Enterキーを押します。
2.) セットアッププログラムは、ホストへのアクセスに使用中のデスクトップまたはコンソールのカラースキームを採用します。

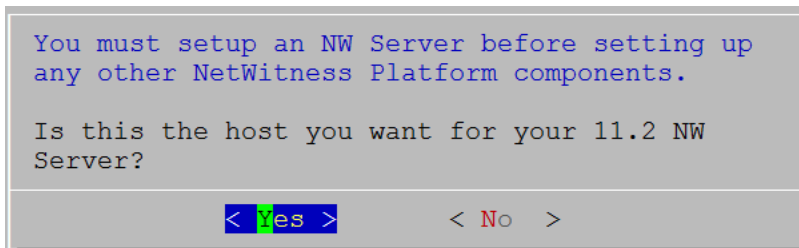
3. Tabキーで[Accept]に移動し、Enterキーを押します。



[Is this the host you want for your 11.2 NW Server]プロンプトが表示されます。

注意: NW Serverに間違ったホストを選択してアップグレードを完了した場合は、セットアッププログラムを再度実行し、すべてのステップ(ステップ2~11)を完了して誤りを修正する必要があります。

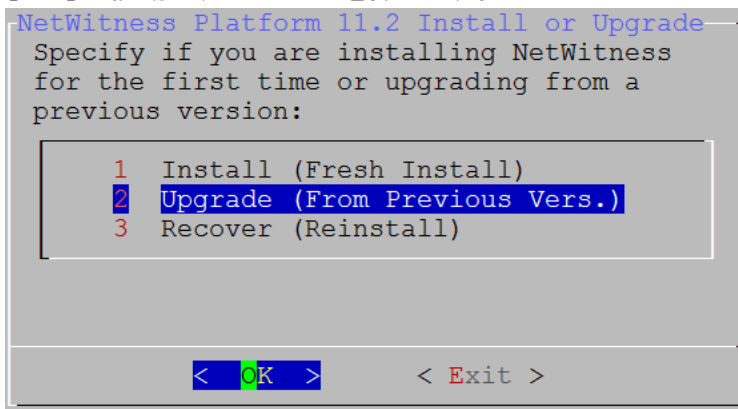
4. Tabキーで[Yes]に移動し、Enterキーを押します。



NW Serverをすでに11.2にアップグレードした場合は、[No]を選択します。

[Install or Upgrade]プロンプトが表示されます。

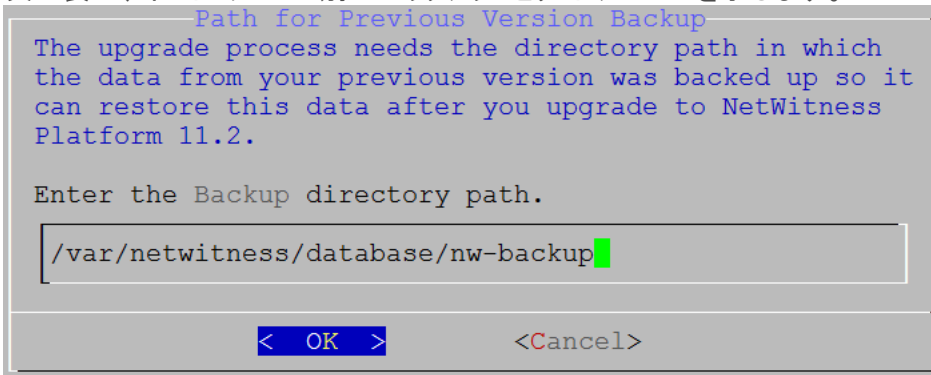
5. 下向き矢印を使用して、[2 Upgrade (From Previous Vers.)]を選択し、Tabキーを使用して[OK]に移動し、Enterキーを押します。



[Backup path]プロンプトが表示されます。

注意: 次のプロンプトのバックアップ パスは、バックアップを保存したパスと同じである必要があります。たとえば、バックアップ スクリプトはデフォルトのパスとして /var/netwitness/database/nw-backup を割り当てます。バックアップ時にデフォルトのバックアップ パスを使用し、その後変更しなかった場合は、次のプロンプトでも /var/netwitness/database/nw-backup を使用する必要があります。

6. 現在のパスを使用する場合は、Tabキーで[OK]に移動し、Enterキーを押します。変更する場合は、パスを編集して、Tabキーで[OK]に移動し、Enterキーを押します。次の表に、ホスト/サービス別のバックアップとリストアのパスを示します。



ホスト	バックアップ パス	リストア パス
Malware	/var/lib/rsamlware/nw-backup	/var/netwitness/malware_analytics_server/nw-backup/restore
Event Stream Analysis	/opt/rsa/database/nw-backup	/var/netwitness/database/nw-backup/restore
NW Server	/var/netwitness/database/nw-backup	/var/netwitness/restore
その他のすべてのホスト	/var/netwitness/database/nw-backup	/var/netwitness/database/nw-backup/restore

[Master Password]プロンプトが表示されます。

マスター パスワードと導入パスワードで使用可能な文字の一覧を、次に示します。

記号 ! @ # % ^ + ,
 数字 0 ~ 9
 小文字 a ~ z
 大文字 A ~ Z

マスター パスワードと導入パスワードでは、紛らわしい文字は使用できません。例：
 スペース { } [] () \ ' " ` ~ ; : . < > -

7. [Password]に入力し、下向き矢印で[Verify]に移動し、パスワードを再入力し、Tabキーで[OK]に移動し、Enterキーを押します。

Master Password

The master password is utilized to set the default password for both the system recovery account and the NetWitness UI "admin" account. The system recovery account password should be safely stored in case account recovery is needed. The NetWitness UI "admin" account password can be updated upon login.

Enter a Master Password.

Password

Verify

< OK > <Cancel>

「Deployment Password」プロンプトが表示されます。

8. [Password]に入力し、下向き矢印で[Verify]に移動し、パスワードを再入力し、Tabキーで[OK]に移動し、Enterキーを押します。

Deployment Password

The Deployment password is used when deploying NetWitness hosts. It needs to be safely stored and available when deploying additional hosts to your NetWitness Platform.

Enter a Deploy Password.

Password

Verify

< OK > <Cancel>

[Update Repository]プロンプトが表示されます。

9. 下向き矢印と上向き矢印を使用し、ホストに適用するバージョン更新を取得する場所を選択し、Tabキーを使用して[OK]へ移動し、Enterキーを押します。

NetWitness Platform Update Repository

The NetWitness Platform Update Repository contains all the RPMs needed to build and maintain all the NetWitness Platform components. All components managed by the NW Server need access to the Repository.

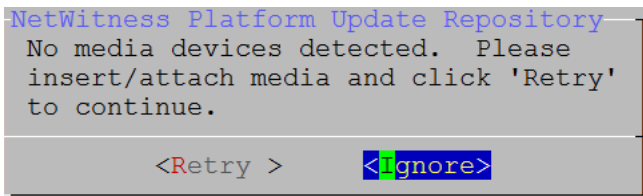
Do you want to set up the NetWitness Platform Update Repository on:

1 The Local Repo (on the NW Server)

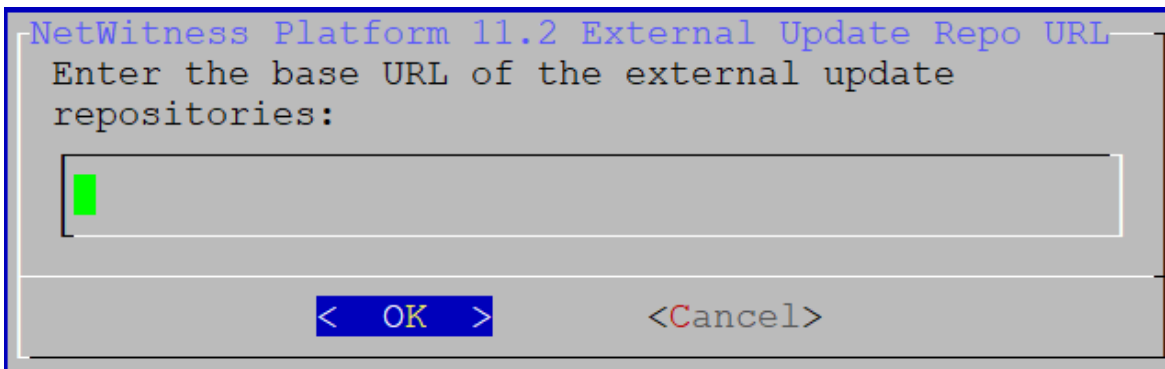
2 An External Repo (on an externally-managed server)

< OK > < Exit >

- セットアッププログラムで[1 The Local Repo (on the NW Server)]を選択する場合、NetWitness Platform 11.2へのアップグレード用の適切なメディア(ビルド スティックなどのISOファイルを含むメディア)が接続されていることを確認します。プログラムが接続メディアを見つけられない場合、次のプロンプトが表示されます。



- [2 An External Repo (on an externally-managed Server)]を選択する場合、URLを入力するプロンプトが表示されます。リポジトリにアクセスして、RSAの更新とCentOSの更新を取得します。「[付録D: 外部リポジトリの作成](#)」を参照して、リポジトリと外部リポジトリURLを作成し、次のプロンプトで入力します。



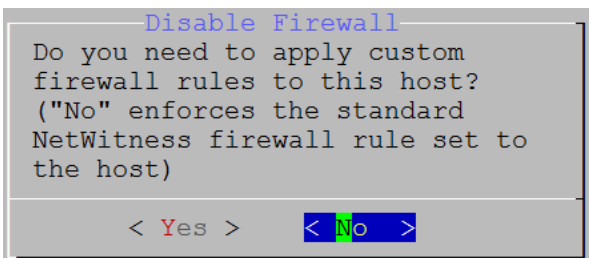
NetWitness Platform外部リポジトリのベースURLを入力し、[OK]をクリックします。

手順については、『*RSA NetWitness Platform*ホストおよびサービス スタート ガイド』の「ホストとサービスの手順」の「RSAおよびOS更新の外部リポジトリのセットアップ」を参照してください。

NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

標準的なファイアウォール構成を使用するか、無効化するかを選択するプロンプトが表示されます。

10. 標準的なファイアウォールの構成を使用するには、Tabキーを使用して[No]に移動し、Enterキーを押します。標準的なファイアウォールの構成を無効化するには、Tabキーを使用して[Yes]に移動し、Enterキーを押します。



- [Yes]を選択すると、選択内容が確定されます。

```
Warning: you chose to disable the default NetWitness
firewall configuration which means you must set up
firewall rules manually.

Select "Yes" to confirm that you will set up firewall
rules manually.

< Yes >      < No >
```

- [No]を選択すると、標準的なファイアウォールの構成が適用されます。

[Install or Upgrade]プロンプトが表示されます。(Recoverは選択できません。11.2の災害復旧用です。)

11. [1 Upgrade Now]を選択し、Tabキーを使用して[OK]に移動し、Enterキーを押します。

```
Start Install/Upgrade
All the required information has been gathered.

Select "1 Upgrade Now" to start the installation
on this host.

1 Upgrade Now
2 Restart

< OK >      < Exit >
```

「Installation complete」が表示されると、10.6.6.x SA Serverの11.2 NW Serverへのアップグレードは完了です。

注: nwsetup-tuiコマンドを開始するときに表示される、次のスクリーンショットに示すようなハッシュコードのエラーは無視します。Yumは、セキュリティ操作にMD5を使用しないため、システムセキュリティに影響することはありません。

```
ValueError: error:3207A06D:lib(50):B_HASH_init:cr new
Checksum type 'md5' disabled
(skipped due to only_if)
* file[/etc/yum.repos.d/CentOS-Base.repo] action delete (up to date)
* ruby_block[yum-cache-reload-CentOS-Base] action nothing (skipped due to action :nothing)
(up to date)
* yum_repository[Remove CentOS-CR repository] action delete
* execute[yum clean all CentOS-CR] action runERROR:root:code for hash md5 was not found.
Traceback (most recent call last):
File "/usr/lib64/python2.7/hashlib.py", line 129, in <module>
globals()[__func_name] = __get_hash(__func_name)
File "/usr/lib64/python2.7/hashlib.py", line 98, in __get_openssl_constructor
f(usedforsecurity=False)
```

12. 非SA Serverホストを11.2にアップグレードする前に、[NW Server](#)のアップグレード後のタスクを完了します。

10.6.6.x 非SA Serverホストの11.2へのアップグレード

ホストの10.6.6.xデータを必ずバックアップします。ホストをバックアップするには、「[バックアップ手順](#)」の手順に従う必要があります。

注意: データができる限り最新になるよう、ホストを11.2にアップグレードする直前にバックアップを実行してください。

10.6.6.x 非SA Serverホストを11.2にアップグレードするには、次の手順を実行します。

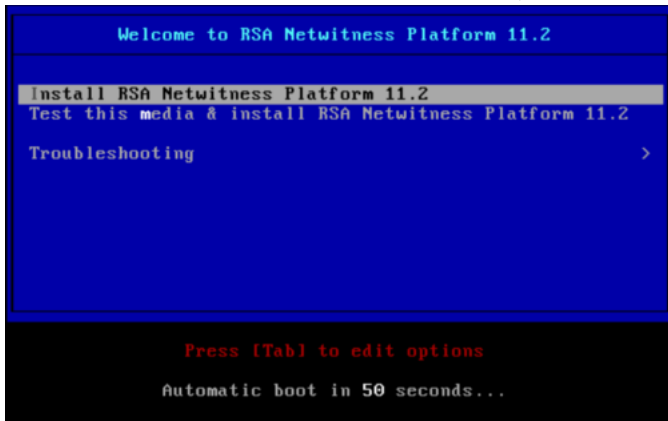
1. ホストで、ベースイメージを作成します。

- a. ホストにメディア(ビルド スティックなどISOファイルを含むメディア)を接続します。
詳細については、「[RSA NetWitness Platformビルド スティックの作成手順](#)」を参照してください。
 - ハイパーバイザーのインストール: ISOイメージを使用します。
 - 物理メディア: ISOを使用し、Universal Netboot Installer(UNetbootin) または他の適切なイメージングツールを使用して起動可能なフラッシュドライブメディアを作成します。ISOからビルド スティックを作成する方法の詳細については、「[RSA NetWitness® Platformビルド スティックの作成手順](#)」を参照してください。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。
 - iDRACのインストール: 仮想メディアタイプは、次の通りです。
 - 仮想フロッピー(フラッシュドライブをマッピングする場合)。
 - 仮想CD(光学メディア デバイスまたはISOファイルをマッピングする場合)。
- b. ホストにログインし、リブートします。

```
login: root
Password:
Last login: Tue Sep 19 13:27:15 on tty1
[root@saserver ~]# reboot
```

