



ホスト およびサービス スタート ガイド

バージョン 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

ホストおよびサービスの基本情報	9
ホストとは	9
ホスト タイプとは	9
サービスとは	10
ホストのセットアップ	11
ホストのメンテナンス	12
更新のバージョン命名規則	12
サービスのメンテナンス	13
NetWitness Serverに実装されるサービス	13
混在モードでの実行	14
時間差更新中に生じる機能のギャップ	14
段階的アップグレードの例	14
例2. 複数のDecoderとConcentrator、代替方法2	15
例3. 複数の地域に分散する場合	16
ホストとサービスの手順	17
ステップ1. ホストの導入	19
ステップ2. ホストへのサービスのインストール	20
ステップ3. 信頼接続のためのSSLポートの確認	21
暗号化されたSSLポート	22
ステップ4. サービスへのアクセスの管理	23
信頼接続のテスト	23
ホストへのバージョン更新の適用	26
[ホスト]ビューから更新を適用する(Webアクセスあり)	26
タスク1: ローカルリポジトリに更新を配置するか、外部リポジトリをセットアップする	26
タスク2: [ホスト]ビューから各ホストに更新を適用する	26
コマンドラインから更新を適用する(Webアクセスなし)	28
ローカル更新リポジトリへの更新の配置	29
RSAおよびOS更新の外部リポジトリのセットアップ	31
ホストグループの作成と管理	34
グループの作成	34
グループ名の変更	35
グループへのホストの追加	35
グループ内のホストの表示	35
グループからのホストの削除	36
グループの削除	37
ホストの検索	37

ホストの検索	37
サービスを実行するホストの検索	37
ホストのタスクリストからのタスクの実行	38
ファイルシステム監視の追加と削除	41
ファイルシステム監視の構成	41
ファイルシステム監視の削除	42
ホストの再起動	42
[ホスト]ビューからのホストのシャットダウンおよび再起動	43
[ホスト タスクリスト]からのホストのシャットダウンおよび再起動	43
ホスト内蔵クロックの設定	43
ローカル クロックでの時刻の設定	44
ネットワーク構成の設定	44
ホストのネットワークアドレスの指定	45
ネットワークタイムソースの設定	45
ネットワーククロックソースの指定	46
SNMPの設定	46
ホスト上のSNMPサービスのオン/オフ	47
Syslog転送の設定	48
Syslog転送の設定と開始	48
ネットワークポートステータスの表示	49
ネットワークポートステータスの表示	49
シリアル番号の表示	50
シリアル番号の表示	50
ホストのシャットダウン	51
ホストのシャットダウン	51
ホスト上のサービスの停止と開始	52
ホストでのサービスの停止	52
ホストでのサービスの開始	53
サービスユーザの追加、レプリケート、削除	53
手順	54
サービスユーザのロールの追加	57
手順	58
サービスユーザのパスワードの変更	59
サービスグループの作成と管理	60
グループの作成	61
グループ名の変更	62
グループへのサービスの追加	62
グループ内のサービスの表示	62
グループからのサービスの削除	62
グループの削除	63

サービス ロールの複製またはレプリケート	63
サービス ロールの複製	64
ロールのレプリケート	64
コア サービス構成 ファイルの編集	65
サービス構成 ファイルの編集	65
バックアップのサービス構成 ファイルへのロールバック	66
他のサービスへの構成 ファイルのプッシュ	66
サービスの編集または削除	75
手順	77
サービスのプロパティ ツリーの表示と編集	78
サービスへの接続の強制終了	80
サービスのセッションの強制終了	80
セッションのアクティブなクエリの強制終了	81
サービスの検索	81
サービスの検索	81
サービスのタイプによるフィルタ	82
ホスト上のサービスの検索	84
サービスの起動、停止、再起動	84
サービスの開始	84
サービスの停止	85
サービスの再起動	85
サービスの詳細の表示	85
各サービスビューの目的	85
サービスビューへのアクセス	86
[ホスト]と[サービス]ビューの参考情報	88
[ホスト]ビュー	89
ワークフロー	90
実行したいことは何ですか?	90
簡単な説明	91
[ホスト]パネル ツールバー	91
[グループ]パネル ツールバー	92
[サービス]ビュー	94
ワークフロー	95
実行したいことは何ですか?	95
関連トピック	96
簡単な説明	96
[サービスの編集]ダイアログ	100
[グループ]パネル ツールバー	102
[サービス]パネル ツールバー	103
サービスの[構成]ビュー	104

トピック	108
機能	109
サービス構成ファイルの編集	111
[ファイル]タブ ツールバー	111
サービスの[エクスプローラ]ビュー	113
ノード リスト	114
[監視]パネル	115
機能	117
[サービス]の[ログ]ビュー	118
[サービス]の[セキュリティ]ビュー	120
ロールとサービスへのアクセス	122
機能	123
[ロール名]パネル	123
[ロールの情報と権限]パネル	124
サービス ユーザ ロール	125
サービス ユーザ権限	126
機能	130
SDKメタ ロール権限のオプション	130
機能	133
[ユーザリスト]パネル	133
[ユーザ定義]パネル	135
[サービス]の[統計]ビュー	138
[サマリ統計]セクション	139
ゲージ	142
タイムライン	142
履歴タイムライン	142
統計チャートトレイ	142
コンポーネント	144
機能	145
システム ビュー	148
[サービス情報]ツールバー	150
機能	152
ホスト タスク選択リスト	153
サービス構成設定	155
Applianceサービスの構成パラメータ	155
Archiverサービスの構成ビュー	155
Brokerサービスの構成パラメータ	157

集計の構成パラメータ	158
Concentratorサービスの構成パラメータ	159
コアサービスのログ構成パラメータ	160
コアサービス間接続の構成パラメータ	161
コアサービスのシステム構成パラメータ	162
Decoderサービスの構成パラメータ	163
DecoderおよびLog Decoderの構成パラメータ	163
Log Decoderサービスの構成パラメータ	166
RESTインタフェースの構成パラメータ	169
NetWitness Platformコアサービスのsystem.rolesモード	169
インストールと更新のトラブルシューティング	171
ホストの更新失敗	171
サービスの更新失敗	172
ホストの更新ダウンロード エラー	173
deploy_adminパスワードの有効期限切れ	174

ホストおよびサービスの基本情報

このガイドは、管理者がNetWitness Platformのホストおよびサービスの追加、構成を行うための標準的な手順を提供します。ホストおよびサービスの基本的な目的とNetWitness Platformネットワーク内での機能の概要を示した後、以下の項目についても説明します。

- ホストやサービスをセットアップするために完了する必要があるタスク。
- 組織の長期的かつ日常的な運用のニーズに基づいて実行する追加の手順。
- ユーザ インタフェースに関するリファレンストピック

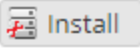
NetWitness Platform Logs & Network 11.xのすべてのドキュメントの一覧は、「[マスター目次](#)」で確認できます。

ホストとは

ホストは、サービスを実行するマシンです。物理マシンと仮想マシンがあります。ホストがどのように導入されるかについては、『*NetWitness Platform 導入ガイド*』の「NetWitness Platform導入環境のホスト詳細図」を参照してください。

ホスト タイプとは

ホスト タイプは、[ホスト]ビューからホストをインストールするときに選択し、ホストにサービスを割り当てま

す。[ホスト タイプ]は、[ホスト]ビューでホストを選択し、 (インストールアイコン) をクリックすると表示される[サービスのインストール]ダイアログで選択します。次の表は、各ホスト タイプと、インストールされるサービスを示しています。ホストがどのように導入されるかについては、『*NetWitness Platform 導入ガイド*』の「NetWitness Platform導入環境のホスト詳細図」を参照してください。

ホスト タイプ	インストールされるサービス
Archiver	WorkbenchとArchiver
Broker	Broker
Cloud Gateway	Cloud Gateway
Concentrator	Concentrator
Endpoint Hybrid	Log Decoder、Endpoint、Concentrator
Endpoint Log Hybrid	Log Collector、Log Decoder、Endpoint、Concentrator
ESAプライマリ	Context Hub、Entity Behavior Analysis、Event Stream Analysis
ESAセカンダリ	Event Stream Analysis、Entity Behavior Analysis
Log Collector	Log Collector

ホスト タイプ	インストールされるサービス
Log Decoder	Log CollectorとLog Decoder
Log Hybrid	Log Collector、Log Decoder、Concentrator
Malware Analysis	Malware AnalysisとBroker
Network Decoder	Decoder(Packets)
Network Hybrid	ConcentratorとDecoder
UEBA	UEBA
Warehouse Connector	Warehouse Connector

サービスとは

サービスは、ログの収集やデータのアーカイブなど、固有の機能を実行します。各サービスは、専用ポートで実行され、ホストの機能に従って有効化または無効化するプラグインとして提供されます。

最初に次のコアサービスを構成する必要があります。

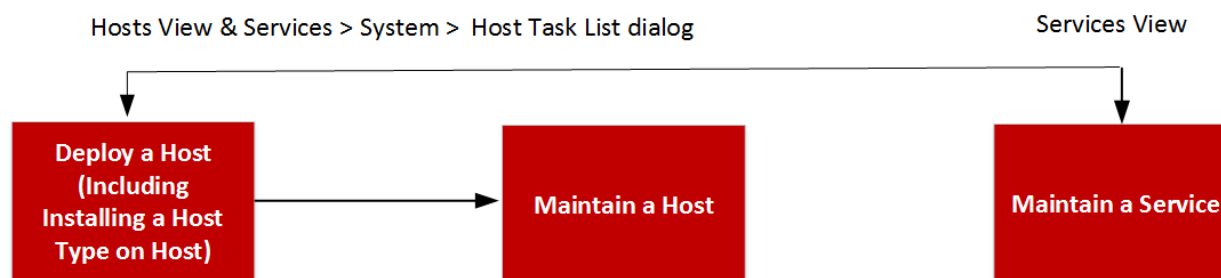
- Decoder
- Concentrator
- Broker
- Log Decoder

次の表にすべてのサービスを示します。Log Collectorを除く各サービスについては、それぞれのガイドまたは共通のガイド「ホストおよびサービスの構成ガイド」が提供されます。Log Collectorには、サポートするすべてのイベント収集プロトコルの構成を処理するため、独自の構成ガイドのセットが提供されます。Log Collectorについては、「ログ収集ガイド」を参照してください。

サービス	暗号化されない 非SSLポート	暗号化された SSLポート	注
管理者	N/A	N/A	NW Serverに実装されます
Archiver	50008	56008	
Broker	50003	56003	コア サービス
Cloud Gateway	N/A	N/A	
Concentrator	50005	56005	コア サービス
Config	N/A	N/A	NW Serverに実装されます。
Content	N/A	N/A	NW Serverに実装されます
Context Hub	N/A	N/A	

サービス	暗号化されない 非SSLポート	暗号化された SSLポート	注
Decoder(Packets)	50004	56004	コア サービス
Endpoint	N/A	N/A	
Entity Behavior Analysis	N/A	N/A	
Event Stream Analysis	N/A	50030	
Integration	N/A	N/A	NW Serverに実装されます。
Investigate	N/A	N/A	NW Serverに実装されます。
Log Collector	50001	56001	
Log Decoder	50002	56002	コア サービス
Malware Analysis	N/A	60007	
Orchestration	N/A	N/A	NW Serverに実装されます。
Reporting Engine	N/A	51113	NW Serverに実装されます。
Respond	N/A	N/A	NW Serverに実装されます。
Security	N/A	N/A	NW Serverに実装されます。
Source	N/A	N/A	NW Serverに実装されます
UEBA	N/A	N/A	
Warehouse Connector	50020	56020	
Workbench	50007	56007	

ホスト やサービスがデータの格納や収集などの機能を実行するには、ネットワークおよび他のホストやサービスと相互に通信するようにホストとサービスを構成する必要があります。



ホストのセットアップ

[ホスト]ビューを使用してホストをNetWitness Platformに追加します。 詳細な手順については、「[ステップ1. ホストの導入](#)」を参照してください。

ホストのメンテナンス

メインの[管理]>[ホスト]ビューを使用して、導入環境内のホストの追加、編集、削除、その他のメンテナンスタスクを実行します。[タスクリスト]ダイアログを使用してホストおよびホストとネットワークの通信に関連するタスクを実行します。詳細な手順については、「[ホストとサービスの手順](#)」を参照してください。

NetWitness Platformの初期導入後、[ホスト]ビューから実行する主なタスクは、NetWitness Platform 導入環境を新しいバージョンに更新することです。

更新のバージョン命名規則

[ローカル更新リポジトリへの更新の配置](#)から最新のバージョン更新を適用するには、[ホスト]ビューを使用します。ホストに適用するバージョンを区別するために、更新のバージョン命名規則を理解しておく必要があります。命名規則は、**メジャー リリース**、**マイナー リリース**、**サービス パック**、**パッチ**です。たとえば、11.6.1.2を選択した場合、次のバージョンがホストに適用されます。

- 11 = メジャー リリース
- 6 = マイナー リリース
- 1 = サービス パック
- 2 = パッチ

NetWitness Platformは、導入環境内での複数のバージョンの使用をサポートしています。NetWitness Server (NW Server) ホストが最初に更新され、他のすべてのホストはNW Serverホストと同じバージョンまたはそれ以前のバージョンである必要があります。

次の例は、すべてのホストが11.2.0.0(この時点での最新リリース)に更新された単一バージョンの導入環境を示しています。

The screenshot shows the 'Hosts' view in the NetWitness Platform interface. The table lists various host types and their service update status. The 'Services' column shows the number of services that need updating, and the 'Status' column shows the current update status.

Name	Host	Services	Current Version	Update Version	Status
<input type="checkbox"/> NW Server (co-located Broker)	IP-address	12	11.2.0.0		Up-to-Date
<input type="checkbox"/> Archiver	IP-address	2	11.2.0.0		Up-to-Date
<input type="checkbox"/> Concentrator	IP-address	1	11.2.0.0		Up-to-Date
<input type="checkbox"/> Endpoint Log Hybrid	IP-address	4	11.2.0.0		Up-to-Date
<input type="checkbox"/> Event Stream Analysis Primary	IP-address	4	11.2.0.0		Up-to-Date
<input type="checkbox"/> Log Decoder	IP-address	2	11.2.0.0		Up-to-Date
<input type="checkbox"/> Log Hybrid	IP-address	3	11.2.0.0		Up-to-Date
<input type="checkbox"/> Malware Analysis	IP-address	2	11.2.0.0		Up-to-Date
<input type="checkbox"/> Network Decoder (Packets)	IP-address	1	11.2.0.0		Up-to-Date
<input type="checkbox"/> Network Hybrid (Packets)	IP-address	2	11.2.0.0		Up-to-Date

サービスのメンテナンス

[管理] > [サービス]ビューを使用して、導入環境内のサービスの追加、編集、削除、監視、その他のメンテナンスタスクを実行します。詳細な手順については、「[ホストとサービスの手順](#)」を参照してください。

NetWitness Serverに実装されるサービス

次の表のサービスは、NW Serverを導入するとインストールされます。次の機能を提供します。

- 物理および仮想プラットフォームの拡張、ホストおよびサービスのメンテナンスの強化。
- コンテンツ、調査、対応、ソースの機能。

注意 : NetWitness Platformを導入するためにこれらのサービスを構成する必要はありません。RSAでは、ヘルスマニタを使用してこれらのサービスの稼働ステータスを監視することを推奨します。RSAカスタマーサポートの指示がある場合を除き、[エクスプローラ]ビューでこれらのサービスのパラメータを変更しないでください。

サービス	目的
Admin	Administration Server(Admin Server) は、NetWitness Platform UI(ユーザインタフェース) の管理タスクのためのバックエンド サービスです。このサービスでは、UIでの認証、グローバル環境設定の管理、許可のサポートを抽象化します。Admin Serverが機能するためには、Config ServerとSecurity Serverがオンラインである必要があります。
Config	Configuration Server(Config Server) は、構成セットを格納および管理します。構成セットは、個々に管理される構成の論理的グループです。Config Serverは、サービス間でのプロパティの共有を促進し、構成のバックアップとリストア機能を提供し、プロパティの変更を追跡します。
Content	Content Serverは、RSA提供のParserルールと、ユーザ作成のParserルールを管理します。Parserの管理の詳細については、RSA Linkで「parsers」を検索してください。
Integration	Integration Serverは外部システムとのやり取りを管理します。このサービスは、次のアウトバウンドまたはインバウンド チャンネルを処理します。 <ul style="list-style-type: none"> • REST API Gateway: 外部RESTクライアントへのゲートウェイとして、呼び出しをNetWitness API(Application Programming Interface) に割り当てます。 • Notifications Dispatcher: NetWitness導入環境からのすべてのアウトバウンド通知の一元化されたディスパッチャーです。
Investigate	Investigate Serverは、調査およびマルウェア解析機能をサポートします。詳細については、『 <i>NetWitness Platform Investigate ユーザガイド</i> 』を参照してください。
Orchestration	Orchestration Server(Orchestration Server) は、NetWitness Platform導入環境のすべてのサービスをプロビジョニング、インストール、構成します。
Respond	Respond Serverは、インシデント対応機能をサポートします。詳細については、『 <i>NetWitness Platform Respond構成ガイド</i> 』を参照してください。

サービス	目的
Security	<p>NetWitness Platform Security Server(Security Server) は、NetWitness Platform導入環境のセキュリティ インフラストラクチャを管理します。次のセキュリティ関連の処理を実行します。</p> <ul style="list-style-type: none"> • ユーザおよび認証アカウント • RBAC(ロール ベースのアクセス制御) • 導入環境のPKIインフラストラクチャ <p>NetWitness Platform導入環境では、ユーザの認証アカウントが管理されます。アナリストのIDを確認する方法(Active Directoryなど)とは別に、NetWitness Platformでは、認証プロバイダーから提供されないユーザの状態(最後のログイン時刻、失敗したログイン試行、ロールなど)を管理する必要があります。ユーザの概念は、ユーザに関連付けられたIDと分離され、Security Serverによって、個別のユーザおよびアカウント エンティティとして管理されます。すべてのNetWitness導入環境で利用可能な標準のローカルNetWitnessアカウントに加え、外部の認証プロバイダーをサポートします。</p> <p>Security Serverは、ロールと権限のエンティティを管理してRBACも実装します。権限をロールに割り当てることができ、ロールをユーザに割り当てることができます。これらが連携して、導入環境に対する柔軟な認証ポリシーを実現できます。Security Serverは、ユーザへの適切な認可をエンコードするため、暗号化されたトークンの生成も管理します。これらのトークンは、導入環境全体の認可の基礎を形成します。</p>
Source	<p>Source Serverは将来の使用のために予約されており、ソース(エンドポイントやログソースなど)の構成を一元的に管理する機能を提供する予定です。</p>

混在モードでの実行

混在モードは、最新バージョンに更新されたサービスと、古いバージョンのままのサービスが混在するときに生じます。この状況は、導入環境のホストを複数のフェーズで最新バージョンに更新する場合(または時間差で更新する場合)に起こります。

時間差更新中に生じる機能のギャップ

時間差で更新する場合は、以下のような状況が発生します。

- 導入環境全体が更新されるまで、機能が完全に動作しないことがあります。
- 導入環境内のすべてのホストを更新するまでサービス管理機能を利用できません。
- 一定期間データが収集されません。

段階的アップグレードの例

次の例では、すべてのホストが11.2.0.xで、ホストをバージョン11.2.1.0に時間差で更新します。

例1. 複数のDecoderとConcentrator、代替方法1

この例では、11.0.2.x導入環境に1つのNW Serverホスト、2つのDecoderホスト、2つのConcentratorホスト、1つのArchiverホスト、1つのBrokerホスト、1つのEvent Stream Analysisホスト、1つのMalware Analysisホストが含まれています。

まずフェーズ1を完了し、フェーズ1に示した順序でホストを更新する必要があります。

RSAでは、フェーズ1に示した順序で、フェーズ2のホストを更新することを推奨しています。

フェーズ1 - セッション1

1. NetWitness Serverホストを更新します。
2. Event Stream Analysisホストを更新します。
3. Malware Analysisホストを更新します。
4. BrokerまたはConcentratorホストを更新します。

フェーズ2 - セッション2

1. 2つのDecoderホストを更新します。
2. 2つのConcentratorホストとArchiverホストを更新します。

フェーズ2 - セッション3

1. 他のすべてのホストを更新します。

例2. 複数のDecoderとConcentrator、代替方法2

この例では、11.0.2.x導入環境に1つのNW Serverホスト、2つのDecoderホスト、2つのConcentratorホスト、1つのBrokerホスト、1つのEvent Stream Analysisホスト、1つのMalware Analysisホストが含まれています。RSAでは、フェーズ2のホストを以下の順番で更新することを推奨しています(最初にフェーズ1を完了し、記載された順序でホストを更新する必要があります)。

フェーズ1 - セッション1

1. NetWitness Serverホストを更新します。
2. Event Stream Analysisホストを更新します。
3. Malware Analysisホストを更新します。
4. Brokerホストを更新します。

フェーズ2 - セッション2

1. 1つのDecoderホストと1つのConcentratorホストを更新します。
NetWitness Platformが特に大量のデータを処理する場合、時間がかかります。

フェーズ2 - セッション3

1. 1つのDecoderホスト、1つのConcentratorホストおよびBrokerホストを更新します。
2. Virtual Log Collectorを更新する前に、すべてのLog Decoderホストを更新します。
3. 他のすべてのホストを更新します。

例3. 複数の地域に分散する場合

この例では、11.2.0.x導入環境に1つのNW Serverホスト、1つのEvent Stream Analysisホスト、1つのMalware Analysisホスト、4つのDecoderホスト、4つのConcentratorホスト、2つのBrokerホスト(2つのサイトに、それぞれ2つのDecoder、2つのConcentrator、および1つのBrokerを配置)が含まれます。

フェーズ1 - サイト1の更新

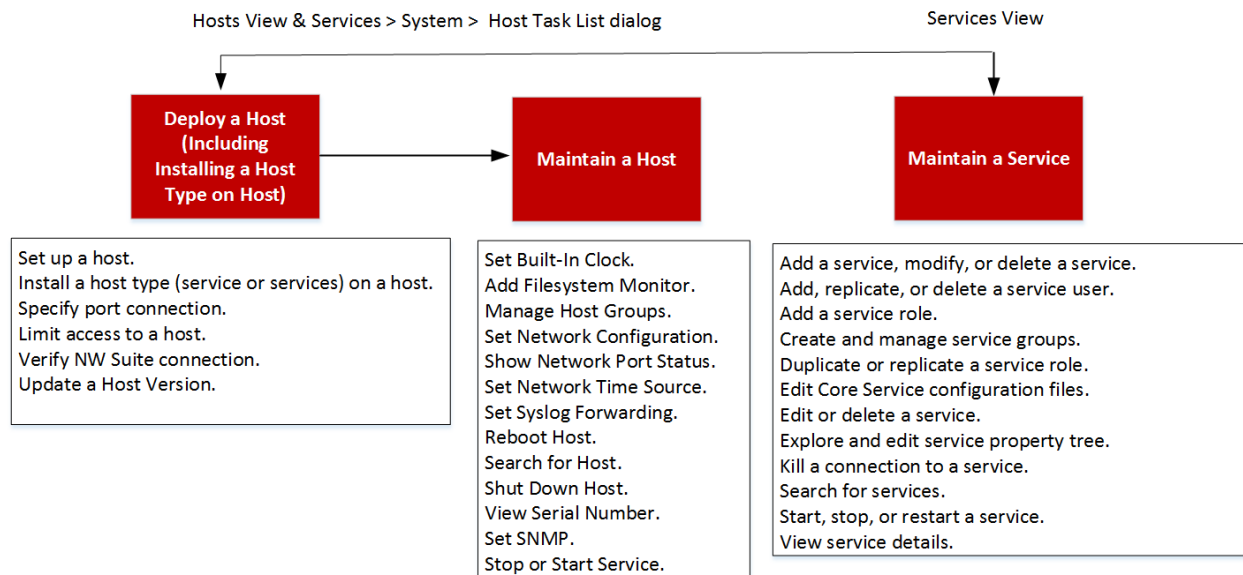
1. NW Serverホストを更新します。
2. Event Stream Analysisホストを更新します。
3. Malware Analysisホストを更新します。
4. 1つのBrokerホスト、2つのDecoderホスト、2つのConcentratorホストを更新します。
5. 他のすべてのホストを更新します。

フェーズ2 - サイト2の更新

1. Brokerホストを更新します。
2. 2つのDecoderホストを更新します。
3. 2つのConcentratorホストを更新します。
4. 他のすべてのホストを更新します。

ホストとサービスの手順

すべてのサービスにホストが必要です。ホストのセットアップ後、このホストにサービスを割り当て、さらに、このホストからNetWitness Platform導入環境の別のホストにサービスを割り当てることができます。



タスクの概要	説明
ホストのセットアップ	<p>ホストをセットアップするには、次のタスクを順番に実行します。</p> <p>ステップ1. ホストを導入します。</p> <p>ステップ2. ホストにサービスをインストールします。</p> <p>ステップ3. 信頼接続のためのSSLポートを確認します。</p> <p>ステップ4. サービスへのアクセスを管理します。</p>

タスクの概要	説明
<p>ホストのメンテナンス - 基本</p>	<p>次のメンテナンス タスクはアルファベット 順になっています。</p> <ul style="list-style-type: none"> • ホストへのバージョン更新の適用 <ul style="list-style-type: none"> • ローカル更新リポジトリへの更新の配置 • RSAおよびOS更新の外部リポジトリのセットアップ • ホスト グループの作成と管理 • ホストの検索 • ネットワーク構成の設定 • ネットワーク タイム ソースの設定 • ネットワーク ポート ステータスの表示 • シリアル番号の表示 • ホストのシャットダウン • ホスト上のサービスの停止と開始
<p>[ホスト タスク リスト] ダイアログからのホストのメンテナンス</p>	<p>[ホスト タスク リスト] ダイアログを使用して、ホストおよびホストとネットワークの通信に関連するタスクを管理できます。コア ホストでは、複数のサービスおよびホストの構成オプションが使用できます。</p> <ul style="list-style-type: none"> • ホストのタスク リストからのタスクの実行 • ファイルシステム監視の追加と削除 • ホストの再起動 • ホスト内蔵クロックの設定 • ネットワーク構成の設定 • ネットワーク タイム ソースの設定 • SNMPの設定 • Syslog転送の設定 • ネットワーク ポート ステータスの表示 • シリアル番号の表示 • ホストのシャットダウン • ホスト上のサービスの停止と開始

タスクの概要	説明
サービスのメンテナンス	<p>次の手順では、サービスのメンテナンス方法について説明します。</p> <ul style="list-style-type: none"> • サービス ユーザの追加、レプリケート、削除 • サービス ユーザのロールの追加 • サービス ユーザのパスワードの変更 • サービス グループの作成と管理 • サービス ロールの複製またはレプリケート • コア サービス構成ファイルの編集 • サービスの編集または削除 • サービスのプロパティツリーの表示と編集 • サービスへの接続の終了 • サービスの検索 • サービスの起動、停止、再起動 • サービスの詳細の表示

ステップ1. ホストの導入

注意: ホスト名に「.」を含める場合は、有効なドメイン名も含める必要があります。

1. ホストを導入します。

物理ホスト(RSAアプライアンス)、オンプレミスの仮想ホスト、AWSの仮想ホスト、Azureの仮想ホストを導入できます。ホストを導入する手順については、次のガイドを参照してください。

- [RSA NetWitness® Platform 物理ホスト インストールガイド](#)
- [RSA NetWitness® Platform 仮想ホスト インストールガイド](#)
- [RSA NetWitness® Platform AWS導入ガイド](#)
- [RSA NetWitness® Platform Azure 導入ガイド](#)

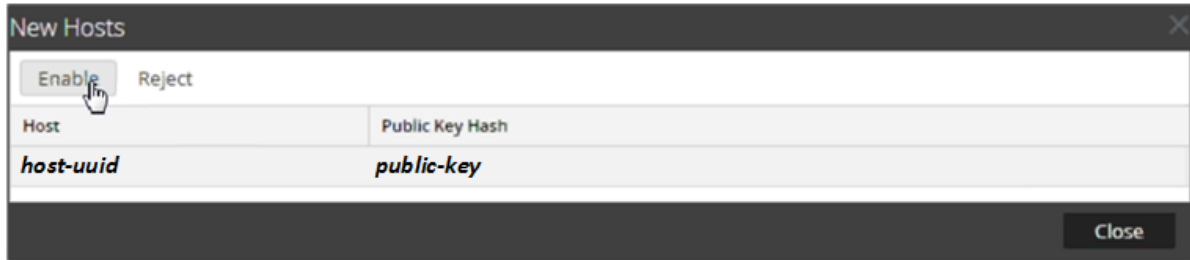
2. [管理] > [ホスト]に移動します。

[新しいホスト]ダイアログが表示され、導入したホストが表示されます。

3. 有効化するホストを選択します。

[有効化]メニュー オプションがアクティブになります。

4. [有効化]をクリックします。





- 有効化したホストを選択します。

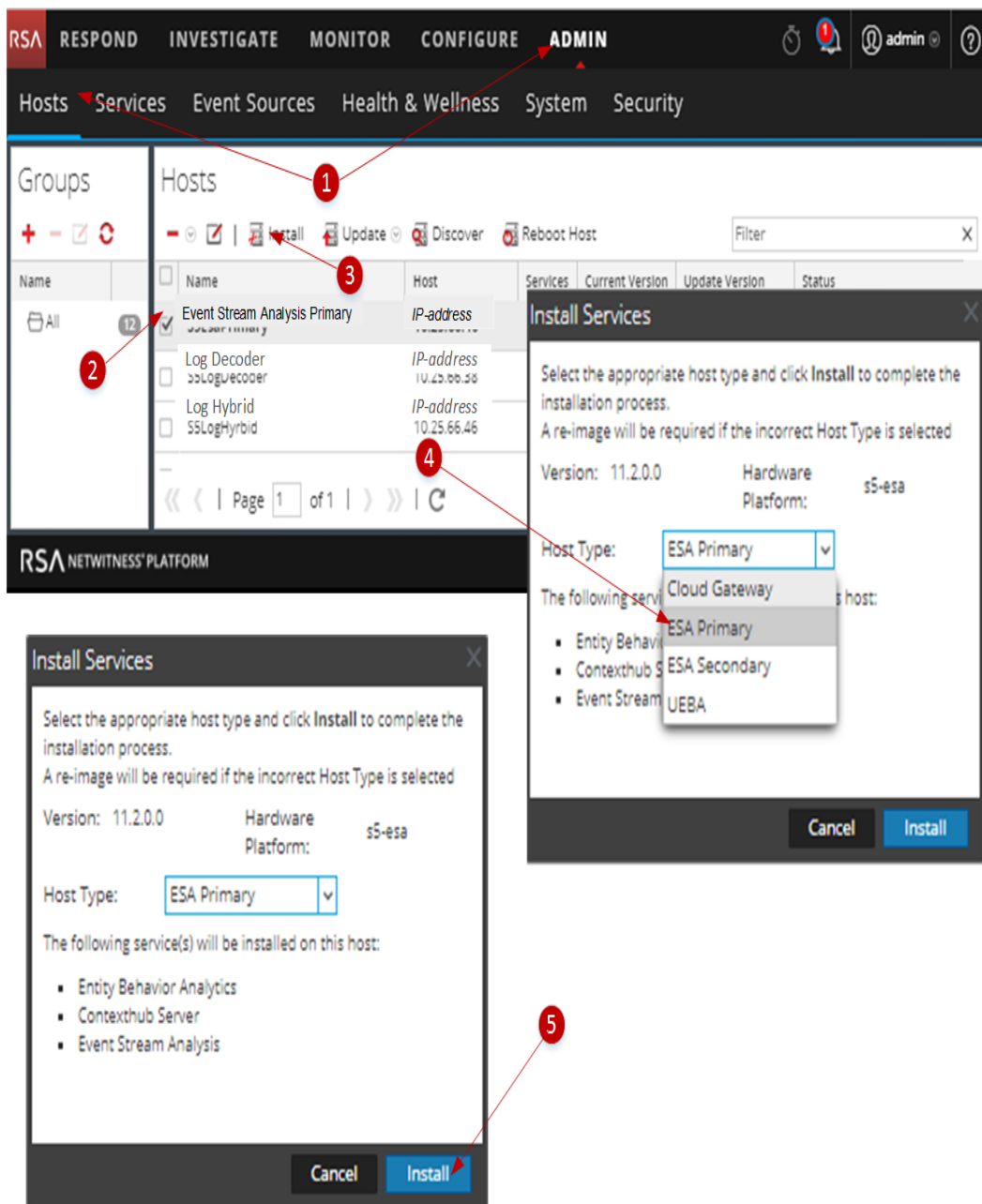
ホストは[ホスト]ビューに表示されます。この時点では、ホストでサービスをインストールできます。

ステップ2. ホストへのサービスのインストール

サービスをホストにインストールするには、次の手順を実行します。

- NetWitness Platformで、[管理]>[ホスト]に移動します。
[ホスト]ビューが表示されます。
- サービスをインストールするホストを選択します(たとえば、Event Stream Analysis)。
- ツールバーの  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。
- [ホスト タイプ]ドロップダウン リストからサービス(ESAプライマリなど)を選択します。
[サービスのインストール]ダイアログで  がアクティブになります。

5. **Install** をクリックします。



ステップ3. 信頼接続のためのSSLポートの確認

各コア サービスは、暗号化されない非SSLポートと暗号化されたSSLポートの2つのポートを使用し、信頼接続をサポートします。信頼接続では、暗号化されたSSLポートを使用します。

暗号化されたSSLポート

10.4以降を新規インストールするかまたはアップグレードすると、デフォルトで次の2つの設定により信頼接続が確立されます。

- SSLが有効になります。
- コア サービスはSSLポートに接続し、通信が暗号化されます。

各NetWitness Platformコア サービスは、次の2つのポートを使用します。

- 暗号化されない非SSLポート
例 : Archiver 50008
- 暗号化されたSSLポート
例 : Archiver 56008

SSLポートは、非SSLポート+6000です。

次の表は、すべてのNetWitness Platformサービスと対応するポートです。各コア サービスが2つのポートを使用します。以下のポート番号はすべてTCP用です。

サービス	暗号化されない非SSLポート	暗号化されたSSLポート	注
管理者	N/A	N/A	NW Serverに実装されます
Archiver	50008	56008	
Broker	50003	56003	コア サービス
Cloud Gateway	N/A	N/A	
Concentrator	50005	56005	コア サービス
Config	N/A	N/A	NW Serverに実装されます。
Content	N/A	N/A	NW Serverに実装されます
Context Hub	N/A	N/A	
Decoder(Packets)	50004	56004	コア サービス
Endpoint	N/A	N/A	
Entity Behavior Analysis	N/A	N/A	
Event Stream Analysis	N/A	50030	
Integration	N/A	N/A	NW Serverに実装されます。
Investigate	N/A	N/A	NW Serverに実装されます。
Log Collector	50001	56001	
Log Decoder	50002	56002	コア サービス

サービス	暗号化されない 非SSLポート	暗号化された SSLポート	注
Malware Analysis	N/A	60007	
Orchestration	N/A	N/A	NW Serverに実装されます。
Reporting Engine	N/A	51113	NW Serverに実装されます。
Respond	N/A	N/A	NW Serverに実装されます。
Security	N/A	N/A	NW Serverに実装されます。
Source	N/A	N/A	NW Serverに実装されます
UEBA	N/A	N/A	
Warehouse Connector	50020	56020	
Workbench	50007	56007	

ステップ4. サービスへのアクセスの管理

信頼接続では、各サービスはNW Serverを明示的に信頼し、ユーザの管理と認証を行います。この信頼関係により、[管理]>[サービス]で、NetWitness Platformの各コア サービスに認証情報を定義する必要がなくなります。サーバで認証されたユーザは、パスワードを入力しないでサービスにアクセスできます。

信頼接続のテスト

前提条件


1. ユーザにロールが割り当てられている必要があります。
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』の「ユーザの追加とロールの割り当て」のトピックを参照してください。
2. ユーザは次の条件を満足する必要があります。
 - NetWitness Platformにログインし、サーバによる認証を受ける
 - サービスへのアクセス権限を持っている

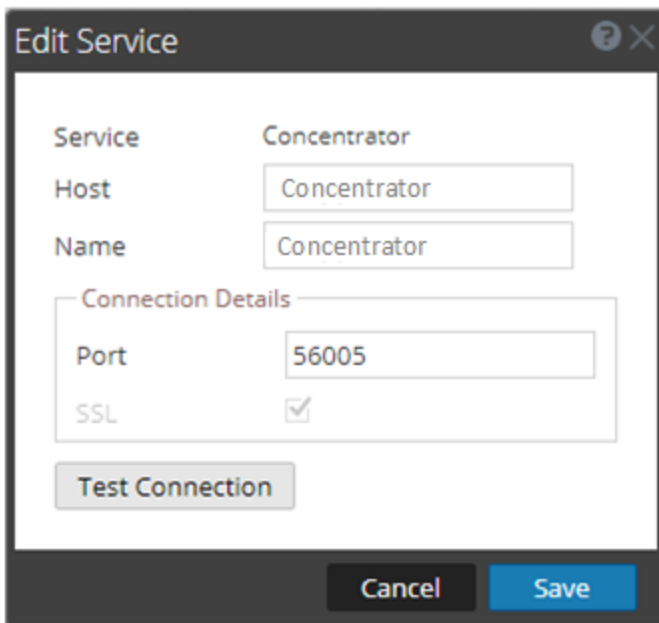
手順

1. NetWitness Platformで、[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。

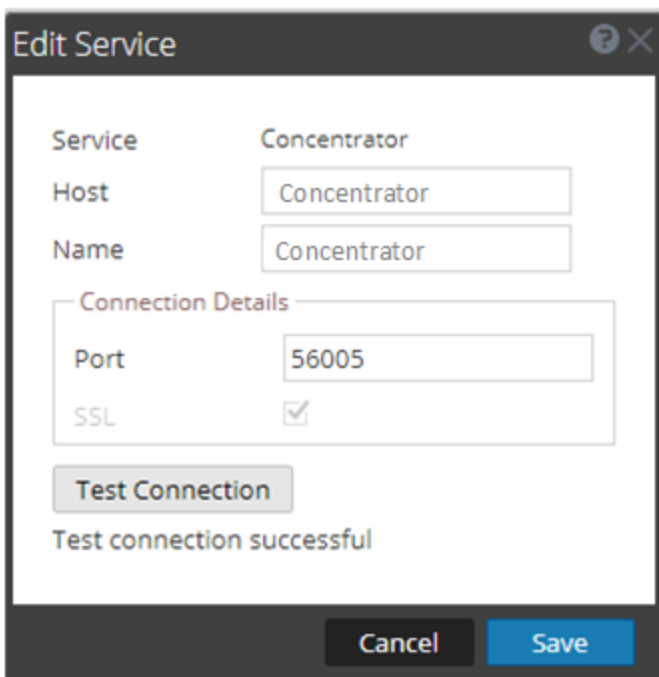
The screenshot shows the RSA NetWitness Platform Admin console. The top navigation bar includes tabs for Hosts, Services, Event Sources, Health & Wellness, System, and Security. The Services page is active, displaying a table of installed services. The table has columns for Name, Licensed, Host, Type, Version, and Actions. A 'Groups' sidebar is visible on the left, showing a list of groups with an 'All' group selected. The bottom of the screen displays the RSA NetWitness Platform logo and the version number 11.2.0.