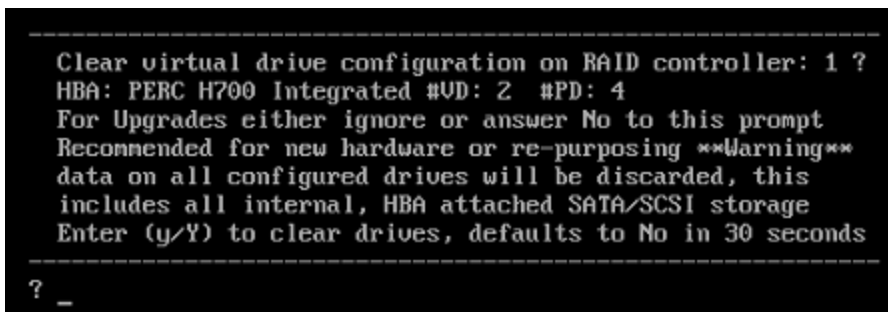
- c. 再起動中にF11(起動メニュー)を選択し、ブート デバイスを選択して、接続されているメディアから起動します。
起動時のシステムチェックの後、[Welcome to RSA NetWitness® Platform 11.2]インストールメニューが表示されます。物理USBフラッシュメディアを使用する場合、メニュー画面の表示は多少異なります。

- d. [Install RSA Netwitness Platform 11.2] (デフォルトの選択) を選択し、Enterキーを押します。



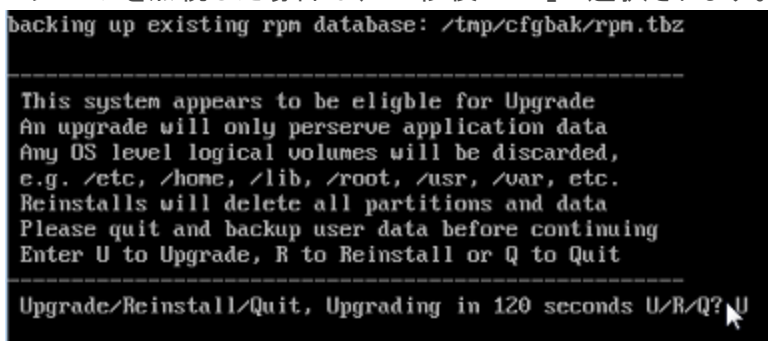
オペレーティングシステムのインストールが実行され、[Enter (y/Y) to clear drives] プロンプトで停止します。

- e. 「n」(No) を入力します。
デフォルトのアクションは「No」です。プロンプトを無視すると、30秒後に「No」が選択され、ドライブはクリアされません。



[Upgrade/Reinstall/Quit (U/R/Q?)] プロンプトが表示されます。

- f. 「U」を入力すると、ホストをアップグレードします。
メッセージを無視した場合は、120秒後に「U」が選択されます。



CentOS7コンポーネントのインストールには数分かかります。インストールプログラムにより、インストール中のコンポーネントが表示されます。表示されるコンポーネントはアプライアンスによって異なります。CentOS7のインストールが完了すると、[Continue (Y/N)?] プロンプトが表示されます。

- g. 「Y」を入力し、Enterキーを押して、このホストをアップグレードすることを確認します。

```
-----
Steps to be executed listed below.  Warning:
this is irreversible.
-----
lremove -f /dev/VolGroup00/rabmq
lremove -f /dev/VolGroup00/root
lremove -f /dev/VolGroup00/swap
lremove -f /dev/VolGroup00/tmp
lremove -f /dev/VolGroup00/usrhome
lremove -f /dev/VolGroup00/var
lremove -f /dev/VolGroup00/vartmp
lremove -f /dev/napper/VolGroup01-uax
lremove -f /dev/napper/VolGroup01-rsasoc
ugrename VolGroup00 netwitness_ug00
ugchange -a n VolGroup01
ugmerge netwitness_ug00 VolGroup01
ugchange -a y netwitness_ug00
Continue (Y/N)? Y
```

[The old operating system is about to be removed. Continue (Y/N)?]の警告が表示されま
す。

- h. 「Y」を入力し、Enterキーを押して、オペレーティングシステムを更新することを確認します。

```
Warning: The old operating system is about to be removed. Continue (Y/N)?
```

ホストをCentOS7にアップグレードすると、ホストは自動的に再起動され、ログインプロンプトが表
示されます。

注意: 接続されたメディア(ビルド スティックなどISOファイルを含むメディア) から再起動しない
てください。

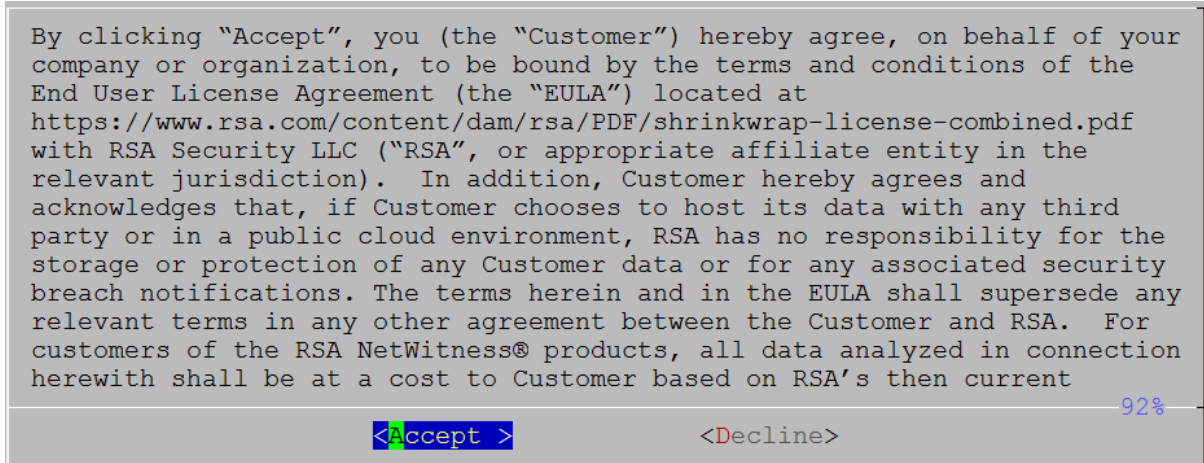
- i. root 認証情報を使用してホストにログオンします。

```
CentOS Linux 7 (Core)
Kernel 3.10.0-514.26.1.el7.x86_64 on an x86_64

NWAPPLIANCE9240 login: root
Password:
[root@NWAPPLIANCE9240 ~]#
```

2. nwsetup-tuiコマンドを実行し、ホストをセットアップします。
nwsetup-tui(セットアッププログラム)が開始され、EULAが表示されます。

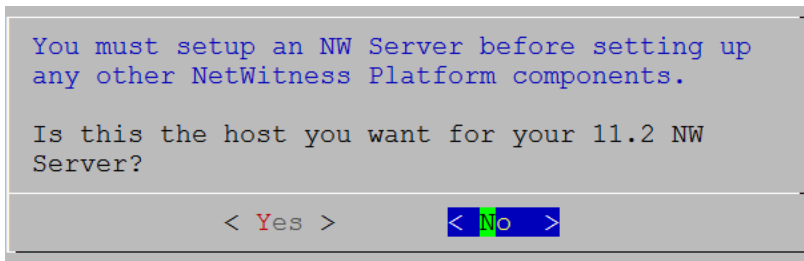
3. Tabキーで[Accept]に移動し、Enterキーを押します。



[Is this the host you want for your 11.2 NW Server]プロンプトが表示されます。

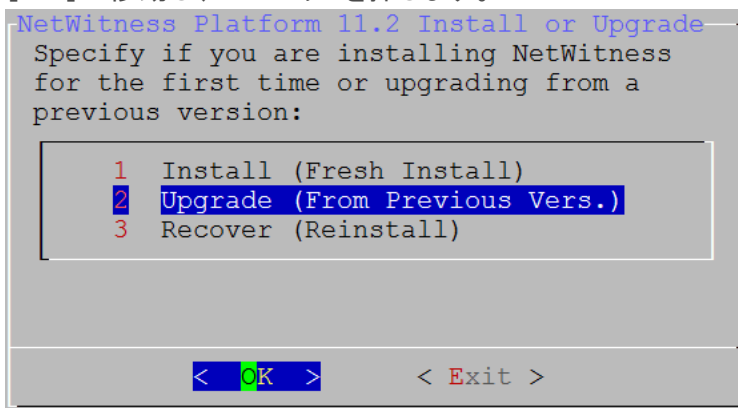
注意: NW Serverに間違ったホストを選択してアップグレードを完了した場合は、セットアッププログラムを再度実行し、「10.6.5.x SA Serverホストの11.2 NW Serverホストへのアップグレード」のすべてのステップ(ステップ2~11)を完了して誤りを修正する必要があります。

4. Tabキーで[No]に移動し、Enterキーを押します。



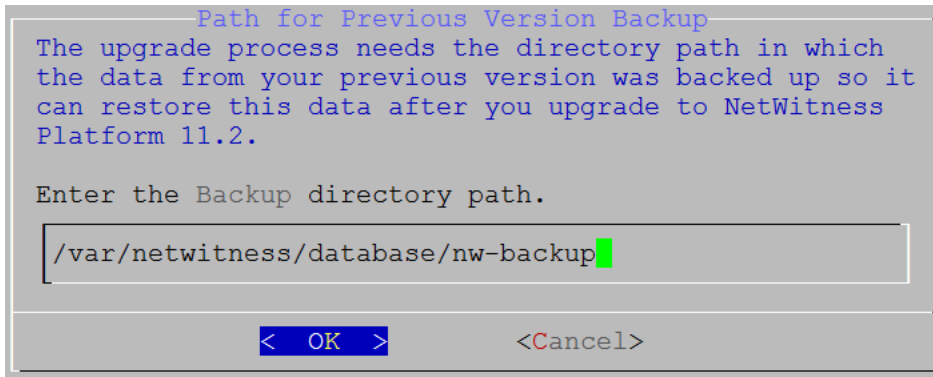
[Install or Upgrade]プロンプトが表示されます。

5. 下向き矢印を使用して、[2 Upgrade (From Previous Vers.)]を選択し、Tabキーを使用して[OK]に移動し、Enterキーを押します。



[Backup path]プロンプトが表示されます。

6. 現在のパスを使用する場合は、Tabキーで[OK]に移動し、Enterキーを押します。変更する場合は、パスを編集して、Tabキーで[OK]に移動し、Enterキーを押します。



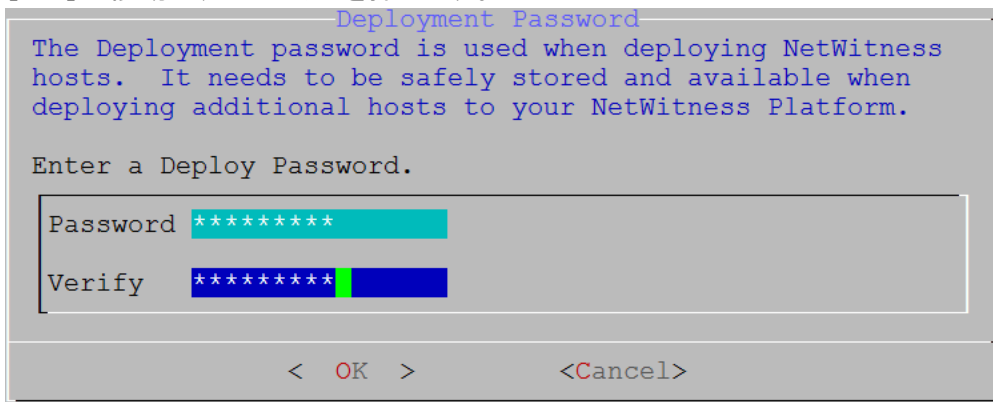
次の表に、ホスト/サービス別のバックアップとリストアのパスを示します。

ホスト	バックアップ パス	リストア パス
Malware	/var/lib/rsamlware/nw-backup	/var/netwitness/malware_analytics_server/nw-backup/restore
Event Stream Analysis	/opt/rsa/database/nw-backup	/var/netwitness/database/nw-backup/restore
NW Server	/var/netwitness/database/nw-backup	/var/netwitness/restore
その他のすべてのホスト	/var/netwitness/database/nw-backup	/var/netwitness/database/nw-backup/restore

「Deployment Password」プロンプトが表示されます。

注: NW Serverのアップグレード時に使用したのと同じ導入パスワードを使用する必要があります。

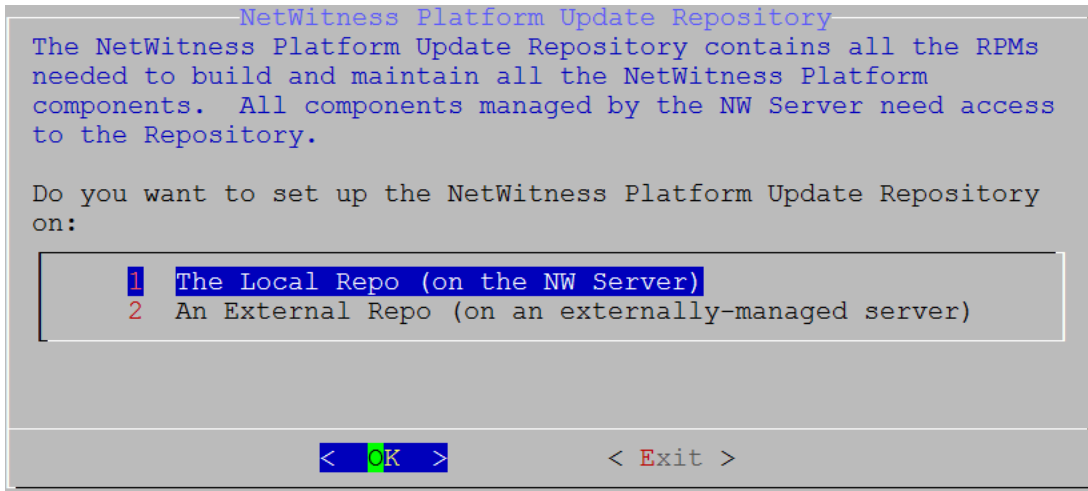
7. [Password]に入力し、下向き矢印で[Verify]に移動し、パスワードを再入力し、Tabキーで[OK]に移動し、Enterキーを押します。



[Update Repository]プロンプトが表示されます。

すべてのホストにNW Serverホストをアップグレードした時に選択したものと同一リポジトリを選択します。

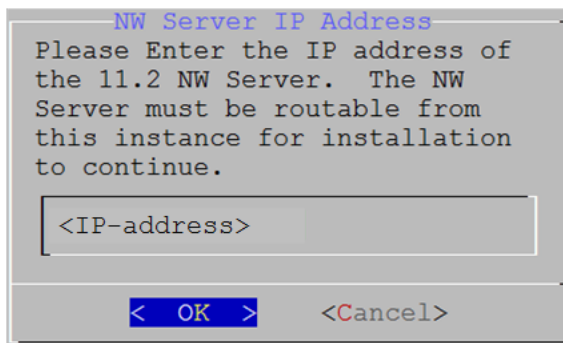
8. 下向き矢印と上向き矢印を使用し、ホストに適用するバージョン更新を取得する場所(たとえば、**1 The Local Repo (on the NW Server)**)を選択し、Tabキーを使用して[OK]へ移動し、Enterキーを押します。



- セットアッププログラムで[1 The Local Repo (on the NW Server)]を選択する場合、NetWitness Platform 11.2へのアップグレード用の適切なメディア(ビルド スティックなどのISOファイルを含むメディア)が接続されていることを確認してください。
- [2 An External Repo (on an externally-managed server)]を選択する場合は、URLを入力するプロンプトが表示されます。リポジトリにアクセスして、RSAの更新とCentOSの更新を取得します。NetWitness Platform外部リポジトリのベースURLを入力し、[OK]をクリックします。リポジトリにアクセスして、RSAの更新とCentOSの更新を取得します。「[付録D: 外部リポジトリの作成](#)」を参照して、リポジトリと外部リポジトリURLを作成し、次のプロンプトで入力します。

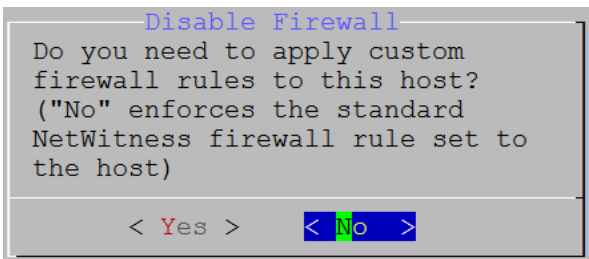
「NW Server IP Address」プロンプトが表示されます。

9. NW ServerのIPアドレスを入力し、Tabキーを使用して[OK]を選択し、Enterキーを押します。

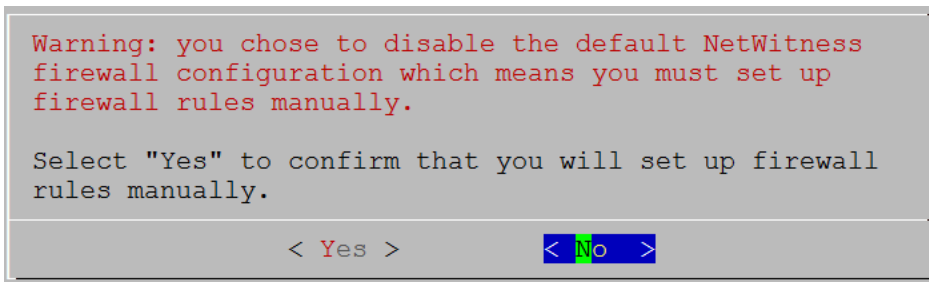


標準的なファイアウォール構成を使用するか、無効化するかを選択するプロンプトが表示されます。

10. 標準的なファイアウォールの構成を使用するには、Tabキーを使用して[No]に移動し、Enterキーを押します。標準的なファイアウォールの構成を無効化するには、Tabキーを使用して[Yes]に移動し、Enterキーを押します。次の例では、[No](標準的なファイアウォール構成を使用)を選択しています。



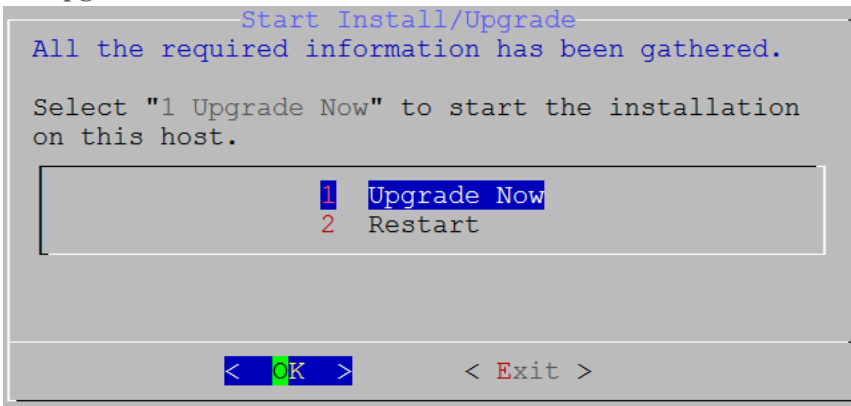
- [Yes]を選択すると、選択内容が確定されます。



- [No]を選択すると、標準的なファイアウォールの構成が適用されます。

[Install or Upgrade] プロンプトが表示されます。(Recoverは選択できません。11.2の災害復旧用です。)

11. [1 Upgrade Now]を選択し、Tabキーを使用して[OK]に移動し、Enterキーを押します。





「Installation complete」が表示されると、ホストの11.2へのアップグレードは完了です。

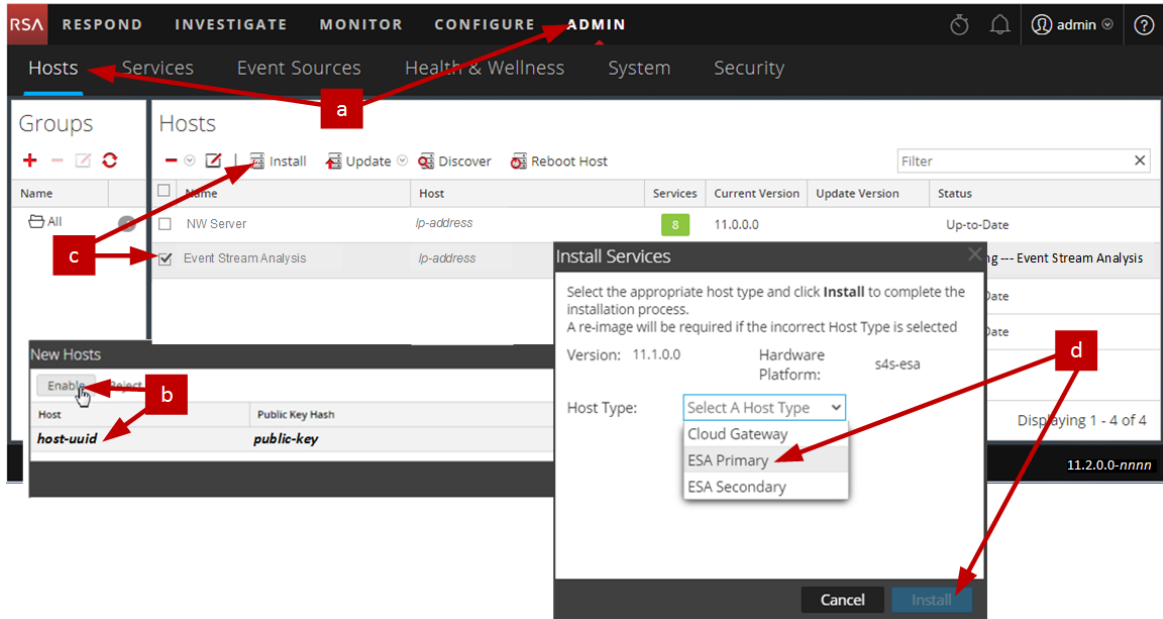
12. 次の手順で、このホストにサービスをインストールします。

- a. NetWitness Platformにログインし、[管理] > [ホスト]に移動します。
[新しいホスト]ダイアログが表示され、[ホスト]ビューがバックグラウンドでグレー表示されます。

注: [新しいホスト]ダイアログが表示されない場合、[ホスト]ビューのツールバーで[検出]をクリックします。

- b. [新しいホスト]ダイアログでホストをクリックし、[有効化]をクリックします。
[新しいホスト]ダイアログが閉じ、[ホスト]ビューにホストが表示されます。

- c. [ホスト]ビューでそのホストを選択し(たとえばEvent Stream Analysis)、 Install  をクリックします。
[サービスのインストール]ダイアログが表示されます。
- d. 適切なサービスを選択し(たとえばESAプライマリ)、[インストール]をクリックします。



NetWitness Platformで非NW Serverホストのアップグレードが完了しました。

Legacy Windows収集の更新またはインストール

「RSA NetWitness Legacy Windows 収集ガイド」を参照してください。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

注 : Legacy Windows収集のインストールまたは更新の後、正常にログを収集するため、システムを再起動します。

アップグレード後のタスク

このトピックでは、ホストを10.6.6.xから11.2にアップグレードした後に実行する必要があるタスクを示します。これらのタスクは、次のカテゴリに分類されます。

- [全般](#)
- [NW Server](#)
- [RSA NetWitness® Endpoint](#)
- [RSA NetWitness® Endpoint Insights](#)
- [Event Stream Analysis](#)
- [Investigate](#)
- [ログ収集](#)
- [DecoderおよびLog Decoder](#)
- [Reporting Engine](#)
- [Respond](#)
- [RSA Archer® Cyber Incident & Breach Response](#)
- [RSA NetWitness® UEBA](#)
- [Warehouse Connector](#)
- [バックアップ](#)

全般

タスク1: ポート15671が正しく設定されていることを確認

ポート15671は11.xで新しく追加されましたが、ファイアウォールでこのポートを開く必要はありません。『*RSA NetWitness® Platform 導入ガイド*』の「ネットワークアーキテクチャとポート」のトピックを参照し、ポート15671を含むすべてのポートが正しく構成されていることを確認してください。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

(オプション) タスク2: カスタムAnalystsロールのリストア

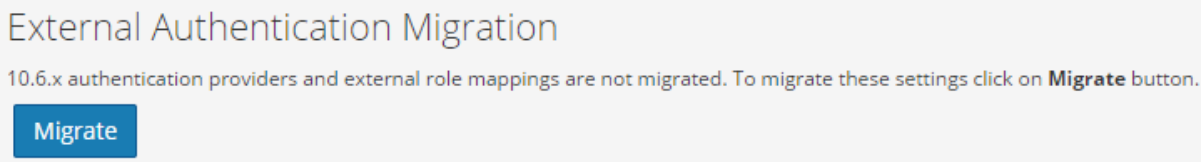
10.6.6.xでカスタマイズしたAnalystsロールを使用していた場合は、11.2で再設定する必要があります。『*RSA NetWitness Platform システムセキュリティとユーザ管理ガイド*』の「ロールの追加と権限の割り当て」を参照してください。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

NW Server

タスク3: AD(Active Directory) の移行

NetWitness Platform 11.2のユーザ インタフェースに最初にログインしたとき、[移行] ボタンをクリックしてADの移行を完了する必要があります。


1. NetWitness Platform 11.2にadmin userの認証情報でログインします。
2. [管理] > [セキュリティ]に移動し、[設定] タブをクリックします。
次のダイアログが表示されます。



3. [移行] をクリックします。
移行が完了するとダイアログが閉じます。

タスク4: 移行したAD構成の変更と証明書のアップロード

10.6.6.xでAD(Active Directory) サーバで認証を行い、ADサーバとの接続にSSLを使用していた場合は、移行後のAD構成を変更し、Active Directoryサーバの証明書をアップロードする必要があります。証明書をアップロードするには、移行後のAD構成で次の手順を実行します。

1. NetWitness Platform 11.2にログインし、[管理] > [セキュリティ]に移動して[設定] タブをクリックします。
2. [Active Directory構成]でAD構成を選択し、 をクリックします。
[構成の編集]ダイアログが表示されます。
3. [証明書ファイル] フィールドで、[参照] をクリックして、証明書ファイルを選択します。
4. [保存] をクリックします。

タスク5: 11.2でのPAM(Pluggable Authentication Module) の再構成

11.2にアップグレードした後、PAMを再構成する必要があります。手順については、『RSA NetWitness® Platform システム セキュリティとユーザ管理ガイド』の「PAMログイン機能の構成」を参照してください。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

10.6.6.xのバックアップ データの/etcディレクトリにある10.6.6.xのPAM構成ファイルを参照できます。

タスク6: NTPサーバのリストア

NetWitness Platform 11.2のユーザ インタフェースを使用し、NTPサーバの構成をリストアする必要があります。NTPサーバ構成情報は、\$BUPATH/restore/etc/ntp.confにあります。

/var/netwitness/restore/etc/ntp.confファイルのNTPサーバ名とホスト名を使用します。NTPサーバを追加する方法の詳細については、「RSA NetWitness® Platform システム構成ガイド」の「NTPサーバの構成」を参照してください。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

タスク7: FlexNet Operations-On Demandを使用しない環境でのライセンスのリストア

ご使用の環境でFlexNet Operations-On Demandにアクセスしない場合は、NetWitness Platformライセンスを再度ダウンロードする必要があります。ライセンスを再ダウンロードする方法については、「RSA NetWitness Platform ライセンス管理ガイド」の「ステップ1.NetWitness Serverの登録」を参照してください。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

(オプション) タスク8: 標準ファイアウォール構成を無効化した場合、カスタムiptablesを追加

アップグレード中に、標準のファイアウォール構成を使用するか、または無効化するかを選択できます。無効化した場合は、無効化したすべてのホストで、次の手順をベースラインとして、ユーザ管理のファイアウォールルールを作成します。

注: バックアップのrestoreフォルダにある\$BUPATH/restore/etc/sysconfig/iptablesと\$BUPATH/restore/etc/sysconfig/ip6tablesを参照し、ip6tablesファイルとiptablesファイルを更新できます。/etc/netwitness/firewall.cfgファイルには、標準のiptablesのファイアウォールのルールが含まれています。

1. SSHで各ホストに接続し、rootでログインします。
2. ip6tablesファイルとiptablesファイルを更新し、カスタムのファイアウォールルールを追加します。
/etc/sysconfig/iptables
/etc/sysconfig/ip6tables
3. iptablesサービスとip6tablesサービスを再ロードします。
service iptables reload
service ip6tables reload