Name	Licensed	Host	Type	Version	Actions
Admin	✓	NW Server	Admin Server	11.2.0.0	[Settings]
Archiver	✓	Archiver	Archiver	11.2.0.0	[Settings]
Broker	✓	Broker	Broker	11.2.0.0	[Settings]
Cloud Gateway	✓	Cloud Gateway	Cloud Gateway Serve	11.2.0.0	[Settings]
Concentrator	✓	Concentrator	Concentrator	11.2.0.0	[Settings]
Config	✓	NW Server	Config Server	11.2.0.0	[Settings]
Content	✓	NW Server	Content Server	11.2.0.0	[Settings]
Context Hub	✓	Event Stream Ana	Contexthub Server	11.2.0.0	[Settings]
Decoder	✓	Decoder	Decoder	1.2.0.0	[Settings]
Endpoint	✓	Endpoint Hybrid	Endpoint	11.2.0.0	[Settings]
Entity Behavior Analysis	✓	Event Stream Ana	Entity Behavior Ana	11.2.0.0	[Settings]
Event Stream Analysis	✓	Event Stream Ana	Event Stream Analys	11.2.0.0	[Settings]
Integration	✓	NW Server	Integration Serv	11.2.0.0	[Settings]
Investigate	✓	NW Server	Investigate Server	11.2.0.0	[Settings]
Log Collector	✓	Log Decoder	Log Collector	11.2.0.0	[Settings]
Log Decoder	✓	Log Decoder	Log Decoder	11.2.0.0	[Settings]
Log Decoder	✓	Endpoint Hybrid	Log Decoder	11.2.0.0	[Settings]
Malware Analysis	✓	Malware Analysis	Malware Analys	11.2.0.0	[Settings]
Orchestration	✓	NW Server	Orchestration Serve	11.2.0.0	[Settings]
Reporting Engine	✓	NW Server	Reporting Engine	11.2.0.0	[Settings]
Respond	✓	NW Server	Respond Server	11.2.0.0	[Settings]
Security	✓	NW Server	Security Server	11.2.0.0	[Settings]
Source	✓	NW Server	Source Server	11.2.0.0	[Settings]
UEBA	✓	UEBA	UEBA	11.2.0.0	[Settings]
Workbench	✓	Archiver	Workbench	11.2.0.0	[Settings]

2. テストするサービス(Concentratorなど) を選択し、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。



3. 認証情報なしで接続をテストするには、[ユーザ名]を削除します。
4. [接続のテスト]をクリックします。



「接続のテストに成功しました」のメッセージが表示される場合は、信頼接続が確立されたことを意味します。

事前に認証されたユーザは、ユーザ名とパスワードを入力せずにサービスにアクセスできます。

5. [保存]をクリックします。

ホストへのバージョン更新の適用

ホストを新しいバージョンに更新するには、次のタスクを実行します。
次の方法を使用して、ホストにバージョン更新を適用します。

注: リポジトリの場所を変更した場合は、「[RSAおよびOS更新の外部リポジトリのセットアップ](#)」の説明を参照してください。

- [ホスト]ビューから更新を適用する(Webアクセスあり)
- コマンド ラインから更新を適用する(Webアクセスなし)

[ホスト]ビューから更新を適用する(Webアクセスあり)

タスク1: ローカルリポジトリに更新を配置するか、外部リポジトリをセットアップする

NW Serverをセットアップする際に、ローカルリポジトリ(Repo)または外部リポジトリ(Repo) を選択します。[ホスト]ビューでは、選択したリポジトリからバージョン更新を取得します。

ローカルリポジトリを選択した場合、セットアップする必要はありませんが、最新バージョンの更新を配置する必要があります。バージョン更新を配置する手順については、「[ローカルリポジトリへの更新の配置](#)」を参照してください。

注: 外部リポジトリを選択した場合は、セットアップする必要があります。リポジトリにバージョン更新を配置する方法の詳細については、「[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。

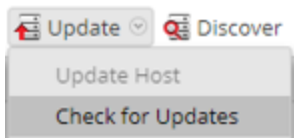
タスク2: [ホスト]ビューから各ホストに更新を適用する

[ホスト]ビューには、ローカル更新リポジトリにある使用可能なソフトウェアの更新バージョンが表示されます。[ホスト]ビューから必要な更新を選択して適用します。

この手順では、ホストをNetWitness Platformの新しいバージョンに更新する方法について説明します。

注: このトピックでは、例としてNetWitness Platform 11.0.x.xから11.2.0.0を使用します。

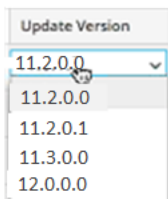
1. NetWitness Platformにログインします。
2. [管理]>[ホスト]に移動します。
3. (オプション)最新の更新をチェックします。



4. 1つまたは複数のホストを選択します。

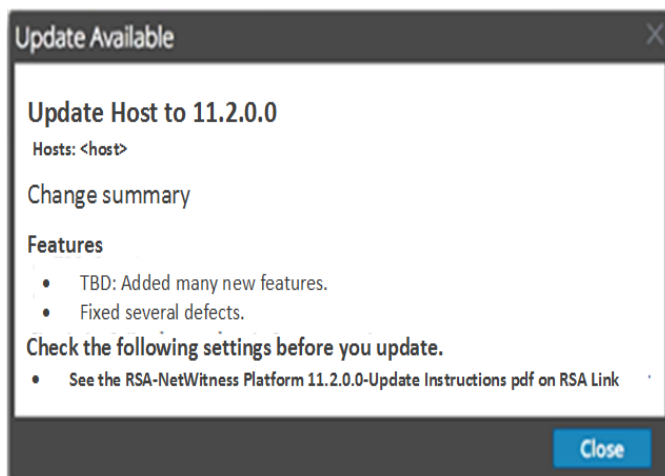
最初にNW Serverを最新バージョンに更新する必要があります。その他のホストは任意の順序で更新することができますが、[混在モードでの実行](#)のガイドラインに従うことを推奨します。選択したホスト用のバージョン更新がローカル更新リポジトリにある場合は、[ステータス]列に[更新あり]が表示されます。

5. [更新のバージョン]列から適用するバージョンを選択します。

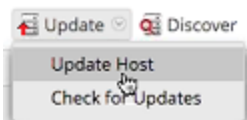


次の手順に従ってください。

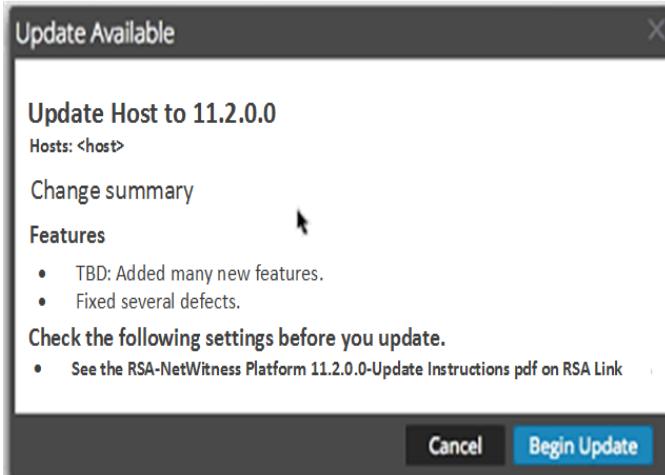
- 複数のホストを同じバージョンに更新する場合は、NW Serverホストを更新した後、対象ホストの左のチェックボックスを選択します。現在サポートされている更新バージョンのみが表示されます。
- 各更新の主な機能をダイアログに表示したい場合は、更新バージョン番号の右側にある ⓘ をクリックします。次に、このダイアログの例を示します。



- 目的のバージョンが見つからない場合は、[更新] > [更新の確認]を選択し、リポジトリ内の使用可能な更新をチェックします。更新が利用可能な場合、「新しい更新が利用可能です」というメッセージが表示され、[ステータス]列が自動的に更新され、[更新あり]と表示されます。デフォルトでは、選択したホストでサポートされている更新のみが表示されます。
6. ツールバーの[更新] > [ホストの更新]をクリックします。



選択した更新に関する情報がダイアログに表示されます。[更新を開始]をクリックします。



[ステータス]列には、次のような更新の各段階の状況が表示されます。

- ステージ1: **更新パッケージのダウンロード** - 選択したホスト上のサービスに適用されるリポジトリアーティファクトをNW Serverにダウンロードします。
- ステージ2: **更新パッケージの構成** - 更新ファイルを正しい形式に構成します。
- ステージ3: **更新が進行中です** - ホストを新しいバージョンに更新しています。

7. 「**更新が進行中です**」が表示されたら、ブラウザをリフレッシュします。

この操作により、[NetWitnessログイン]画面が表示される場合がありますが、再度ログインして[ホスト]ビューに戻ることができます。

ホストの更新が完了すると、NetWitness Platformが**ホストの再起動**を求めるメッセージを表示します。

8. ツールバーの[**ホストの再起動**]をクリックします。

NetWitness Platformは、ホストがオンラインに戻るまで「**再起動中...**」のステータスを表示します。ホストがオンラインに戻ると、[ステータス]には[**最新**]と表示されます。ホストがオンラインに戻らない場合は、カスタマー サービスにお問い合わせください。

注: Defense Information Systems Agency Security Technical Implementation Guides(DISA STIG) を有効にしている場合、コア サービスを開始するには約5~10分かかります。この遅延は新しい証明書を生成するために生じます。

コマンド ラインから更新を適用する(Webアクセスなし)

NetWitness Platform導入環境がWebアクセスできない場合は、次の手順に従ってバージョン更新を適用します。

注: 次の手順では、例として、11.1.0.0へのバージョン更新を使用しています。

1. 目的のバージョンの.zip更新パッケージ(たとえば、netwitness-11.1.0.0.zip)をRSA Linkからローカルディレクトリにダウンロードします。
2. SSHでNW Serverホストに接続します。

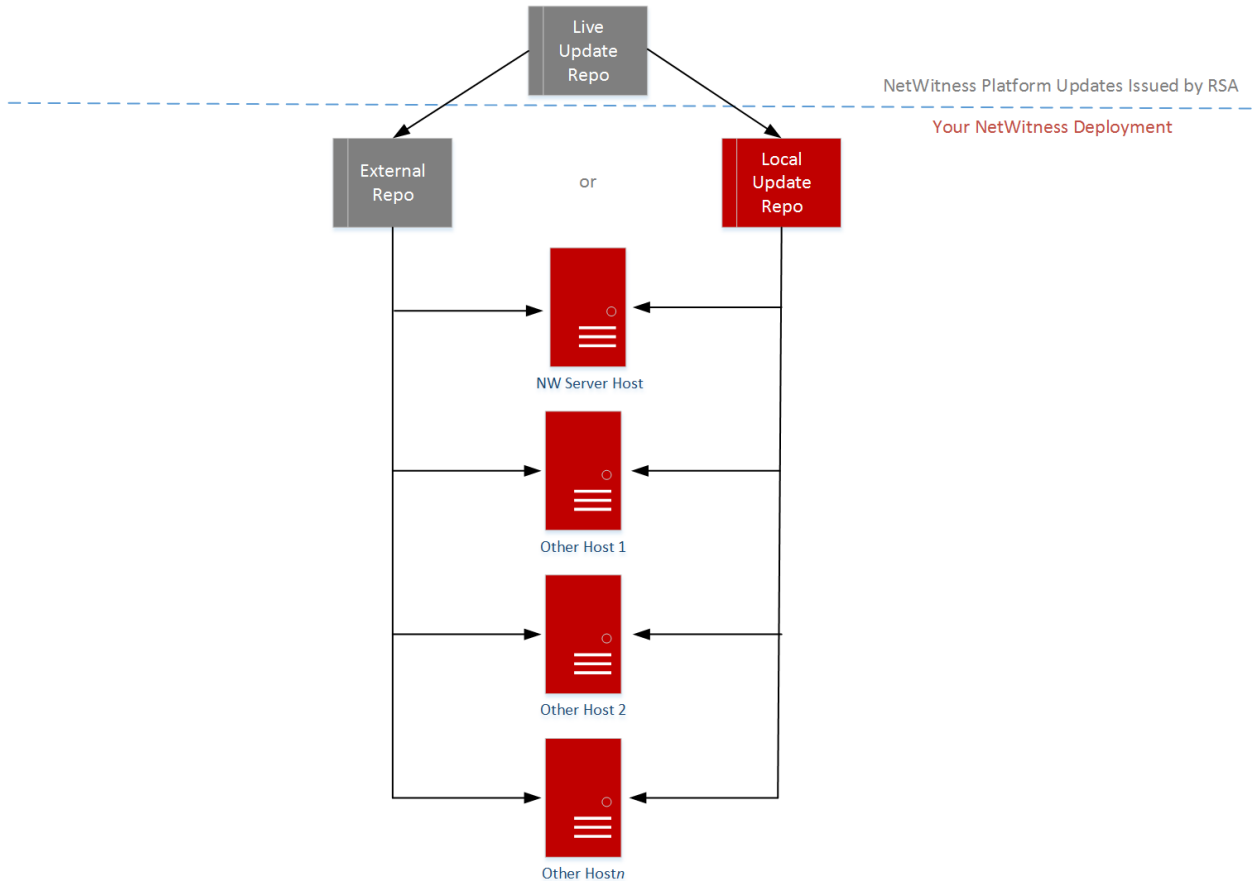
3. 目的のバージョン用に/tmp/upgrade/<version>ステージング ディレクトリを作成します(たとえば、tmp/upgrade/11.1.0.0)。
`mkdir -p /tmp/upgrade/11.1.0.0`
4. .zip更新パッケージを、ステージング ディレクトリ以外のNW Server上のディレクトリ(/tmpなど)にコピーします。
5. 作成したステージング ディレクトリ(たとえば、/tmp/upgrade/11.1.0.0)にパッケージを解凍します。
`unzip /<download-location>/netwitness-11.1.0.0.zip -d /tmp/upgrade/11.1.0.0`
6. NW Serverで更新を初期化します。
`upgrade-cli-client --init --version 11.1.0.0 --stage-dir /tmp/upgrade/`
7. NW Serverに更新を適用します。
`upgrade-cli-client --upgrade --host-addr <NW Server IP> --version 11.1.0.0`
8. NetWitness Platformにログインし、[ホスト]ビューでNW Serverホストを再起動します。
9. 非NW Serverの各ホストに更新を適用します。
`upgrade-cli-client --upgrade --host-addr <non-NW Server IP address> --version 11.1.0.0`
更新は、ポーリングが完了した時点で完了します。
10. NetWitness Platformにログインし、[ホスト]ビューでホストを再起動します。
次のコマンドを使用して、ホストに適用されたバージョンを確認できます。
`upgrade-cli-client --list`

ローカル更新リポジトリへの更新の配置

NetWitness Platformは、バージョンの更新をLive更新リポジトリからローカル更新リポジトリに送信します。Live更新リポジトリへのアクセスには、[管理]>[システム]>[Live]で構成したLiveアカウントの認証情報を使用する必要があります。さらに、最新の更新を毎日取得して、ローカルリポジトリに配置するために、[管理]>[システム]>[更新]の[Automatically download information about new updates every day]チェックボックスをオンにする必要があります。

次の図は、Webアクセスが可能なNetWitness Platform導入環境で、バージョンの更新を取得する方法を示しています。

RSA NetWitness Platform® 11.x.x Version Update Workflow – Web Access



注: Live更新リポジトリに最初に接続する場合、CentOS 7のシステムパッケージとRSA製品パッケージすべてにアクセスすることになります。この同期では、2.5GBを超えるデータがダウンロードされます。同期に要する時間は、使用するNW Serverのインターネット接続環境やRSA Live更新リポジトリのトラフィックによって異なります。Live更新リポジトリの使用は必須ではありません。また、「[RSAおよびOS更新の外部リポジトリのセットアップ](#)」の説明に従って、外部リポジトリを使用することもできます。

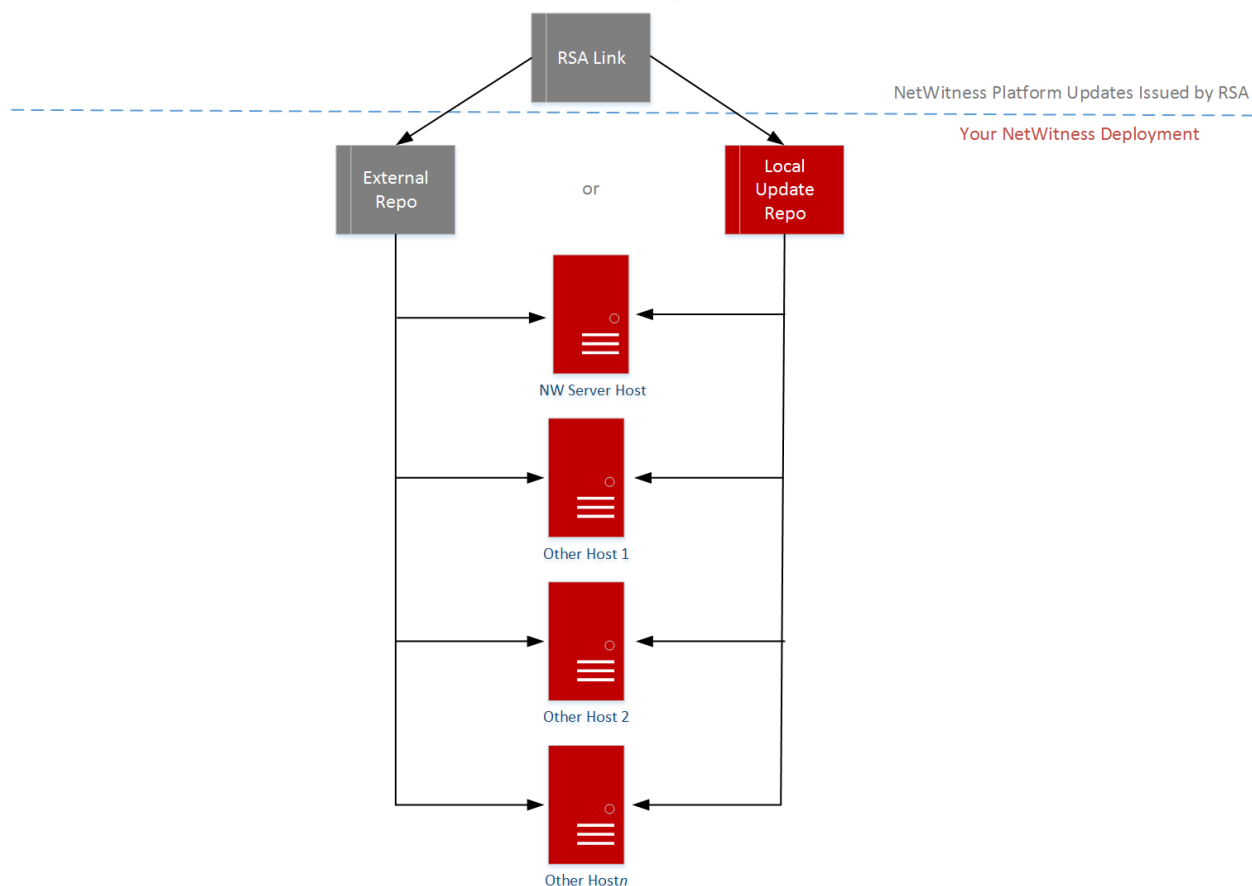
Live更新リポジトリに接続するには、[管理] > [システム]ビューに移動し、オプションパネルで[Liveサービス]を選択して、認証情報が構成されていることを確認します([接続済み]ボタンが緑色)。緑色でない場合は、[サインイン]をクリックして、接続します。

注: Live更新リポジトリへの接続にプロキシを使用する必要がある場合、プロキシホスト、プロキシユーザ名、プロキシパスワードを構成できます。詳細については、『*NetWitness Platform 11.2 システム構成ガイド*』の「NetWitness Platformのプロキシの構成」を参照してください。

WebアクセスができないNetWitness Platform導入環境の場合は、「[コマンドラインから更新を適用する \(Webアクセスなし\)](#)」を参照してください。

次の図は、WebアクセスがないNetWitness Platform導入環境で、バージョンの更新を取得する方法を示しています。

RSA NetWitness Platform® 11.x.x.x Version Update Workflow – No Web Access



RSAおよびOS更新の外部リポジトリのセットアップ

注: 次の手順では、例として、11.1.0.0へのバージョン更新を使用しています。

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. (オプション) 外部リポジトリがあり、それを上書きする場合に、この手順を実行します。
 - ケース1: 外部リポジトリからホストをセットアップしたが、Admin Server上のローカルリポジトリを使用してアップグレードしたい場合。
 - a. `/etc/netwitness/platform/repobase`ファイルを作成します。
`vi /etc/netwitness/platform/netwitness/repobase`
 - b. `repobase`ファイルを編集して、ファイル内の情報が次のURLだけになるようにします。
`https://nw-node-zero/nwrpmrepo`
 - c. `upgrade-cli-client` ツールを使用したアップグレードの手順を完了します。

- ケース2: Admin Server(NW Serverホスト) のローカルリポジトリからホストをセットアップしたが、外部リポジトリを使用してアップグレードしたい場合。
 - a. `/etc/netwitness/platform/repobase`ファイルを作成します。
`vi /etc/netwitness/platform/netwitness/repobase`
 - b. `repobase`ファイルを編集して、ファイル内の情報が次のURLだけになるようにします。
`https://<webserver-ip>/<alias-for-repo>`
 - c. `upgrade-cli-client`ツールを使用したアップグレードの手順を完了します。
[「コマンドラインから更新を適用する\(Webアクセスなし\)」](#)の手順を参照します。
- 2. 外部リポジトリをセットアップします。
 - a. Webサーバホストにログインします
 - b. 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`の下に`ziprepo`)。たとえば、`/var/netwitness`が`web-root`場合、次のコマンドを実行します。
`mkdir -p /var/netwitness/<your-zip-file-repo>`
 - c. `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`
 - d. 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`
 - e. `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。
 - f. 以下のように解凍します。
 - i. `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

- ii. 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
jpmiitool-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。

- g. (オプション: Azureの場合): Azureの更新の場合は、次の手順を実行します。

- i. `mkdir -p /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS/other`
- ii. `unzip nw-azure-11.2-extras.zip -d /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS/other`

- iii. `cd /var/netwitness/<your-zip-file-repo>/11.2.0.0/OS`
- iv. `createrepo .`
- h. 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。

ホスト グループの作成と管理

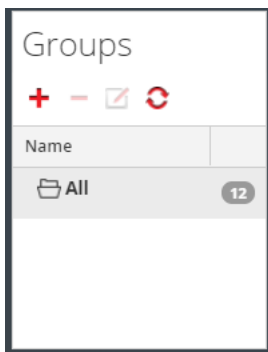
[ホスト]ビューでは、ホストのグループを作成および管理するためのオプションが提供されます。[グループ]パネルツールバーには、ホスト グループの作成、編集、削除のオプションがあります。グループの作成後、[ホスト]パネルからグループに各ホストをドラッグできます。

グループは、機能別、地域別、あるいはプロジェクト別など、組織における運用管理方式に従って構成できます。1つのホストが複数のグループに属することができます。ここでは、考えられる分類の例をいくつか示します。

- すべてのBroker、Decoder、Concentratorの構成と監視を容易にするために、ホスト タイプごとにグループ化。
- 同じデータ フローを構成しているホスト(たとえば、Brokerとそれに関連するすべてのConcentratorとDecoder)をグループ化。
- ホストが配置されている地域や場所に従ってグループ化。これにより、ある地域で大規模な停電が発生した場合に、影響を受ける可能性があるホストを容易に識別可能です。

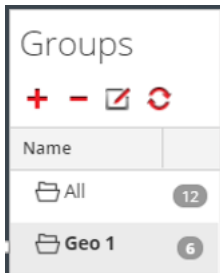
グループの作成

1. [管理] > [ホスト]を選択します。
[ホスト]ビューが表示されます。
2. [グループ]パネルのツールバーで、**+**をクリックします。
新しいグループのフィールドが表示され、カーソルが点滅します。




3. このフィールドに新しいグループの名前(「Geo 1」など)を入力し、Enterキーを押します。
グループはツリー内にフォルダとして作成されます。グループの横にある数値は、そのグループ内のホ

ストの数を示します。



グループ名の変更

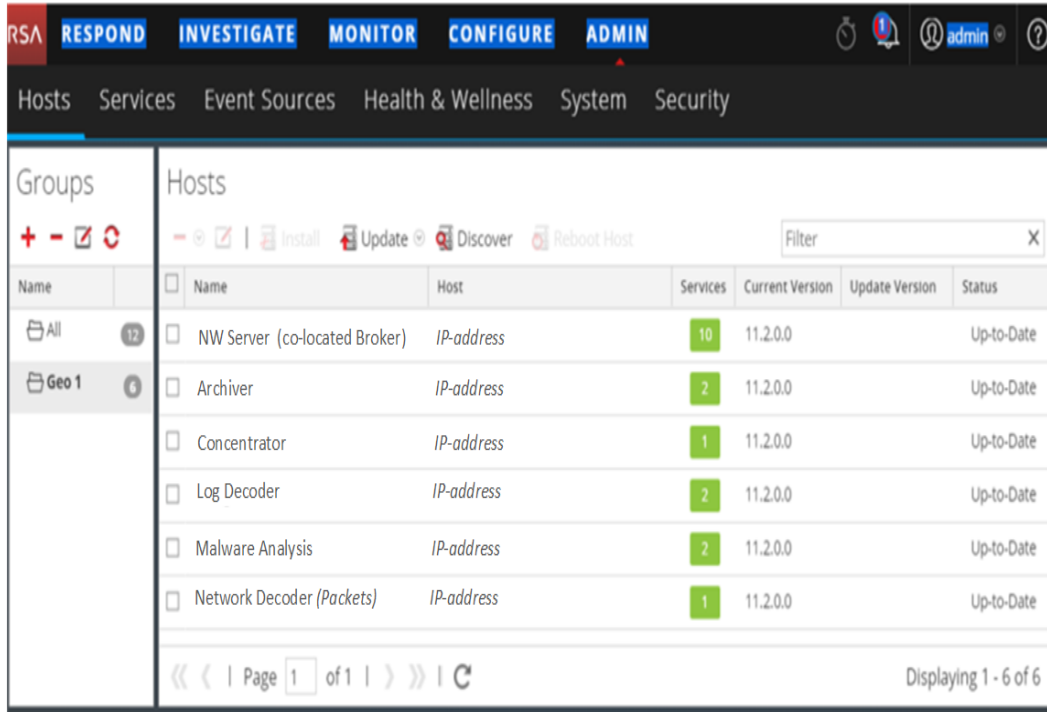
1. [ホスト]ビューの[グループ]パネルで、グループ名をダブルクリックするか、グループを選択し、をクリックします。
名前フィールドが表示され、カーソルが点滅します。
2. グループの新しい名前を入力し、Enterキーを押します。
[名前]フィールドが閉じ、新しいグループ名がツリーに表示されます。

グループへのホストの追加

[ホスト]ビューの[ホスト]パネルで、ホストを選択して、[グループ]パネルのグループフォルダにドラッグします。
グループにホストが追加されます。

グループ内のホストの表示

グループ内のホストを表示するには、[グループ]パネルのグループをクリックします。
[ホスト]パネルには、そのグループ内のホストが一覧表示されます。

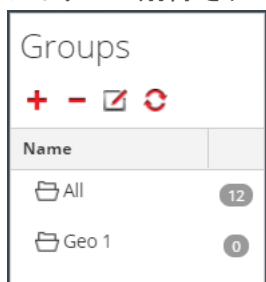


グループからのホストの削除


1. [ホスト]ビューの[グループ]パネルで、削除するホストが含まれているグループを選択します。そのグループ内のホストが[ホスト]パネルに表示されます。
2. [ホスト]パネルで、グループから削除するホストを1つ以上選択し、ツールバーで **-** > [グループから削除]を選択します。

選択したホストはグループから削除されますが、NetWitness Platformユーザ インタフェースからは削除されません。表示されているホスト数は、グループから削除されたホストの数だけ減ります。[すべて]グループには、グループから削除されたホストが含まれます。

次の例では、[Geo 1]という名前のホスト グループにはホストが含まれていません。グループ内のホストはすべて削除されているためです。



グループの削除

1. [ホスト]ビューの[グループ]パネルで、削除するグループを選択します。
2.  をクリックします。
選択したグループが[グループ]パネルから削除されます。グループに含まれていたホストは NetWitness Platform ユーザ インタフェースからは削除されません。[すべて]グループには、削除されたグループのホストが含まれています。

ホストの検索

[ホスト]ビューに表示されるホストの一覧からホストを検索できます。[ホスト]ビューでは、名前やホスト名でホストの一覧をすばやくフィルタ表示できます。多数の NetWitness Platform ホストを管理する場合に便利です。ホスト リストをスクロールするのではなく、フィルタを設定することによって、管理するホストに迅速にアクセスすることができます。

[サービス]ビューでは、サービスを検索して、そのサービスを実行するホストを迅速に見つけることができます。

ホストの検索

1. [管理] > [ホスト] を選択します。
2. [ホスト] パネル ツールバーの[フィルタ]フィールドに、ホストの名前またはホスト名を入力します。

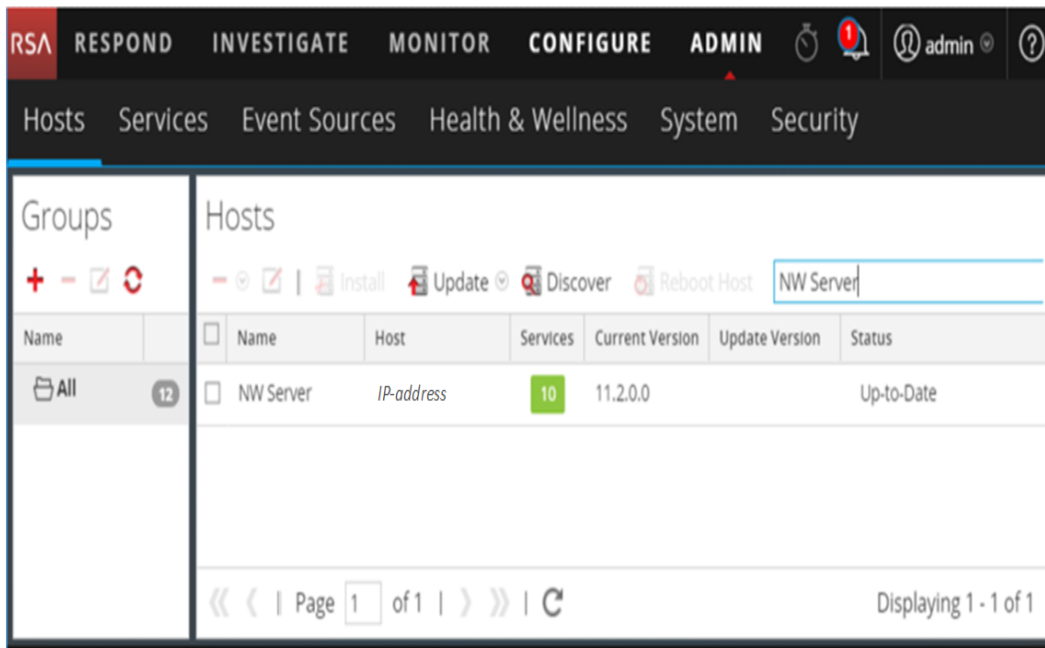
 

[フィルタ]フィールドに入力した名前に一致するホストが、[ホスト]パネルに表示されます。

サービスを実行するホストの検索

1. [管理] > [サービス] を選択します。
2. [サービス]ビューで、サービスを選択します。関連づけられたホストが、そのサービスの[ホスト]列に表示されます。

3. [ホスト]ビューでホストを管理するには、そのサービスの[ホスト]列のリンクをクリックします。選択したサービスに関連づけられたホストが[ホスト]ビューに表示されます。



ホストのタスクリストからのタスクの実行

1. [管理] > [サービス]を選択します。
2. [サービス]グリッドで、サービスを選択し、 > [表示] > [システム]をクリックします。

注: Admin、Config、Orchestration、Security、Investigate、Respondの各サービスには[システム]ビューはありません。これらのサービスには[エクスプローラ]ビューしかありません。サービスの[システム]ビューが表示されます。

The screenshot shows the RSA Admin console interface. At the top, there are navigation tabs: Hosts, Services, Event Sources, Health & Wellness, System, and Security. Below these, there are sub-tabs: Change Service, Broker, and System. A toolbar contains buttons for Start Aggregation, Stop Aggregation, Host Tasks, Shutdown Service, Shutdown Appliance Service, and Reboot. The main content area is divided into four sections:

- Broker Service Information:** Name: NW Server (Broker), Version: 11.2.0.0 (Rev null), Memory Usage: 38376 KB (0.03% of 126 GB), CPU: 0%, Running Since: 2018-May-22 13:51:43, Uptime: 1 week 1 day 4 hours 14 minutes, Current Time: 2018-May-30 18:05:43.
- Appliance Service Information:** Name: NW Server (Host), Version: 11.2.0.0 (Rev null), Memory Usage: 23076 KB (0.02% of 126 GB), CPU: 0%, Running Since: 2018-May-22 13:51:43, Uptime: 1 week 1 day 4 hours 13 minutes 59 seconds, Current Time: 2018-May-30 18:05:42.
- Broker User Information:** Name: admin, Groups: Administrators, Roles: aggregate.manage, concentrator.manage, connections.manage, index.manage, logs.manage, sdk.content, sdk.manage, sdk.meta, sdk.packets, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage.
- Host User Information:** Name: admin, Groups: Administrators, Roles: appliance.manage, connections.manage, logs.manage, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage.