(オプション) タスク9: 信頼接続を設定していない場合、SSLポートを指定


信頼接続を設定していない場合のみ、このタスクを実行します。次の場合は、信頼接続が設定されていません。

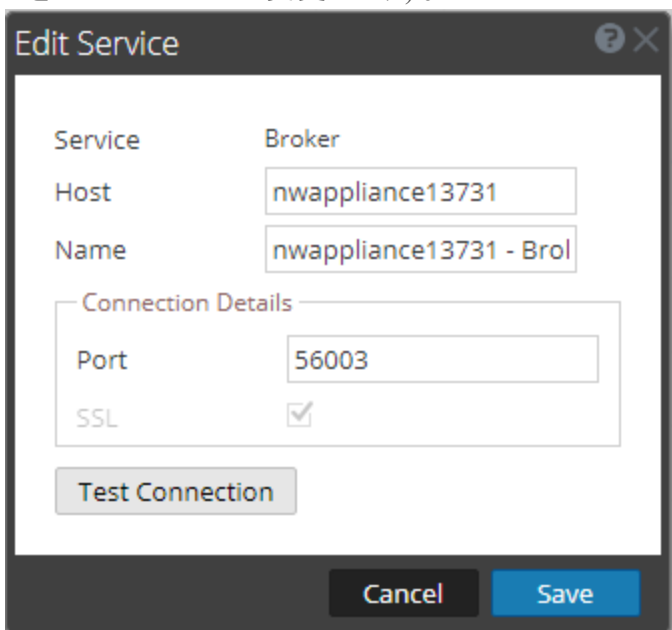
- 10.3.2またはそれ以前の基本ISOイメージを使用している。
- RPMパッケージだけを使用して、システムを10.6.6.xに更新した。

非SSLポート500XXを使用している場合、NetWitness Platform 11.2はコアサービスと通信できません。[サービスの編集]ダイアログで、コアサービスポートをSSLポートに更新する必要があります。

1. NetWitness Platformにログインし、[管理] > [サービス]に移動します。
2. 各コア サービスを選択し、ポートを非SSLからSSLに変更します。

サービス	非SSL	SSL
Broker	50003	56003
Concentrator	50005	56005
Decoder	50004	56004
Log Decoder	50002	56002

3. [サービス]ビューのツールバーで、 (編集アイコン) をクリックします。
[サービスの編集]ダイアログが表示されます。
4. 表に示すように、ポートを非SSLからSSLに変更し、[保存]をクリックします(たとえば、Brokerのポートを50003から56003に変更します)。




The image shows a screenshot of the 'Edit Service' dialog box in NetWitness Platform. The dialog is titled 'Edit Service' and has a question mark icon and a close button in the top right corner. It contains the following fields and controls:

- Service:** Broker
- Host:** nwappliance13731
- Name:** nwappliance13731 - Bro
- Connection Details:**
 - Port:** 56003
 - SSL:**
- Test Connection:** A button below the connection details.
- Cancel:** A button at the bottom left.
- Save:** A button at the bottom right.

タスク10: (オプション) Logstash出力構成ファイルで更新されていない監査ログテンプレートの修正

11.0.xでグローバル監査が構成されている場合、最新のグローバル監査の構成を適用するために、次の手順を実行する必要があります。

1. NetWitness Platformにログインし、[管理] > [システム] > [グローバル通知]に移動します。
[グローバル通知]ビューが表示されます。
2. [サーバ]タブをクリックして、任意のsyslogサーバを選択します。
3.  (編集アイコン) をクリックして、[Syslog通知サーバの定義]ダイアログの[保存]をクリックします。

RSA NetWitness® Endpoint

タスク11: メッセージ バス経路のEndpointアラートの再構成

1. NetWitness Endpoint Server上で、C:\Program Files\RSA\ECAT\Server\ConsoleServer.exeファイル内の仮想ホストの構成を、次のように変更します。

```
<add key="IMVirtualHost" value="/rsa/system" />
```

注: NetWitness Platform 11.2では、仮想ホストは/rsa/systemです。10.6.6.x以前のバージョンでは、仮想ホストは/rsa/saです。

2. API ServerとConsole Serverを再起動します。
3. SSHでNW Serverに接続し、rootの認証情報でログインします。
4. 次のコマンドを実行して、すべての証明書をトラストストアに追加します。

```
orchestration-cli-client --update-admin-node
```
5. 次のコマンドを実行して、RabbitMQ Serverを再起動します。

```
systemctl restart rabbitmq-server
```

NetWitness Endpointアカウントは自動的にRabbitMQで利用可能になります。
6. /etc/pki/nw/ca/nwca-cert.pemファイルと/etc/pki/nw/ca/ssca-cert.pemファイルをNW Serverからインポートし、Endpoint Serverの信頼できるルート証明書ストアに追加します。

タスク12: Javaバージョンの変更により、レガシーEndpointからの定期実行Feedを再構成

Javaバージョンの変更により、レガシーEndpointの定期実行Feedを再構成する必要があります。この問題を解決するには、次の手順を実行します。

- 『RSA NetWitness Endpoint統合ガイド』にある「繰り返しFeedを通じたEndpointからのコンテキストデータの構成」トピックの「NetWitness EndpointのSSL証明書のエクスポート」の説明に従い、NetWitness Endpoint CA証明書をNetWitness Platformのトラストストアにインポートします。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

RSA NetWitness® Endpoint Insights

(オプション) タスク13: Endpoint HybridまたはEndpoint Log Hybridのインストール

以下を参照してください。


『RSA NetWitness Platform 11.2 物理ホスト インストールガイド』(物理ホストのインストールの手順)。

『RSA NetWitness Platform 11.2 仮想ホスト インストールガイド』(仮想ホストのインストールの手順)。

Event Stream Analysisタスク

タスク14: ESAの自動脅威検出の再構成

10.6.6.xで自動脅威検出を使用していた場合、次の手順を実行し、11.2のESA Analyticsサービスに再構成する必要があります。

1. NetWitness Platformにログインして、[管理] > [システム] > [ESA Analytics]に移動します。Suspicious Domainsモジュールである、ネットワーク データ用C2(コマンド&コントロール) モジュールとログ用C2モジュールには、「domains_whitelist」という名前のホワイトリストが必要です。
2. (オプション) Context Hubサービスの[リスト]タブに古い自動脅威検出のホワイトリストが表示される場合、次の操作を実行します。
 - a. [管理] > [サービス]に移動して、Context Hubサービスを選択し、アクション()ドロップダウンメニューで、[表示] > [構成] > [リスト]タブをクリックします。
 - b. 古い自動脅威検出のホワイトリストの名前を、Suspicious Domainsモジュールが使用する「domains_whitelist」に変更します。

詳細については、『NetWitness Platform 自動脅威検出ガイド』および『NetWitness Platform ESA構成ガイド』の「ESA Analyticsの構成」セクションを参照してください。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

タスク15: Web Threat Detection、Archer Cyber Incident & Breach ResponseまたはNetWitness Endpointとの統合のためのSSL相互認証の構成

Web Threat Detection、Archer Cyber Incident & Breach Response、NetWitness Endpointと統合する場合、RabbitMQメッセージバスへの接続時の認証のために、統合する各システムにSSL相互認証を構成する必要があります。

注: 10.6.6.xデータをバックアップしたときに取得したRabbitMQユーザ名とパスワードを使用します(「[バックアップ手順](#)」を参照してください)。

1. NetWitness Platformに統合するホスト システムにユーザを作成します。ホストにログインし、次のrabbitmqctlコマンドを実行します。


```
> rabbitmqctl add_user <username> <password>
```

 例:


```
> rabbitmqctl add_user wtd-incidents incidents
```
2. 次のコマンドを実行して、ユーザの権限を設定します(ステップ1のユーザ名を使用)。


```
> rabbitmqctl set_permissions -p /rsa/system <username> ".*", ".*", ".*"
```

 例:


```
> rabbitmqctl set_permissions -p /rsa/system wtd-incidents ".*", ".*", ".*"
```

タスク16: Threat - Malware Indicatorsダッシュボードの有効化

11.2では、10.6.6.xのThreat - IndicatorsダッシュボードがThreat - Malware Indicatorsダッシュボードに名称変更されました。10.6.6.xでこのダッシュボードを使用していた場合は、次の操作を実行する必要があります。


- 11.2のThreat - Malware Indicatorsダッシュボードを有効化します。
- 新しいダッシュレットのデータソースを設定します。
NetWitness Platformのダッシュレットについては、RSA Link(<https://community.rsa.com/docs/DOC-81463>)の「ダッシュレット」を参照してください。

注: 11.2にアップグレードした後で、Threat-IndicatorsとThreat-Malware Indicatorsの両方のダッシュボードがユーザインタフェースに表示される場合があります。その場合は、Threat-Indicatorsダッシュボードを無効にして、Threat-Malware Indicatorsのレポートチャートとダッシュボードを有効にしてください。ダッシュボードの無効化については、『RSA NetWitness Platform スタートガイド』の「ダッシュボードの管理」トピックを参照してください。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

Investigate

タスク17: カスタマイズしたユーザロールにイベント分析にアクセスするInvestigate-server権限があることを確認

11.2.0.0にアップグレードした後、カスタマイズされたどのユーザロールもデフォルトではinvestigate-server.* 権限が有効になっていません。適切なユーザロールにイベント分析へのアクセス権限があることを確認するには、次の手順を実行します。

- Admin userの認証情報を使用してNetWitness Platform 11.2.0.0にログインし、[管理] > [セキュリティ]に移動します。
- [ロール]タブをクリックします。
- investigate-server.* 権限が必要なロールを選択して、 (編集アイコン) をクリックします。
- [権限]セクションにある[Investigate-server]タブを選択します。
- [investigate-server]チェックボックスがオンでない場合、イベント分析にアクセスする必要のあるユーザのロールでは、オンに設定します。

Permissions

Assigned	Description ^
<input type="checkbox"/>	Investigate-server
<input checked="" type="checkbox"/>	investigate-server.*

- [保存]をクリックします。

ログ収集

タスク18: アップグレード後のLog CollectorのStable System Valueのリセット


11.2にアップグレードした後、次のタスクを実行して、Log CollectorのStable System Valueをリセットし、すべての収集プロトコルが正常に再開したことを確認します。

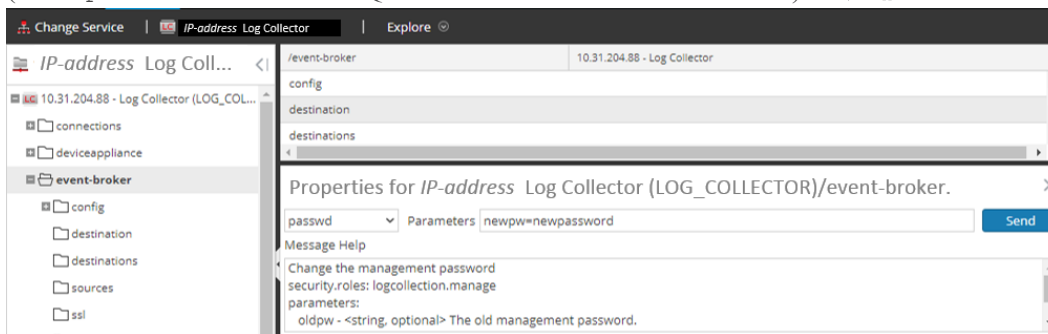
LockboxのStable System Valueのリセット

Lockboxには、Log Collectorのイベントソースとその他のパスワードを暗号化するためのキーが保存されます。Log Collectorサービスは、Stable System Valueが変更されたため、Lockboxを開くことができません。そのため、LockboxのStable System Valueをリセットする必要があります。「ログ収集: ステップ3. Lockbox設定」(『RSA NetWitness® Platform ログ収集構成ガイド』内)を参照してください。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

Log CollectorサービスのRabbitMQユーザアカウントのパスワードの更新

logcollectorサービスのRabbitMQユーザアカウントのパスワードが変更された場合は、11.2へのアップグレード後に再入力する必要があります。

1. NetWitness Platformにログインし、[管理] > [サービス]に移動します。
2. Log Collectorを選択します。
3.  (アクション) > [表示] > [エクスプローラ]をクリックします。
4. event-brokerを右クリックして、[プロパティ]を選択します。
5. ドロップダウンリストから「passwd」を選択し、[パラメータ]に「newpw=<newpassword>」と入力し (<newpassword>はRabbitMQユーザアカウントのパスワードです)、[送信]をクリックします。



(オプション: FIPSが有効な10.6.6.xのLog Collector、Log Decoder、Network Decoderをアップグレードした場合)

タスク19: FIPSモードの有効化


Log Collector、Log Decoder、Decoderを除くすべてのサービスではFIPSが有効になっています。Log Collector、Log Decoder、Decoder以外のサービスではFIPSを無効にできません。これらのサービスでFIPSを有効にする方法については、『RSA NetWitness® Platform システム メンテナンス ガイド』の「FIPSの有効化/無効化」を参照してください。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

DecoderおよびLog Decoder

(オプション) タスク20: GeoIP2 Parserのメタデータの有効化

デフォルトでは、GeoIP2 Parserが生成するメタデータはGeoIP Parserよりも少なくなります。11.2にアップグレードした後、追加のメタデータが必要な場合は、各Decoderで(1回だけ)それらのメタデータを有効化する必要があります。この設定はアップグレード後に変更することもできます。ispおよびorgのメタフィールドは、通常、domainと同じ値を生成します。

メタデータを有効にするには、次の手順を実行します。

1. [管理] > [サービス]に移動します。
2. [管理] > [サービス]ビューで、Log DecoderまたはDecoderを選択します。
3. アクション アイコン()をクリックし、[表示] > [構成]を選択します。[Parser構成]パネルが表示されるので、そこから[GeoIP2]を選択して目的のメタデータを有効にすることができます。

GeoIP2 Parserの詳細については、『*DecoderおよびLog Decoder構成ガイド*』の「GeoIP2 ParserとGeoIP Parser」のトピックを参照してください。

Reporting Engine

(オプション) タスク21: 外部 Syslog サーバのCA証明書をReporting Engineにリストア

アップグレード前に作成したバックアップからCA証明書をリストアする必要があります。バックアップ スクリプトは、10.6.6.xのCA証明書を/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.111-0.b15.e16_8.x86_64/jre/lib/security/cacertsディレクトリにバックアップします。

次の手順を実行し、CA証明書を11.2にリストアします。

1. SSHでNW Serverホストに接続します。
2. CA証明書をエクスポートします。

```
keytool -export -alias <alias_name> -keystorepath_to_keystore_file -rfc -file path_to_certificate_file
```
3. /etc/pki/nw/trust/importディレクトリにCA PEMファイルをコピーします。