At the bottom, there is a **Session Information** table:

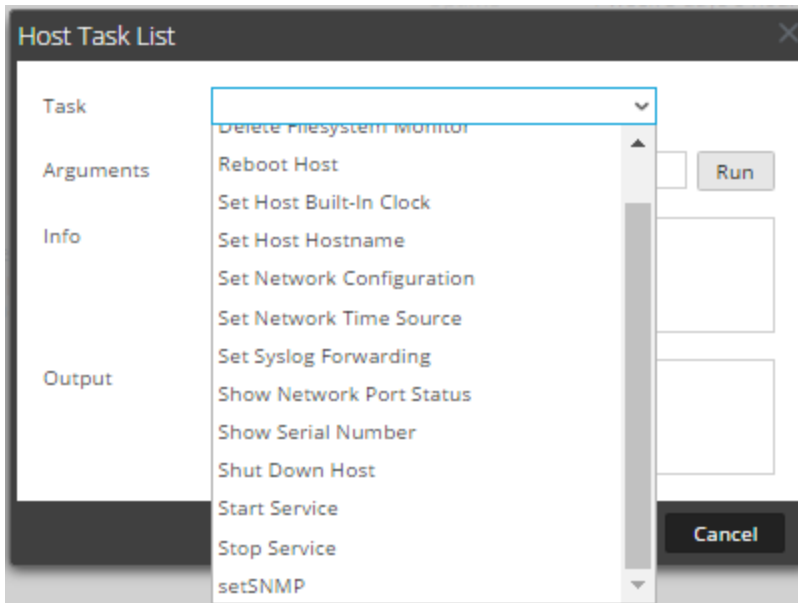
Session	User	IP Address	Login Time	Active Queries
315	admin	IP Address	2018-May-22 13:51:51	0
342	admin	IP Address	2018-May-22 13:51:52	0
381	escalateduser	IP Address	2018-May-22 13:52:43	0
31612	escalateduser	IP Address	2018-May-30 18:04:38	0

3. サービスの[システム]ビューのツールバーで、 Host Tasks をクリックします。

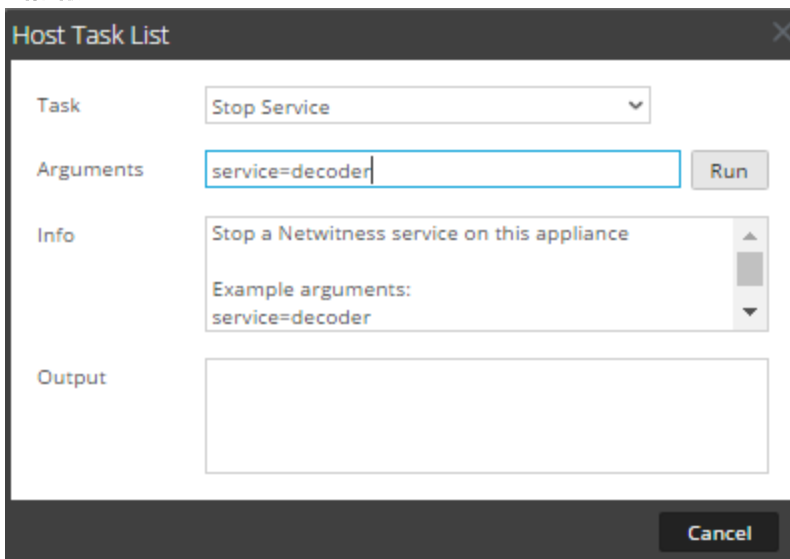
The screenshot shows a dialog box titled "Host Task List". It contains the following fields and controls:

- Task:** A dropdown menu.
- Arguments:** A text input field with a "Run" button to its right.
- Info:** A large empty text area.
- Output:** A large empty text area.
- Cancel:** A button at the bottom right of the dialog.

4. [ホスト タスクリスト]で、[タスク]フィールドをクリックし、ホストで実行するタスクのドロップダウン リストを表示します。



5. タスクを選択します。たとえば、[サービスの停止]をクリックします。タスクが[タスク]フィールドに表示され、タスクの説明、引数の例、セキュリティロール、パラメータが[情報]セクションに表示されます。




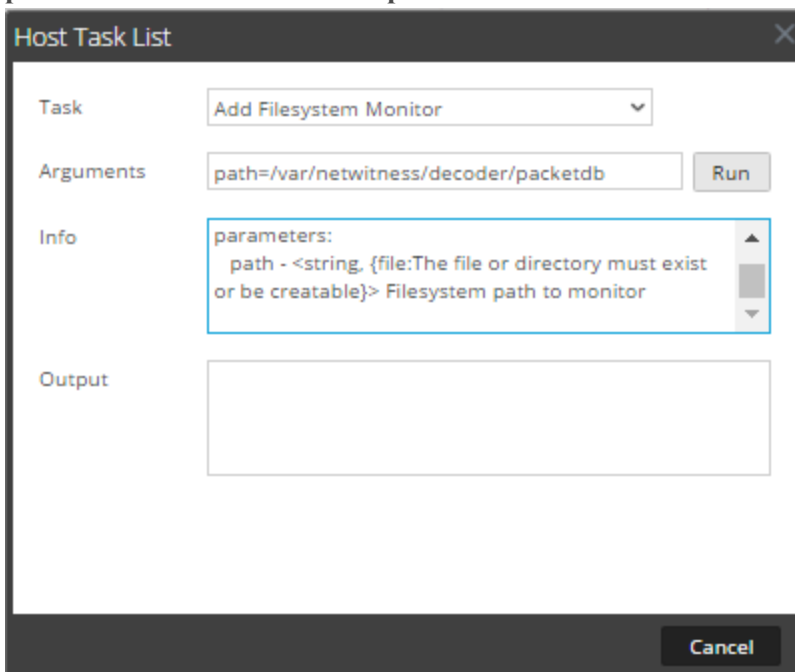
6. 必要に応じて引数を入力し、[実行]をクリックします。コマンドが実行され、結果が[出力]セクションに表示されます。

ファイルシステム監視の追加と削除

サービスによって特定のファイルシステムを監視する必要がある場合、サービスを選択してパスを指定し、監視を設定できます。NetWitness Platformによって、ファイルシステム監視が追加されます。ファイルシステム監視をサービスに追加すると、ファイルシステム監視を削除するまで、そのサービスは指定されたパスのトラフィックを監視します。

ファイルシステム監視の構成

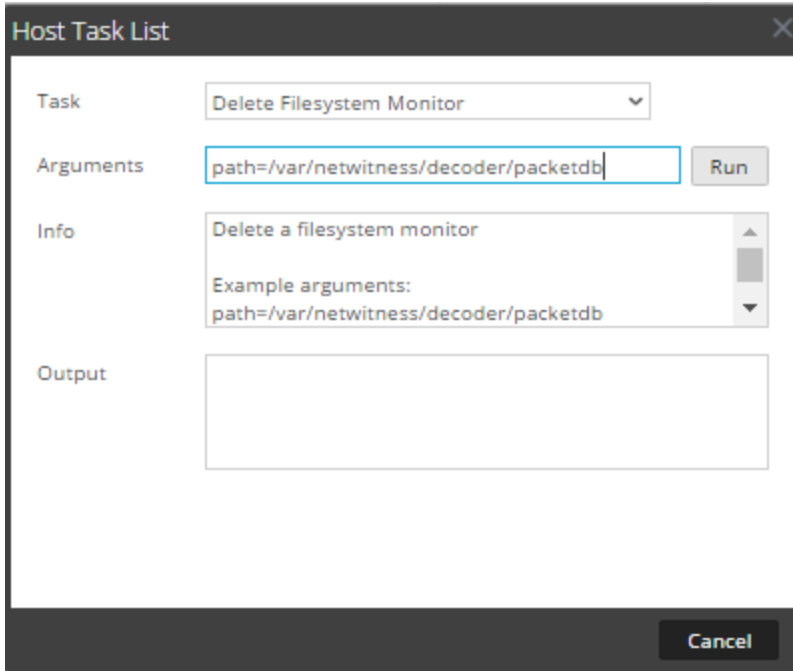
1. [管理] > [サービス] を選択します。
2. [サービス] グリッドで、サービスを選択し、 > [表示] > [システム] をクリックします。サービスの[システム]ビューが表示されます。
3. サービスの[システム]ビューのツールバーで、[ホスト タスク] をクリックします。
4. [ホスト タスク リスト] で、[ファイルシステム監視の追加] を選択します。[情報] セクションに、タスクの概要とタスクの引数が表示されます。
5. [引数] フィールドに、監視するファイルシステムのパスを入力します。例：
path=/var/netwitness/decoder/packetdb



6. [実行] をクリックします。結果が[出力]領域に表示されます。サービスによってファイルシステムの監視が開始され、ファイルシステム監視を削除するまで監視が継続されます。

ファイルシステム監視の削除

1. [ホスト タスク リスト] ダイアログに移動します。
2. [ホスト タスク リスト] で、[ファイル システム監視の削除] を選択します。
[情報] セクションに、タスクの概要とタスクの引数が表示されます。
3. [引数] フィールドに、監視を停止するファイル システムのパスを入力します。例：
`path=/var/netwitness/decoder/packetdb`



4. [実行] をクリックします。
結果が[出力] 領域に表示されます。サービスによってファイル システムの監視が停止されます。


ホストの再起動

特定の状況 (たとえば、ソフトウェア アップグレードをインストールした後など) では、ホストの再起動が必要になります。この手順では、[ホスト タスク リスト] を使用してホストのシャットダウンと再起動を行います。



NetWitness Platform では、他の方法でホストをシャットダウンすることもできます。

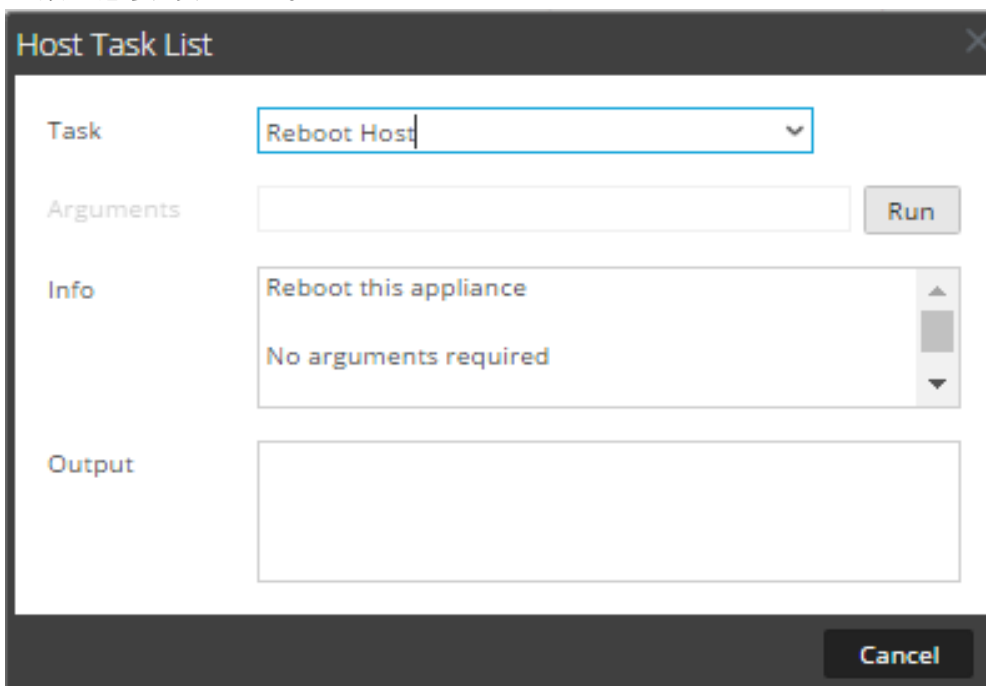
- ホスト上のサービスを選択して、ホストをシャットダウンし、再起動する場合は、[サービス] ビューのサービスから [ホスト] ビューに移動し (「[ホストの検索](#)」を参照)、 「[ホスト] ビューからのホストのシャットダウンおよび再起動」の手順を実行します。
- 再起動ではなく、物理ホストをシャットダウンする手順については、「[ホストのシャットダウン](#)」を参照してください。

[ホスト]ビューからのホストのシャットダウンおよび再起動

1. [管理] > [ホスト] を選択します。
2. [ホスト] パネルでホストを選択します。
3. ツールバーから  Reboot Host を選択します。

[ホスト タスクリスト]からのホストのシャットダウンおよび再起動

1. [管理] > [サービス] を選択します。
2. [サービス] パネルで、サービスを選択し、  > [表示] > [システム] をクリックします。
サービスの[システム]ビューが表示されます。
3. サービスの[システム]ビューのツールバーで、[ホスト タスク] をクリックします。
4. [ホスト タスクリスト] で、[タスク] フィールドから [ホストの再起動] を選択します。
引数は必要ありません。




5. [実行] をクリックします。
ホストが再起動され、結果が [出力] 領域に表示されます。

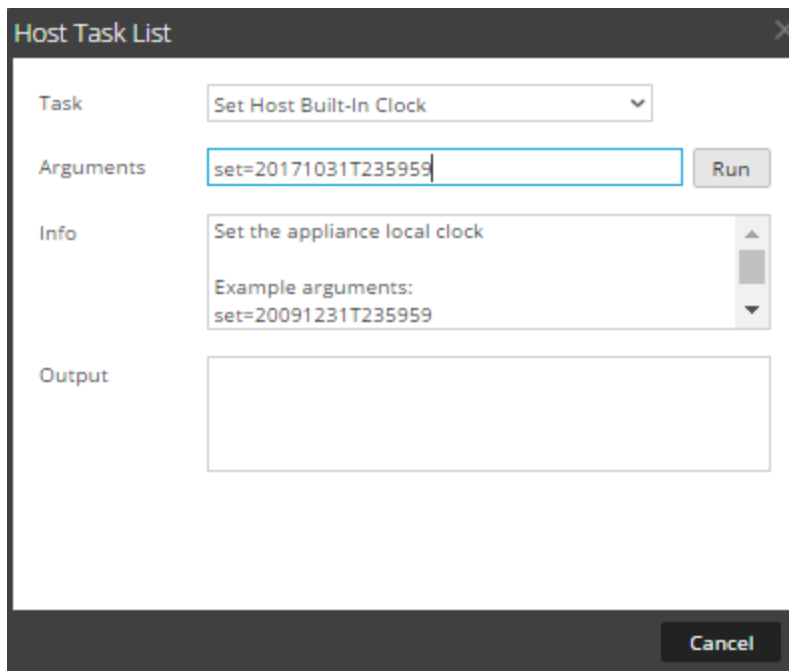
ホスト内蔵クロックの設定

シャットダウンまたはバッテリー故障の後に、ホスト上でローカルクロックの設定が必要な場合があります。ホスト内蔵クロックの設定タスクにより、クロックの時刻がリセットされます。

ローカルクロックでの時刻の設定

1. [管理]>[サービス]を選択します。
2. [サービス]グリッドで、サービスを選択し、 > [表示]>[システム]を選択します。
サービスの[システム]ビューが表示されます。
3. サービスの[システム]ビューのツールバーで、[ホスト タスク]をクリックします。
4. [ホスト タスクリスト]で、[ホスト内蔵クロックの設定]を選択します。タスクのヘルプが[情報]領域に表示されます。
5. [引数]フィールドに日付と時刻の引数を入力します。たとえば、2017年10月31日 11:59:59 PMを指定するには、次のように入力します。

set=20171031T235959




6. [実行]をクリックします。
クロックが指定した時間に設定され、メッセージが[出力]領域に表示されます。

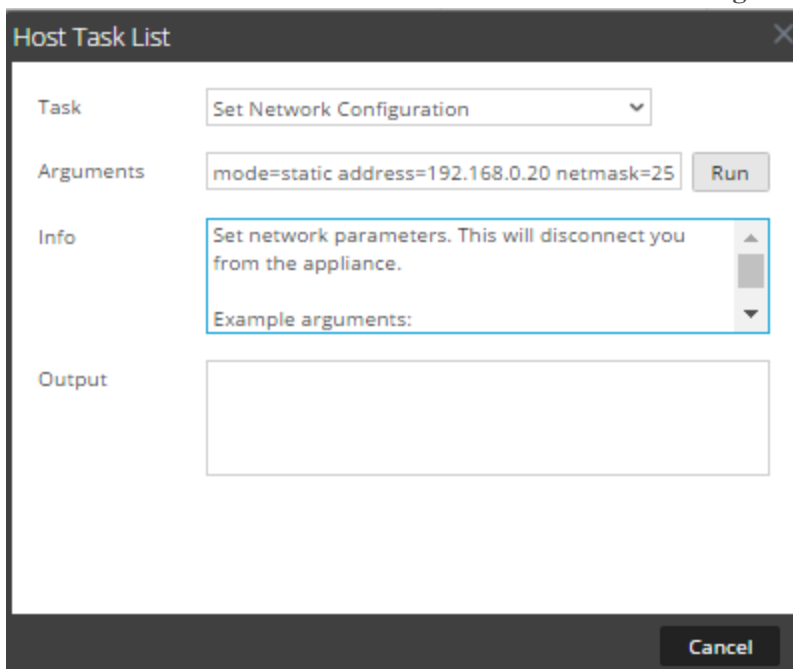
ネットワーク構成の設定

構成済みのコアホストでアドレスを変更する必要がある場合、[ホスト タスクリスト]で、[ネットワーク構成の設定]タスクを選択して、ホスト用に新しいネットワークアドレス、サブネット マスク、ゲートウェイを設定できます。

注意: 変更がただちに有効になり、ホストがNetWitness Platformから切断されます。切断されたホストは、新しいネットワークアドレスを使用してNetWitness Platformに再度追加する必要があります。

ホストのネットワークアドレスの指定

1. [管理] > [サービス] を選択します。
2. [サービス] グリッドで、サービスを選択し、 > [表示] > [システム] をクリックします。サービスの[システム]ビューが表示されます。
3. サービスの[システム]ビューのツールバーで、[ホスト タスク] をクリックします。
4. [ホスト タスク リスト] で、[ネットワーク構成の設定] をクリックします。タスクが[タスク]フィールドに表示され、ヘルプが[情報]セクションに表示されます。
5. [引数]フィールドに引数を入力します。例：
mode=static address=192.168.0.20 netmask=255.255.255.0 gateway=192.168.0.1




6. [実行] をクリックします。タスクが実行され、結果が[出力]領域に表示されます。ホストがNetWitness Platformから切断されます。新しいアドレスでホストを再度追加する必要があります。

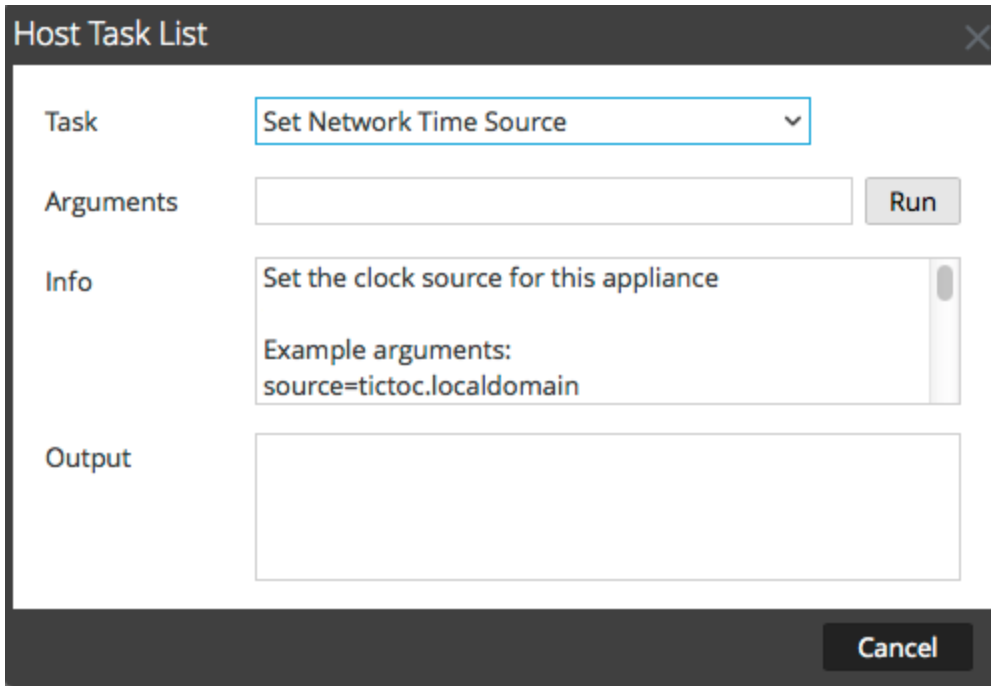
注: ネットワーク インタフェースのmodeがDHCPの場合、NetWitness Platformからは新しいアドレスを確認できません。新しいアドレスを確認するには、ホストに直接接続する必要があります。

ネットワーク タイム ソースの設定

ホストでネットワーク クロック ソースを使用する場合には、ホストのネットワーク クロック ソースとなるNTP サーバのホスト名またはアドレスを設定します。ホストでローカル クロック ソースを使用する場合には、ここにlocalを指定し、ローカルクロックソースの設定を有効にする必要があります。

ネットワーク クロック ソースの指定

1. [管理]>[サービス]を選択します。
2. [サービス]グリッドで、サービスを選択し、 > [表示]>[システム]をクリックします。
サービスの[システム]ビューが表示されます。
3. サービスの[システム]ビューのツールバーで、[ホスト タスク]をクリックします。
4. [ホスト タスクリスト]で、[ネットワーク タイム ソースの設定]を選択します。




5. 次のいずれかを実行します。
 - このホストのクロックソースとして使用するNTPサーバのホスト名またはアドレスを入力します。たとえば、次のように入力します。 `source=tictoc.localdomain`
 - クロックソースとしてホスト クロックを使用する場合は、次のように入力します。
`source=local`
6. [実行]をクリックします。
クロックソースが設定され、メッセージが[出力]領域に表示されます。

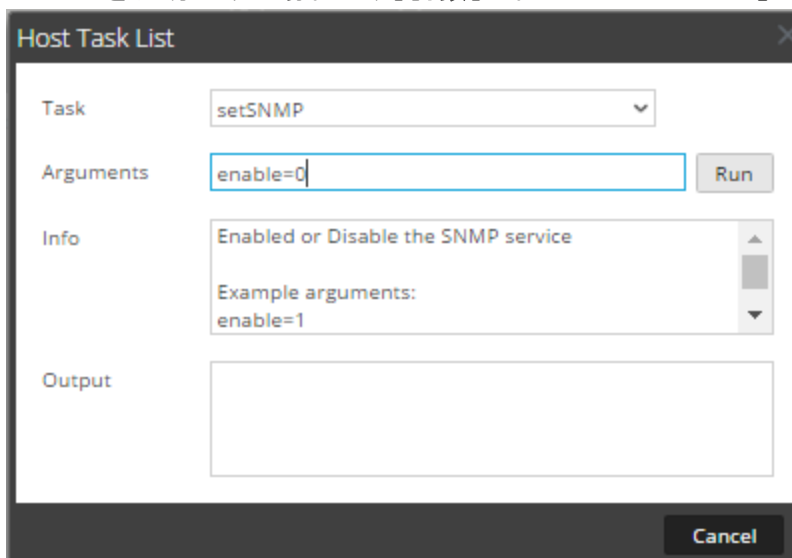
注: NTPクロックソースとしてlocalを指定した場合、ホスト クロックがクロックソースとして使用され、時刻は「[ホスト内蔵クロックの設定](#)」を使用して構成されます。

SNMPの設定

[ホスト タスクリスト]の[SNMPの設定]により、ホスト上のSNMPサービスを有効化または無効化します。ホストがSNMP通知を受信できるようにするには、SNMPサービスを有効化します。NetWitness Platformの通知でSNMPを使用しない場合、このサービスを有効化する必要はありません。

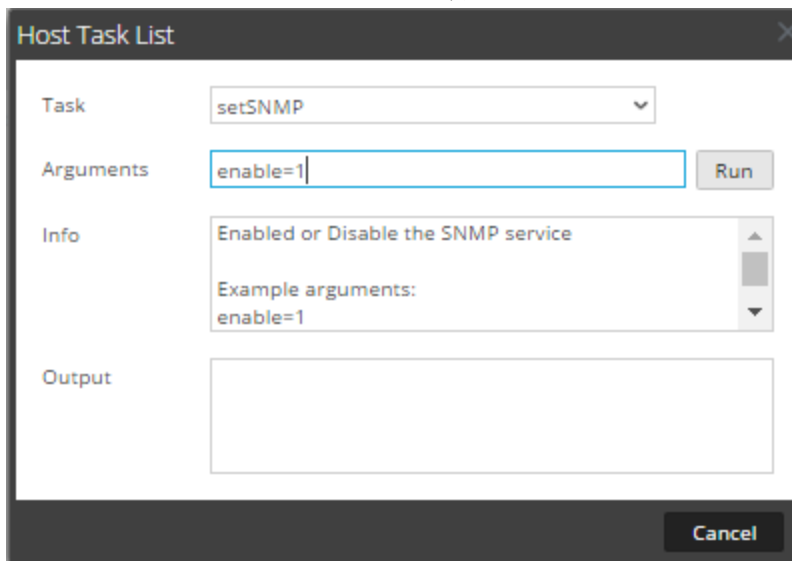
ホスト上のSNMPサービスのオン/オフ

1. [管理]>[サービス]を選択します。
2. [サービス]グリッドで、サービスを選択し、 > [表示]>[システム]をクリックします。
サービスの[システム]ビューが表示されます。
3. サービスの[システム]ビューのツールバーで、[ホスト タスク]をクリックします。
4. [ホスト タスク リスト]で、[setSNMP]を選択します。
[情報]セクションに、タスクの概要とタスクの引数が表示されます。
5. 次のいずれかを実行します。
 - サービスを無効化する場合は、[引数]フィールドに「enable=0」と入力します。



The screenshot shows the 'Host Task List' dialog box. The 'Task' dropdown is set to 'setSNMP'. The 'Arguments' text box contains 'enable=0'. The 'Info' section displays 'Enabled or Disable the SNMP service' and 'Example arguments: enable=1'. The 'Output' area is empty. A 'Run' button is visible next to the arguments field, and a 'Cancel' button is at the bottom right.

- サービスを有効化する場合は、[引数]フィールドに「enable=1」と入力します。




The screenshot shows the 'Host Task List' dialog box. The 'Task' dropdown is set to 'setSNMP'. The 'Arguments' text box contains 'enable=1'. The 'Info' section displays 'Enabled or Disable the SNMP service' and 'Example arguments: enable=1'. The 'Output' area is empty. A 'Run' button is visible next to the arguments field, and a 'Cancel' button is at the bottom right.

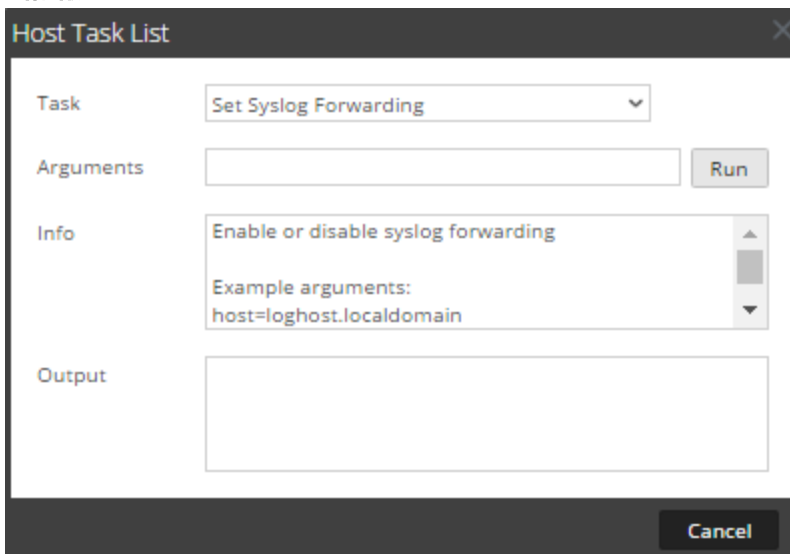
6. [実行]をクリックします。
結果が[出力]領域に表示されます。

Syslog転送の設定

Syslog転送を設定し、NetWitness PlatformホストのオペレーティングシステムのログをリモートSyslogサーバに転送することができます。Syslog転送を有効化または無効化するには、[ホスト タスク リスト]で [Syslog転送の設定] タスクを選択します。

Syslog転送の設定と開始

1. [管理] > [サービス]を選択します。
2. [サービス]グリッドで、サービスを選択し、 > [表示] > [システム]をクリックします。
サービスの[システム]ビューが表示されます。
3. サービスの[システム]ビューのツールバーで、[ホスト タスク]をクリックします。
4. [ホスト タスク リスト]で、[Syslog転送の設定]を選択します。
[情報]セクションに、タスクの概要とタスクの引数が表示されます。



5. [引数]フィールドで、次のいずれかを実行します。
 - Syslog転送を有効化するには、次のいずれかの形式を指定します。
 - **host=<loghost>.<localdomain>**(例 : host=syslogserver.local)。
 - **host=<loghost>.<localdomain>:<port>**(例 : host=syslogserver.local:514)。
 - **host=<IP>**(例 : host=10.31.244.244)。
 - **host=<IP>:<port>**(例 : host=10.31.244.244:514)。
- 次の表に、Syslog転送を有効化するために使用されるパラメータを示します。

パラメータ	説明
loghost	リモート Syslog サーバのホスト名。
localdomain	リモート Syslog サーバのドメイン。
port	リモート Syslog サーバの IP アドレス。
IP	リモート Syslog サーバが Syslog メッセージを受け取るポートのポート番号。

- Syslog 転送を無効化するには、**host=disable**と入力します。

6. **[実行]**をクリックします。

結果が**[出力]**領域に表示されます。

Syslog 転送が有効化または無効化されると、`/etc/rsyslog.conf` ファイルが自動的に更新されて、リモートの Syslog 転送先への Syslog 転送が有効化または無効化され、Syslog サービスが再起動されます。


Syslog 転送を有効化した場合、構成されたサービスからのログは定義された Syslog サーバに転送され、無効化されるまで転送を続けます。

注: リモート Syslog サーバにログインし、Syslog 転送を構成した NetWitness Platform サービスからのメッセージが受信されているかどうかを確認できます。

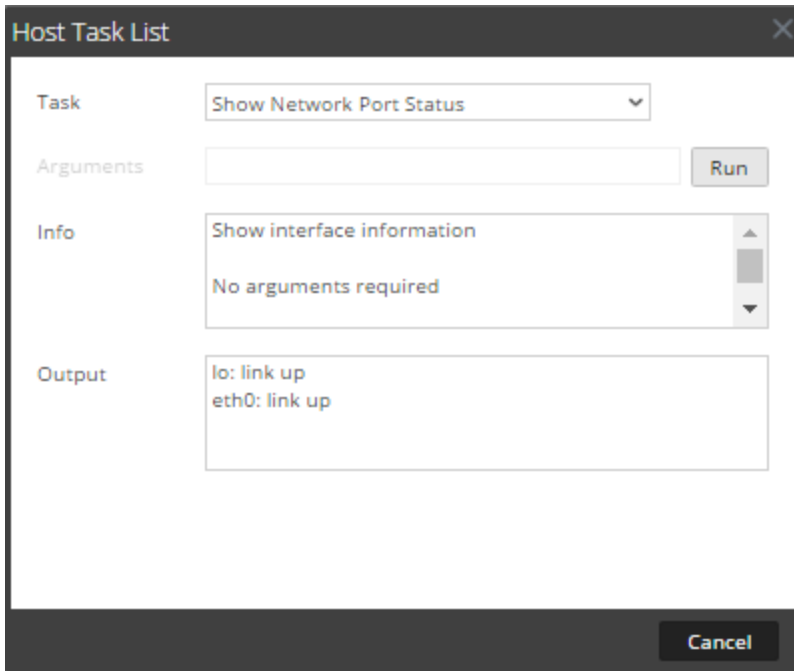
ネットワークポート ステータスの表示

ホスト タスク リストの**[ネットワークポート ステータスの表示]**タスクは、ホストに構成されたすべてのポートのステータスを表示します。

ネットワークポート ステータスの表示

1. **[管理]** > **[サービス]**を選択します。
2. **[サービス]** グリッドで、サービスを選択し、 > **[表示]** > **[システム]**を選択します。
選択したサービスの**[システム]**ビューが表示されます。
3. サービスの**[システム]**ビューのツールバーで、**[ホスト タスク]**をクリックします。
4. **[ホスト タスク リスト]**で、**[ネットワークポート ステータスの表示]**をクリックします。
タスクが**[タスク]**フィールドに表示され、タスクに関する情報が**[情報]**セクションに表示されます。


5. タスクを実行するには、[実行]をクリックします。
ホスト上の各ポートのステータスが[出力]領域に表示されます。



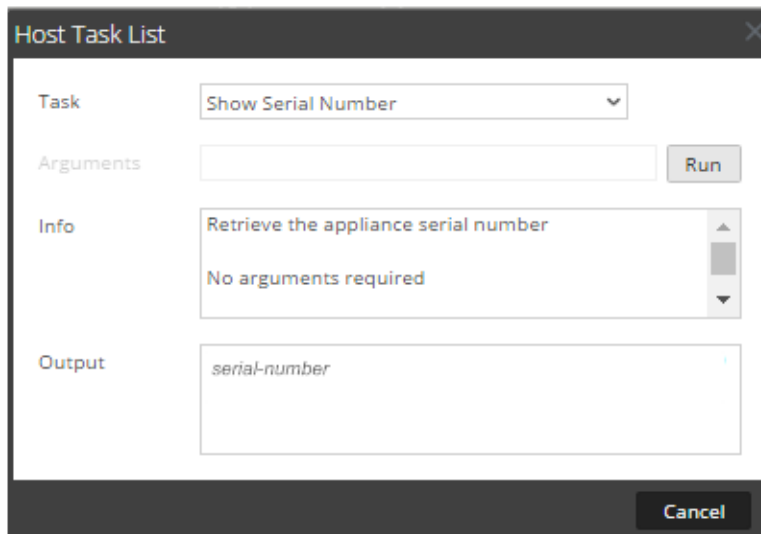
シリアル番号の表示

[ホスト タスク リスト]の[シリアル番号の表示]タスクでは、ホストのシリアル番号が表示されます。

シリアル番号の表示

1. [管理] > [サービス]を選択します。
2. [サービス]グリッドで、サービスを選択し、 > [表示] > [システム]をクリックします。
サービスの[システム]ビューが表示されます。
3. サービスの[システム]ビューのツールバーで、[ホスト タスク]をクリックします。
4. [ホスト タスク リスト]で、[シリアル番号の表示]を選択します。
[情報]セクションに、タスクの概要とタスクの引数が表示されます。

- このタスクでは、引数は必要ありません。[実行]をクリックします。選択したホストのシリアル番号が[出力]領域に表示されます。



ホストのシャットダウン

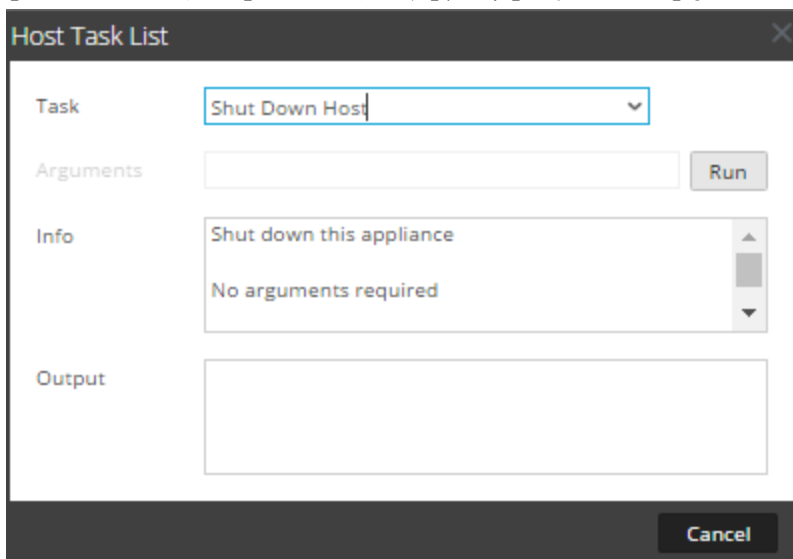
特定の状況(たとえばハードウェアのアップグレード、バックアップ電源容量を超過する長時間の停電など)で、物理ホストのシャットダウンが必要になることがあります。ホストをシャットダウンすると、ホストで実行されているすべてのサービスが停止し、物理ホストの電源がオフになります。

物理ホストは自動的に再起動しません。電源スイッチを使用してホストを再起動します。物理ホストが再起動すると、ホストとサービスは自動的に再起動するように構成されます。

ホストをシャットダウンすることなく開始および停止するには、[ホストを再起動](#)します。

ホストのシャットダウン

- [ホスト タスクリスト] ダイアログで、[タスク] フィールドの[ホストのシャットダウン]を選択します。




2. タスクを実行するには、[実行]をクリックします。
ホストがシャットダウンし、電源がオフになります。

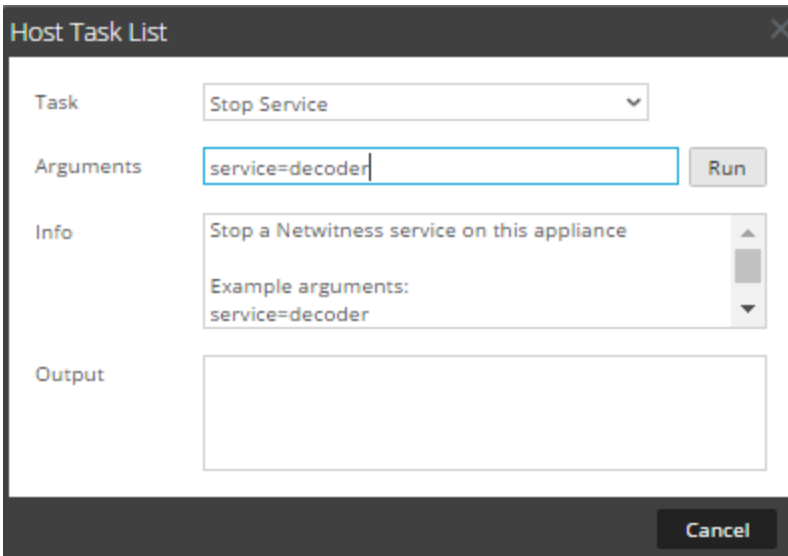
ホスト上のサービスの停止と開始

ホスト タスク リストには、ホスト上のサービスを停止および開始するためのオプションが2つあります。[サービスの停止]タスクを使用してサービスを停止した場合、サービスのすべてのプロセスが停止し、サービスに接続していたユーザは切断されます。サービスに問題がない限り、自動的に再起動します。これは、サービスの[システム]ビューの[サービスのシャットダウン]オプションと同じです。

停止後にサービスが自動的に再起動しない場合、[サービスの開始]タスクを使用して手動でサービスを再起動できます。

ホストでのサービスの停止

1. [管理] > [サービス]を選択します。
2. [サービス]グリッドで、サービスを選択し、 > [表示] > [システム]をクリックします。
サービスの[システム]ビューが表示されます。
3. サービスの[システム]ビューのツールバーで、[ホスト タスク]をクリックします。
4. [ホスト タスク リスト]で、[サービスの停止]をクリックします。
タスクが[タスク]フィールドに表示され、タスクに関する情報が[情報]セクションに表示されます。
5. 停止するサービス(decoder、concentrator、broker、logdecoder、logcollector)を[引数]フィールドに指定します。例: `service=decoder`



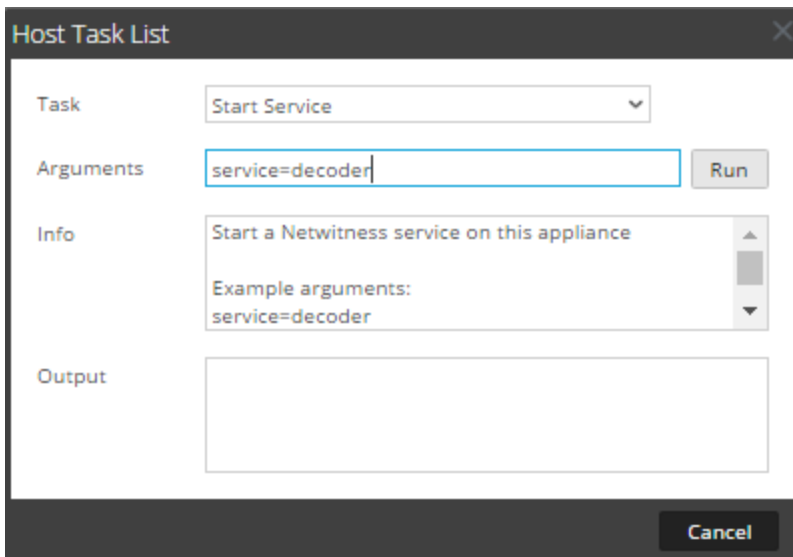
The screenshot shows a dialog box titled "Host Task List". It has a "Task" dropdown menu currently showing "Stop Service". Below it is an "Arguments" text input field containing "service=decoder" and a "Run" button. The "Info" section contains a scrollable text area with the text "Stop a Netwitness service on this appliance" and "Example arguments: service=decoder". At the bottom right, there is a "Cancel" button.

6. タスクを実行するには、[実行]をクリックします。
サービスが停止し、ステータスが[出力]セクションに表示されます。サービスのすべてのプロセスが停止し、サービスに接続するユーザが切断されます。サービスに問題がない限り、自動的に再起動します。

ホストでのサービスの開始

1. [ホスト タスクリスト]で、[タスク]ドロップダウン リストから[サービスの開始]を選択します。
タスクが[タスク]フィールドに表示され、タスクに関する情報が[情報]セクションに表示されます。
2. [引数]フィールドで、開始するサービス(decoder、concentrator、broker、logdecoder、logcollector)を指定します。たとえば、次のように指定します。

`service=decoder`



3. タスクを実行するには、[実行]をクリックします。
サービスが開始し、ステータスが[出力]セクションに表示されます。

サービス ユーザの追加、レプリケート、削除

次の場合は、ユーザをサービスに追加する必要があります。

- 集計
- 下記を使用してサービスにアクセスする場合：
 - シック クライアント
 - REST API

注：このトピックは、NetWitness Serverのユーザ インタフェースをからサービスにアクセスするユーザには適用されません。それらのユーザは、サービスではなく、システムに追加する必要があります。詳細については、「システム セキュリティとユーザ管理」の「ユーザの設定」のトピックを参照してください。

各 サービス ユーザについて、次のタスクを実行できます。

- サービスのユーザ認証とクエリ処理プロパティを構成する
- ユーザをロールのメンバに追加する。このロールにより、ユーザに付与される権限が決まります。

- 他のサービスにユーザ アカウントをレプリケートする
- 選択したサービス上のユーザ パスワードを変更する

「[サービス ユーザのパスワードの変更](#)」では、複数のサービスのサービス ユーザのパスワードを変更する手順について説明します。


手順

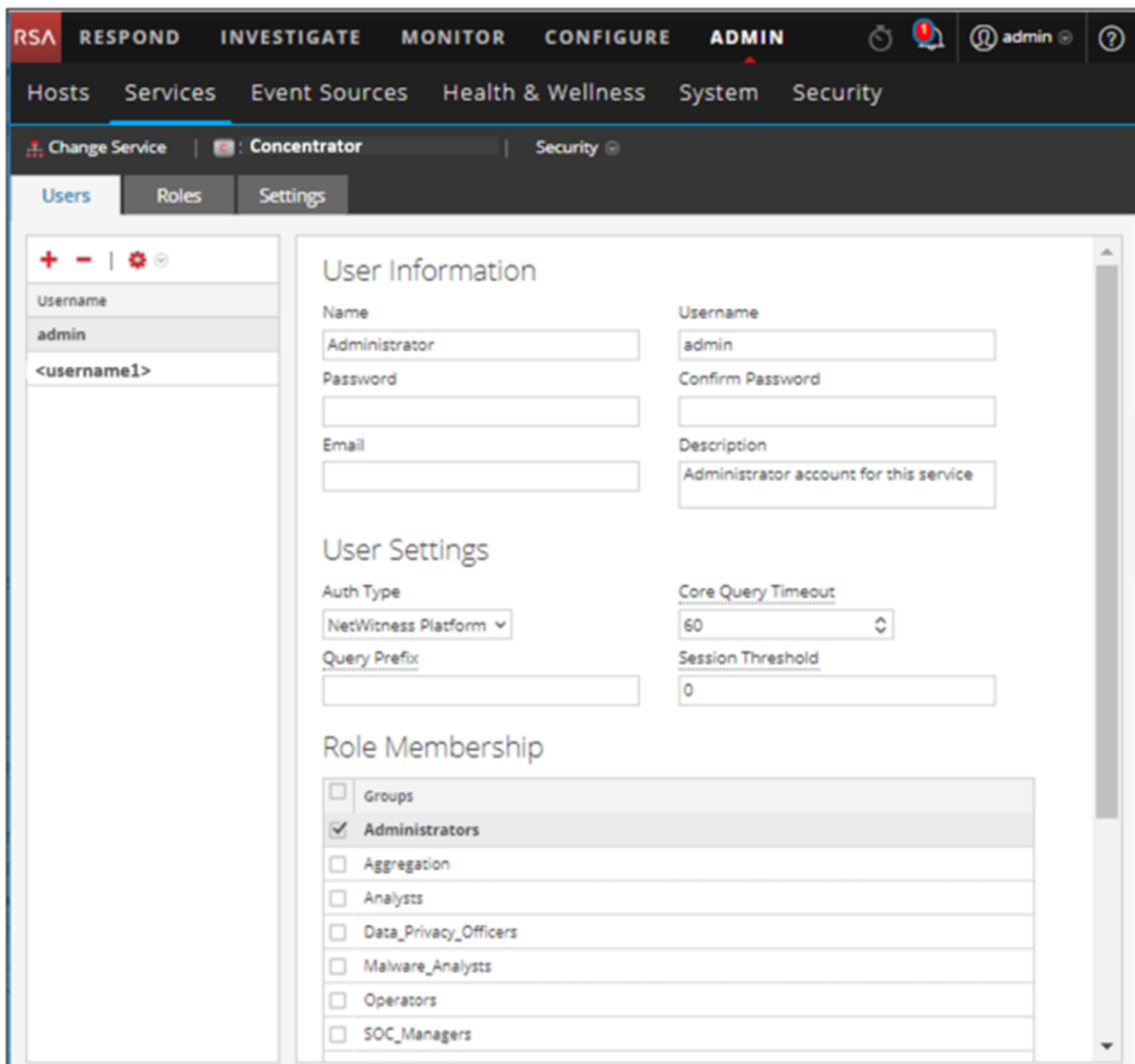
[セキュリティ]ビューへのアクセス

以下の各手順は、サービスの[セキュリティ]ビューから開始します。

サービスの[セキュリティ]ビューに移動するには、次の手順を実行します。

1. NetWitness Platformで、**[管理]** > **[サービス]**に移動します。

2. サービスを選択し、 > [表示] > [セキュリティ]をクリックします。
 選択したサービスの[セキュリティ]ビューが表示され、[ユーザ]タブが開きます。





注 : NetWitness Platform 10.4以前のサービスバージョンでは、[ユーザ設定]セクションに[Coreクエリタイムアウト]ではなく[クエリレベル]フィールドが表示されます。

サービス ユーザの追加

1. [ユーザ]タブで、**+**をクリックします。
2. サービスにアクセスするユーザ名を入力し、Enterキーを押します。
 [ユーザ情報]セクションにユーザ名が表示され、残りのフィールドが編集可能になります。
3. [パスワード]および[パスワードの確認]フィールドで、サービスにログオンするためのパスワードを入力します。
4. (オプション) 追加情報を提供します。


- NetWitness Platformにログオンするための名前
 - メールアドレス
 - ユーザの説明
5. [ユーザ設定]セクションで、次の情報を選択します。
- **認証タイプ**
 - NetWitness Platformがユーザを認証する場合は、[Netwitness]を選択します。
 - NetWitness Serverのユーザ認証のためにActive DirectoryまたはPAMが構成されている場合は、[外部]を選択します。
 - [Coreクエリタイムアウト]は、ユーザがサービスに対して1つのクエリを実行できる最長時間(分)です。このフィールドはNetWitness Platform 10.5以降のサービスバージョンで使用され、10.4以前のバージョンには表示されません。
6. (オプション) 追加のクエリ条件を指定します。
- [クエリプレフィックス]はクエリをフィルタします。プレフィックスを入力して、ユーザに表示される結果を制限します。
 - [セッション閾値]は、スキャンするセッションのカウント数を制御します。メタ値のセッション数が閾値を上回ると、セッション数のカウントを停止します。
7. [ロールメンバシップ]セクションで、ユーザに割り当てるロールを選択します。ユーザがサービス上のロールのメンバになると、ロールに割り当てられた権限が付与されます。
8. 新しいサービスユーザをアクティブ化するには、[適用]をクリックします。

他のサービスへのユーザのレプリケート

1. [ユーザ]タブで、ユーザを選択して、  > [レプリケート]をクリックします。
[他のサービスへのユーザのレプリケート]ダイアログが表示されます。

2. パスワードを入力し、確認のためもう一度入力します。
3. ユーザのレプリケート先となる各サービスを選択します。
4. [レプリケート]をクリックします。

サービスユーザの削除

1. [ユーザ]タブで、ユーザ名を選択し、をクリックします。
NetWitness Platformによって、選択したユーザの削除を確認するプロンプトが表示されます。
2. ユーザを削除するには、[はい]をクリックします。

サービスユーザのロールの追加

NetWitness Platformには、サーバおよび各サービスに事前定義されたロールがあります。カスタムロールを追加することもできます。次の表に、事前構成されたシステムロールとその権限を示します。

ロール	権限
Administrators	フル システム アクセス
Operators	構成 へのアクセス権を持つが、メタおよびセッションのコンテンツへのアクセス権は持たない
Analysts	メタおよびセッションのコンテンツへのアクセス権を持つが、構成 へのアクセス権は持たない

ロール	権限
SOC_Managers	Analystsと同じアクセス権に加えて、インシデントの処理に必要な権限を持つ
Malware_Analysts	マルウェア イベントへのアクセス権、およびメタおよびセッションのコンテンツへのアクセス権を持つ
Data_Privacy_Officers	メタおよびセッションのコンテンツへのアクセス権と、システム内の機微データの難読化と表示を管理する設定オプションへのアクセス権を持つ(「データ プライバシーの管理」を参照)


以下のユーザやロールを追加した場合、サービス ロールを追加する必要があります。

- 新しい権限のセットを必要とするサービス ユーザ。
- **NetWitness Server上のカスタム ロール。** 信頼接続では、サーバと、カスタム ロールがアクセスする各サービスの両方に、同一のカスタム ロールが存在する必要があるためです。これらの名前は同一である必要があります。たとえば、サーバ上にJunior Analystsロールを追加した場合、そのロールがアクセスする各サービスにJunior Analystsロールを追加する必要があります。詳細については、「システムセキュリティとユーザ管理」の「**ロールの追加と権限の割り当て**」を参照してください。

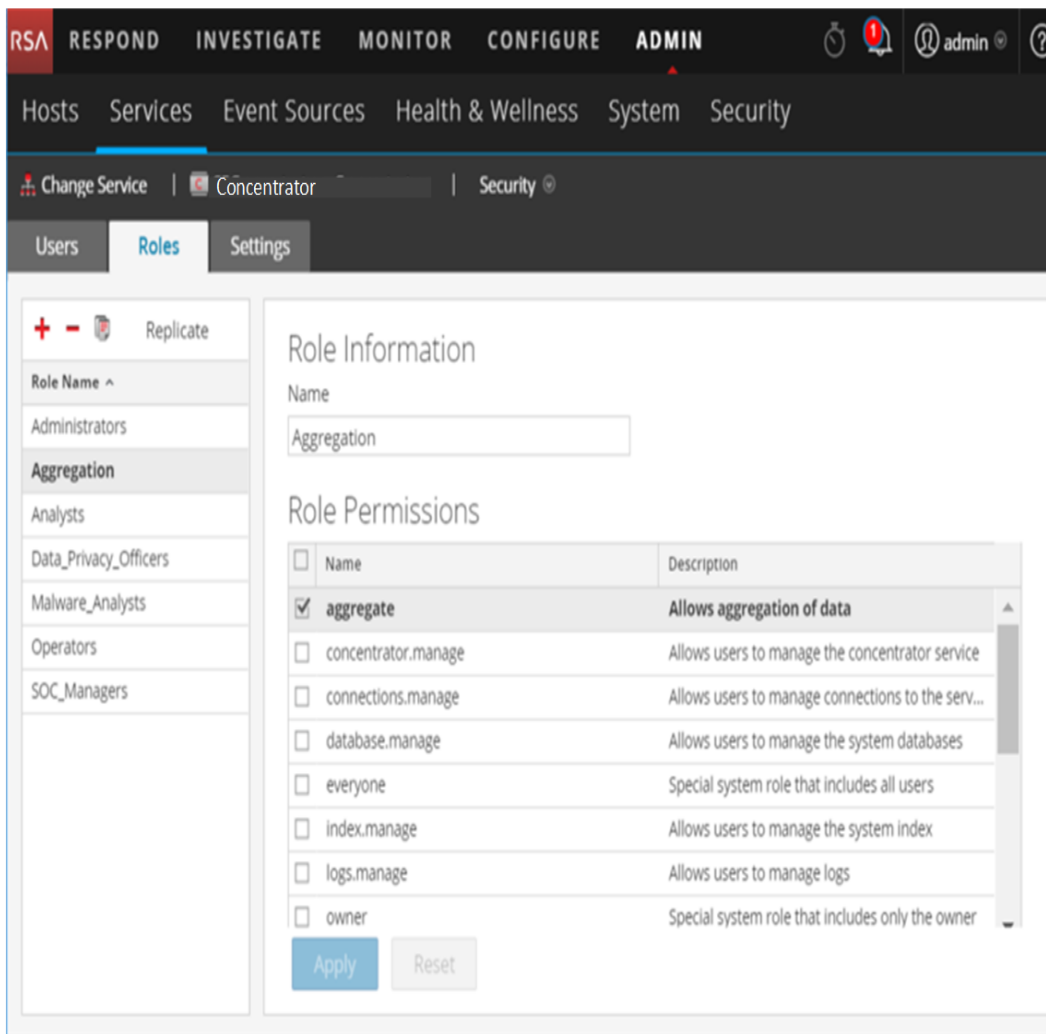
事前構成されたAggregationサービス ロールもあります。詳細については、「Aggregationロール」と「サービスのユーザ ロールと権限」を参照してください。

手順

サービス ユーザ ロールを追加して権限を割り当てるには:

1. NetWitness Platformで、**[管理]** > **[サービス]**に移動します。
2. サービスを選択し、 > **[表示]** > **[セキュリティ]**を選択します。
選択したサービスの**[セキュリティ]**ビューが表示され、**[ユーザ]**タブが開きます。

3. [ロール] タブを選択し、**+**をクリックします。
[ロール] タブには、5つの事前構成されたロールが一覧表示されます。




4. **+**をクリックし、**ロール名**を入力して、**Enter**キーを押します。
ロール名は、**ロールの権限**セクションの上部に表示されます。
5. サービス上でロールに付与する各権限を選択します。
6. [適用]をクリックします。
[ユーザ]タブで、サービスユーザをロールのメンバに追加できます。

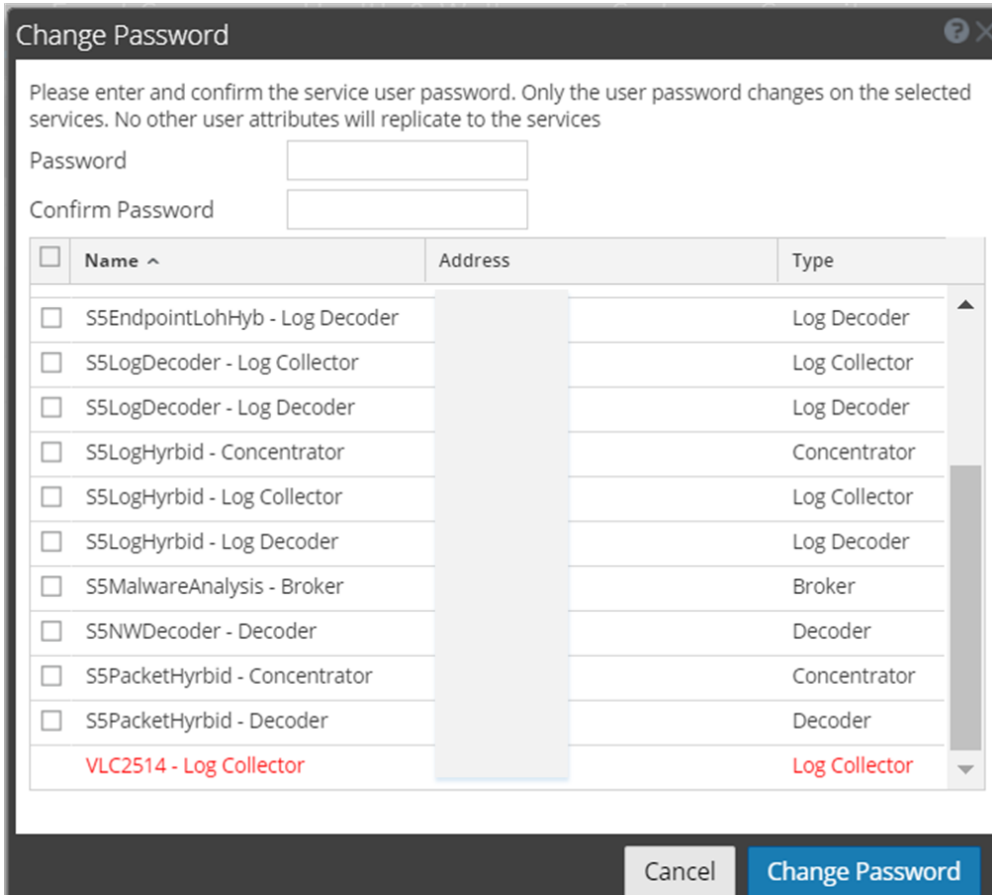
サービスユーザのパスワードの変更

この手順により、管理者がサービスユーザのパスワードを変更し、新しいパスワードを、そのユーザアカウントが定義されているすべてのコアサービスにレプリケートできます。選択されたコアサービスにレプリケートされるのは、ユーザアカウント全体ではなく、パスワードの変更のみです。また、管理者は、コアサービスのadminアカウントのパスワードを変更することもできます。

注: [パスワードの変更] オプションは、外部ユーザには適用されません。

サービス ユーザのパスワードを変更するには:

1. NetWitness Platformで、[管理]>[サービス]に移動します。
[管理]の[サービス]ビューが表示されます。
2. サービスを選択し、 > [表示]> [セキュリティ]をクリックします。
選択したサービスの[セキュリティ]ビューが表示されます。
3. [ユーザ]タブで、ユーザを選択して、アクション アイコンから[パスワードの変更]を選択します。
[パスワードの変更]ダイアログが表示されます。



4. ユーザの新しいパスワードを入力し、パスワードを確認します。
5. ユーザのパスワードを変更するサービスを選択します。
6. [パスワードの変更]をクリックします。
選択したサービスのパスワード変更のステータスが表示されます。

サービス グループの作成と管理

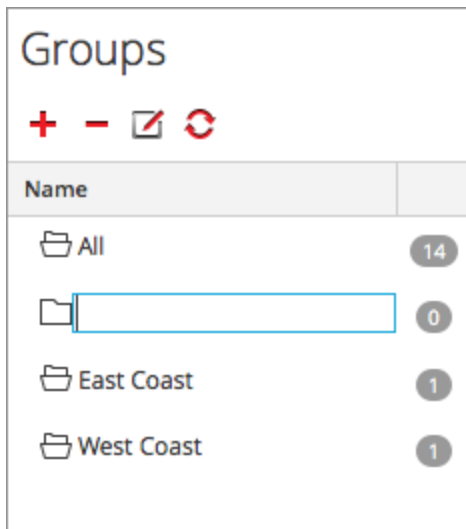
[管理]の[サービス]ビューでは、サービスのグループを作成および管理するためのオプションが提供されます。[サービス]パネル ツールバーには、サービス グループの作成、編集、削除のオプションがあります。グループの作成後、[サービス]パネルからグループに各 サービスをドラッグできます。

グループは、機能別、地域別、あるいはプロジェクト別など、組織における運用管理方式に従って構成できます。1つのサービスが複数のグループに属することができます。ここでは、考えられる分類の例をいくつか示します。

- すべてのBroker、Decoder、Concentratorの構成と監視を容易にするために、サービスタイプごとにグループ化。
- 同じデータフローを構成しているサービス(たとえば、Brokerとそれに関連するすべてのConcentratorとDecoder)をグループ化。
- サービスが配置されている地域や場所に従ってグループ化。これにより、ある地域で大規模な停電が発生した場合に、影響を受ける可能性があるサービスを容易に識別可能です。

グループの作成

1. NetWitness Platformで、**[管理]** > **[サービス]**に移動します。
[管理]の[サービス]ビューが表示されます。
2. **[グループ]**パネルのツールバーで、**+**をクリックします。
新しいグループのフィールドが表示され、カーソルが点滅します。




3. このフィールドに新しいグループの名前(「A New Group」など)を入力し、**Enter**キーを押します。
グループはツリー内にフォルダとして作成されます。グループの横にある数値は、そのグループ内の

サービスの数を示します。

Groups	
Name	
📁 All	14
📁 A New Group	0
📁 East Coast	1
📁 West Coast	1

グループ名の変更

1. [サービス]ビューの[グループ]パネルで、グループ名をダブルクリックするか、グループを選択し、をクリックします。[名前]フィールドが表示され、カーソルが点滅します。
2. グループの新しい名前を入力し、Enterキーを押します。
[名前]フィールドが閉じ、新しいグループ名がツリーに表示されます。


グループへのサービスの追加

[サービス]ビューの[サービス]パネルで、サービスを選択し、[グループ]パネル内のグループフォルダ(たとえば、[Log Collectors])にサービスをドラッグします。
グループにサービスが追加されます。

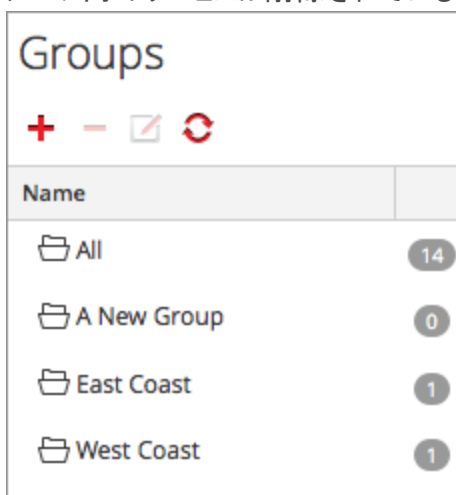
グループ内のサービスの表示

グループ内のサービスを表示するには、[グループ]パネルでグループをクリックします。
[サービス]パネルに、そのグループ内のサービスが表示されます。


グループからのサービスの削除

1. [サービス]ビューの[グループ]パネルで、削除するサービスが含まれているグループを選択します。そのグループ内のサービスが[サービス]パネルに表示されます。
2. [サービス]パネルで、グループから削除するサービスを1つ以上選択し、ツールバーで  > [グループから削除] を選択します。
選択したサービスはグループから削除されますが、NetWitness Platformユーザ インタフェースからは削除されません。表示されているサービス数は、グループから削除されたサービスの数だけ減ります。
[すべて]グループには、グループから削除されているサービスが含まれます。
次の例では、[A New Group]という名前のサービスグループにはサービスが含まれていません。グ

グループ内のサービスが削除されているためです。



グループの削除

1. [サービス]ビューの[グループ]パネルで、削除するグループを選択します。
2.  をクリックします。
 選択したグループが[グループ]パネルから削除されます。グループに含まれていたサービスは NetWitness Platform ユーザ インタフェースからは削除されません。[すべて]グループには、削除されたグループのサービスが含まれています。


サービス ロールの複製またはレプリケート

新しいサービス ロールを追加するための効率的な方法として、同じロールを複製して新しい名前で作成し、すでに割り当てられている権限を変更することができます。たとえば、Analysts ロールを複製できます。複製したら、Junior Analysts という名前で作成し、権限を変更します。

既存のロールを別のサービスに簡単に追加する方法として、ロールをレプリケートすることができます。たとえば、BrokerにあるJunior Analysts ロールをConcentratorおよびLog Decoderにレプリケートできます。

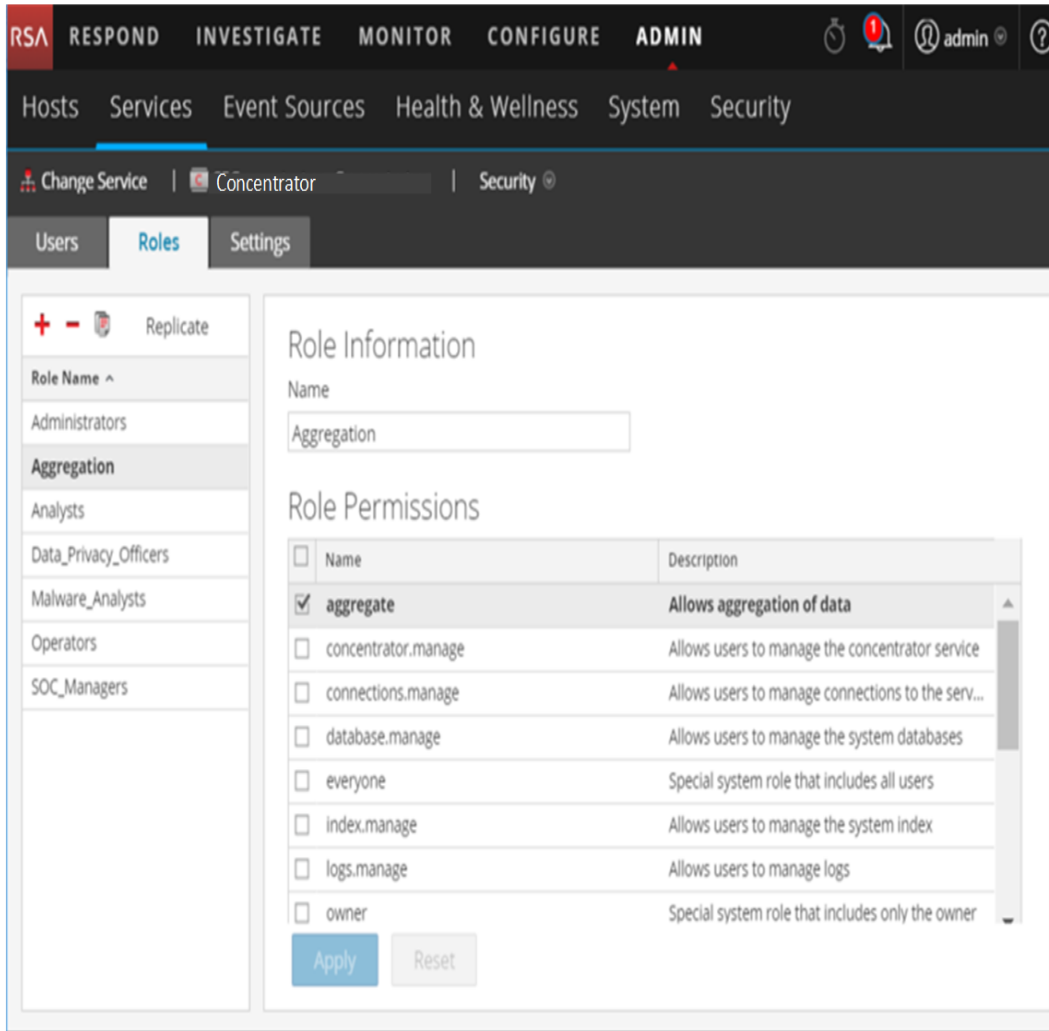
以下の各手順は、サービスの[セキュリティ]ビューから開始します。


サービスの[セキュリティ]ビューに移動するには、次の手順を実行します。

1. NetWitness Platformで、[管理]>[サービス]に移動します。
2. サービスを選択し、 > [表示]> [セキュリティ] をクリックします。
 選択したサービスの[セキュリティ]ビューが表示され、[ユーザ]タブが開きます。
3. [ロール]タブを選択します。

サービス ロールの複製

1. [ロール] タブで、複製するロールを選択します。



2.  (ロールの複製) をクリックします。
3. 新しい名前を入力し、[適用] をクリックします。
4. 新しいロールを選択します。
5. [ロールの権限] セクションで、権限を選択または選択解除し、新しいロールで実行できる内容を変更します。

ロールのレプリケート

1. [ロール] タブで、レプリケートするロールを選択し、[レプリケート] をクリックします。
2. [他のサービスへのロールのレプリケート] ダイアログで、ロールの追加先の各サービスを選択します。
3. [レプリケート] をクリックします。

コア サービス構成ファイルの編集

Decoder、Log Decoder、Broker、Concentrator、Archiver、Workbenchサービスのサービス構成ファイルは、テキストファイルとして編集できます。[サービス]の[構成]ビュー>[ファイル]タブでは、次のタスクを実行できます。

- NetWitness Platformシステムが現在使用しているサービス構成ファイルを表示および編集する。
- ファイルの最新のバックアップを取得したり、バックアップをリストアする。
- ファイルを他のサービスにプッシュする。
- ファイルの変更を保存する。