(オプション) タスク22: Reporting Engineの外部ストレージのリストア

Reporting Engineの外部ストレージ(レポート保存用のSANやNASなど)がある場合は、アップグレード前にリンクを解除し、アップグレード後に再マウントする必要があります。手順については、「Reporting Engine: サイズの大きなレポートに対応するためのスペースの追加」(『*RSA NetWitness® Platform Reporting Engine構成ガイド*』内)を参照してください。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

Respond

タスク23: Respondサービスのカスタム キーのリストア

10.6.6.xでは、**groupBy**句で使用するためのカスタム キーを追加した場合、`alert_rules.json`ファイルが変更されました。`alert_rules.json`ファイルには、集計スキーマが含まれています。`alert_rules.json`ファイルは次の新しい場所に移動しました。
`/var/lib/netwitness/respond-server/scripts`

1. バックアップ ディレクトリ内の`/opt/rsa/im/fields/alert_rules.json`ファイルから、カスタム キーをコピーします。
このディレクトリは、10.6.6.xのバックアップから`alert_rules.json`ファイルがリストアされる場所です。
2. 11.2の`/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json`に移動します。
これは、11.2の新しいファイルです。
3. `/var/lib/netwitness/respond-server/data/aggregation_rule_schema.json`を編集し、ステップ1でコピーしたカスタム キーを追加します。

タスク24: Respondサービスのカスタム正規化スクリプトのリストア

11.2では、Respondサービスの正規化スクリプトが再設計され、次の新しい場所に移動しました。
`/var/lib/netwitness/respond-server/scripts`
10.6.6.xでこれらのスクリプトをカスタマイズした場合は、次の操作を実行する必要があります。

1. `/opt/rsa/im/scripts`ディレクトリに移動します。
このディレクトリは、次のRespondサービスの正規化スクリプトが10.6.6.xのバックアップからリストアされる場所です。
`data_privacy_map.js`
`normalize_alerts.js`
`normalize_core_alerts.js`
`normalize_ecat_alerts.js`
`normalize_ma_alerts.js`
`normalize_wtd_alerts.js`
`utils.js`
2. 10.6.6.xのスクリプトから、カスタム ロジックをコピーします。
3. `/var/lib/netwitness/respond-server/scripts`ディレクトリに移動します。
このディレクトリは、NetWitness Platform 11.2で再設計されたスクリプトを格納する場所です。
4. 新しいスクリプトを編集して、ステップ2で10.6.6.xスクリプトからコピーしたカスタム ロジックを追加します。
5. `/opt/rsa/im/fields/alert_rules.json`ファイルからカスタム ロジックをコピーします。
`alert_rules.json`ファイルには、集計スキーマが含まれています。

タスク25: カスタムロールに対応の通知設定の権限を追加する

対応の通知設定の権限により、Respond Administrators、Data Privacy Officers、SOC Managersは対応の通知設定([構成]>[対応の通知])にアクセスでき、インシデントが作成または更新されたときにメール通知を送信することが可能になります。

これらの設定にアクセスするには、既存のNetWitness Platformの標準のユーザロールに権限を追加する必要があります。カスタムロールにも権限を追加する必要があります。『NetWitness Respond構成ガイド』の「対応の通知設定の権限」トピックを参照してください。ユーザ権限の詳細については、「システムセキュリティとユーザ管理ガイド」を参照してください。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。


タスク26: 対応の通知設定を手動で構成

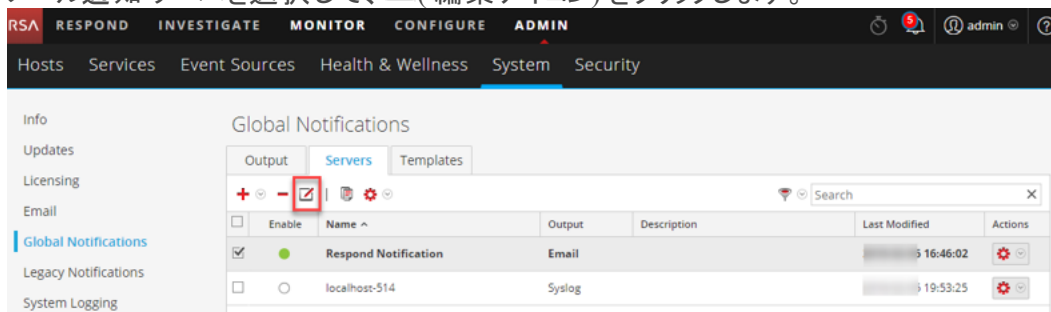
NetWitness Platform 10.6.6.xのIncident Managementの通知設定は、11.2で使用可能な対応の通知設定とは異なるため、既存の10.6.6.xの設定は11.2には移行されません。

NetWitnessの対応の通知設定によって、インシデントが作成または更新されたときに、SOCマネージャや、インシデントに割り当てられたアナリストにメール通知を送信することができます。

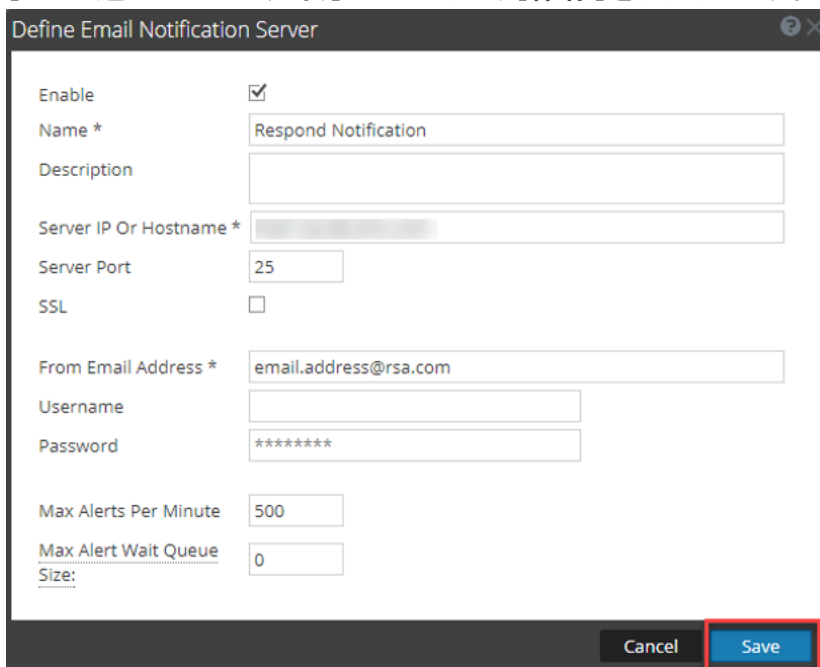
対応の通知設定を手動で構成するには、[構成]>[対応の通知]にアクセスします。『NetWitness Respond構成ガイド』の「対応のメール通知設定の構成」の手順を参照してください。

10.6.6.xの通知サーバは、[メールサーバ]ドロップダウンリストには表示されません。メールサーバはグローバル通知の[サーバ]パネル([管理]>[システム]>[グローバル通知]>[サーバ]タブ)で編集および保存する必要があります。

1. NetWitness Platformにログインし、[管理]>[システム]>[グローバル通知]>[サーバ]タブに移動します。
2. [構成]>[対応の通知]にアクセスします。[対応の通知の設定]ビューが表示されます。この時点では、[メールサーバ]ドロップダウンリストにメール通知サーバは表示されません。
3. [メールサーバ設定]リンクをクリックします。[グローバル通知]パネルが表示されます。
4. [サーバ]タブをクリックします。
5. 各メール通知サーバについて、次の手順を実行します。
 - a. メール通知サーバを選択して、 (編集アイコン) をクリックします。



- b. [メール通知 サーバの定義] ダイアログで、[保存] をクリックします。



6. [構成] > [対応の通知]に戻ります。サーバが[メールサーバ]ドロップダウン リストに表示されません。
Incident Managementのカスタム通知テンプレートは11.2に移行することはできません。11.2ではカスタムテンプレートはサポートされていません。

タスク27: デフォルトのインシデント ルールのGroup By値の更新

デフォルトのインシデント ルールのうち4つは、Group By値として「Source IP Address」を使用するようになりました。デフォルトのルールを更新するには、次のデフォルトのルールのGroup By値を「Source IP Address」に変更します。

- High Risk Alerts: Reporting Engine
- High Risk Alerts: Malware Analysis
- High Risk Alerts: NetWitness Endpoint
- High Risk Alerts: ESA

1. [構成] > [インシデント ルール]にアクセスして、更新するルールの[名前]列のリンクをクリックします。[インシデント ルールの詳細]ビューが表示されます。
2. [Group By]フィールドで、新しいGroup By値を選択します。
3. [保存]をクリックしてルールを更新します。

タスク28: インシデント ルールへの[Group By]フィールドの追加

[Group By]フィールドは10.6.6では必須ではありませんでしたが、11.2では必須です。11.1にアップグレードした後、

一部のインシデント ルールには[Group By]フィールドがないため、ルールに追加する必要があります。追加しないと正常に機能せず、インシデントを作成できません。

インシデント ルールごとに、次の手順を実行します。

1. NetWitness Platformにログインします。
2. [構成] > [インシデント ルール]にアクセスして、更新するルールの[名前]列のリンクをクリックします。

SELECT	ORDER	ENABLED	NAME	DESCRIPTION	LAST MATCHED	MATCHED ALERTS	INCIDENTS
<input type="radio"/>	1	▶	User Behavior	This incident rule captures network user behavior.		0	0
<input type="radio"/>	2	▶	Suspected Command & Control Communicate...	This incident rule captures suspected communication with a Co...		0	0
<input type="radio"/>	3	■	High Risk Alerts: Malware Analysis	This incident rule captures alerts generated by the RSA Malware...		0	0
<input type="radio"/>	4	■	High Risk Alerts: NetWitness Endpoint	This incident rule captures alerts generated by the RSA NetWitn...		0	0
<input type="radio"/>	5	■	High Risk Alerts: Reporting Engine	This incident rule captures alerts generated by the RSA Reportin...		0	0
<input type="radio"/>	6	■	High Risk Alerts: ESA	This incident rule captures alerts generated by the RSA ESA platf...		0	0
<input type="radio"/>	7	■	IP Watch List: Activity Detected	This incident rule captures alerts generated by IP addresses that...		0	0
<input type="radio"/>	8	■	User Watch List: Activity Detected	This incident rule captures alerts generated by network users w...		0	0
<input type="radio"/>	9	■	Suspicious Activity Detected: Windows Worm Pr...	This incident rule captures alerts that are indicative of worm pro...		0	0
<input type="radio"/>	10	■	Suspicious Activity Detected: Reconnaissance	This incident rule captures alerts that identify common ICMP ho...		0	0
<input type="radio"/>	11	■	Monitoring Failure: Device Not Reporting	This incident rule captures any instance of an alert designed to ...		0	0
<input type="radio"/>	12	■	Web Threat Detection	This incident rule captures alerts generated by the RSA Web Thr...		0	0

3. [Group By]フィールドで、Group By値が選択されていることを確認します。選択されていない場合は、Group By値を選択します。

The screenshot shows the 'CONFIGURE' page for an incident rule. The rule name is 'User Watch List: Activity Detected'. The description states: 'This incident rule captures alerts generated by network users whose user names have been added as a "Source Username" condition. To add more than one Username to the watch list, simply add an additional Source Username condition.' The 'MATCH CONDITIONS*' section is set to 'Rule Builder' and shows two conditions: 'Source Username is equal to jsmith' and 'Source Username is equal to jdoe'. The 'ACTION*' section has 'Group into an incident' selected. The 'GROUPING OPTIONS' section has 'GROUP BY*' set to 'Source Username' (highlighted with a red box) and 'TIME WINDOW' set to '4 Hours'. 'Cancel' and 'Save' buttons are at the bottom right.

4. [保存]をクリックしてルールを更新します。
インシデント ルールの詳細については、「[NetWitness Respond構成ガイド](#)」を参照してください。
NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

タスク29: アップグレード準備タスクで特定した一致条件で「Domain」を使用するインシデントルールの更新

アップグレード準備タスクの「[タスク5: 「Domain」または「Domain for Suspected C&C」を使用した統合ルールの一致条件を確認](#)」で特定したインシデント ルールを変更します。

特定した各ルールについて、次の手順を実行します。

1. NetWitness Platformにログインして[構成] > [インシデント ルール]に移動し、更新するルールの[名前]列のリンクをクリックします。

SELECT	ORDER	ENABLED	NAME	DESCRIPTION	LAST MATCHED	MATCHED ALERTS	INCIDENTS
<input type="radio"/>	1	<input checked="" type="checkbox"/>	User Behavior	This incident rule captures network user behavior.		0	0
<input type="radio"/>	2	<input checked="" type="checkbox"/>	Suspected Command & Control Communicatio...	This incident rule captures suspected communication with a Co...		0	0
<input type="radio"/>	3	<input checked="" type="checkbox"/>	High Risk Alerts: Malware Analysis	This incident rule captures alerts generated by the RSA Malware...		0	0
<input type="radio"/>	4	<input checked="" type="checkbox"/>	High Risk Alerts: NetWitness Endpoint	This incident rule captures alerts generated by the RSA NetWitn...		0	0
<input type="radio"/>	5	<input checked="" type="checkbox"/>	High Risk Alerts: Reporting Engine	This incident rule captures alerts generated by the RSA Reportin...		0	0
<input type="radio"/>	6	<input checked="" type="checkbox"/>	High Risk Alerts: ESA	This incident rule captures alerts generated by the RSA ESA platf...		0	0
<input type="radio"/>	7	<input checked="" type="checkbox"/>	IP Watch List: Activity Detected	This incident rule captures alerts generated by IP addresses that...		0	0
<input type="radio"/>	8	<input checked="" type="checkbox"/>	User Watch List: Activity Detected	This incident rule captures alerts generated by network users w...		0	0
<input type="radio"/>	9	<input checked="" type="checkbox"/>	Suspicious Activity Detected: Windows Worm Pr...	This incident rule captures alerts that are indicative of worm pro...		0	0
<input type="radio"/>	10	<input checked="" type="checkbox"/>	Suspicious Activity Detected: Reconnaissance	This incident rule captures alerts that identify common ICMP ho...		0	0
<input type="radio"/>	11	<input checked="" type="checkbox"/>	Monitoring Failure: Device Not Reporting	This incident rule captures any instance of an alert designed to ...		0	0
<input type="radio"/>	12	<input checked="" type="checkbox"/>	Web Threat Detection	This incident rule captures alerts generated by the RSA Web Thr...		0	0