編集可能なファイルは、構成するサービスのタイプによって異なります。すべてのコア サービスに共通のファイルは次のとおりです。


- サービス インデックス ファイル
- netwitnessファイル
- crash reporterファイル
- schedulerファイル

さらに、Decoderには、Parser、Feed定義、Wireless LANアダプタを構成するためのファイルがあります。

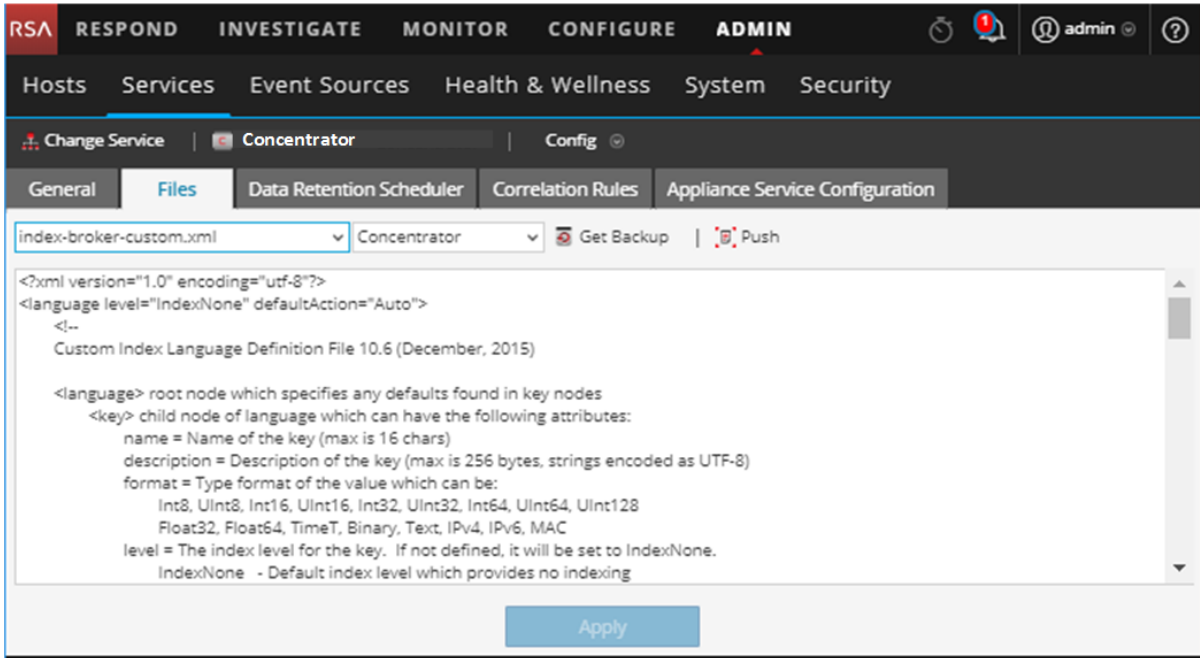
注:これらの構成ファイルのデフォルト値は一般的な状況では変更する必要はありませんが、crash reporterやschedulerなどのオプション サービスでは編集が必要です。これらのファイルを[ファイル]タブで変更する場合には、ネットワーク環境やデータ収集および解析への影響について十分に理解している管理者のみが実施するようにしてください。

サービス構成ファイルの編集

ファイルを編集するには、次の手順を実行します。

1. NetWitness Platformで、[管理]>[サービス]に移動します。
2. [サービス]グリッドでサービスを選択します。
3.  > [表示]>[構成]を選択します。
[サービス]の[構成]ビューが表示され、[全般]タブが開きます。
4. [ファイル]タブをクリックします。
選択したサービス(Concentratorなど)が右側のドロップダウンリストに表示されます。
5. (オプション) サービスではなくホストのファイルを編集するには、ドロップダウンリストで[ホスト]を選択します。

6. [編集するファイルを選択してください]ドロップダウン リストからファイルを選択します。ファイルの内容が編集モードで表示されます。




7. ファイルを編集して、[適用]をクリックします。

現在のファイルは上書きされ、バックアップファイルが作成されます。変更はサービスの再起動後に有効になります。


バックアップのサービス構成ファイルへのロールバック

構成ファイルに変更を加えて保存し、サービスを再起動すると、バックアップファイルが使用可能になります。バックアップした構成ファイルにロールバックする場合は、次の手順を実行します。

1. このトピックの最初の手順のステップ1～6を実行して、構成ファイルを選択します。
2.  Get Backup をクリックします。
バックアップファイルが開きます。
3. 構成ファイルをバックアップバージョンに戻すには、[保存]をクリックします。
変更はサービスの再起動後に有効になります。

他のサービスへの構成ファイルのプッシュ

サービス構成ファイルを編集した後、同じタイプの他のサービスに同じ構成をプッシュできます。

1. このトピックの最初にある「サービス構成ファイルの編集」手順のステップ1～6を実行して、構成ファイルを選択します。
2.  Push をクリックします。[サービスの選択]ダイアログが表示されます。

- 構成ファイルをプッシュするサービスを選択します。
[サービス]ビューで選択したサービスと同じタイプのサービスを選択する必要があります。

注意: 構成ファイルをプッシュしない場合は、[キャンセル]をクリックします。

- 選択したすべてのサービスに構成ファイルをプッシュする場合は、[OK]をクリックします。
構成ファイルは、選択したすべてのサービスにプッシュされます。

タスク スケジューラの構成

schedulerファイル

schedulerファイルは、[サービス]の[構成]ビュー>[ファイル]タブで編集できます。このファイルは、サービスに標準で組み込まれたタスク スケジューラを構成します。タスク スケジューラは、指定された間隔または指定された時間に自動的にタスク メッセージを送信してタスクを実行します。

タスク スケジューラの構文

schedulerファイルのタスク行は、次の構文で記述します。<Value>にはスペースを含めることはできません。

```
<ParamName>=<Value>
```

<Value>にスペースが含まれる場合は、次のように記述します。

```
<ParamName>="<Value>"
```

各タスク行では、次のガイドラインに従います。

- timeパラメータ、またはインターバルパラメータ(seconds、minutes、hours) のいずれかが必要です。
- 特殊文字は(バックスラッシュ)によってエスケープします。

タスク行パラメータ

スケジューラでは、次のタスク行パラメータを使用できます。

構文	説明
daysOfWeek: <string, optional, {enum-any:sun mon tue wed thu fri sat all}>	タスクを実行する曜日。デフォルト値はall。
deleteOnFinish: <bool, optional>	正常完了時にタスクを削除する。
hours: <uint32, optional, {range:1 to 8760}>	実行間隔(時間)。
logOutput: <string, optional>	指定したモジュール名を使用して出力をログに記録。
minutes: <uint32, optional, {range:1 to 525948}>	実行間隔(分)。
msg: <string>	ノードに送信するメッセージ。
params: <string, optional>	メッセージのパラメータ。
pathname: <string>	メッセージを受信するノードのパス。
seconds: <uint32, optional, {range:1 to 31556926}>	実行間隔(秒)。

構文	説明
<code>time</code> : <string>	HH::MM:SS形式の実行時間(このサーバのローカル時間)。
<code>timesToRun</code> : <uint32, optional>	サービス開始後のタスク実行回数、0は無制限(デフォルト)

メッセージ

次に、タスク スケジューラの `msg` パラメータに指定するメッセージ文字列を示します。

メッセー ジ	説明
<code>addInter</code>	指定された間隔で実行するタスクを追加します。たとえば、次のメッセージは6時間ごとに <code>/index save</code> コマンドを実行します。 <code>addInter hours=6 pathname=/index msg=save</code>
<code>addMil</code>	1日の特定の時間、または特定の曜日の特定の時間に実行するタスクを追加します。たとえば、次のメッセージは各営業日の午前1時に <code>/index save</code> コマンドを実行します。 <code>addMil time= 01:00:00 pathname=/index msg=save daysOfWeek=mon,tue,wed,thu,fri</code>
<code>delSched</code>	既存のスケジュール設定されたタスクを削除します。このタスクの <code>id</code> パラメータは、 <code>print</code> メッセージから取得する必要があります。
<code>print</code>	スケジュール設定されたタスクを表示します。
<code>replace</code>	単一のメッセージでスケジュール設定されたすべてのタスクを割り当て、既存のタスクをすべて削除します。
<code>save</code>	ノードを保存。

サンプルタスク行

`scheduler` ファイルの次のタスク行の例は、Feedのホスト サーバから120分ごとに `Decoder` に `Feed` パッケージ ファイル(`feeds.zip`) をダウンロードします。

```
minutes=120 pathname=/parsers msg=feed params="type\=wget
file\=http://feedshost/nwlive/feeds.zip"
```

サービス インデックス ファイルの編集

このピックでは、[サービス]の[構成]ビュー> [ファイル]タブで編集可能なサービス カスタム インデックス ファイルを構成するための重要な情報やガイドラインについて説明します。

インデックス ファイルは、他の構成ファイルとともに、各コア サービスの処理を制御します。NetWitness Platformの[サービス]の[構成]ビューでインデックス ファイルを開くと、ファイルを編集できます。

注: インデックス ファイルの変更は、コア サービス構成に関する詳細で包括的な知識を持つ管理者のみが実施するようにしてください。インデックス ファイルは、アプライアンス サービスの核となる構成ファイルの1つです。すべてのコア サービスで一貫性のある変更を行う必要があります。無効な値が入力されたりファイルが誤って構成されたりすると、システムが開始できない状態になることがあります。結果的にRSAのサポートが必要になる場合もあります。

インデックス ファイルには次のものがあります。

- `index-broker.xml`および `index-brokereustom.xml`
- `index-concentrator.xml`および`index-concentrator-custom.xml`
- `index-decoder.xml`および`index-decodereustom.xml`
- `index-logdecoder.xml`および`index-logdecodereustom.xml`
- `index-archiver.xml`および `index-archiver-custom.xml`
- `index-workbench.xml`および`index-workbench-custom.xml`

インデックス ファイルとカスタム インデックス ファイル

ユーザ固有のインデックスの変更はすべて、`index-<service>-custom.xml`に記述します。このファイルの設定は、RSAのみが管理する`index-<service>.xml`の設定を上書きします。

カスタム インデックス ファイル(`index-<service>-custom.xml`)を使用することによって、アップグレードによる変更の影響を受けることなく、独自のlanguageキーの定義や設定の上書きを行うことができます。

- `index-<service>-custom.xml`に定義されたキーは、`index-<service>.xml`の定義を置き換えます。
- `index-<service>eustom.xml`に追加され、`index-<service>.xml`に存在しないキーは、新しいキーとしてlanguageに追加されます。

インデックス ファイルの編集は、次のような場合に必要です。

- 新しいカスタム メタ キーを追加して、NetWitness Platformのユーザ インタフェースに新しいフィールドを追加する。
- 「データ プライバシーの管理」ガイドの説明に従い、データのプライバシー対策の一環として保護されたメタ キーを構成する。
- 「NetWitness Platform コア データベース チューニング ガイド」の説明に従い、NetWitness Platform コア データベースのクエリ パフォーマンスを調整する。

注意 : Decoderから集計するConcentratorまたはArchiverがある場合は、DecoderのIndexKeysまたはIndexValuesにインデックス レベルを設定しないでください。デフォルトのtimeメタ キーを超えるインデックス作成をサポートするには、インデックスのパーティション サイズが小さ過ぎます。

Crash Reporterサービスの有効化

Crash Reporterは、NetWitness Platformサービスのオプション サービスです。コア サービスでアクティブ化すると、Crash Reporterは、サービスに障害が発生したときに、その原因の診断や解決に使用する情報のパッケージを自動的に生成します。パッケージは、解析のためにRSAに自動的に送信するよう設定できます。送信された内容は、調査のためにRSAサポート部門に転送されます。

RSAに送信される情報パッケージには、収集されたデータは含まれません。このパッケージには、次の情報が含まれます。

- スタックトレース
- ログ
- 構成設定

- ソフトウェア バージョン
- CPU情報
- インストールされたRPM
- ディスク ジオメトリ

Crash Reporterによるクラッシュの解析は、コア製品に対してアクティブ化できます。

crashreporter.cfgファイル

[サービス]の[構成]ビュー>[ファイル]タブで編集可能なファイルの1つに、Crash Reporterクライアントサーバ設定ファイル、**crashreporter.cfg**があります。

このファイルは、ホスト上でCrash Reportのチェック、更新、作成を行うスクリプトによって使用されます。監視する製品としては、Decoder、Concentrator、ホスト、Brokerを含めることができます。


次の表で、**crashreporter.cfg**ファイルの設定について説明します。


設定	説明
applicationlist=decoder, concentrator, host	監視する製品のリストを定義します。
sitedir=/var/crashreporter	レポートのサイト ディレクトリの場所。
webdir=/usr/share/crashreporter/Web	Webディレクトリの場所。
devdir=/var/crashreporter/Dev	Devディレクトリの場所。
datadir=/var/crashreporter/data	データ ファイルを保存するディレクトリの場所。
perldir=/usr/share/crashreporter/perl	perlファイルの場所。
bindir=/usr/share/crashreporter/bin	バイナリ実行プログラムの場所。
libdir=/usr/share/crashreporter/lib	バイナリライブラリの場所。
cfgdir=/etc/crashreporter	構成ファイルの場所。
logdir=/var/log/crashreporter	ログ ファイルの場所。
scriptdir=/usr/share/crashreporter/scripts	スクリプトを含むディレクトリの場所。
workdir=/var/crashreporter/work	プロセスの作業 ディレクトリの場所。
sqldir=/var/crashreporter/sql	作成されたsqlファイルが配置される場所。
reportdir=/var/crashreporter/reports	一時レポートが作成される場所。
packagedir=/var/crashreporter/packages	作成されたパッケージ ファイルの場所。
gdbconfig=/etc/crashreporter/crashreporter.gdb	gdb構成ファイルの場所。

設定	説明
corewaittime=30	コアファイルが書き込み中かどうかを判断するためにコアの検出後に待機する秒数を定義します。
cyclewaittime=10	検索サイクルの待機時間 (分) を定義します。
deletecores=1	レポート後にコアファイルを削除するかどうかを指定します。 0=いいえ 1=はい 注: コアファイルは、削除されるまで、crashreporterが再開されるたびにレポートされます。
deletereportdir=1	レポート後にレポートディレクトリを削除するかどうかを指定します。コアレポートをまとめて表示する場合に役立ちます。 0=いいえ 1=はい 注: ディレクトリを削除しない場合、ディレクトリには各パッケージが含まれます。
debug=1	crashreporter]のログ出力でデバッグメッセージをオンまたはオフにするかを指定します。 0=いいえ 1=はい
posturl=https://www.netwitnesslive.com/crash...ter/submit.php	送信先となるWebサーバのURLを定義します。
postpackages=0	パッケージをWebサーバに送信するかどうかを指定します。 0=いいえ 1=はい
deletepackages=1	Webサーバへの送信後にパッケージを削除するかどうかを指定します。 0=いいえ 1=はい

Crash Reporter Serviceの構成



Crash Reporter Serviceを構成するには、次の手順を実行します。

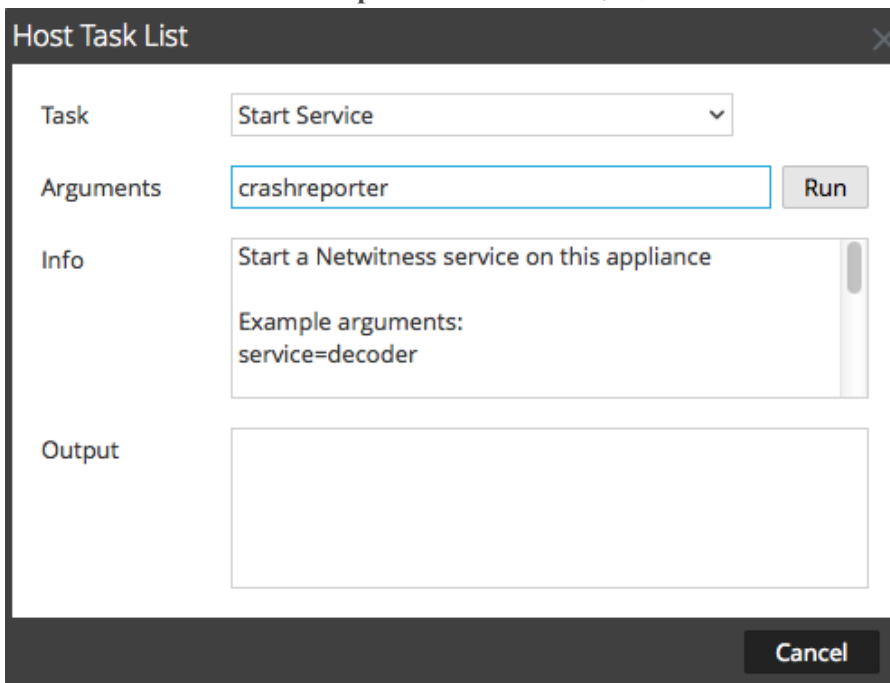
1. [管理] > [サービス] を選択します。
2. サービスを選択し、 > [表示] > [構成] をクリックします。
3. [ファイル] タブを選択します。

4. `crashreporter.cfg`を編集します。
5. [保存]をクリックします。
6. [サービス]の[システム]ビューを表示するため、[構成]>[システム]を選択します。
7. サービスを再起動するため、 Shutdown Service をクリックします。
サービスがシャットダウンして再起動します。

Crash Reporterサービスの開始と停止

Crash Reporterサービスを開始するには、次の手順を実行します。

1. [管理]>[サービス]を選択します。
2. サービスを選択し、 > [表示]> [システム]をクリックします。
3. ツールバーで  Host Tasks をクリックします。
[ホスト タスク リスト]が表示されます。
4. [タスク]ドロップダウン リストで、[サービスの開始]を選択します。
5. [引数]フィールドに「`crashreporter`」と入力し、[実行]をクリックします。



Crash Reporterサービスが起動されます。サービスは停止するまでアクティブです。

Crash Reporterサービスを停止するには、[タスク]ドロップダウン リストで[サービスの停止]を選択します。

テーブル マップ ファイルの維持

RSAが提供するテーブル マッピング ファイル、`table-map.xml`は、Log Decoderを構成する非常に重要な要素です。このファイルは、ログParserが使用するキーをMetaDBのキーにマッピングするメタ定義ファイルです。

注: `table-map.xml`ファイルは編集しないでください。変更が必要な場合は、`table-map-custom.xml`ファイルを変更します。最新の`table-map.xml`ファイルはLiveから入手でき、RSAでは必要に応じてこのファイルを更新しています。`table-map.xml`ファイルを変更しても、サービスまたはコンテンツのアップグレードにより、変更が上書きされる可能性があります。

`table-map.xml`では、`Transient`に設定されたメタキーと`None`に設定されたメタキーがあります。メタキーを保存し、インデックスを作成するには、`None`に設定する必要があります。マッピングを変更するには、Log Decoderで`table-map-custom.xml`という名前のファイルのコピーを作成し、メタキーを`None`に設定する必要があります。

メタキーのインデックス作成について

- Log Decoderの`table-map.xml`ファイルで、メタキーに`None`が設定されている場合、そのメタキーのインデックスが作成されます。
- Log Decoderの`table-map.xml`ファイルで、メタキーに`Transient`が設定されている場合、そのメタキーのインデックスは作成されません。そのメタキーのインデックスを作成する場合は、`table-map-custom.xml`ファイルにエントリーをコピーして、`flags="Transient"`を`flags="None"`に変更します。
- メタキーがLog Decoderの`table-map.xml`ファイルに存在しない場合は、`table-map-custom.xml`ファイルにエントリーを追加します。

注意: `table-map.xml`ファイルはアップグレードによって上書きされる可能性があるため、更新しないでください。必要な変更はすべて`table-map-custom.xml`ファイルに追加します。

前提条件

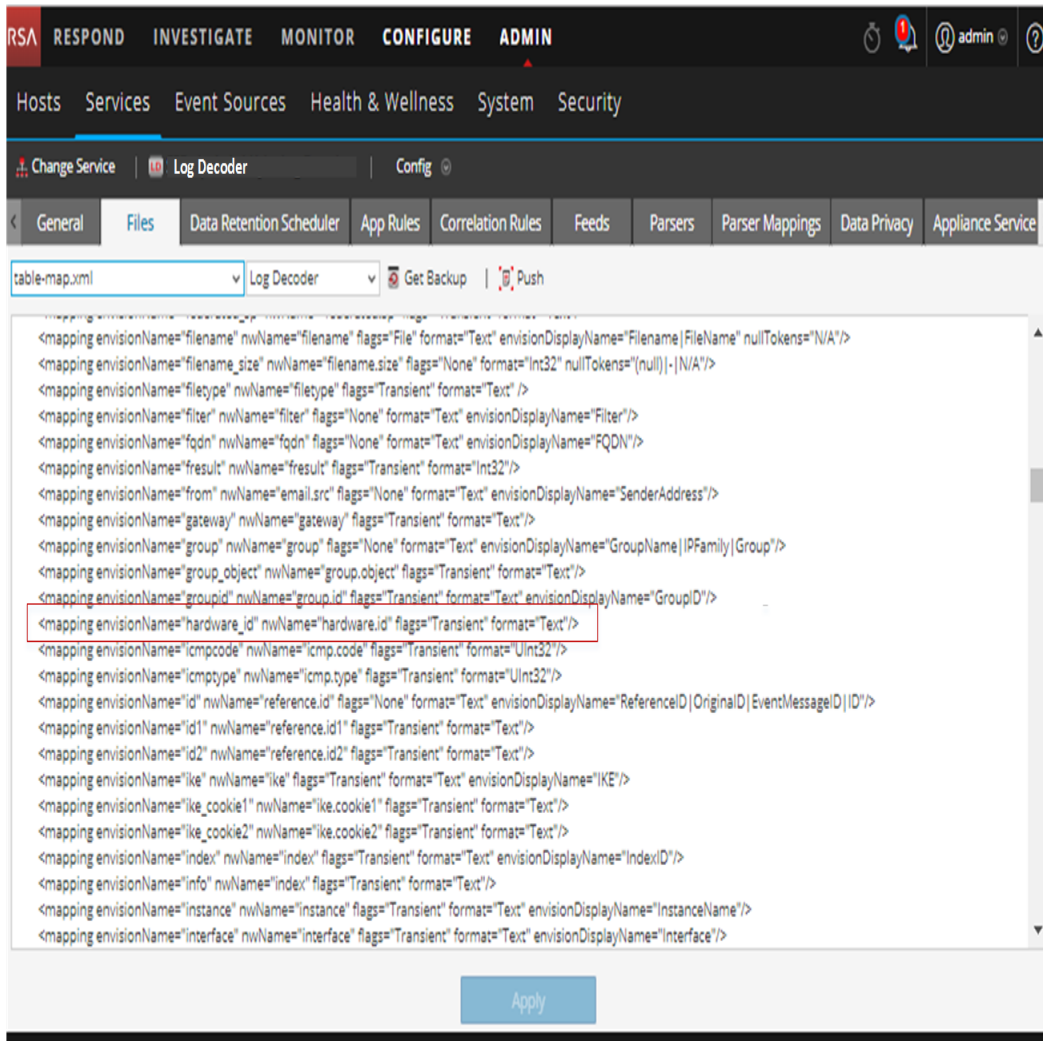
Log Decoderに`table-map-custom.xml`ファイルがない場合は、`table-map.xml`のコピーを作成し、名前を`table-map-custom.xml`に変更します。

手順

テーブル マッピング ファイルを検証して更新するには、次の手順を実行します。

1. [管理] > [サービス]に移動します。
2. [サービス]グリッドで、Log Decoderを選択し、 > [表示] > [構成]をクリックします。

3. [ファイル] タブをクリックして、table-map.xml ファイルを選択します。



4. flags キーワードが Transient または None に正しく設定されていることを確認します。
5. エントリを変更する必要がある場合は、table-map.xml ファイルを変更しないでください。代わりに、エントリをコピーし、table-map-custom.xml ファイルを選択して、table-map-custom.xml ファイルでエントリを検索し、flags キーワードを Transient から None に変更します。
たとえば、次の hardware.id メタキー (table-map.xml ファイル内) はインデックスが作成されず、flags キーワードは Transient に設定されています。

```
<mapping envisionName="hardware_id" nwName="hardware.id"
flags="Transient" />
```

hardware.id メタキーのインデックスを作成するには、table-map-custom.xml で flags キーワードを Transient から None に変更します。

```
<mapping envisionName="hardware_id" nwName="hardware.id" flags="None" />
```
6. エントリが table-map.xml ファイルに含まれていない場合は、table-map-custom.xml ファイルにエントリを追加します。

7. `table-map-custom.xml` ファイルに変更を加えた後で、**[適用]** をクリックします。

注意: テーブル マッピング ファイルを変更する前に、インデックスを `Transient` から `None` に変更することによる影響を慎重に検討してください。使用可能なストレージ容量と Log Decoder のパフォーマンスに影響が及ぶ可能性があります。そのため、デフォルトでインデックスを作成するメタキーは限られています。`table-map-custom.xml` ファイルはさまざまな用途で使用します。

サービスの編集または削除

ホスト名またはポート番号の変更など、サービス設定を変更したり、必要なくなったサービスを削除できます。

[サービス]ビューで次の各手順を実行します。

[サービス]ビューに移動するには、NetWitness Platform で、**[管理]** > **[サービス]** に移動します。



The screenshot shows the RSA NetWitness Platform Admin console. The top navigation bar includes 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN'. Below this are tabs for 'Hosts', 'Services', 'Event Sources', 'Health & Wellness', 'System', and 'Security'. The 'Services' tab is selected, showing a list of services. On the left, there is a 'Groups' sidebar with an 'All' group containing 25 items. The main area displays a table of services with columns for Name, Licensed, Host, Type, Version, and Actions.

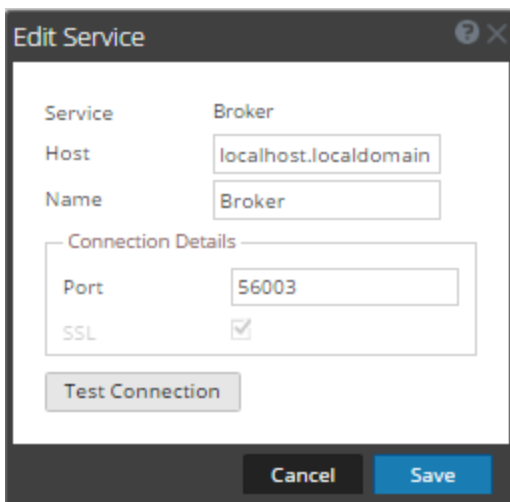
Name	Licensed	Host	Type	Version	Actions
Admin	✓	NW Server	Admin Server	11.2.0.0	[Settings]
Archiver	✓	Archiver	Archiver	11.2.0.0	[Settings]
Broker	✓	Broker	Broker	11.2.0.0	[Settings]
Cloud Gateway	✓	Cloud Gateway	Cloud Gateway Serve	11.2.0.0	[Settings]
Concentrator	✓	Concentrator	Concentrator	11.2.0.0	[Settings]
Config	✓	NW Server	Config Server	11.2.0.0	[Settings]
Content	✓	NW Server	Content Server	11.2.0.0	[Settings]
Context Hub	✓	Event Stream Ana	Contexthub Server	11.2.0.0	[Settings]
Decoder	✓	Decoder	Decoder	1.2.0.0	[Settings]
Endpoint	✓	Endpoint Hybrid	Endpoint	11.2.0.0	[Settings]
Entity Behavior Analysis	✓	Event Stream Ana	Entity Behavior Ana	11.2.0.0	[Settings]
Event Stream Analysis	✓	Event Stream Ana	Event Stream Analys	11.2.0.0	[Settings]
Integration	✓	NW Server	Integration Serv	11.2.0.0	[Settings]
Investigate	✓	NW Server	Investigate Server	11.2.0.0	[Settings]
Log Collector	✓	Log Decoder	Log Collector	11.2.0.0	[Settings]
Log Decoder	✓	Log Decoder	Log Decoder	11.2.0.0	[Settings]
Log Decoder	✓	Endpoint Hybrid	Log Decoder	11.2.0.0	[Settings]
Malware Analysis	✓	Malware Analysis	Malware Analys	11.2.0.0	[Settings]
Orchestration	✓	NW Server	Orchestration Serve	11.2.0.0	[Settings]
Reporting Engine	✓	NW Server	Reporting Engine	11.2.0.0	[Settings]
Respond	✓	NW Server	Respond Server	11.2.0.0	[Settings]
Security	✓	NW Server	Security Server	11.2.0.0	[Settings]
Source	✓	NW Server	Source Server	11.2.0.0	[Settings]
UEBA	✓	UEBA	UEBA	11.2.0.0	[Settings]
Workbench	✓	Archiver	Workbench	11.2.0.0	[Settings]

At the bottom of the console, the RSA NetWitness Platform logo and version number 11.2.0.0 are visible.

手順

サービスの編集



1. [サービス]ビューで、サービスを選択し、または > [編集]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。ここには、選択したサービスに適用されるフィールドのみが表示されます。



2. 次のいずれかのフィールドを変更して、サービスの詳細を編集します。
 - 名前
 - ポート - 各コア サービスには、SSLと非SSLの2つのポートがあります。信頼接続の場合、SSLポートを使用する必要があります。
 - SSL - 信頼接続の場合、SSLを使用する必要があります。
 - [ユーザ名]および[パスワード] - これらの認証情報を使用して、サービスへの接続をテストします。
 - a. 信頼接続を使用する場合、ユーザ名は削除します。
信頼接続を使用しない場合、ユーザ名およびパスワードを入力します。
 - b. [接続のテスト]をクリックします。

3. [保存]をクリックします。

サービスの削除

1. [サービス]ビューで、1つ以上のサービスを選択し、または > [削除]をクリックします。
 2. 確認のダイアログが表示されます。サービスを削除するには、[はい]をクリックします。
- 削除されたサービスは、NetWitness Platformで使用できなくなります。


サービスのプロパティ ツリーの表示と編集

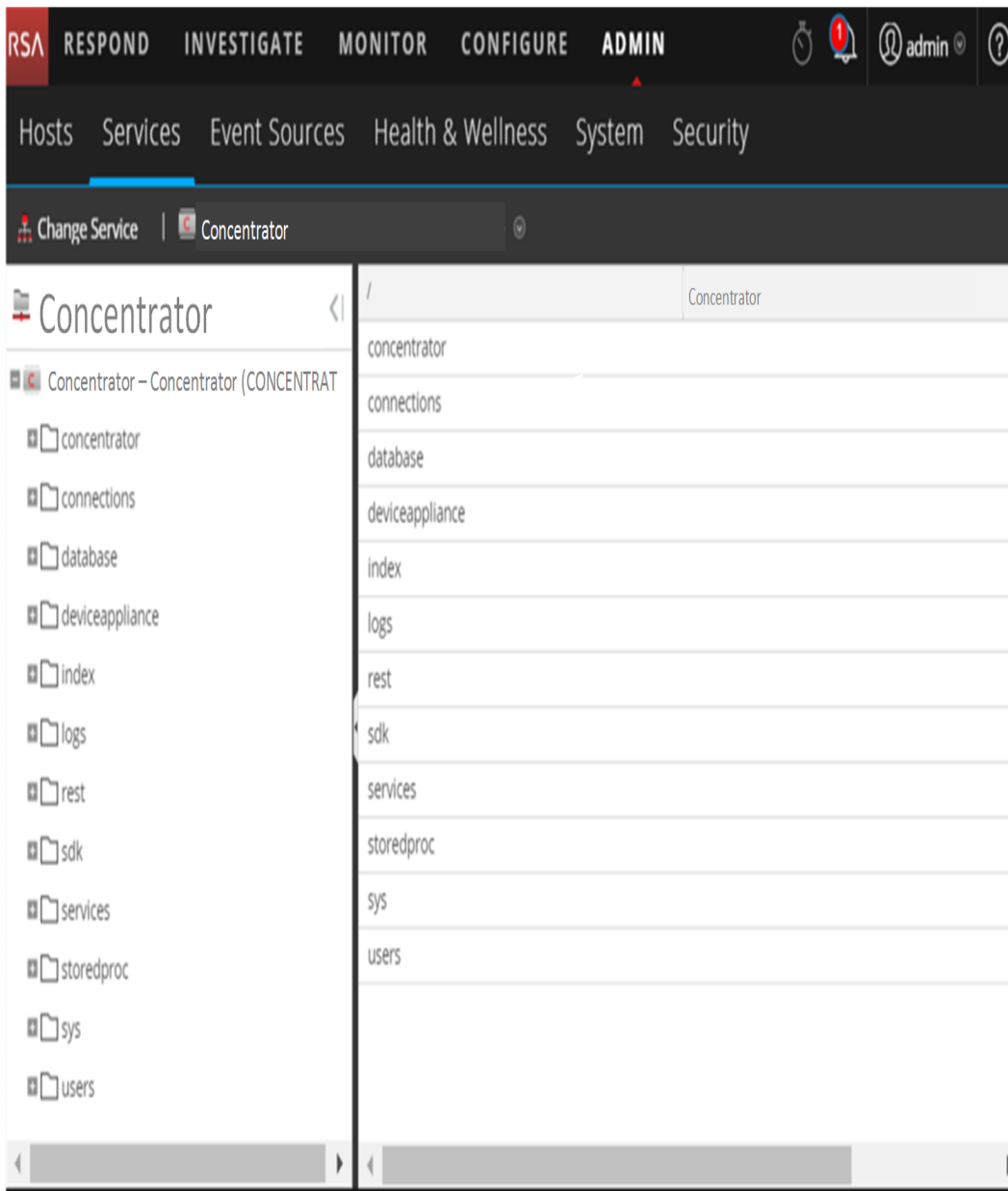
[サービス] の [エクスプローラ] ビューでは、サービスの詳細な設定にアクセスし、制御することができます。このビューは2つの部分で構成されます。[ノード] リストには、フォルダのツリー構造でサービス機能が表示されます。[監視] パネルには、[ノード] リストで選択したフォルダまたはファイルのプロパティが表示されます。

[エクスプローラ] ビューで次の各手順を実行します。

[エクスプローラ] ビューに移動する方法

1. NetWitness Platformで、**[管理]** > **[サービス]** に移動します。

2. サービスを選択して、 > [表示] > [エクスプローラ]を選択します。
[エクスプローラ]ビューが表示されます。[ノード]リストは左側に、[監視]パネルは右側にあります。



サービス プロパティの表示または編集

サービス プロパティを表示する方法

1. [ノード]リストまたは[監視]パネルでファイルを右クリックします。
2. プロパティをクリックします。

サービス プロパティの値を編集する方法

1. [監視]パネルで、編集可能なプロパティ値を選択します。
2. 新しい値を入力します。


ノードへのメッセージの送信

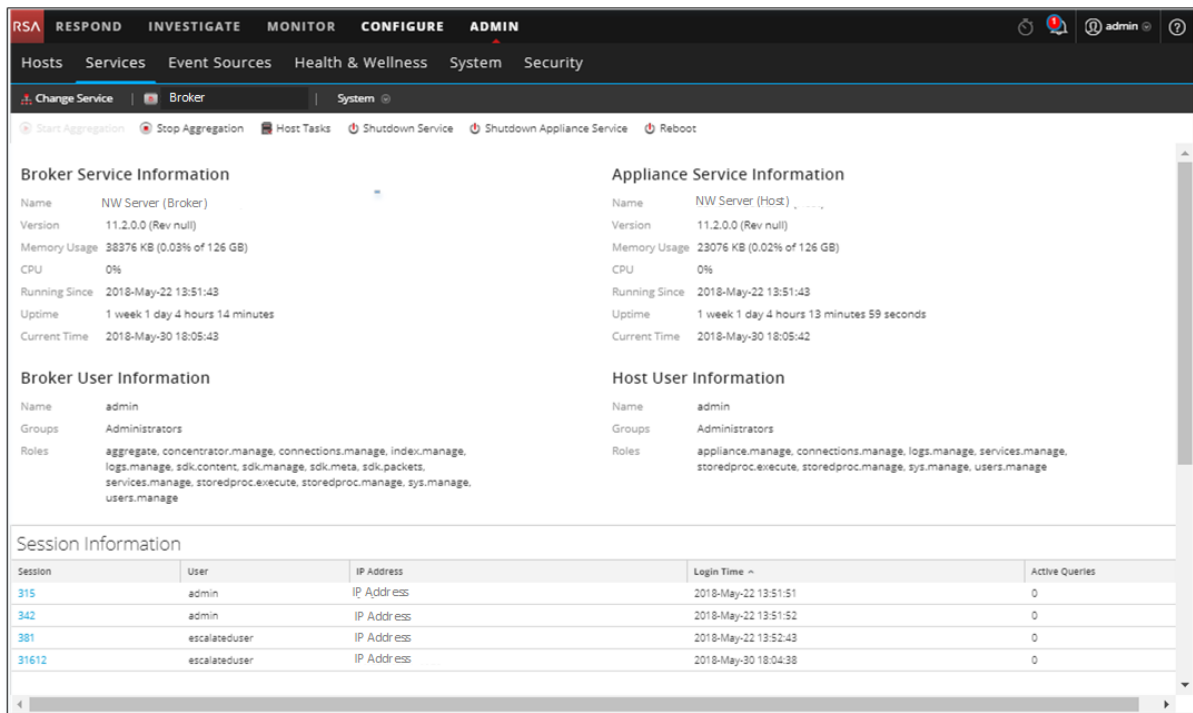
1. [プロパティ]ダイアログで、**メッセージ タイプ**を選択します。[ノード]リストで選択したファイルによってオプションは異なります。
選択したメッセージ タイプの説明が[**メッセージのヘルプ**]フィールドに表示されます。
2. (オプション) メッセージの実行に必要な場合は、**パラメータ**を入力します。
3. [**送信**]をクリックします。
値または形式が、[**応答出力**]フィールドに表示されます。

サービスへの接続の強制終了

サービスの[システム]ビューで、サービスが実行しているセッションを表示できます。セッション リストからセッションを強制終了したり、セッション内でアクティブなクエリを強制終了することができます。

サービスのセッションの強制終了

1. NetWitness Platformで、[管理]>[サービス]に移動します。
[管理]の[サービス]ビューが表示されます。
2. サービスを選択し、 > [表示]> [システム]を選択します。
[サービス]の[システム]ビューが表示されます。



The screenshot displays the 'System' view for a service in the NetWitness Platform. The top navigation bar includes 'RSA RESPOND INVESTIGATE MONITOR CONFIGURE ADMIN'. The main content area is divided into several sections:

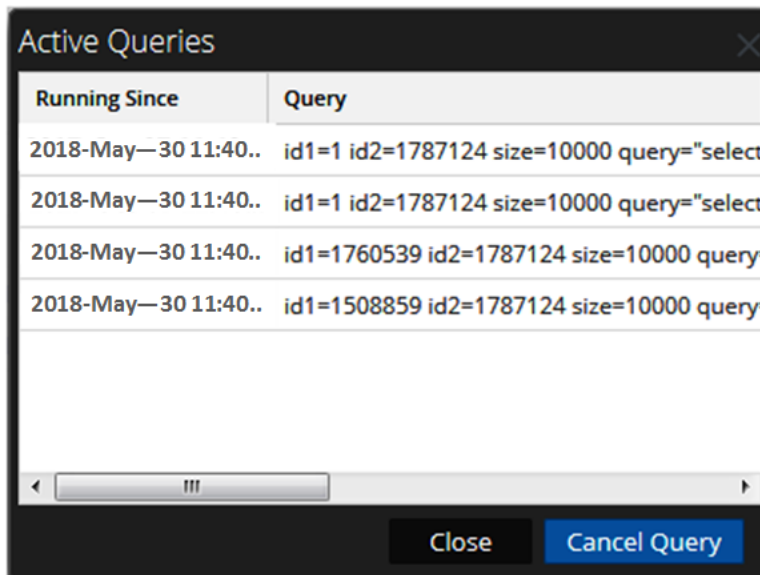
- Broker Service Information:** Name: NW Server (Broker), Version: 11.2.0.0 (Rev null), Memory Usage: 38376 KB (0.03% of 126 GB), CPU: 0%, Running Since: 2018-May-22 13:51:43, Uptime: 1 week 1 day 4 hours 14 minutes, Current Time: 2018-May-30 18:05:43.
- Appliance Service Information:** Name: NW Server (Host), Version: 11.2.0.0 (Rev null), Memory Usage: 23076 KB (0.02% of 126 GB), CPU: 0%, Running Since: 2018-May-22 13:51:43, Uptime: 1 week 1 day 4 hours 13 minutes 59 seconds, Current Time: 2018-May-30 18:05:42.
- Broker User Information:** Name: admin, Groups: Administrators, Roles: aggregate, concentrator.manage, connections.manage, index.manage, logs.manage, sdk.content, sdk.manage, sdk.meta, sdk.packets, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage.
- Host User Information:** Name: admin, Groups: Administrators, Roles: appliance.manage, connections.manage, logs.manage, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage.
- Session Information Table:**

Session	User	IP Address	Login Time	Active Queries
315	admin	IP Address	2018-May-22 13:51:51	0
342	admin	IP Address	2018-May-22 13:51:52	0
381	escalateduser	IP Address	2018-May-22 13:52:43	0
31612	escalateduser	IP Address	2018-May-30 18:04:38	0

3. 下部の[セッション情報]グリッドで、**セッション番号**をクリックします。
確認ダイアログが表示されます。
4. [**はい**]をクリックします。

セッションのアクティブなクエリの強制終了

1. [セッション情報] グリッドまでスクロールします。
2. [アクティブなクエリ] 列で、ゼロ以外の数をクリックします。アクティブなクエリの数がゼロの場合は、クリックできません。
[アクティブなクエリ] ダイアログが表示されます。



3. クエリを選択し、[クエリのキャンセル] をクリックします。
クエリが停止し、[アクティブなクエリ] の列が更新されます。

サービスの検索

[サービス]ビューに表示されるサービスの一覧から目的のサービスを検索することができます。[サービス]ビューでは、名前、ホスト、サービスタイプによって、サービスの一覧をすばやくフィルタすることができます。[フィルタ]ドロップダウンメニューと[フィルタ]フィールドを別々に使用するか、同時に使用して[サービス]ビューをフィルタできます。

サービスの検索

1. NetWitness Platformで、[管理]>[サービス]に移動します。
2. [サービス]パネルツールバーの[フィルタ]フィールドに、サービスの名前またはホストを入力します。



[フィルタ]フィールドに入力した名前と一致するサービスが[サービス]パネルに一覧表示されます。次の例は、[フィルタ]フィールドにlogと入力した後の検索結果を示しています。

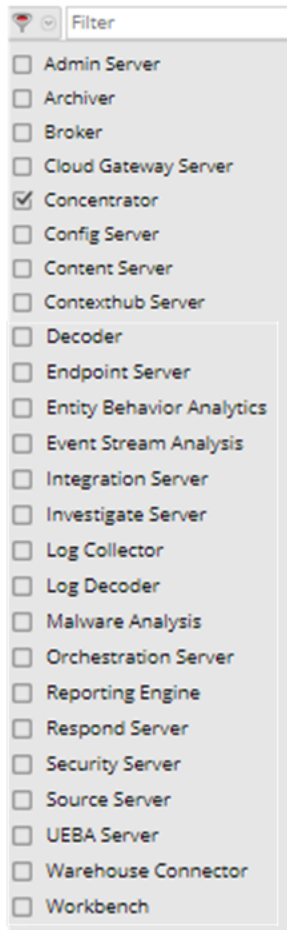
The screenshot shows a web interface titled "Services". At the top, there is a search bar with a filter icon and a dropdown arrow, containing the text "log". Below the search bar is a table with the following columns: Name, Licensed, Host, Type, Version, and Actions. The table contains two rows of data:

<input type="checkbox"/>	Name	Licensed	Host	Type	Version	Actions
<input type="checkbox"/>	Log Collector	or	✓	Log Decoder	Log Collector	11.2.0...
<input type="checkbox"/>	Log Decoder	r	✓	Log Decoder	Log Decoder	11.2.0...

At the bottom of the table, there is a pagination control showing "Page 1 of 1" and "Displaying 1 - 2 of 2".

サービスのタイプによるフィルタ

1. NetWitness Platformで、[管理]>[サービス]に移動します。
2. [サービス]ビューで、 をクリックし、[サービス]ビューに表示したいサービスタイプを選択します。



選択したサービス タイプが[サービス]ビューに表示されます。次の例は、[Concentrator]と[Decoder]でフィルタした[サービス]ビューを示しています。

Services

<input type="checkbox"/>	Name	Licensed	Host	Type	Ver
<input type="checkbox"/>	Concentrator	✔	Concentrator	Concentrator	11
<input type="checkbox"/>	Concentrator	✔	EndpointLogHybrid	Concentrator	11
<input type="checkbox"/>	Log Decoder	✔	EndpointLogHybrid	Log Decoder	11
<input type="checkbox"/>	Log Decoder	✔	Log Decoder	Log Decoder	11
<input type="checkbox"/>	Concentrator	✔	LogHybrid	Concentrator	11
<input type="checkbox"/>	Log Decoder	✔	LogHybrid	Log Decoder	11
<input type="checkbox"/>	Concentrator	✔	NetworkHybrid	Concentrator	11

Page 1 of 1

ホスト上のサービスの検索

[サービス]ビューで各ホストのサービスを確認できます。また、[ホスト]ビューでも、各ホスト上で実行されるサービスをすばやく見つけることができます。

1. NetWitness Platformで、[管理]>[ホスト]に移動します。
2. [ホスト]ビューでホストを選択し、[サービス]列の数字(サービス数)が表示されているボックスをクリックします。
選択したホスト上のサービスが一覧表示されます。

次の例は、4という数字が表示されているボックスをクリックしたイメージです。選択したホスト上の4つのサービスが一覧表示されています。

Name	Host	Services	Current Version	Update Version	Status
NW Server (co-located Broker)	IP-address	10	11.2.0.0		Up-to-Date
Archiver	IP-address	2	11.2.0.0		Up-to-Date
Concentrator	IP-address	1	11.2.0.0		Up-to-Date
Endpoint Log Hybrid	IP-address	4			Up-to-Date
Event Stream Analysis Primary	IP-address				Up-to-Date
Log Decoder	IP-address				Up-to-Date
Log Hybrid	IP-address				Up-to-Date
Malware Analysis	IP-address				Up-to-Date
Network Decoder (Packets)	IP-address	1	11.2.0.0		Up-to-Date
Network Hybrid (Packets)	IP-address	2	11.2.0.0		Up-to-Date

Services tooltip:

- Concentrator
- Endpoint Server
- Log Collector
- Log Decoder

3. サービスのリンクをクリックすると、選択したサービスの[サービス]ビューが表示されます。

サービスの起動、停止、再起動

これらの手順は、コア サービスのみに適用されます。

[サービス]ビューで次の各手順を実行します。NetWitness Platformで、[管理]>[サービス]に移動します。


サービスの開始

サービスを選択して  > [開始]をクリックします。

サービスの停止

サービスを停止すると、そのサービスのプロセスもすべて停止し、アクティブ ユーザはサービスから切断されます。


サービスを停止するには、次の手順を実行します。

1. サービスを選択し、 > [停止] をクリックします。
2. 確認のダイアログが表示されます。サービスを停止するには、[はい] をクリックします。

サービスの再起動

構成変更の適用などで、サービスの再起動が必要な場合があります。再起動が必要なパラメータを変更した場合は、NetWitness Platform にメッセージが表示されます。

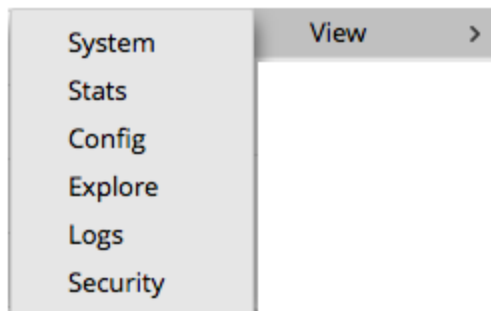
サービスを再起動するには、次の手順を実行します。

1. サービスを選択し、 > [再起動] をクリックします。
2. 確認のダイアログが表示されます。サービスを再起動するには、[はい] をクリックします。

サービスがいったん停止してから自動的に再起動します。

サービスの詳細の表示

サービスの情報を表示および編集するには、サービスの[表示]メニューにあるオプションを使用します。



各サービスビューの目的


各ビューには、サービスの機能とその説明が個別に表示されます。

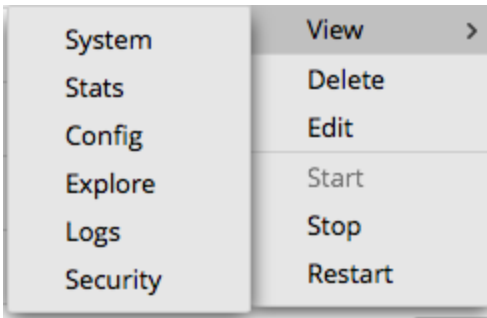
- [システム]ビューには、サービス、アプライアンス サービス、ホスト ユーザ、セッションに関する情報のサマリーが表示されます。
- [サービス]の[統計]ビューには、サービスの動作とステータスを監視する方法が用意されています。
- [サービス]の[構成]ビューでは、サービスの詳細を構成できます。
- [サービス]の[エクスプローラ]ビューでは、ホストとサービスの構成を表示および編集できます。
- [システム ログ]パネルには、検索可能なサービス ログが表示されます。

- [サービス]の[セキュリティ]ビューでは、NetWitness Platformのコア ユーザアカウント(集計用)、シッククライアント ユーザ、REST APIユーザを追加できます。

サービスビューへのアクセス

サービスの各ビューにアクセスするには、次の手順を実行します。

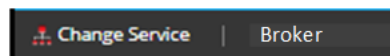
1. NetWitness Platformで、[管理]>[サービス]に移動します。
2. サービスを選択し、 > [表示]をクリックします。
[表示]メニューが表示されます。



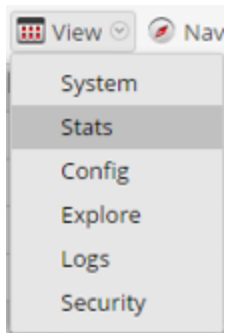
3. オプションからビューを選択します。
以下はBrokerの[システム]ビューです。

Session	User	IP Address	Login Time ~	Active Queries
315	admin	IP Address	2018-May-22 13:51:51	0
342	admin	IP Address	2018-May-22 13:51:52	0
381	escalateduser	IP Address	2018-May-22 13:52:43	0
31612	escalateduser	IP Address	2018-May-30 18:04:38	0

4. 以下のツールバーを使用してナビゲートします。



- a. 別のサービスを選択するには、[サービスの変更]をクリックします。
[サービスの管理]ダイアログが表示されます。
- b. 目的のサービスの左側にあるチェックボックスをオンにします。
- c. [表示]ドロップダウンメニューで選択したサービスのビューを選択します。



選択したサービスの新しいビュー(たとえば、統計)が表示されます。

[ホスト]と[サービス]ビューの参考情報

このトピックは、NetWitness Platformの[管理]ユーザ インタフェースで使用できる機能の参考情報です。このトピックでは、NetWitness Platformの[管理]ユーザ インタフェースで使用できる機能について説明します。管理モジュールでは、NetWitness Platformの管理機能が1つのビューにまとめられており、ホスト (アプライアンス)、サービス、タスク、セキュリティを監視および管理することができます。

トピック

- [\[ホスト\]ビュー](#)
- [\[サービス\]ビュー](#)
- [サービスの\[構成\]ビュー](#)
- [サービスの\[エクスプローラ\]ビュー](#)
- [\[サービス\]の\[ログ\]ビュー](#)
- [\[サービス\]の\[セキュリティ\]ビュー](#)
- [\[サービス\]の\[統計\]ビュー](#)

[ホスト]ビュー

[ホスト]ビューでは、NetWitness Platformサービスを実行する物理マシンまたは仮想マシンのセットアップおよび管理を実行します。

重要: 新バージョンのインストールや更新で発生したエラーを解決するには、「[インストールと更新のトラブルシューティング](#)」を参照してください。

サービスは、ログの収集やデータのアーカイブなど、固有の機能を実行します。各サービスは、専用ポートで実行され、ホストの機能に従って有効化または無効化するプラグインとして提供されます。最初にコアサービスを構成する必要があります。

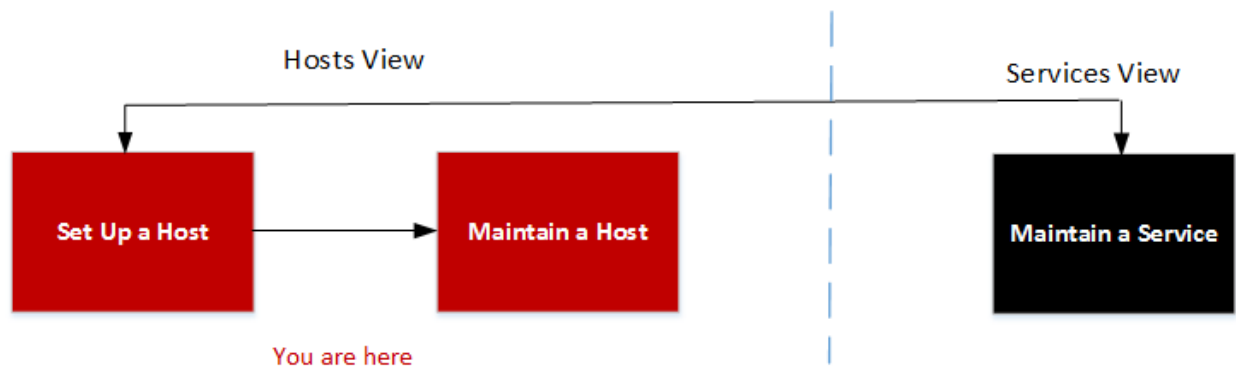
サービス	暗号化されない 非SSLポート	暗号化された SSLポート	注
管理者	N/A	N/A	NW Serverに実装されます
Archiver	50008	56008	
Broker	50003	56003	コア サービス
Cloud Gateway	N/A	N/A	
Concentrator	50005	56005	コア サービス
Config	N/A	N/A	NW Serverに実装されます。
Content	N/A	N/A	NW Serverに実装されます
Context Hub	N/A	N/A	
Decoder(Packets)	50004	56004	コア サービス
Endpoint	N/A	N/A	
Entity Behavior Analysis	N/A	N/A	
Event Stream Analysis	N/A	50030	
Integration	N/A	N/A	NW Serverに実装されます。
Investigate	N/A	N/A	NW Serverに実装されます。
Log Collector	50001	56001	
Log Decoder	50002	56002	コア サービス
Malware Analysis	N/A	60007	
Orchestration	N/A	N/A	NW Serverに実装されます。
Reporting Engine	N/A	51113	NW Serverに実装されます。
Respond	N/A	N/A	NW Serverに実装されます。

サービス	暗号化されない 非SSLポート	暗号化された SSLポート	注
Security	N/A	N/A	NW Serverに実装されます。
Source	N/A	N/A	NW Serverに実装されます
UEBA	N/A	N/A	
Warehouse Connector	50020	56020	
Workbench	50007	56007	

ホストやサービスがデータの格納や収集などの機能を実行するには、ネットワークおよび他のホストやサービスと相互に通信するようにホストとサービスを構成する必要があります。

ワークフロー

このワークフローは、ホストをセットアップし、ホストを管理し、ホストを新しいNetWitness Platformバージョンに更新するために実行する手順を示します。このワークフローの最初のタスクは、ホストのセットアップです。コアサービスのホストは、追加設定なしでセットアップされます。その後、追加のホストをセットアップして、NetWitness Platform導入環境を拡張することができます。その他2つのタスク(ホストの管理とホストのバージョンの更新)は必要に応じて実行し、特定の順序で実行する必要はありません。



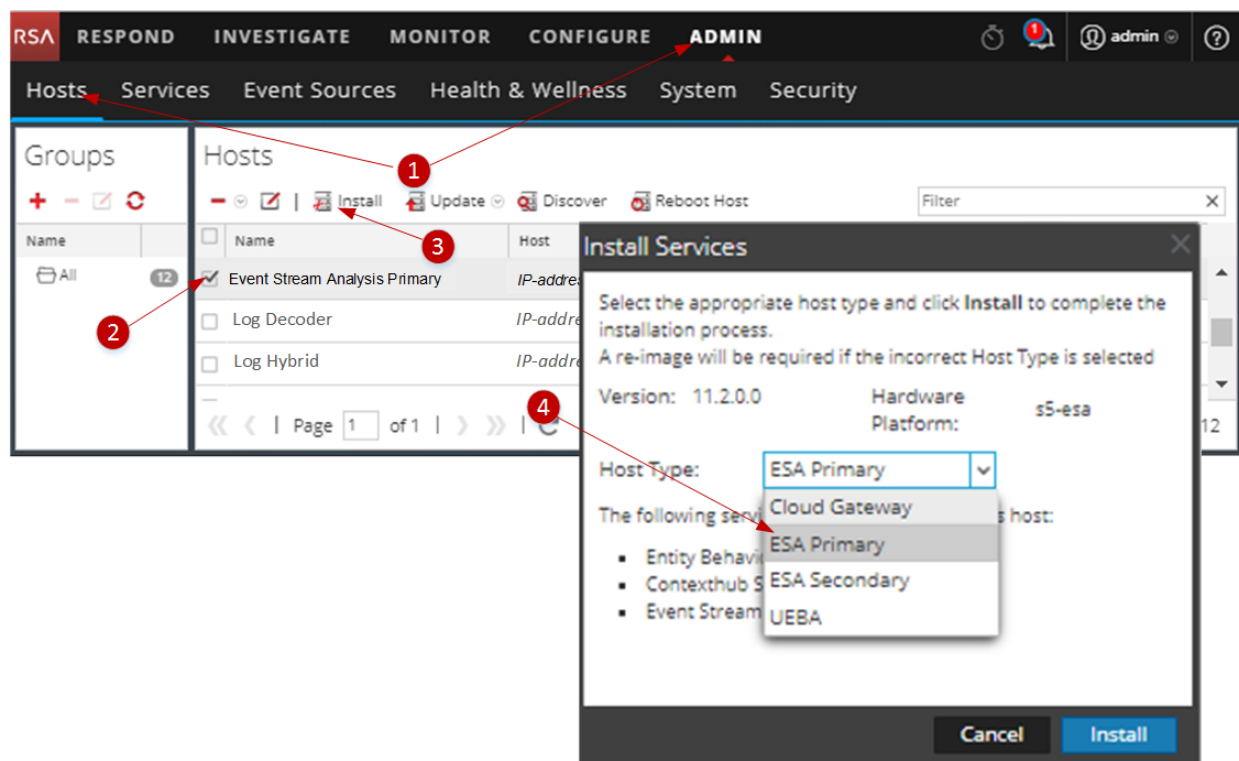
実行したいことは何ですか？

次のタスクの詳細な手順については、「[ホストとサービスの手順](#)」を参照してください。


ロール	実行したいこと
管理者	ホストをセットアップする。
管理者	ホストを管理する。
管理者	バージョンの更新をホストに適用する。

*このタスクは現在のビューで実行できます。

簡単な説明



次の例では、ホストをセットアップする方法を示します。

- 1 [管理] > [ホスト] を選択します。
- 2 導入したホストを選択します(たとえば、[Event Stream Analysisプライマリ])。
- 3  Install ([インストール] アイコン) をクリックします。
- 4 [サービスのインストール] ダイアログからインストールするホストタイプを選択します(たとえば、[ESAプライマリ])。このホストタイプは、Entity Behavior Analytics、Context Hub、Event Stream Analysisサービスをインストールします。

[ホスト] パネル ツールバー

[ホスト] ビューのツールバーには、NetWitness Platform導入環境でホストをメンテナンスするために使用するツールが含まれています。

[ホスト] ビューにアクセスするには、NetWitness Platformメニューで、[管理] > [ホスト] を選択します。
[ホスト] パネル ツールバーは、[ホスト] ビューの[ホスト] グリッドの上部にあります。

機能

次の表では、[ホスト] パネル ツールバーの機能について説明します。

機能	説明
	<p>[グループから削除]: ホストがホスト グループに属している場合、ホストをグループから削除できます。</p>
	<p>[ホストの編集] ダイアログを開きます。このダイアログで、ホストまたはサービスのIDと基本的な通信設定を編集します。このダイアログには、[ホストの追加] ダイアログと同じ機能があります。 関連する手順: ステップ1. ホストの導入</p>
	<p>[サービスのインストール] ダイアログが表示されます。ここから導入済みのホストにサービスをインストールできます。関連する手順: ステップ2. ホストへのサービスのインストール</p>
	<ul style="list-style-type: none"> • [更新]: [更新のバージョン] 列で選択したバージョンで、選択したホスト (複数可) を更新します。 • [更新の確認]: RSAの使用可能な最新の更新がないかローカル更新リポジトリをチェックします。 <p>関連する手順: ホストへのバージョン更新の適用</p>
	<p>ほとんどの場合、検出機能は自動的に実行されるため、[検出] ボタンをクリックする必要はありません。新規インストールの場合は、[検出] ボタンをクリックして[プロビジョニング] ダイアログ ボックスにアクセスし、プロビジョニング フェーズを完了します。プロビジョニング フェーズ完了後、NetWitness Platformはホスト上で実行されるサービスを自動的に検出するため、[検出] ボタンをクリックする必要はありません。</p> <p>新規インストールの場合は、[検出] ボタンをクリックして[プロビジョニング] ダイアログ ボックスにアクセスし、プロビジョニング フェーズを完了します。プロビジョニング フェーズ完了後、NetWitness Platformはホスト上で実行されるサービスを自動的に検出します。</p>
	<p>ホストを再起動します。</p>
<p>フィルタ</p>	<p>名前またはホストでホストをフィルタリングします。</p>

[グループ] パネル ツールバー

[グループ] パネル ツールバーには、ホスト グループを管理するためのオプションが用意されています。ツールバーを使用してグループを作成、編集、削除します。グループの作成後、[ホスト] パネルからグループに各ホストをドラッグできます。





グループを使用して、機能別、地域別、プロジェクト別など、組織における運用管理方式に従ってホストをまとめることができます。1つのホストが複数のグループに属することができます。

NetWitness Platformで、[管理] > [ホスト] に移動します。[グループ] パネル ツールバーは、[ホスト] ビューの[グループ] グリッドの上にあります。

[グループ] パネルでは、ホストの論理的なグループを作成できます。ホストをグループ化すると、複数のホストに対する操作を簡単に実行することができます。

注: NetWitness Liveでは、個別のホストごとにリソースをサブスクライブすることはできませんが、グループを利用すると、グループごとにリソースをサブスクライブできます。

[グループ] パネルは、定義されたホスト グループのリストが表示されるグリッドと、[グループ] パネルツールバーによって構成されます。

列	説明
	新しいグループを追加します。[グループ]グリッドに新しい行が表示され、グループの名前を入力します。
	グループを削除します。確認のプロンプトが表示され、削除を続行またはキャンセルすることができます。
	グループを編集します。[グループ]グリッドのグループの名前フィールドに新しい名前を入力できるようになります。
	選択したグループを更新します。
名前	ホスト グループの名前。グループ名をクリックすると、そのグループに含まれるホストが[ホスト]パネルに表示されます。
<空欄>	グループ内のホストの数を示します。ホストの数をクリックすると、そのグループに含まれるホストが[ホスト]パネルに表示されます。

[サービス]ビュー

[サービス]ビューではNetWitness Platformのサービスをセットアップして管理します。[サービス]ビューでは、次のタスクを実行できます。

- Log DecoderやWarehouse Connectorなどの特定のサービスまたはサービスタイプを素早く検索および特定
- ショートカットを使用して管理タスクにアクセス
- サービスの追加、編集、削除
- 名前およびホストでサービスをソート
- タイプ、名前、ホストでサービスをフィルタ
- サービスの開始、停止、再起動

サービスは、ログの収集やデータのアーカイブなど、固有の機能を実行します。各サービスは、専用ポートで実行され、ホストの機能に従って有効化または無効化するプラグインとして提供されます。最初に次の表のコアサービスを構成する必要があります。

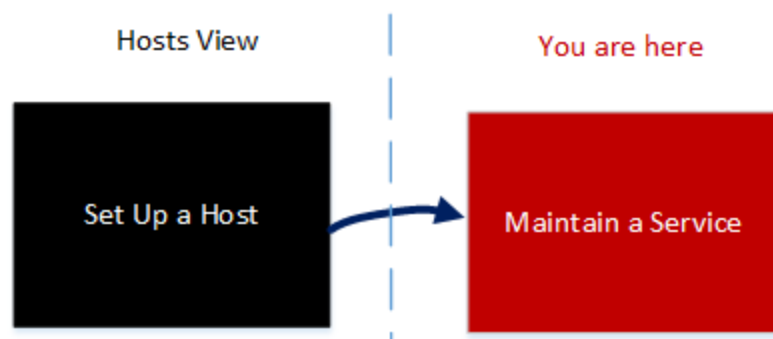
サービス	暗号化されない 非SSLポート	暗号化された SSLポート	注
管理者	N/A	N/A	NW Serverに実装されます
Archiver	50008	56008	
Broker	50003	56003	コア サービス
Cloud Gateway	N/A	N/A	
Concentrator	50005	56005	コア サービス
Config	N/A	N/A	NW Serverに実装されます。
Content	N/A	N/A	NW Serverに実装されます
Context Hub	N/A	N/A	
Decoder(Packets)	50004	56004	コア サービス
Endpoint	N/A	N/A	
Entity Behavior Analysis	N/A	N/A	
Event Stream Analysis	N/A	50030	
Integration	N/A	N/A	NW Serverに実装されます。
Investigate	N/A	N/A	NW Serverに実装されます。
Log Collector	50001	56001	
Log Decoder	50002	56002	コア サービス

サービス	暗号化されない 非SSLポート	暗号化された SSLポート	注
Malware Analysis	N/A	60007	
Orchestration	N/A	N/A	NW Serverに実装されます。
Reporting Engine	N/A	51113	NW Serverに実装されます。
Respond	N/A	N/A	NW Serverに実装されます。
Security	N/A	N/A	NW Serverに実装されます。
Source	N/A	N/A	NW Serverに実装されます
UEBA	N/A	N/A	
Warehouse Connector	50020	56020	
Workbench	50007	56007	

ホストやサービスがデータの格納や収集などの機能を実行するには、ネットワークおよび他のホストやサービスと相互に通信するようにホストとサービスを構成する必要があります。

ワークフロー

このワークフローは、サービスのセットアップと管理の手順を示します。このワークフローの最初のタスクは、ホストにサービスを追加することです。コアサービスのホストは、追加設定なしでセットアップされます。その後、ホストに追加サービスをセットアップし、NetWitness Platform導入環境を拡張することができます。



実行したいことは何ですか？

次のタスクの詳細な手順については、「[ホストとサービスの手順](#)」を参照してください。

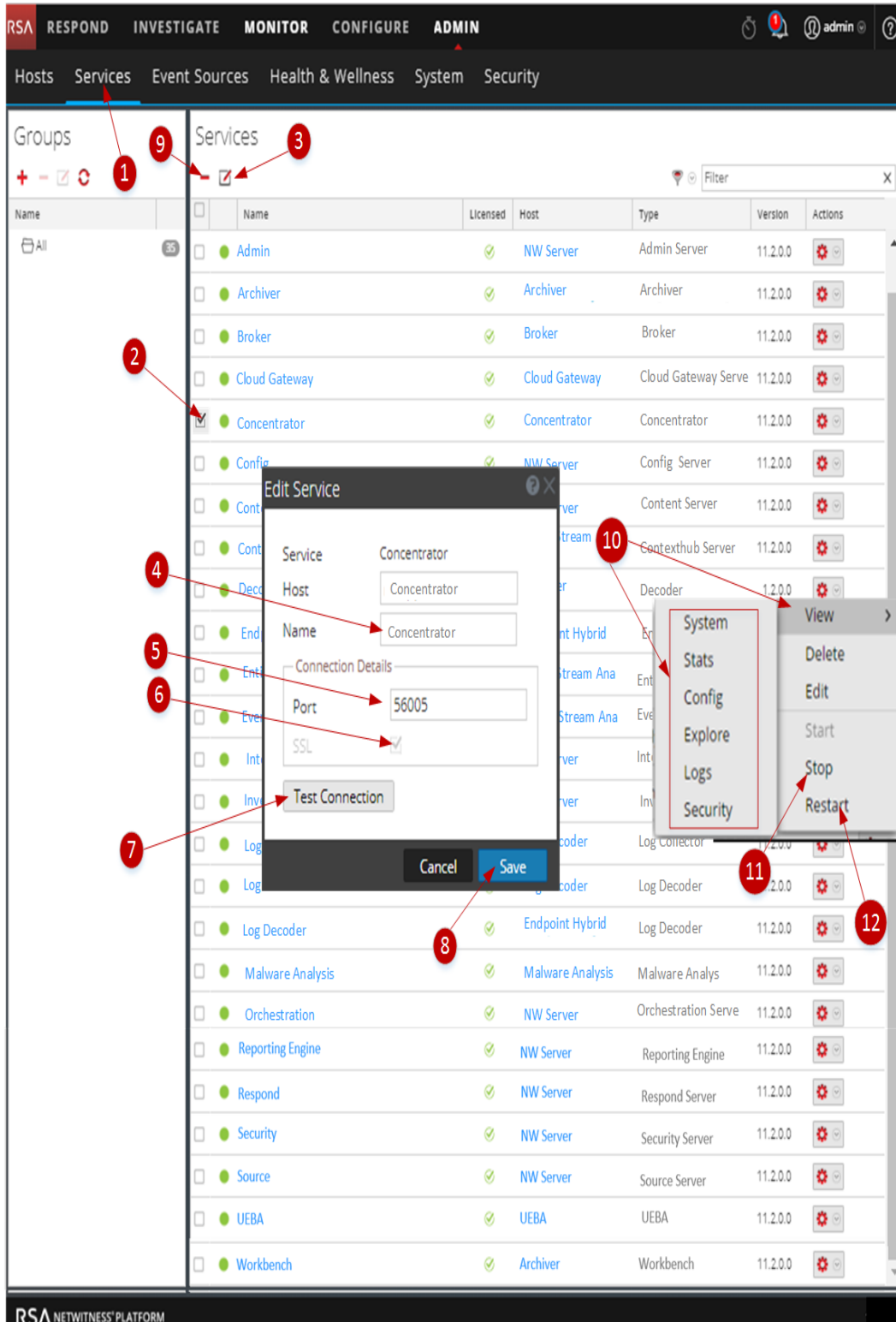
ロール	実行したいこと
管理者	サービスを管理する。
管理者	ホストをセットアップする。

関連トピック

- [インストールと更新のトラブルシューティング](#)

簡単な説明



次の例では、ホストを管理する方法を示します。



サービスを選択します。

- 1 [管理] > [サービス]ビューに移動します。
- 2 選択するサービスの左側にあるチェックボックスをクリックします。

サービスの名前と接続を編集します。

- 3  をクリックします(または、 ([アクション]ドロップダウンメニュー)から[編集]を選択します)。
- 4 ホスト名を編集します。
- 5 ポート番号を編集します。
- 6 SSL通信を選択または選択解除します。
- 7 [接続のテスト]をクリックします。
- 8 [保存]をクリックします。

サービスを削除します。

- 9 サービスを選択し、削除アイコンをクリックします。

サービスの統計の表示とパラメータの構成

- 10 サービスの統計を表示し、サービスパラメータを構成するには、次の手順を実行します。
 - a. サービスを選択し、アクションアイコンをクリックします。
 - b. [表示]をクリックして次を選択します。
 - [システム]を選択すると、
 - サービスとそのホストに関する現在の概要情報を表示します。
 - [システム]ビューのツールバーにアクセスします。
 - [統計]では、サービスの詳細な統計情報を表示します。
 - [構成]では、サービスのパラメータを表示して構成します。
 - [エクスプローラ]では、NetWitness Platformの[エクスプローラ]ビューでサービスのパラメータを表示して構成します。
 - [ログ]では、サービスによって発行されたログメッセージを表示します。
- 11 サービスを選択してアクションアイコンをクリックし、[停止]をクリックすると、実行中のサービスを停止します。
- 12 サービスを選択してアクションアイコンをクリックし、[再起動]をクリックすると、停止したサービスを再起動します。

トピック

個々のサービスの詳細については、次に示すRSA NetWitness Platformのガイド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。を参照してください。