2. [一致条件]セクションの空白のフィールドで、ドロップダウン リストから[Domain]と[Domain for Suspected CC]を選択し、アップグレード前のタスクで確認した条件を選択します。

BASIC SETTINGS

ENABLED

NAME*

Verify Domain for Suspected C&C field

DESCRIPTION

This rule match Conditions for Domain & Domain for Suspected C&C in rule builder

MATCH CONDITIONS*

QUERY MODE

Rule Builder

All of these

Add Condition

FIELD

FIELD

ACTION*

CHOOSE THE ACTION TAKEN IF THE RULE MATCHES AN ALERT

Group into an Incident Suppress the Alert

Cancel Save

3. [保存]をクリックしてルールを更新します。
インシデント ルールの詳細については、「*NetWitness Respond構成ガイド*」を参照してください。
NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

RSA Archer Cyber Incident & Breach Response

タスク30: RSA Archer Cyber Incident & Breach Response統合の再構成

Event Stream Analysis、Reporting Engine、Respondに関してRSA Archer Cyber Incident & Breach Responseを再構成する方法については、『*RSA Archerとの統合ガイド*』を参照してください。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

RSA NetWitness® UEBA

タスク31: NetWitness UEBAのインストール

NetWitness UEBAはNetWitness Platform 11.2から新しく導入された機能です。

以下を参照してください。

『*RSA NetWitness Platform 11.2 物理ホスト インストールガイド*』(物理ホストのインストールの手順)。

『*RSA NetWitness Platform 11.2 仮想ホスト インストールガイド*』(仮想ホストのインストールの手順)。

『*RSA NetWitness UEBAユーザガイド*』(NetWitness UEBAに関する情報)。

Warehouse Connector

タスク32: keytab ファイルのリストア、NFSのマウント、サービスのインストール

1. keytabファイルを<backup-path>/restoreディレクトリからリストアします。
2. <backup-path>/restore/etc/krb5.confから/etc/krb5.confにKerberos Realm構成をリストアします。
3. (オプション) 非FIPS環境からアップグレードし、isCheckValidationRequiredパラメータが移行先で有効化されていない場合、SFTPの宛先を設定します。
 - a. SSHでWarehouse Connectorホストに接続し、次のコマンドを実行します。

```
cd /root/.ssh/  
mv id_dsa id_dsa.old  
OWB_FORCE_FIPS_MODE_OFF=1 openssl pkcs8 -topk8 -v2 des3 -in id_dsa.old -  
out id_dsa
```

パスフレーズの入力を求められます。
 - b. 暗号化パスワードを入力します。
 - c. 次のコマンドを実行します。

```
chmod 600 id_dsa
```
4. Warehouse Connectorをインストールします。
手順については、『*NetWitness Platform Warehouse Connector構成ガイド*』を参照してください。

NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

タスク33: Warehouse Connector Lockboxの更新とストリームの開始

注: 10.6.6.xでストリームの自動開始を有効にしていた場合、NetWitness PlatformユーザインタフェースにWarehouse Connectorサービスが表示されるまでに多少の遅延があります。

- Warehouse ConnectorのLockboxを更新します。
- Warehouse ConnectorにSSH接続し、rootの認証情報を使用してログインします。
- サービスを再起動します。

```
service nwarehouseconnector restart
```
- (オプション) 10.6.6.xで自動開始を有効にしていない場合、サービスの再起動後に手動でストリームを開始する必要があります。

バックアップ

タスク34: ホストのローカル ディレクトリからバックアップ関連ファイルを削除

注意: 1) すべてのバックアップ ファイルのコピーを外部ホスト上に保持する必要があります。2) 11.2ホスト上のローカル ディレクトリからバックアップ関連ファイルを削除する前に、バックアップのデータをすべて11.2上にリストアしたことを確認します。

.tarファイルのバックアップ

すべてのホストを11.2にアップグレードしたら、次のファイルを削除する必要があります。

- ホスト上のローカル ディレクトリにあるバックアップ ファイル。
- ホスト上のnw-backupディレクトリとrestore ディレクトリにあるすべてのファイル。

ホスト	バックアップ パス	リストア パス
Malware	/var/lib/rsamlware/nw-backup	/var/netwitness/malware_analytics_server/nw-backup/restore
Event Stream Analysis	/opt/rsa/database/nw-backup	/var/netwitness/database/nw-backup/restore
NW Server	/var/netwitness/database/nw-backup	/var/netwitness/restore
その他のすべてのホスト	/var/netwitness/database/nw-backup	/var/netwitness/database/nw-backup/restore

付録A:トラブルシューティング

この付録には2つのセクションがあります。

- [セクション1: 一般的なトラブルシューティングの情報](#)
- [セクション2: ハードウェアに関するトラブルシューティングの情報](#)

セクション1: 一般的なトラブルシューティングの情報

このセクションでは、インストールとアップグレードで発生する可能性のある問題の解決策について説明します。ほとんどの場合、これらの問題が発生すると、NetWitness Platformがログメッセージを出力します。

注: 次のトラブルシューティングの解決策で解決できないアップグレードの問題がある場合は、カスタマーサポートにお問い合わせください。

このセクションでは、次のサービス、機能、プロセスのトラブルシューティングについて記載しています。

- [CLI\(コマンド ライン インタフェース\)](#)
- [バックアップ スクリプト](#)
- [Event Stream Analysis](#)
- [Log Collectorサービス\(nwlogcollector\)](#)
- [Orchestration](#)
- [NW Server](#)
- [Reporting Engine](#)
- [NetWitness UEBA](#)

CLI(コマンド ライン インタフェース)

エラー メッ セー ジ	<p>CLI(コマンド ライン インタフェース)に、「Orchestration failed.」と表示される。</p> <pre>Mixlib::ShellOut::ShellCommandFailed: Command execution failed. STDOUT/STDERR suppressed for sensitive resource in/var/log/netwitness/config-management/chef-solo.log</pre>
原因	nwsetup-tuiで間違ったdeploy_adminのパスワードを指定しました。
解決 策	<p>deploy_adminのパスワードを取得します。</p> <ol style="list-style-type: none"> SSHでNW Serverホストに接続し、次のコマンドを実行します。 <pre>security-cli-client --get-config-prop --prop-hierarchy nw.security- client --prop-name deployment.password</pre> SSHで失敗したホストに接続します。 正しいdeploy_adminのパスワードを使用してnwsetup-tuiを再実行します。
エラー メッセー ジ	<pre>ERROR com.rsa.smc.sa.admin.web.controller.ajax.health. AlarmsController - Cannot connect to System Management Service</pre>
原因	アップグレードの完了後、SMS(Service Management Service) が実行されているにもかかわらず、NetWitness Platformはこのサービスがダウンしていると認識します。
解決 策	<p>SMSサービスを再起動します。</p> <pre>systemctl restart rsa-sms</pre>
エラー メッ セー ジ	<p>ホストをオフラインで更新してリポートした後に、ユーザ インタフェースにホストをリポートするようメッセージが表示されます。</p> 
原因	CLIを使用してホストをリポートすることはできません。ユーザ インタフェースを使用する必要があります。
解決 策	ユーザ インタフェースの[ホスト]ビューでホストをリポートします。

バックアップ(nw-backupスクリプト)

エラーメッセージ	WARNING: Incorrect ESA Mongo admin password for host <hostname>.
原因	ESA MongoDB adminのパスワードに特殊文字が含まれています(「!@#\$%^」など)。
解決策	バックアップを実行する前に、ESA MongoDB adminのパスワードをデフォルトの「netwitness」に変更します。

エラー	immutable属性の設定が原因でバックアップエラーが発生します。表示されるエラーの例を示します。 <pre>Backing up NetWitness Config (/etc/netwitness) files from: saserver1 WARNING: Errors occurred while backing up NetWitness Configuration files. Verify contents of saserver1-192.168.2.102-etc-netwitness.tar.gz Located in /var/netwitness/database/nw-backup/2018-03-01/saserver1-192.168.2.102-backup.tar.gz Backing up SA UI Web Server (/var/lib/netwitness/uax) files from: saserver1</pre>
原因	immutable(変更不可)フラグが設定されたファイルがある場合(例えば、Puppetプロセスがカスタマイズしたファイルを上書きしないようにするため)、バックアップにはそのファイルが含まれず、エラーが生成されます。
解決策	immutableフラグが設定されたファイルが存在するホストで、次のコマンドを実行し、ファイルのimmutableフラグを削除します。 <code>chattr -i <filename></code>

エラー	<p>Error creating Network Configuration Information file due to duplicate or bad entries in primary network configuration file: <code>/etc/sysconfig/network-scripts/ifcfg-em1</code> Verify contents of <code>/var/netwitness/logdecoder/packetdb/nw-backup/2018-02-23/S5-BROK-36-10.25.53.36-network.info.txt</code></p>
原因	<p>次のいずれかのフィールドで、不正または重複したエントリーがあります: DEVICE、BOOTPROTO、IPADDR、NETMASK、GATEWAY。このエラーは、バックアップされるホストのプライマリEthernetインタフェース構成ファイルの読み取り時に検出されたものです。</p>
解決策	<p>外部バックアップ サーバのバックアップ場所、およびホスト上のローカルなバックアップ場所(この場所には他のバックアップがステージングされています)に、ファイルを手動で作成します。ファイル名の形式は<code><hostname>-<hostip>-network.info.txt</code>で、次のエントリーを含める必要があります。</p> <pre> DEVICE=<devicename> ; # from the host's primary ethernet interface config file BOOTPROTO=<bootprotocol> ; # from the host's primary ethernet interface config file IPADDR=<value> ; # from the host's primary ethernet interface config file NETMASK=<value> ; # from the host's primary ethernet interface config file GATEWAY=<value> ; # from the host's primary ethernet interface config file search <value> ; # from the host's /etc/resolv.conf file nameserver <value> ; # from the host's /etc/resolv.conf file </pre>

Event Stream Analysis

問題	FIPSが有効化された構成で11.2.0.0にアップグレードした後、ESAサービスがクラッシュします。
原因	ESAサービスが、無効なキーストアを参照しています。
解決策	<ol style="list-style-type: none">1. ESAプライマリホストにSSHで接続し、ログインします。2. /opt/rsa/esa/conf/wrapper.confファイル内の次の行を変更します。 wrapper.java.additional.5=- Djavax.net.ssl.keyStore=/opt/rsa/esa/../carlos/keystore 変更後： wrapper.java.additional.5=- Djavax.net.ssl.keyStore=/opt/rsa/carlos/keystore3. 次のコマンドを実行し、ESAを再起動します。 systemctl restart rsa-nw-esa-server <p>注: 複数のESAホストがあり、同じ問題が発生する場合は、各ESAセカンダリホストでステップ1から3を繰り返します。</p>

Log Collectorサービス(`nwlogcollector`)

Log Collectorのログは、`nwlogcollector` サービスを実行しているホスト上の `/var/log/install/nwlogcollector_install.log`に保存されます。

エラーメッセージ	<timestamp>.NwLogCollector_PostInstall: Lockbox Status : Failed to open lockbox: The lockbox stable value threshold was not met because the system fingerprint has changed. To reset the system fingerprint, open the lockbox using the passphrase.
原因	更新後、Log CollectorのLockboxを開くことができませんでした。
解決策	NetWitness Platformにログインし、LockboxのStable System Valueをリセットすることにより、システムフィンガープリントをリセットします。詳細については、「ログ収集の構成ガイド」の「Lockboxのセキュリティ設定の構成」トピックにある「Stable System Valueのリセット」セクションを参照してください。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「 マスター目次 」で確認できます。
エラーメッセージ	<timestamp> NwLogCollector_PostInstall: Lockbox Status : Not Found
原因	更新後、Log CollectorのLockboxが構成されていません。
解決策	Log CollectorのLockboxを使用する場合は、NetWitness Platformにログインし、Lockboxを構成します。詳細については、『 ログ収集の構成ガイド 』の「Lockboxのセキュリティ設定の構成」トピックを参照してください。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「 マスター目次 」で確認できます。。

エラーメッセージ	<timestamp>: NwLogCollector_PostInstall: Lockbox Status : Lockbox maintenance required: The lockbox stable value threshold requires resetting. To reset the system fingerprint, select Reset Stable System Value on the settings page of the Log Collector.
原因	Log CollectorのLockboxのStable System Value閾値フィールドをリセットする必要があります。
解決策	NetWitness Platformにログインし、LockboxのStable System Valueをリセットします。詳細については、「ログ収集の構成ガイド」の「Lockboxのセキュリティ設定の構成」トピックにある「Stable System Valueのリセット」セクションを参照してください。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「 マスター目次 」で確認できます。

問題	Log Collectorのアップグレードを準備していましたが、現時点ではアップグレードしないことにしました。
原因	アップグレードの遅延。
解決策	次のコマンドを実行して、アップグレードの準備をしていたLog Collectorを元の状態に戻し、通常の運用を再開します。 # /opt/rsa/nwlogcollector/nwtools/prepare-for-migrate.sh --revert

NW Server

これらのログは、NW Serverホスト上の`/var/netwitness/uax/logs/sa.log`に書き込まれます。

問題	<p>アップグレード後、監査ログが、グローバル監査に設定された宛先に転送されていないことが分かりました。</p> <p>または</p> <p>次のメッセージが<code>sa.log</code>に記録されました。</p> <pre>Syslog Configuration migration failed. Restart jetty service to fix this issue</pre>
原因	NW Serverのグローバル監査設定は、10.6.6.xから11.2.0.0への移行に失敗しました。
解決策	<ol style="list-style-type: none"> SSHでNW Serverに接続します。 次のコマンドを実行します。 <pre>orchestration-cli-client --update-admin-node</pre>

Orchestration

Orchestration Serverのログは、NW Serverホスト上の`/var/log/netwitness/orchestration-server/orchestration-server.log` に書き込まれます。

問題	<ol style="list-style-type: none"> 非NW Serverホストをアップグレードしようとしたが、失敗しました。 このホストのアップグレードを再試行しましたが、再度失敗しました。 <p><code>orchestration-server.log</code>に次のメッセージが記録されます。</p> <pre>"'file' _virtual_ returned False: cannot import name HASHES"</pre>
原因	失敗した非NW Serverホストでsalt minionがアップグレードされ、再起動されていない可能性があります。
解決策	<ol style="list-style-type: none"> アップグレードに失敗した非NW ServerホストにSSHで接続します。 次のコマンドを実行します。 <pre>systemctl unmask salt-minion systemctl restart salt-minion</pre> <ol style="list-style-type: none"> 非NW Serverホストのアップグレードを再試行します。