Archiver構成ガイド

BrokerおよびConcentrator構成ガイド

Cloud Behavioral Analytics Gateway構成ガイド

Context Hub構成ガイド

DecoderおよびLog Decoder構成ガイド

Endpoint Insights構成ガイド

Event Stream Analysis (ESA)構成ガイド

Investigateユーザガイド

ログ収集の構成ガイド

Malware Analysis構成ガイド

Reporting Engineユーザガイド

Respond構成ガイド

RSA NetWitness UEBAユーザガイド


Workbench構成ガイド

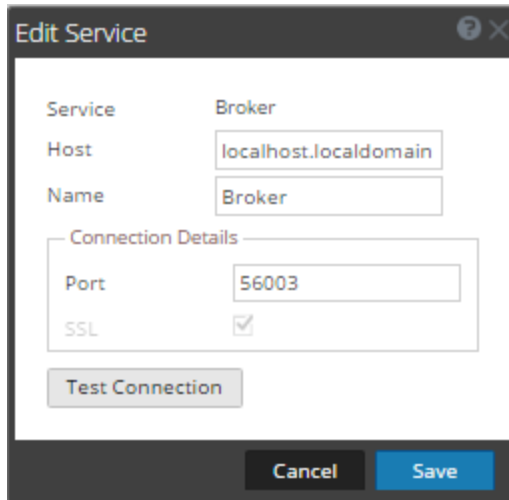
Warehouse Connector構成ガイド

[サービスの編集]ダイアログ

このトピックでは、[管理]の[サービス]ビュー([管理]>[サービス])からアクセスできる[サービスの編集]ダイアログについて説明します。

NetWitness Platformサービスは、NetWitness Platformで自動的に検出されます。

[サービスの編集]ダイアログでは、サービスを変更できます。[サービスの編集]ダイアログにアクセスするには、[管理]>[サービス]に移動し、[サービス]パネルのツールバーでをクリックします。



サービスに関連する手順については、「[ホストとサービスの手順](#)」を参照してください。

機能

この表は、[サービスの追加]ダイアログまたは[サービスの編集]ダイアログの機能について説明しています。

フィールドまたはオプション	説明
サービス	サービスのタイプを表示します。次のサービスを追加できます。Archiver、Broker、Concentrator、Decoder、Event Stream Analysis、Incident Management、IPDB Extractor、Log Collector、Log Decoder、Malware Analysis、Reporting Engine、Warehouse Connector、Workbench。
ホスト	サービスが存在するホストを指定します。
名前	サービスを識別する名前を指定します。例: Broker 。サービスには、分かりやすい名前を付けておくと管理が容易になります。たとえば、([ホスト]フィールドで指定する)ホスト名やIPアドレスを名前の中で使用すると便利な場合があります。
ポート	このサービスとの通信に使用するポートを指定します。[サービス]フィールドで選択したサービスタイプに基づいて、デフォルトポートが自動入力されます。[SSL]を選択すると、このポートはSSLポートになります。[SSL]を選択しないと、非SSLポートになります。このポートは任意の値に変更できますが、その場合はファイアウォールで追加するポートを開く必要があります。ポートの詳細については、「導入ガイド」の「ネットワークアーキテクチャとポート」を参照してください。

フィールドまたはオプション	説明
SSL	NetWitness Platformがこのサービスとの通信にSSLを使用する場合に指定します。
ユーザ名	このサービスにログインするためのユーザ名を指定します。デフォルトのユーザ名は admin です。
パスワード	このサービスにログインするためのパスワードを指定します。デフォルトのパスワードは netwitness です。
接続のテスト	追加するサービスの接続をテストします。
キャンセル	[サービスの追加] または [サービスの編集] ダイアログを閉じます。サービスを保存しないでダイアログを閉じると、サービスは追加されません。
保存	新しいサービスを保存します。

[グループ] パネル ツールバー

このピックでは、[管理] > [サービス] ビュー > [グループ] パネル ツールバーの機能とオプションについて紹介します。





[グループ] パネル ツールバーは、サービス グループを管理するためのオプションを提供します。ツールバーには、グループの作成、編集、削除のオプションがあります。グループの作成後、[サービス] パネルからグループに各サービスをドラッグできます。

グループは、機能別、地域別、あるいはプロジェクト別など、組織における運用管理方式に従って構成できます。1つのサービスが複数のグループに属することができます。

[サービス] ビューにアクセスするには、NetWitness Platformで[管理] > [サービス] を選択します。[グループ] パネル ツールバーは、[サービス] ビューの[グループ] グリッドの上にあります。

機能

この表はツールバーの機能について説明しています。

オプション	説明
	新しいグループを追加します。[グループ] グリッドに新しい行が表示され、グループの名前を入力します。
	グループを削除します。確認のプロンプトが表示され、削除を続行またはキャンセルすることができます。
	グループを編集します。[グループ] グリッドのグループの名前フィールドに新しい名前を入力できるようになります。
	選択したグループを更新します。





[サービス] パネル ツールバー

このトピックでは、サービスの追加、削除、編集、ライセンスに関連した、[サービス] パネル ツールバーのオプションについて説明します。[サービス] パネルのサービス一覧をフィルタすることもできます。

管理の[サービス]ビューにアクセスするには、NetWitness Platformで[管理]>[サービス]に移動します。[サービス] パネル ツールバーは、[サービス]ビューの[サービス]グリッドの上にあります。

機能

この表では[サービス] パネル ツールバーの機能について説明します。

機能	説明
	RSA NetWitness Platform環境にサービスを追加します(「 ステップ2. ホストへのサービスのインストール 」を参照)。
	NetWitness Platform環境からサービスを削除します(「 サービスの編集または削除 」を参照)。
	サービスのIDと基本的な通信設定を編集します。
	[サービス]ビューに表示されるサービスの一覧をフィルタします。 [フィルタ]ドロップダウンメニューでは、1つまたは複数のサービスタイプを選択して、サービスをフィルタできます。例えば、[Concentrator]と[Decoder]を選択すると、ConcentratorサービスとDecoderサービスだけが[サービス]ビューに表示されます。 [フィルタ]フィールドでは、名前とホストを指定してサービスをフィルタできます。 [フィルタ]ドロップダウンメニューと[フィルタ]フィールドを同時に使用して[サービス]ビューに表示されるサービスの一覧をフィルタすることができます。

サービスの[構成]ビュー

このトピックでは、[サービス]の[構成]ビューで使用できる機能について説明します。

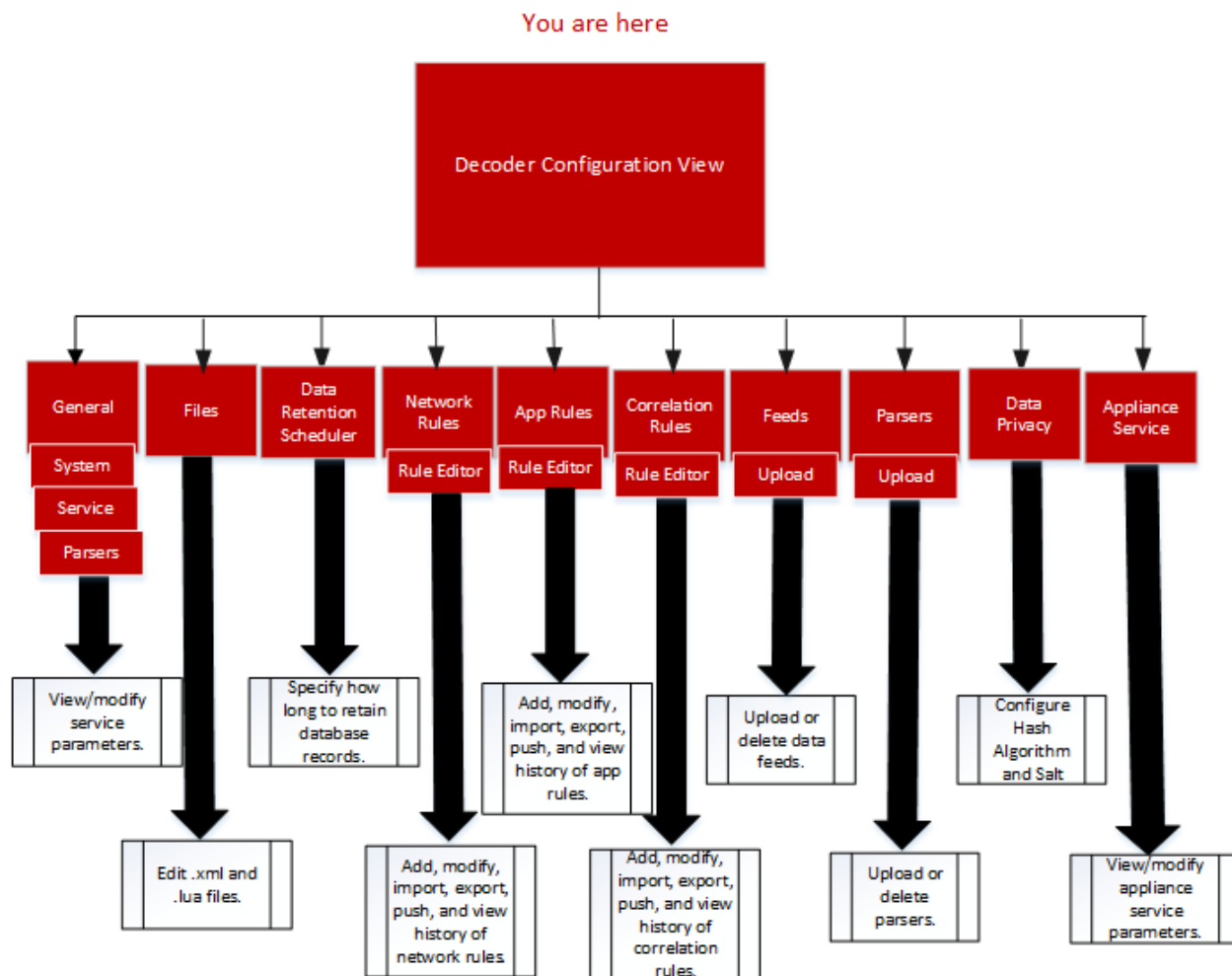
サービスの[構成]ビューは、[サービス]ビューの[アクション]()メニューから表示できるビューの一つです。このビューには、コア サービスまたはNetWitness Platformサービスの詳細な構成を管理するためのユーザ インタフェースがあります。

サービスの[構成]ビューにある構成オプションは、複数のタブに分類されており、各タブには関連するパラメータのセットが表示されています。これらのタブは、すべての構成ファイルへの直接的なアクセスを提供するサービスの[エクスプローラ]ビューとは異なり、サービス構成で最もよく変更されるパラメータを分かりやすいビューで表示しています。


このビューでは、デバイスやサービスのタイプごとに使用可能なタブや構成パラメータが提供されています。個別のトピックで、ホスト(BrokersとConcentrators、DecodersとLog Decoders)またはサービス(Reporting Engine、IPDB Extractor、Log Collector、Warehouse Connectorなど)に固有の構成パラメータについて説明しています。

ワークフロー

次のワークフローは、このビューの例として、Decoderサービスの構成タスクを示しています。[管理]>[サービス]>[構成]ビューの詳細については、各サービスの構成ガイド(『RSA NetWitness® Platform BrokerおよびConcentrator構成ガイド』など)を参照してください。

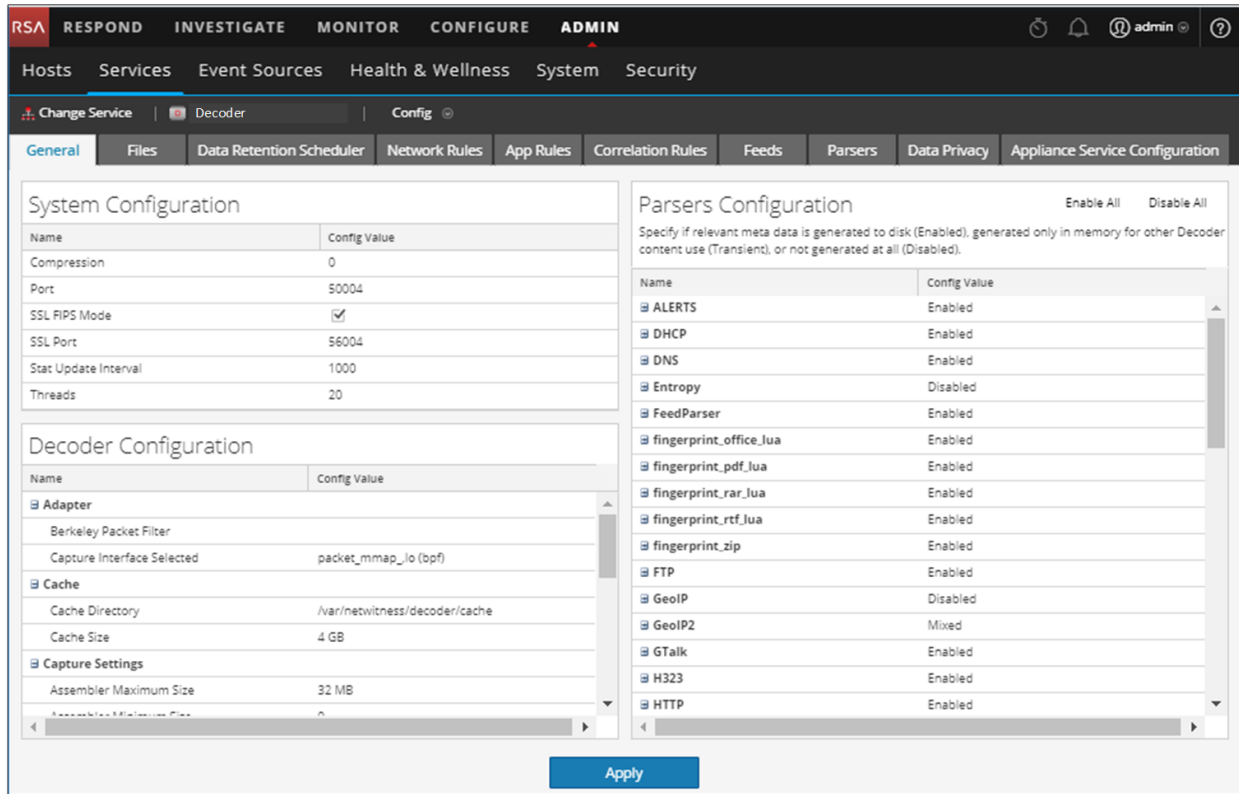


[サービス]の[構成]ビューにアクセスするには、次の手順を実行します。

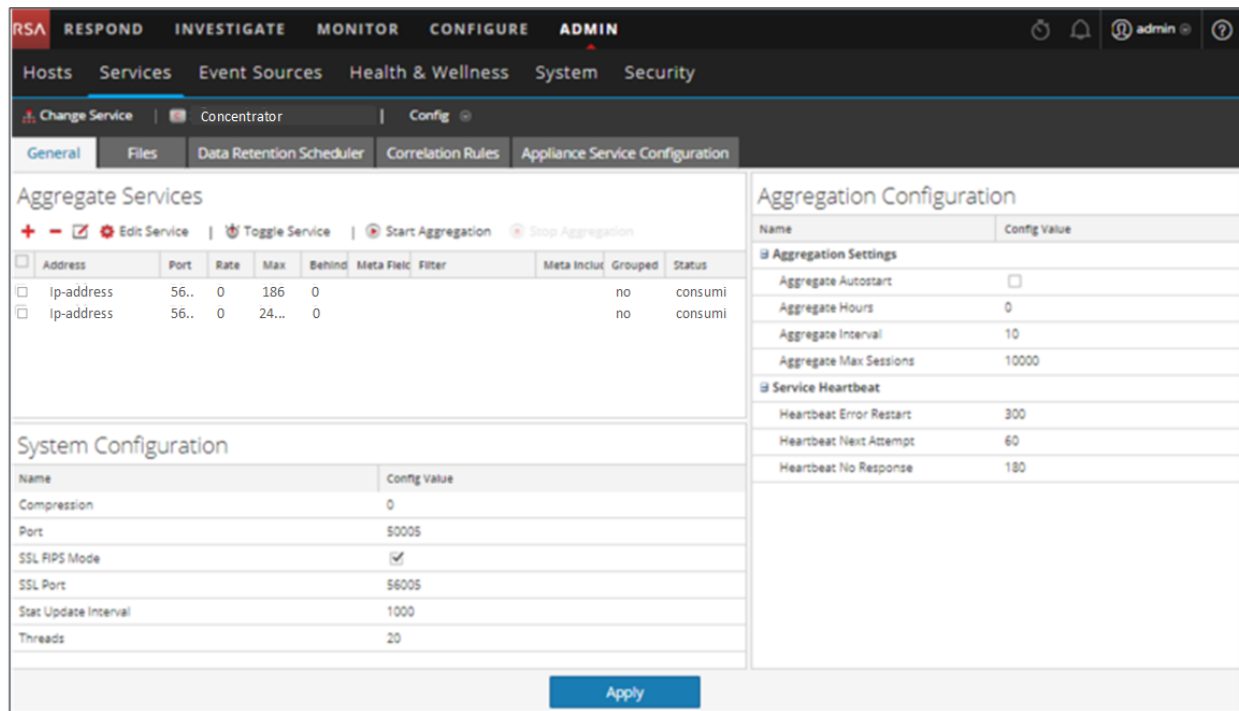
1. NetWitness Platformで、[管理]>[サービス]に移動します。
[管理]の[サービス]ビューが表示されます。
2. サービスを選択し、 >[表示]>[構成]を選択します。
選択したサービスの[構成]ビューが表示されます。

簡単な説明

これは、Decoderの[サービス]の[構成]ビューの例です。



これは、Concentratorの[サービス]の[構成]ビューの例です。



トピック


- [トピック](#)
- [機能](#)
- [サービス構成ファイルの編集](#)

[Applianceサービス構成]タブ

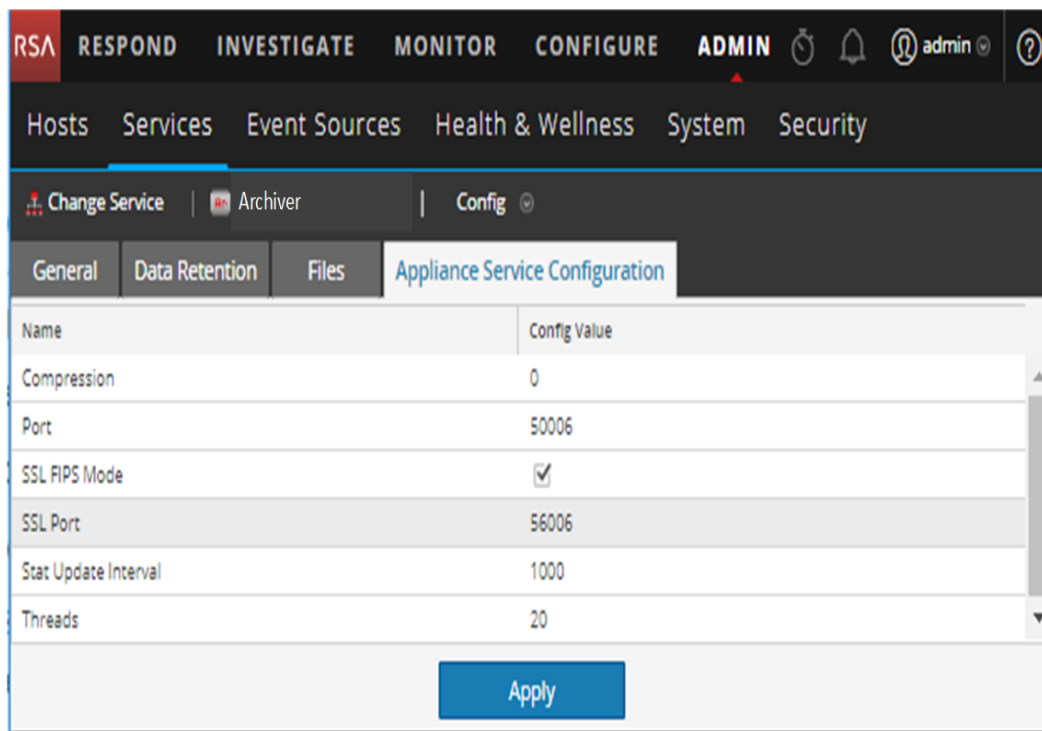
このトピックでは、NetWitness Platform Core Applianceサービスで利用可能な構成パラメータのリストと説明を示します。NetWitness Platform Core Applianceサービスは、レガシーNetWitnessハードウェアのハードウェア モニタリングを提供します。

Archiver、Broker、Concentrator、IPDB Extractor、Decoder、Log Collector、Log Decoderサービスの [構成]ビューには、[Applianceサービス構成]タブがあります。

[Applianceサービス構成]タブにアクセスするには、次の手順に従います。

1. NetWitness Platformで、[管理]>[サービス]に移動します。
[管理]の[サービス]ビューが表示されます。
2. サービスを選択し、 > [表示]> [構成]を選択します。
Archiverサービスの[構成]ビューが表示されます。
3. [Applianceサービス構成]タブをクリックします。

これは、Archiverの[Applianceサービス構成]タブの例です。



名前	構成値の説明	変更が有効になるタイミング
Compression	指定した正の数(バイト単位)に到達すると、メッセージが圧縮されます。	このサービスに次回接続するとき。
Port	暗号化されていないリスニングポート。0はポートが無効であることを示します。	サービスの再起動時。
SSL FIPS Mode	FIPS(連邦情報処理標準)を有効または無効にするために必要なパラメータの1つ。詳細な手順については、『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。	サービスの再起動時。
SSL Port	SSL(Secure Sockets Layer)のリスニングポート。0はポートが無効であることを示します。SSLは、Webサーバとブラウザの間に暗号化されたリンクを確立するための標準のセキュリティテクノロジーです。このリンクにより、Webサーバとブラウザ間で渡されるすべてのデータのプライバシーと整合性が維持されます。	サービスの再起動時。
統計情報の更新間隔	ヘルスマニタの監視用にシステムが統計ノードを更新する頻度(ミリ秒単位)。	即時。
Threads	リクエストを処理するために使用する必要があるスレッドプール内のスレッド数。[Threads]パラメータはイベントおよびログスレッドの[Polling Interval]パラメータと連携します。	即時。

トピック

Applianceサービス構成パラメータ

[データ保存スケジューラ]タブ


このトピックでは、Decoder、Log Decoder、Concentratorの[データ保存スケジューラ]タブで構成できるオプションについて説明します。

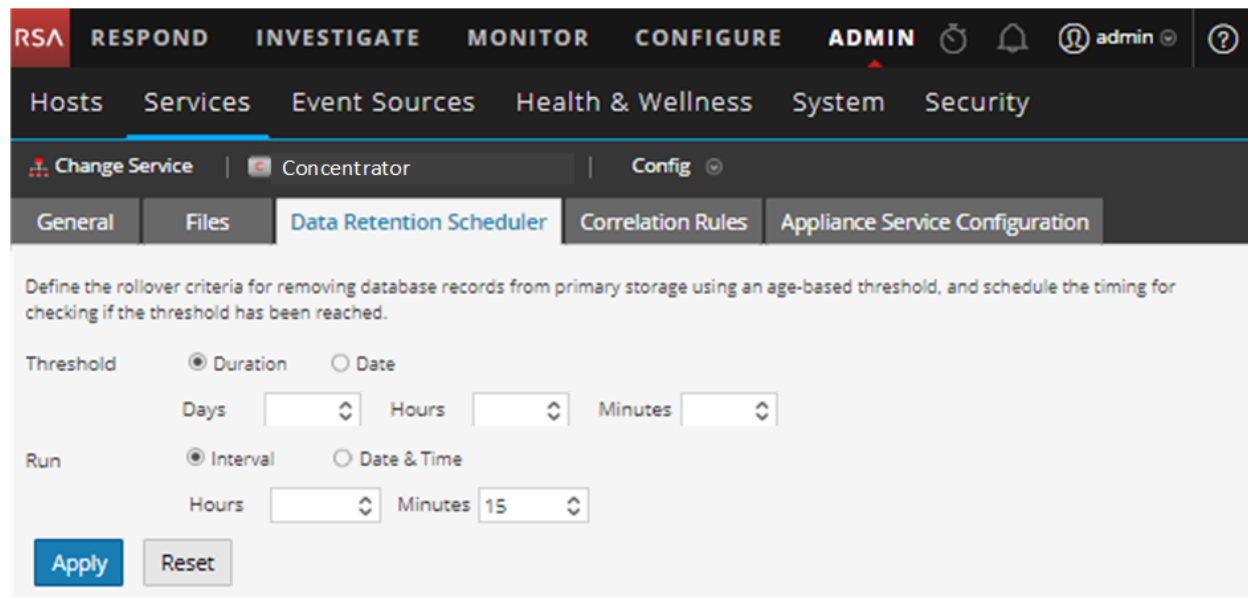
[データ保存スケジューラ]タブでは、Decoder、Log Decoder、Concentratorの各サービスに搭載されたプライマリストレージからデータベースレコードを削除するための条件を定義し、閾値をチェックするタイミングをスケジュールできます。

Archiverの[データ保存]タブの詳細については、「Archiver構成ガイド」の「[データ保存]タブ: Archiver」を参照してください。

注: 追加のカスタマイズが必要な場合は、[サービス]の[構成]ビューの[ファイル]タブにあるschedulerファイルを使用します。たとえば、メタデータよりもrawデータを保存するためのストレージ容量が大きい場合は、容量を閾値として使用し、データベース(メタとパケット)ごとに異なる閾値を設定した方が合理的なことがあります。

[データ保存スケジューラ]タブにアクセスするには、次の手順を実行します。

1. NetWitness Platformで、[管理]>[サービス]に移動します。
2. Decoder、Log Decoder、Concentratorのいずれかを選択し、 > [表示]>[構成]を選択します。
3. 選択したサービスの[サービス]の[構成]ビューで、[データ保存スケジューラ]タブをクリックします。次の図は、Concentratorの[データ保存スケジューラ]タブに表示されるパラメータを示しています。



機能

[データ保存スケジューラ]タブには、閾値と実行を設定するセクションがあります。次の表に、データ保存構成のパラメータを示します。

パラメータ	説明
閾値	<p>閾値は、データの経過時間を、データが格納されている期間またはデータの格納日によって指定します。日付は、実際のセッション時間からではなく、データベースファイルから取得されます。</p> <ul style="list-style-type: none"> • 期間 : データが削除されるまで格納しておくことのできる期間。データのタイムスタンプから経過した日数(最大値は365)、時間数(最大値は24)、分数(最大値は60)を指定します。 • 日付 : データの削除をタイムスタンプの日付に基づいて行います。[カレンダー]フィールドと[時刻]フィールドに、毎月の日時を指定します。

パラメータ	説明
実行	<p>ロールオーバー条件をチェックするジョブの実行スケジュール。</p> <ul style="list-style-type: none"> • 間隔: データベースチェックを定期的な間隔で行うようスケジュールします。定期チェックの間隔を時間数と分数で指定します。 • 日付と時刻: 決まった日と時刻にデータベースチェックを行うようスケジュールします。ドロップダウンリストから日を指定し、システム時刻をhh:mm:ss形式で指定します。日には[毎日]、[平日]、[週末]、[カスタム]を指定できます。[カスタム]を指定した場合は、特定の曜日を選択できます。
適用	<p>このサービスの以前のスケジュールを上書きして、新しい設定をただちに適用します。</p> <div style="border: 1px solid yellow; padding: 5px;"> <p>注意: これらの設定を適用した後、閾値が満たされると、システムは古いデータをデータベースから削除し、アクセスできなくなります。</p> </div>
リセット	<p>スケジュールを前回適用された状態にリセットします。</p>

[ファイル]タブ

このトピックでは、[サービス]の[構成]ビュー> [ファイル]タブに表示される、サービス構成ファイルについて説明します。

[サービス]の[構成]ビューにある[ファイル]タブを使用し、サービス構成ファイル(Decoder、Log Decoder、Broker、Archiver、Concentratorの各サービス用)をテキストファイルとして編集します。

編集可能なファイルは、構成するサービスのタイプによって異なります。次のファイルはすべてのコアサービスに共通です。

- サービス インデックス ファイル
- netwitnessファイル
- crash reporterファイル
- schedulerファイル
- Feed定義ファイル

さらに、Decoderには、Parser、Feed定義、Wireless LANアダプタを構成するためのファイルがあります。

注: 構成ファイルのデフォルト値は、最も一般的な状況をカバーしています。crash reporterやschedulerなどのオプション サービスでは構成パラメータの編集が必要になります。ネットワークと、サービスのデータ収集および解析に影響する要因について理解していない限り、[ファイル]タブでこれらの値を変更しないでください。

サービス構成パラメータの詳細については、「[サービス構成設定](#)」を参照してください。

[ファイル]タブにアクセスするには、次の手順を実行します。

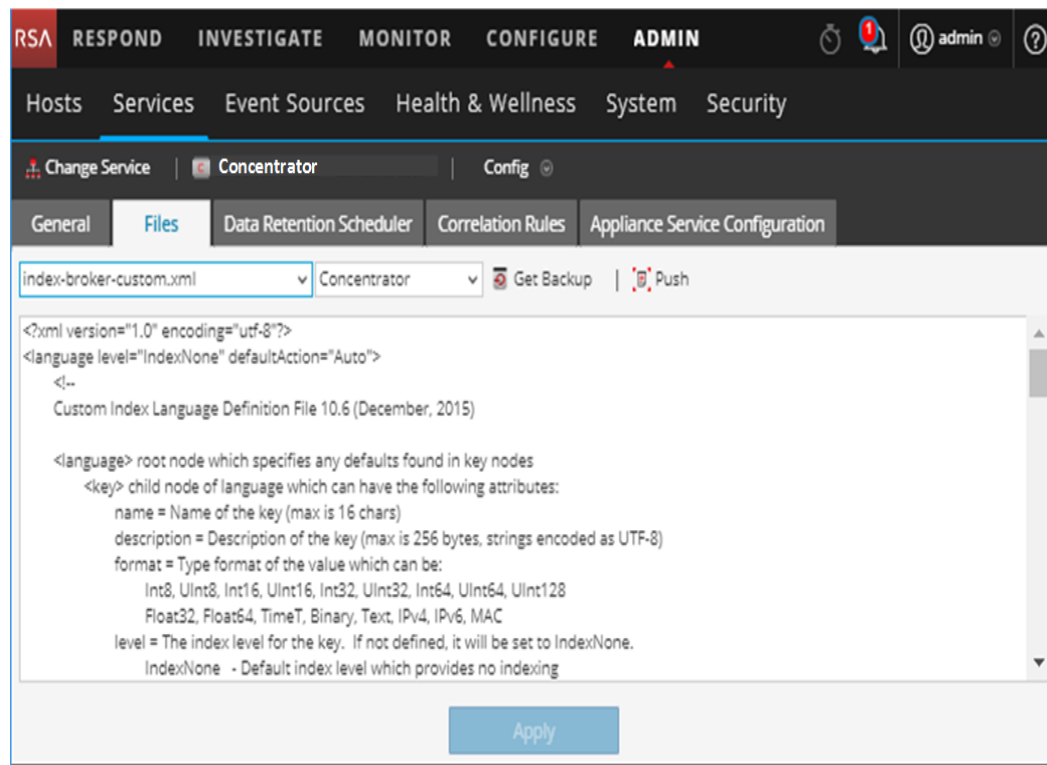
1. NetWitness Platformで、[管理]> [サービス]に移動します。
2. サービスを選択し、 > [表示]> [構成]の順に選択します。

[サービス]の[構成]ビューが表示され、[全般]タブが開きます。

3. [ファイル]タブをクリックします。

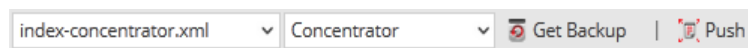
サービス構成ファイルの編集

これは、[ファイル]タブの例です。





[ファイル]タブ ツールバー

[ファイル]タブには、ツールバーと編集 ウィンドウがあります。これは、ツールバーの例です。



[ファイル]タブ ツールバーの機能は次のとおりです。

機能	説明
[ファイル]ドロップダウンリスト	システムが現在使用しているファイルのリストを表示します。ファイルを選択すると、ファイルのコンテンツがテキスト編集ウィンドウに表示されます。テキスト ウィンドウで、ファイルを編集して変更を保存するか、代替のファイルを作成できます。
[サービス/ホスト]ドロップダウン リスト	サービス タイプまたはホストを表示します。選択したサービスまたはホストの構成ファイルを開いて編集できます。

機能	説明
 Get Backup	現在のファイルを最新のバックアップからリストアします。これは、ファイルに変更を加えたものの、以前のバージョンに戻りたい場合に便利です。[保存]をクリックするまではリストアした内容は保存されません。
 Push	同じタイプのサービスを選択して、現在表示しているファイルをサービスにプッシュできるダイアログを表示します。
適用	現在のファイルを上書きし、バックアップ ファイルを作成します。

サービスの[エクスプローラ]ビュー

NetWitness Platformサービスの[エクスプローラ]ビューでは、ホストとサービスの構成を表示および編集できます。

[サービス]の[エクスプローラ]ビューでは、すべてのNetWitness Platformホストとサービスにアクセスし、制御を行うことができます。[エクスプローラ]ビューは、Windowsエクスプローラのインターフェイスに似ており、ノードとツリーの構造で表示されます。このパネルでは、以下の機能を実行できます。

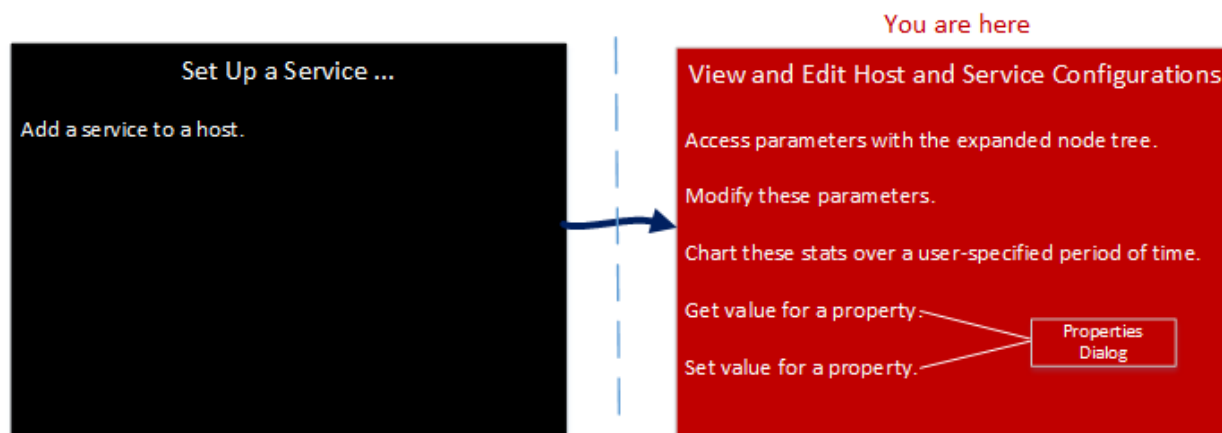
- 選択されたサービスのすべての構成ファイルのディレクトリツリーを表示(複数のサービスを選択した場合、すべてのサービスに共通する構成ファイルを表示)します。
- ディレクトリを移動し、ファイルにアクセスします。
- 複数のサービスに共通するファイルを開き、内容を横に並べて表示します。
- ファイルのエントリを選択し、値を編集します。
- あるサービスから別のサービスにプロパティ値をコピーします。

[サービス]の[エクスプローラ]ビューは、[プロパティ]ダイアログを表示することもできます。これは、次の図に示すように、各ノードのプロパティの表示や各ノードへのメッセージの送信を行えるシンプルなインターフェイスです。