Reporting Engineサービス

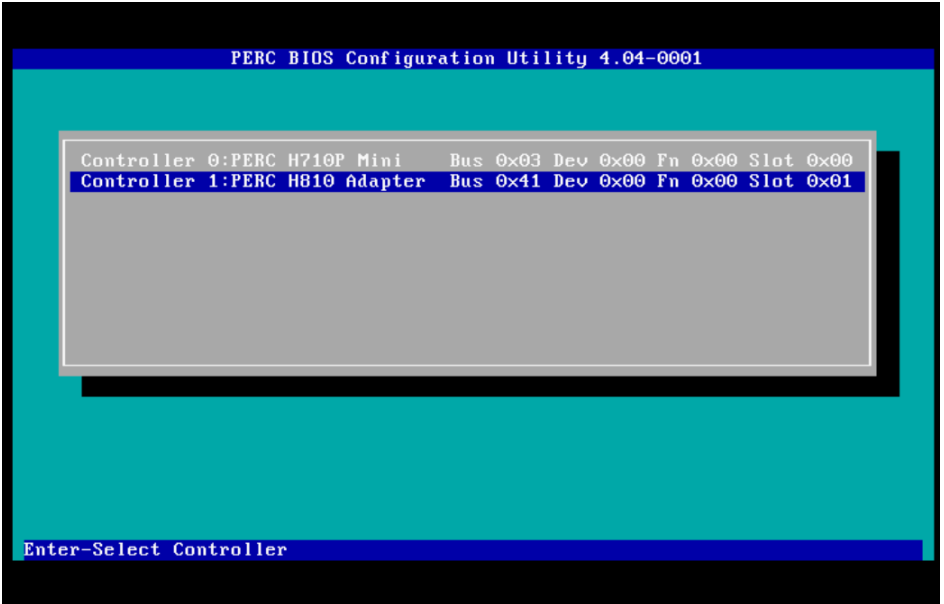
Reporting Engineの更新ログは、Reporting Engineを実行しているホスト上の/var/log/re_install.logファイルに保存されます。

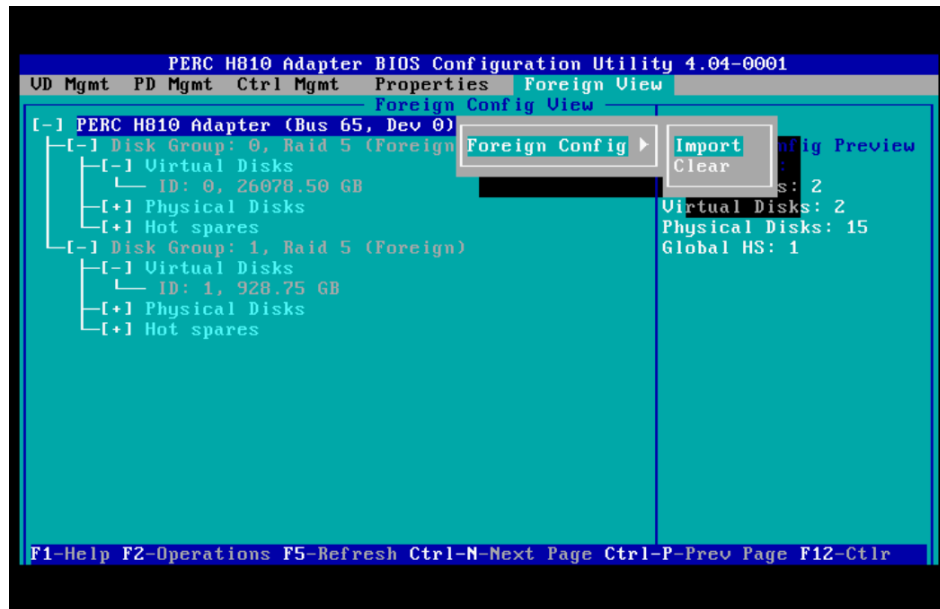
エラーメッセージ	<timestamp> : Available free space in /var/netwitness/re-server/rsa/soc/reporting-engine [><existing-GB] is less than the required space [<required-GB>]
原因	Reporting Engineの更新は、十分なディスク領域がないために失敗しました。
解決策	ログメッセージに示されている必要な容量に合わせてディスク領域を解放します。ディスク領域を解放する方法については、「 <i>Reporting Engine構成ガイド</i> 」の「サイズの大きなレポートに対応するためのスペースの追加」を参照してください。NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「 マスター目次 」で確認できます。

NetWitness UEBA

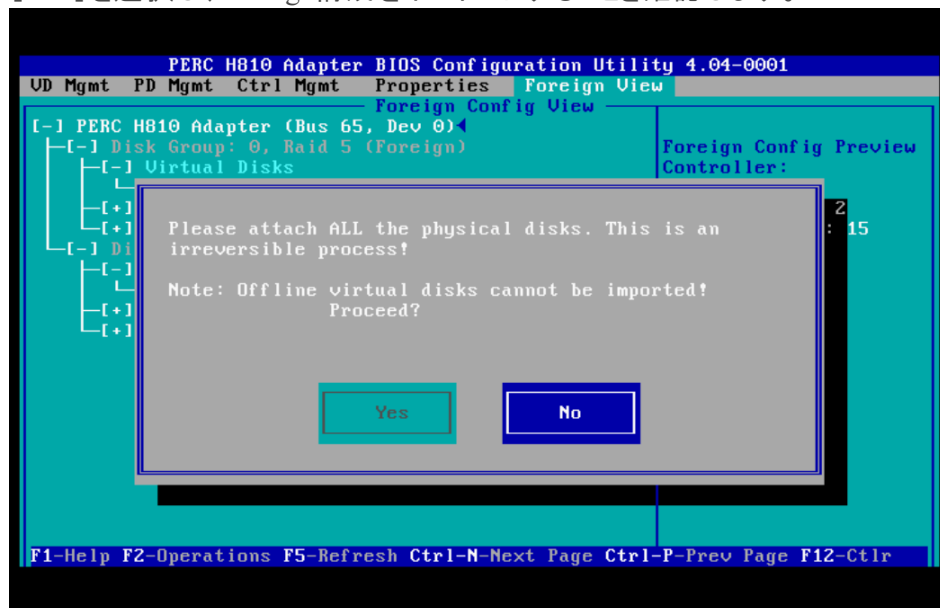
問題	ユーザ インタフェースにアクセスできません。
原因	NetWitness導入環境に複数のNetWitness UEBAサービスが存在しています(1つのNetWitness UEBAサービスしか導入できません)。
解決策	<p>余分なNetWitness UEBAサービスを削除するには、次の手順を実行します。</p> <ol style="list-style-type: none"> NW ServerにSSHで接続し、次のコマンドを実行して、インストールされているNetWitness UEBAサービスのリストを照会します。 <pre># orchestration-cli-client --list-services grep presidio-airflow ... Service: ID=7e682892-b913-4dee-ac84-ca2438e522bf, NAME=presidio-airflow, HOST=xxx.xxx.xxx.xxx:null, TLS=true ... Service: ID=3ba35fbc-7220-4e26-a2ad-9e14ab5e9e15, NAME=presidio-airflow, HOST=xxx.xxx.xxx.xxx:null, TLS=true</pre> サービスのリストから、ホストアドレスをもとに、削除するpresidio-airflowサービスを決定します 次のコマンドを実行し、Orchestrationから余分なサービスを削除します。サービスのリストに表示された、サービスIDを指定します。 <pre># orchestration-cli-client --remove-service --id <ID-for-presidio-airflow-form-previous-output></pre> 次のコマンドを実行し、ノード0を更新してNGINXをリストアします。 <pre># orchestration-cli-client --update-admin-node</pre> NetWitness Platformにログインし、[管理]>[ホスト]に移動し、余分なNetWitness UEBAホストを削除します。

セクション2: ハードウェアに関するトラブルシューティングの情報

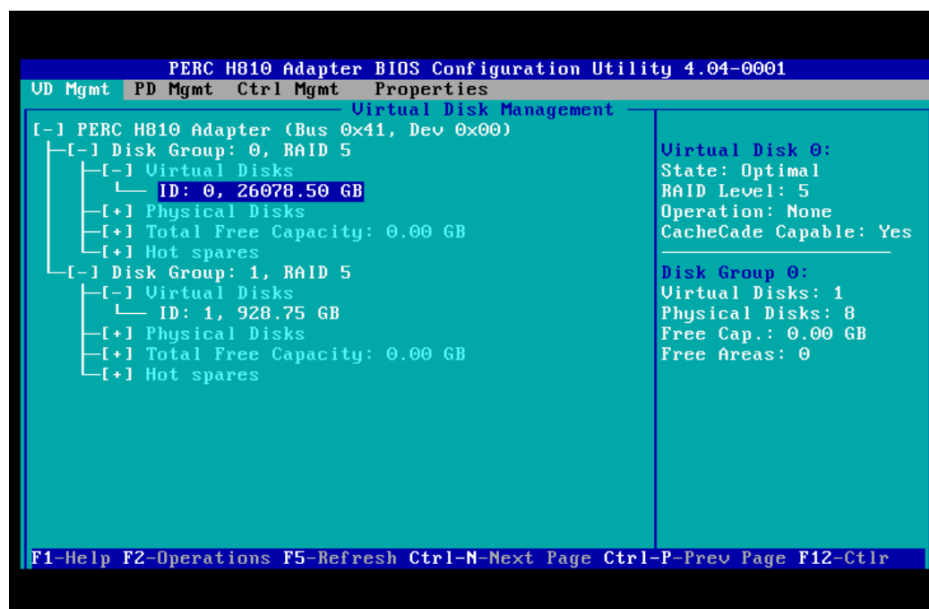
エラーメッセージ	<p>外部ストレージを持つシリーズ4アプライアンスを再起動すると、次のメッセージが表示されます。</p> <pre>Foreign configuration(s) found on adapter Press any key to continue or 'C' to load the configuration utility, or 'F' to import foreign configuration(s) and continue. All of the disks from your previous configuration are gone. If this is an unexpected message, then please power off your system and check your cables to ensure all disks are present. Press any key to continue, or 'C' to load the configuration utility. Entering the configuration utility in this state will result in drive configuration changes. Press 'Y' to continue loading the configuration utility or please power off your system and check your cables to ensure all disks are present and reboot.</pre>
原因	<p>外部ストレージ(たとえばDAC)を持つシリーズ4アプライアンス ホストを11.2にアップグレードし、アプライアンスを再起動しようとする、システムがForeign構成があると認識する可能性があります。</p>
解決策	<ol style="list-style-type: none"> 1. Fキーを押して、アプライアンスを再起動します。 正常に構成をインポートし、アプライアンスを再起動できた場合は、終了です。これが機能しない場合は、ステップ3に進みます。 2. Cキーを押して、構成ユーティリティを起動します。 <ol style="list-style-type: none"> a. PERC H8x0アダプタを選択します。  <ol style="list-style-type: none"> b. 一番上の行をハイライト表示します(たとえば、PERC H810 Adapter (Bus 65, Dev 0))。 c. メニューバーから[Foreign View]を選択します。 d. F2キーを押して[Foreign Config]ドロップダウンメニューを表示し、[Import]を選択します。



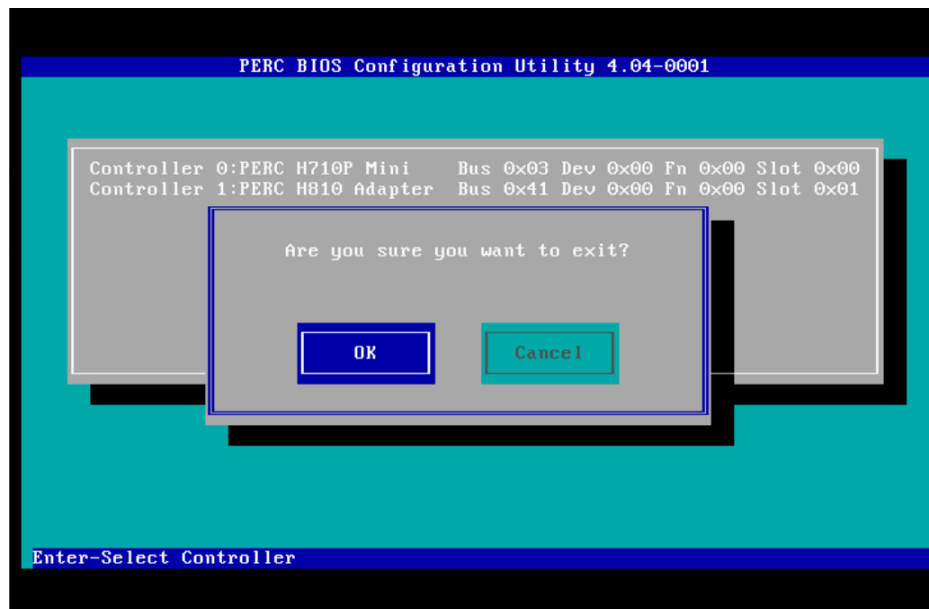
- e. [Yes]を選択し、Foreign構成をインポートすることを確認します。



- f. システムにこれ以外のForeign構成がないことを確認します。



- g. Escキーを押して、終了します。
- h. [Yes]を選択して、終了することを確認します。



- 3. Ctrl-Alt-Deleteキーを押して、アプライアンスを再起動(リブート)します。

注意 : Foreign構成が失敗した場合は、カスタマー サポートまでご連絡ください。

問題	10G Decoderのmtu.conf ファイルとpf_ringファイルがアップグレード後に./etc/init/pfring_bkupディレクトリからリストアされませんでした。
原因	10G Decoderのハードウェアドライバを使用しており、/etc/pf_ring/mtu.confファイルからMTUを使用するように/etc/init.d/pf_ringスクリプトをカスタマイズした場合、./etc/init/pfring_bkupディレクトリのmtu.conf ファイルとpf_ringファイルはアップグレード後にリストアされません。
解決策	次の手順を実行してファイルをリストアします。 <ol style="list-style-type: none">1. pf_ringファイルを11.2の/etc/init.d/ディレクトリにリストアします。 /etc/init.d/pf_ring2. mtu.confファイルを11.2の/etc/pf_ring/ディレクトリにリストアします。 /etc/pf_ring/mtu.conf

付録B: データ収集と集計の停止と再開

RSAでは、Decoder、Concentrator、Brokerホストを11.2.0.0にアップグレードする前に、ネットワークおよびログの収集と集計を停止することを推奨します。停止した場合は、これらのホストをアップグレードした後でネットワークおよびログの収集と集計を再開する必要があります。

データ収集と集計の停止

ネットワーク収集の停止

1. NetWitness Platformにログインし、[管理] > [サービス]に移動します。
[サービス]ビューが表示されます。
2. Decoderサービスを選択します。

The screenshot shows the NetWitness Platform Admin console. The top navigation bar includes RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The main menu has HOSTS, SERVICES, EVENT SOURCES, HEALTH & WELLNESS, SYSTEM, and SECURITY. The current view is SERVICES, specifically for SIT-DEC1 - Decoder. The breadcrumb trail is Change Service > SIT-DEC1 - Decoder > System. The toolbar contains Upload Packet Capture File, Stop Capture, Host Tasks, Shutdown Service, Shutdown Appliance Service, and Reboot. The main content area is divided into four sections: Decoder Service Information, Appliance Service Information, Decoder User Information, and Host User Information. The Decoder Service Information table shows Name: SIT-DEC1 (Decoder), Version: [redacted], Memory Usage: 414 MB (2.57% of 16081 MB), CPU: 51%, Running Since: 2016-Nov-15 10:12:07, Uptime: 3 days 4 hours 25 minutes, and Current Time: 2016-Nov-18 14:37:07. The Appliance Service Information table shows Name: SIT-DEC1 (Host), Version: [redacted], Memory Usage: 24876 KB (0.15% of 16081 MB), CPU: 52%, Running Since: 2016-Nov-15 10:12:04, Uptime: 3 days 4 hours 25 minutes 4 seconds, and Current Time: 2016-Nov-18 14:37:08. The bottom of the page features the RSA NETWITNESS logo.

3.  (アクション) で、[表示] > [システム]を選択します。
4. ツールバーで  Stop Capture をクリックします。


ログ収集の停止

1. NetWitness Platform にログインし、[管理] > [サービス]に移動します。
[サービス]ビューが表示されます。

2. Log Decoderサービスを選択します。

The screenshot shows the NetWitness Platform Admin console. The top navigation bar includes RESPOND, INVESTIGATE, MONITOR, CONFIGURE, and ADMIN. The main menu has HOSTS, SERVICES, EVENT SOURCES, HEALTH & WELLNESS, SYSTEM, and SECURITY. The current page is titled 'SIT-DEC1 - Decoder' and 'System'. Below the navigation, there are buttons for 'Upload Packet Capture File', 'Stop Capture', 'Host Tasks', 'Shutdown Service', 'Shutdown Appliance Service', and 'Reboot'. The main content area is divided into two columns: 'Decoder Service Information' and 'Appliance Service Information'. The 'Decoder Service Information' section shows details for SIT-DEC1 (Decoder), including Name, Version, Memory Usage (414 MB), CPU (51%), Running Since (2016-Nov-15 10:12:07), Uptime (3 days 4 hours 25 minutes), and Current Time (2016-Nov-18 14:37:07). The 'Appliance Service Information' section shows details for SIT-DEC1 (Host), including Name, Version, Memory Usage (24876 KB), CPU (52%), Running Since (2016-Nov-15 10:12:04), Uptime (3 days 4 hours 25 minutes 4 seconds), and Current Time (2016-Nov-18 14:37:08). Below these sections are 'Decoder User Information' and 'Host User Information'. At the bottom, the RSA NETWITNESS logo is visible.

3.  (アクション) で、[表示] > [システム]を選択します。

4. ツールバーで  Stop Capture をクリックします。

集計の停止

1. NetWitness Platformにログインし、[管理] > [サービス]に移動します。

2. Brokerサービスを選択します。

3.  (アクション) で、[表示] > [構成]を選択します。

4. [全般]タブが表示されます。



The screenshot shows the NetWitness Platform Admin console for the Broker service configuration. The top navigation bar is the same as in the previous screenshot. The main menu has HOSTS, SERVICES, EVENT SOURCES, HEALTH & WELLNESS, SYSTEM, and SECURITY. The current page is titled 'BROKER - Broker' and 'Config'. Below the navigation, there are buttons for 'Change Service' and 'Config'. The main content area is divided into two columns: 'Aggregate Services' and 'Aggregation Configuration'. The 'Aggregate Services' section shows a table with columns for Address, Port, Rate, Max, and Stop consuming session from the list of attached services. The 'Aggregation Configuration' section shows a table with columns for Name and Config Value. The 'System Configuration' section shows a table with columns for Name and Config Value. At the bottom, there is an 'Apply' button. The footer shows 'admin | English (United States) | GMT+00:00' and 'Send Us Feedback'.

5. [サービスの集計]の下にある、 Stop Aggregation をクリックします。



データ収集と集計の開始

11.2.0.0に更新した後、ネットワークおよびログの収集と集計を再開します。



ネットワーク収集の開始

1. NetWitness Platformにログインし、[管理] > [サービス]に移動します。
[サービス]ビューが表示されます。
2. Decoderサービスを選択します。
3.  (アクション) で、[表示] > [システム]を選択します。
4. ツールバーで  Start Capture をクリックします。

ログ収集の開始

1. NetWitness Platformにログインし、[管理] > [サービス]に移動します。
[サービス]ビューが表示されます。
2. Log Decoderサービスを選択します。
3.  (アクション) で、[表示] > [システム]を選択します。
4. ツールバーで  Start Capture をクリックします。

集計の開始

1. NetWitness Platformにログインし、[管理] > [サービス]に移動します。
[サービス]ビューが表示されます。
2. 各 Concentratorサービスおよび各 Brokerサービスで、次の手順を実行します。
 - a. サービスを選択します。
 - b.  (アクション) で、[表示] > [構成]を選択します。
 - c. ツールバーで  Start Aggregation をクリックします。

付録C: DVD ISOイメージでのiDRACの使用

多くのお客様は、物理的なアクセスが制限され、管理者のデスクトップからの帯域幅も制限されたりモートサイトにホストを設置しています。このような場合、アップグレードまたはインストールするデバイスのローカルディスクに作成したNFS共有にISOイメージを保存し、そのISOイメージをiDRACから使用することができます。この方法により、既存のNetWitnessデバイスを共有ホストとして使用することもできます。

たとえば、次のような状況が考えられます。

- 遠隔地のサイトにConcentratorとDecoderを設置している。
- 管理者のサイトから目的のサイトまでの帯域幅が比較的小さい。
- USBスティックを発送し、管理者がアップグレードを実施する間、遠隔地の担当者がUSBスティックをデバイスに差し込むという方法が現実的ではない。

このような場合、次の操作を実行できます。

1. nfs-utils rpmをインストールします。
2. NFS共有を構成します。
3. iDRACを構成し、NFS共有への接続を追加します。
サポート対象のWindowsまたはLinuxオペレーティングシステムで、iDRACファームウェアを更新します。更新は、DellサポートWebサイト (<http://www.support.dell.com>) からサポート対象のWindowsまたはLinuxオペレーティングシステム用のDell Update Packageをダウンロードして、実行します。詳細については、DellサポートWebサイト (http://topics-cdn.dell.com/pdf/dell-update-packages-v17.10.00_User's%20Guide_en-us.pdf) の「Dell Update Package User's Guide」を参照してください。
4. ISOファイルを含む仮想メディアからブートし、アップグレードを実行します。

NFSサーバの構成

1. yumを使用してNFSとその共有ユーティリティをインストールします。
`yum install nfs-utils`
2. NFSサービスをブート時に実行するよう構成します。
`chkconfig nfs on`
3. rpcbindサービスをブート時に実行するよう構成します。
このサービスはNFSが必要とするサービスです。NFSを開始する前に開始する必要があります。
`chkconfig rpcbind on`
4. rpcbindサービスを開始します。
`service rpcbind start`
5. NFSサービスを開始します。
`service nfs start`
6. 最初のエクスポート用のディレクトリを作成します。
`mkdir /exports/files`

7. NFSのexportsファイルをテキスト エディタで開きます。
`vi /etc/exports`
8. すべてのユーザに読み取り専用アクセスでディレクトリをエクスポートするには、次の行を追加します。
`/exports/files *(ro)`
9. 変更内容を保存して、エディタを終了します。
`:wq!`
10. 上記で定義したディレクトリをエクスポートします。
`exportfs -a`
11. アップグレードの実行中は、ファイアウォールのルールを無効化します。
`service iptables stop`
12. ISOファイルを含むインストールメディアを/exports/files ディレクトリにコピーします。

iDRACでのNFSとブートの構成

注: iDRACファームウェアがシリーズ4 (R620) の1.57.57以上であることを確認する必要があります。

1. iDRACインタフェースにログインします。
2. リモート ファイル共有をメディアとして接続します。
`<server ip>:/export/files/11.2.0.0.iso`
例: `10.10.10.10:/exports/files/rsa-11.2.0.0.1948.el7-usb.iso`
3. [Connect]をクリックします。
4. コンソールを起動します。
5. [Next Boot]メニューから[Virtual DVD/CD]を選択します。
6. デバイスをリブートします。

付録D: 外部リポジトリの作成

外部リポジトリ (Repo) をセットアップするには、次の手順を実行します。

注: 1.) この手順を完了するには、ホストに解凍ユーティリティがインストールされている必要があります。2.) 次の手順を実行する前に、Webサーバの作成方法を理解する必要があります。

1. Webサーバホストにログインします。
2. NWリポジトリ (netwitness-11.2.0.0.zip) をホストするディレクトリを作成します(例: Webサーバのweb-root の下のziprepo)。たとえば、/var/netwitnessがweb-rootの場合、次のコマンドを実行します。

```
mkdir -p /var/netwitness/<your-zip-file-repo>
```
3. 11.2.0.0 ディレクトリを/var/netwitness/<your-zip-file-repo>の下に作成します。

```
mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0
```
4. OSおよびRSAディレクトリを/var/netwitness/<your-zip-file-repo>/11.2.0.0の下に作成します。

```
mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS  
mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0/RSA
```
5. netwitness-11.2.0.0.zipファイルを/var/netwitness/<your-zip-file-repo>/11.2.0.0ディレクトリに解凍します。

```
unzip netwitness-11.2.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.2.0.0
```

netwitness-11.2.0.0.zipを解凍すると、2つのzipファイル(OS-11.2.0.0.zipおよびRSA-11.2.0.0.zip)とその他のファイルがいくつか現れます。
6. 以下のように解凍します。
 - a. OS-11.2.0.0.zipを /var/netwitness/<your-zip-file-repo>/11.2.0.0/OSディレクトリに解凍します。

```
unzip /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS-11.2.0.0.zip -d /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS
```

次の例は、ファイル解凍後のOS(オペレーティングシステム)ファイルの構造を示しています。

Parent Directory		
GeoIP-1.5.0-11.el7.x86_64.rpm	20-Nov-2016 12:49	1.1M
HostAgent-Linux-64-x86-en_US-1.2.25.1.0163-1.x86_64.rpm	03-Oct-2017 10:07	4.6M
Lib_Utils-1.00-09.noarch.rpm	03-Oct-2017 10:05	1.5M
OpenIPMI-libs-2.0.19-15.el7.x86_64.rpm	20-Nov-2016 14:43	502K
OpenIPMI-modalias-2.0.19-15.el7.x86_64.rpm	20-Nov-2016 14:43	15K
PyYAML-3.11-1.el7.x86_64.rpm	19-Dec-2017 12:30	160K
SDL-1.2.15-14.el7.x86_64.rpm	25-Nov-2015 10:39	204K
acl-2.2.51-12.el7.x86_64.rpm	03-Oct-2017 10:04	81K
adobe-source-sans-pro-fonts-2.020-1.el7.noarch.rpm	13-Feb-2018 05:10	706K
alsa-lib-1.1.3-3.el7.x86_64.rpm	10-Aug-2017 10:52	421K
at-3.1.13-22.el7_4.2.x86_64.rpm	25-Jan-2018 17:56	51K
atk-2.22.0-3.el7.x86_64.rpm	10-Aug-2017 10:53	258K
attr-2.4.46-12.el7.x86_64.rpm	03-Oct-2017 10:04	66K

- b. RSA-11.2.0.0.zipを/var/netwitness/<your-zip-file-repo>/11.2.0.0/RSAディレクトリに解凍します。

```
unzip /var/netwitness/<your-zip-file-repo>/11.2.0.0/RSA-11.2.0.0.zip -d
/var/netwitness/<your-zip-file-repo>/11.2.0.0/RSA
```

次の例は、ファイル解凍後のRSAバージョン更新ファイルの構造を示しています。

Parent Directory		
MegaCli-8.02.21-1.noarch.rpm	03-Oct-2017 10:07	1.2M
OpenIPMI-2.0.19-15.el7.x86_64.rpm	03-Oct-2017 10:07	173K
bind-utils-9.9.4-51.el7_4.2.x86_64.rpm	22-Jan-2018 09:03	203K
bzip2-1.0.6-13.el7.x86_64.rpm	03-Oct-2017 10:07	52K
cifs-utils-6.2-10.el7.x86_64.rpm	10-Aug-2017 11:14	85K
device-mapper-multipath-0.4.9-111.el7_4.2.x86_64.rpm	25-Jan-2018 17:56	134K
dnsmasq-2.76-2.el7_4.2.x86_64.rpm	02-Oct-2017 19:36	277K
elasticsearch-5.6.9.rpm	17-Apr-2018 09:37	32M
erlang-19.3-1.el7.centos.x86_64.rpm	03-Oct-2017 10:07	17K
fineserver-4.6.0-2.el7.x86_64.rpm	27-Feb-2018 09:11	1.3M
htop-2.1.0-1.el7.x86_64.rpm	14-Feb-2018 19:23	102K
i40e-zc-2.3.6.12-1dkms.noarch.rpm	04-May-2018 11:08	399K
ipmitool-1.8.18-5.el7.x86_64.rpm	10-Aug-2017 12:41	441K
iptables-services-1.4.21-18.3.el7_4.x86_64.rpm	08-Mar-2018 09:20	51K
ixgbe-zc-5.0.4.12-dkms.noarch.rpm	04-May-2018 11:08	374K

Repoの外部URLはhttp://<web server IP address>/<your-zip-file-repo>です。

7. NW 11.2.0.0セットアッププログラム(nwsetup-tui)が[Enter the base URL of the external update repositories]プロンプトを表示したら、http://<web server IP address>/<your-zip-file-repo>と入力します。

改訂履歴

リビジョン	日付	説明	作成者
1.0	2018年8月17日	Release to Operations	IDD