注意: このビューで編集を行う場合には、各ノードとパラメータに関する十分な知識が必要です。不適切な設定が原因で、パフォーマンス上の問題が発生する場合があります。


ワークフロー

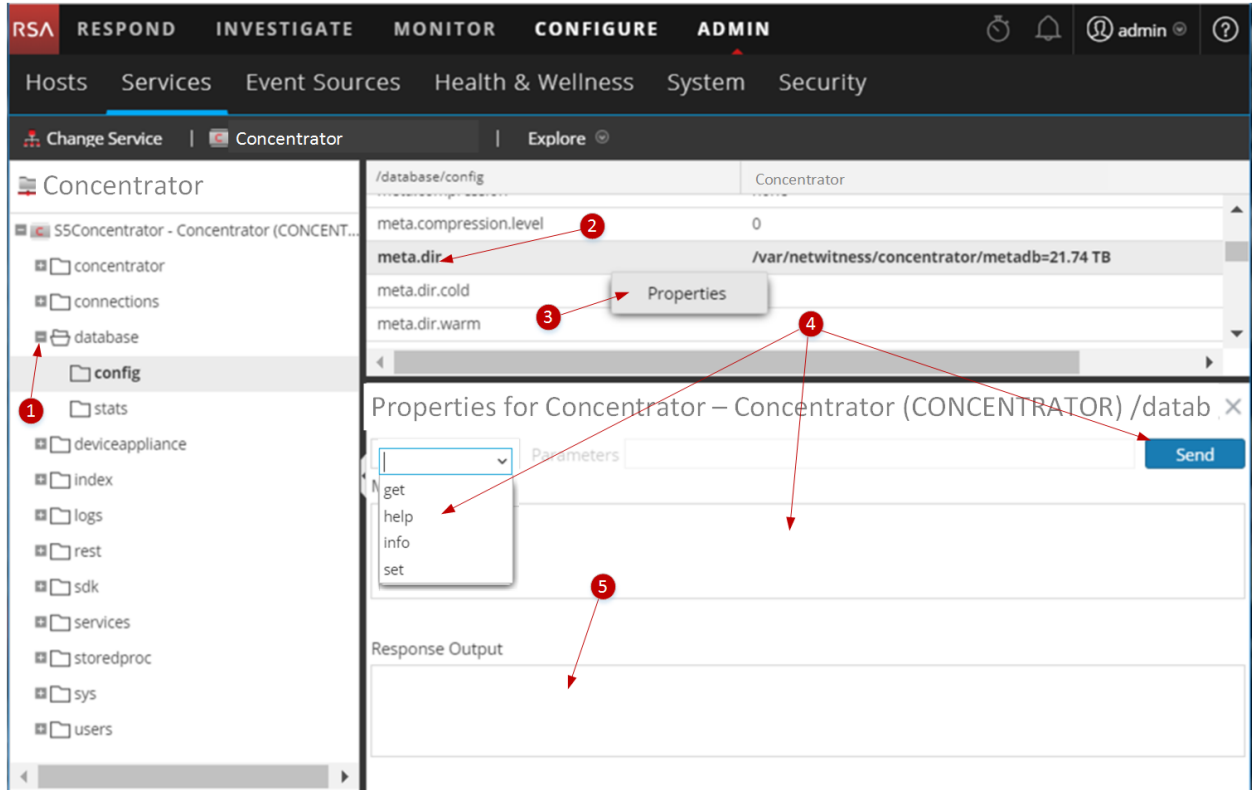
このワークフローは、[エクスプローラ]ビューから実行するタスクを示します。



簡単な説明

[サービス]の[エクスプローラ]ビューにアクセスするには、次の手順を実行します。

1. NetWitness Platformで、[管理]>[サービス]に移動します。
2. サービスを選択し、 > [表示]> [エクスプローラ]を選択します。



- 1 ノードを展開して、パラメータのカテゴリを表示します。
- 2 プロパティ(たとえば、`meta.dir`)をクリックして選択します。
- 3 ノードまたはカテゴリを右クリックして[プロパティ]をクリックし、[プロパティ]ダイアログを表示します。
- 4 ノードまたはカテゴリに対する操作を実行します。
 - a. ドロップダウン リストからコマンドを選択します。
 - b. (必要な場合)パラメータを入力します。
 - c. [送信]をクリックします。
- 5 出力を確認します。

機能

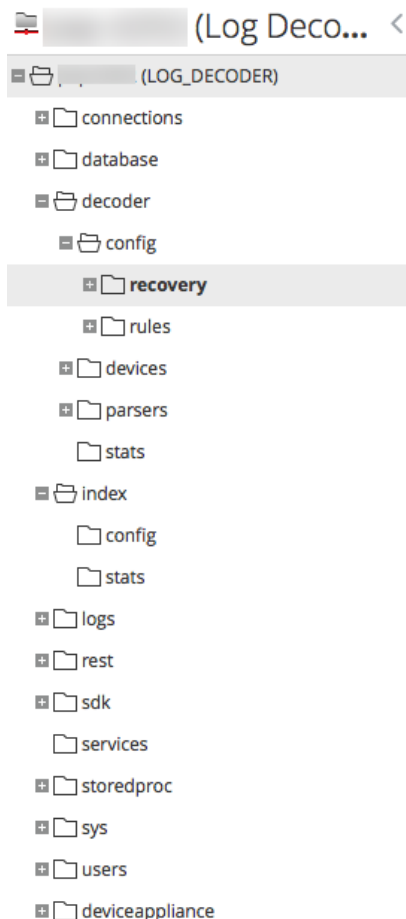
[サービス]の[エクスプローラ]ビューには、2つのメイン パネルがあります。

- ノード リスト
- [監視]パネル

ファイルを右クリックし、[プロパティ]を選択してアクセスします。

ノード リスト

ノード リストは、ノードとフォルダの一連のツリー構造で各サービスを表示します。ノード リストのレベルを展開したり、折りたたんで、完全な階層を表示できます。



各ルート フォルダは、その機能に基づいて名前が付けられています。たとえば、/connectionsフォルダは、接続されているすべてのIPアドレスを表示します。各IP:Portの下には、sessionsとstatsの2つのフォルダがあります。

- sessionsフォルダでは、各IP:Portからのすべての認証済みユーザセッションが表示されます。
- statsフォルダは、送受信したメッセージ数、送受信したバイト数など、各サービスごとの特定の値を表示します。これらは編集できません。

ツリービューでフォルダを選択すると、[監視]パネルにフォルダの内容が表示されます。ツリーの各ノードは常に監視されているため、statsノードまたはconfigノードの値が変更されたときは、すぐにツリーと監視パネルに反映されます。

[監視]パネル

[監視]パネルは、選択されたノード(たとえば、index)のプロパティと値およびサブフォルダ(たとえば、config)を表示します。値を編集する方法は2つあります。

- 値をクリックして新しい値を入力します。
- [プロパティ]ダイアログでsetメッセージを送信します

/Index/Config	(Concentrator)
index.dir	/var/netwitness/concentrator/index=7.08 GB
index.dir.cold	
index.dir.warm	
page.compression	huffhybrid
save.session.count	0

トピック

- [機能](#)
- [Log Decoderサービスの構成パラメータ](#)

[プロパティ]ダイアログ

[サービス]の[エクスプローラ]>[プロパティ]ダイアログを使用して、次のタスクを実行します。

- システム ノード へのメッセージの送信
- 複数のサービスのプロパティ値の取得
- 複数のサービスのプロパティ値の設定


[プロパティ]ダイアログは、コンテキスト メニューからプロパティを選択すると、[監視]パネルの下に開きます。

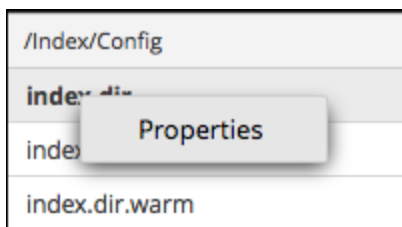
すべてのノードは、次の情報を含むヘルプを提供します。

- ノードの説明
- サポートされているメッセージと対応する説明のリスト
- メッセージへのアクセスに必要なセキュリティ ロール。

使用できるメッセージは、サービスやフォルダによって異なります。メッセージの多くは、NetWitness Platformのダッシュボードやビューを介して利用できる機能です。

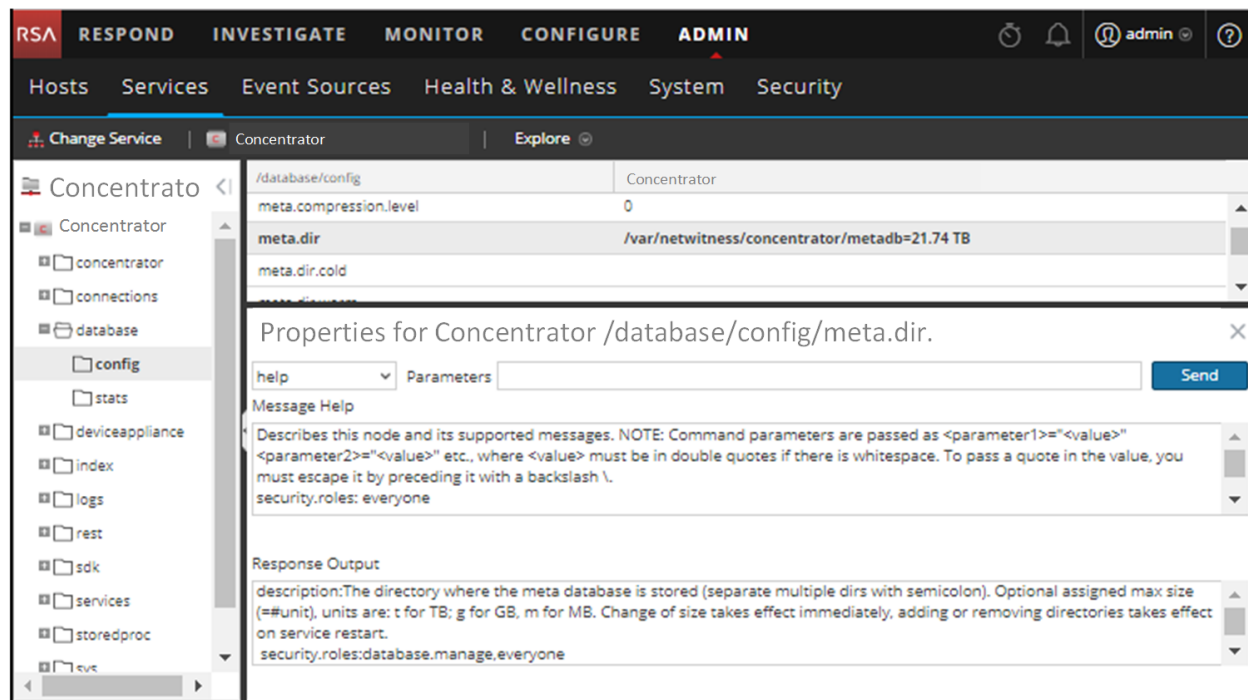
[プロパティ]ダイアログにアクセスするには、次の手順に従います。

1. NetWitness Platformで、[管理]>[サービス]に移動します。
2. サービスを選択し、>[表示]>[エクスプローラ]を選択します。
3. [ノード]リストで、ファイルを選択します。
4. [監視]パネルで、プロパティを右クリックし、[プロパティ]を選択します。



[プロパティ] ダイアログが表示されます。[ノード] リストで任意のファイルを右クリックして、[プロパティ] ダイアログを表示することもできます。

次の例は、メッセージ(help) のヘルプが表示された[プロパティ] ダイアログを示しています。



機能

[プロパティ] ダイアログには次の機能があります。

機能	説明
[メッセージ] ドロップダウン リスト	現在のノードで使用可能なすべてのメッセージをリストしています。ノードに送信するメッセージを選択します。
[パラメータ] 入力フィールド	このフィールドにメッセージのパラメータを入力します。
[送信] ボタン	ノードにメッセージを送信します。
メッセージのヘルプ	現在のメッセージのヘルプ テキストを表示します。
応答出力	メッセージのレスポンスまたはメッセージからの出力を表示します。

[サービス]の[ログ]ビュー


このピックでは、[サービス]の[ログ]ビューについて紹介します。

[サービス]の[ログ]ビューでは、特定のサービスのログを表示して検索することができます。[サービス]の[ログ]ビューは、次の2つの点を除いて[システム]の[システム ログ]パネルと同一です。

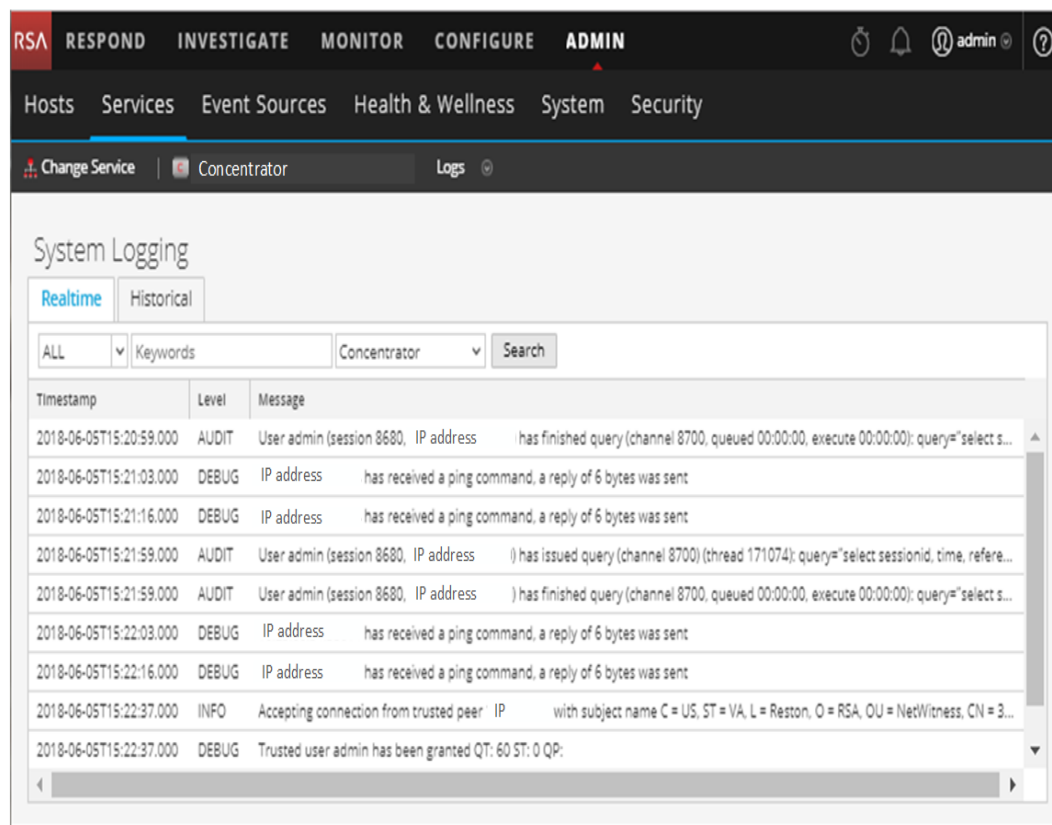
- [サービス]の[ログ]ビューには、サービスまたはホストのメッセージを選択するための追加のフィルタがあります。
- [システム]の[システム ログ]パネルには、ログの設定を行うための追加のタブがあります。

NetWitness Platformのログ機能の詳細については、[管理] > [システム] > [システム ログ]パネルを参照してください。

サービス ログを表示するには、次の手順を実行します。

1. NetWitness Platformで、[管理] > [サービス]に移動します。
2. サービスを選択し、 > [ビュー] > [ログ]を選択します。

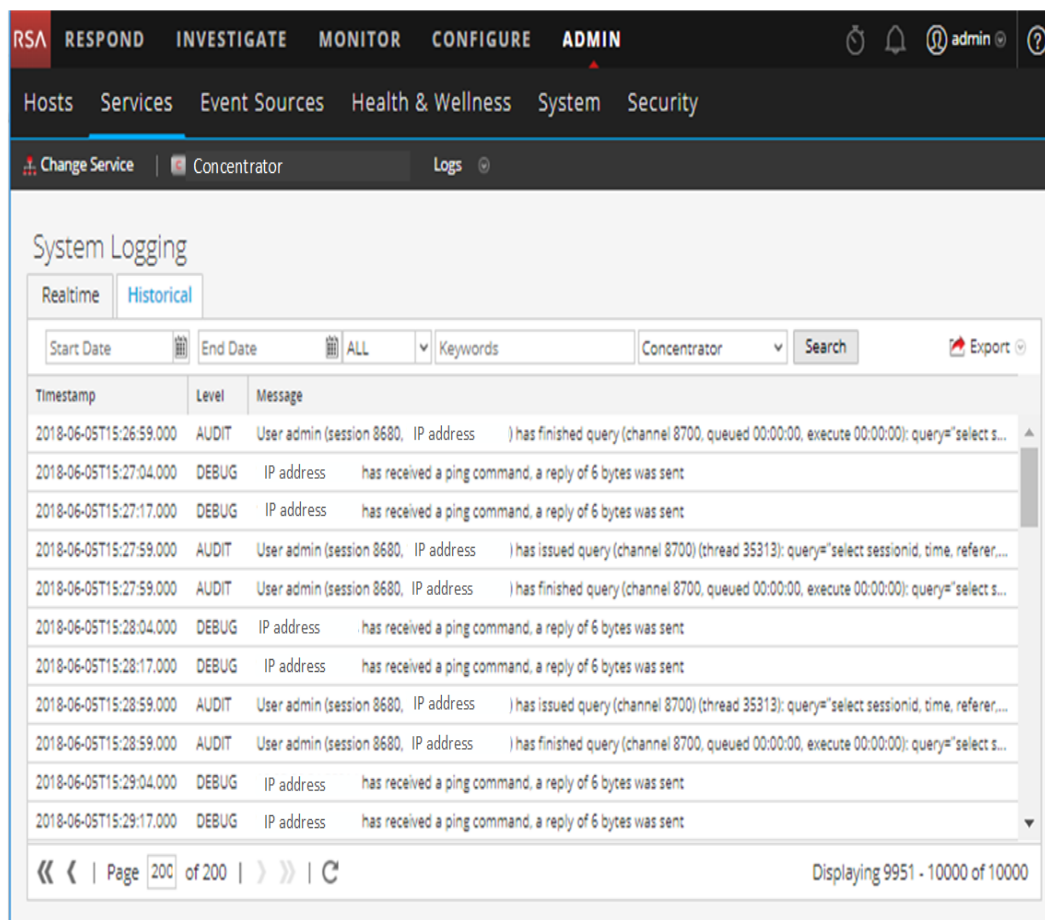
次の図に、[サービス]の[ログ]ビューの[リアルタイム]タブを示します。



The screenshot shows the 'System Logging' interface in NetWitness Platform. The 'Realtime' tab is active, and the log entries are as follows:

Timestamp	Level	Message
2018-06-05T15:20:59.000	AUDIT	User admin (session 8680, IP address) has finished query (channel 8700, queued 00:00:00, execute 00:00:00): query="select s...
2018-06-05T15:21:03.000	DEBUG	IP address has received a ping command, a reply of 6 bytes was sent
2018-06-05T15:21:16.000	DEBUG	IP address has received a ping command, a reply of 6 bytes was sent
2018-06-05T15:21:59.000	AUDIT	User admin (session 8680, IP address) has issued query (channel 8700) (thread 171074): query="select sessionid, time, refere...
2018-06-05T15:21:59.000	AUDIT	User admin (session 8680, IP address) has finished query (channel 8700, queued 00:00:00, execute 00:00:00): query="select s...
2018-06-05T15:22:03.000	DEBUG	IP address has received a ping command, a reply of 6 bytes was sent
2018-06-05T15:22:16.000	DEBUG	IP address has received a ping command, a reply of 6 bytes was sent
2018-06-05T15:22:37.000	INFO	Accepting connection from trusted peer: IP with subject name C = US, ST = VA, L = Reston, O = RSA, OU = NetWitness, CN = 3...
2018-06-05T15:22:37.000	DEBUG	Trusted user admin has been granted QT: 60 ST: 0 QP:

次の図に、[サービス]の[ログ]ビューの[履歴]タブを示します。



機能

[システム ログ] パネルには次のタブがあります。ログ機能については、システムメンテナンスの一環として説明しています(『システムメンテナンスガイド』の「NetWitness Platformのヘルスマニタの監視」を参照)。

機能	説明
[リアルタイム]タブ	このタブでは、サービスのリアルタイムのログを表示します。
[履歴]タブ	サービスの履歴ログの検索可能なビューです。

[サービス]の[セキュリティ]ビュー

このトピックでは、[サービス]の[セキュリティ]ビューで実行するサービスのセキュリティ管理の概要について説明します。

NetWitness Platformでは、サービスごとにユーザ、ロール、ロールの権限の構成があり、[サービス]の[セキュリティ]ビューで管理されます。


NetWitness Platformでサービス情報にアクセスし、サービスに関する操作を実行するには、ユーザはそのサービスに対する権限が付与されたロールに属している必要があります。信頼接続を使用する10.4以降のNetWitness Platform Coreサービスの場合、WebクライアントからログオンするユーザのためにNetWitness Platform Coreユーザアカウントを作成する必要がなくなりました。NetWitness Platform Coreユーザアカウントを作成する必要があるのは、集計、シッククライアント、REST APIを使用する場合です。

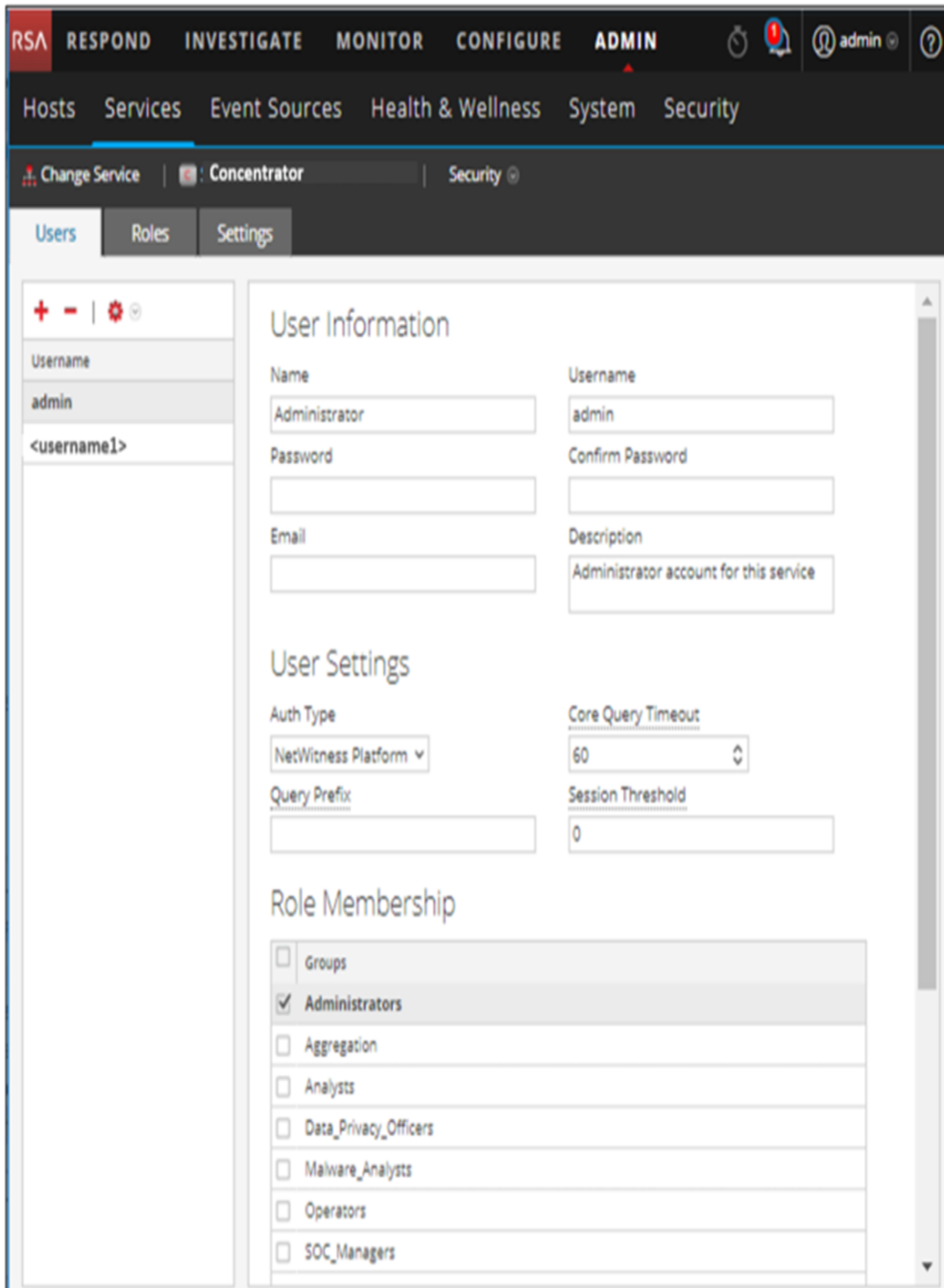
注: デフォルトでは、すべてのサービスにNetWitness Platformのデフォルトのadminユーザのみが作成されています。サービスのセキュリティを管理する前提条件として、NetWitness Platformの[管理]>[サービス]ビューにデフォルトのadminユーザアカウントが存在している必要があります。その他のユーザについては、NetWitness Platformから特定のサービスごとにアクセスを構成する必要があります。

このタブに関連する手順については、「[ホストとサービスの手順](#)」で説明します。

[サービス]の[セキュリティ]ビューにアクセスするには、次の手順を実行します。

1. NetWitness Platformで、[管理]>[サービス]に移動します。

2. サービスを選択し、 > [表示] > [セキュリティ]を選択します。
選択したサービスの[セキュリティ]ビューが表示されます。



機能

[サービス]の[セキュリティ]ビューには、[ユーザ]タブ、[ロール]タブ、[設定]タブの3つのタブがあります。

ロールとサービスへのアクセス

サービスのセキュリティ構成における重要な考慮事項は、ロールの定義とロールへのユーザの割り当てです。[サービス]の[セキュリティ]ビューは、これら2つの機能を[ユーザ]タブと[ロール]タブに分けています。

- [ロール]タブでは、ロールを作成し、選択したサービスのロールに権限を割り当てることができます。
- [ユーザ]タブでは、選択したサービスのユーザの追加、ユーザ設定の編集、ユーザパスワードの変更、ユーザのロールメンバシップの編集を行うことができます。[サービス]の[セキュリティ]ビューでは単一のサービスを選択しますが、あるサービスの設定を他のサービスにも適用できます。

トピック

- [\[ロール\]タブ](#)
- [サービス ユーザ ロールと権限](#)
- [Aggregationロール](#)
- [\[設定\]タブ](#)
- [\[ユーザ\]タブ](#)

[ロール]タブ


このトピックでは、サービスの[セキュリティ]ビュー> [ロール]タブの機能について説明します。

[ロール]タブでは、ロールを作成して権限を割り当てることができます。各ロールは、サービスごとにそれぞれ異なる権限を持つことができます。たとえば、Analystsロールは、定義されたサービスごと、異なる権限を持つことができます。

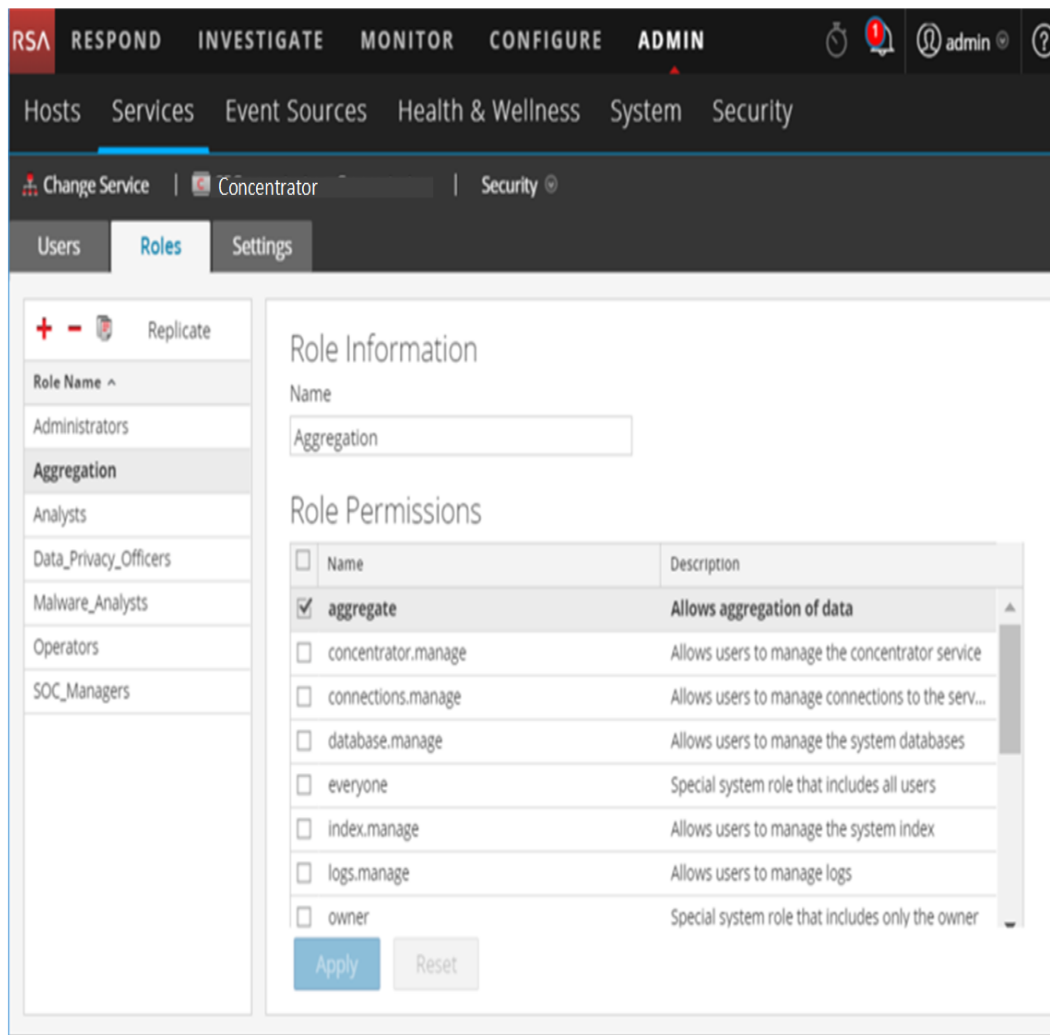
ユーザをロールに追加する場合、通常は機能別のロールを定義して権限を割り当てておく必要があります。

このタブに関連する手順については、「[ホストとサービスの手順](#)」で説明します。

サービスの[セキュリティ]ビュー> [ロール]タブを表示するには、次の手順を実行します。

1. NetWitness Platformで、[管理]> [サービス]に移動します。
2. ロールを追加するサービスを選択し、 > [表示]> [セキュリティ]を選択します。
3. [ロール]タブを選択します。

次の図は、サービスの[セキュリティ]ビューの[ロール]タブを示しています。






機能

[ロール] タブには、左側に[ロール名]パネルがあります。ロール名を選択すると、右側にそのロールの[ロール情報]パネルが表示されます。

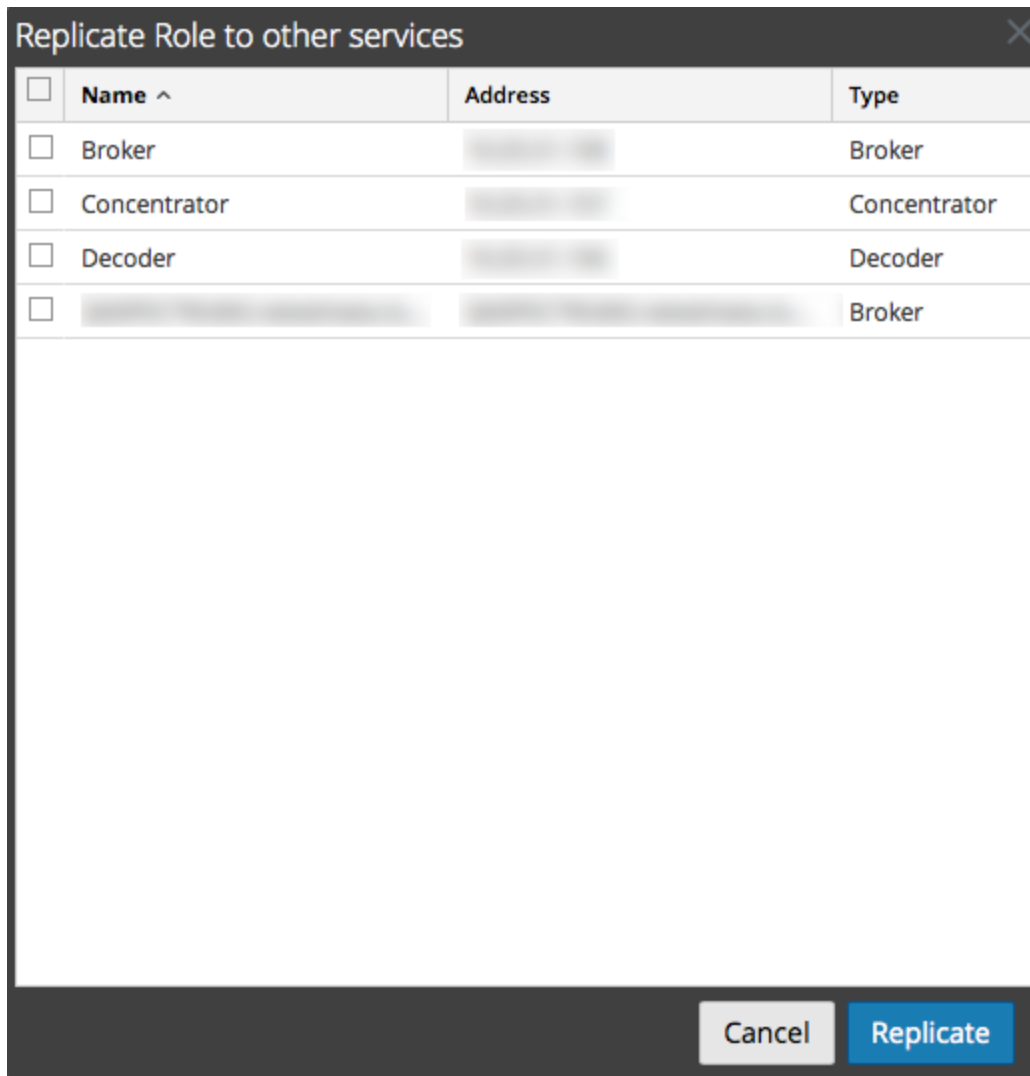
[ロール名]パネル

[ロール名]パネルには次の機能があります。

機能	説明
	現在のサービスに新しいロールを追加します。
	現在のサービスから選択したロールを削除します。

機能	説明
	ロールと割り当てられた権限を新しいロールにコピーします。新しいロールの名前は一意である必要があります。たとえば、Analystsロールをコピーし、Analyst_Managersなどの新しい名前で作成できます。
レプリケート	ロールと割り当てられた権限を別のサービスにプッシュします。ロールを選択して[レプリケート]をクリックすると、[他のサービスへのロールのレプリケート]ダイアログが表示されます。このダイアログでは、ロールをレプリケートするサービスを選択できます。

次の図は、[他のサービスへのロールのレプリケート]ダイアログを示しています。



[ロールの情報と権限]パネル

[ロールの情報と権限]パネルではロールの権限を定義します。

ボタンが2つあります。

- [適用] ボタンは、[ロールの権限] パネルでの変更を保存し、変更はすぐに有効になります。
- [リセット] ボタンは、[ロールの権限] パネルで変更を保存していない場合、すべてのフィールドと設定を編集前の値にリセットします。

サービス ユーザ ロールと権限

このピックでは、事前構成されたサービス ユーザ ロールと権限について説明します。

[サービス] の[セキュリティ] ビューの[ロール] タブでは、サービス ユーザ ロールを作成し、権限を割り当てることができます。NetWitness Platformに含まれる事前構成されたロールを使用して、ユーザ権限を割り当てることもできます。

サービス ユーザ ロール

NetWitness Platformには、以下の事前構成されたサービス ユーザ ロールがあります。

ロール	割り当てられた権限	担当者/アカウント
Administrators	すべての権限	NetWitness Platformシステム管理者
Aggregation	aggregate sdk.content sdk.meta sdk.packets	このロールを使用して、Aggregationアカウントを作成できます。 このロールは、データの集計を実行するために必要な最低限の権限を提供します。NetWitness Platform 10.5以降のサービスでのみ利用可能です。
Analysts、 Malware_ Analysts、SOC_ Managers	sdk.meta sdk.content sdk.packets storedproc.execute	ユーザは、分析を目的として、特定のアプリケーションを使用し、クエリを実行し、コンテンツを表示することができます。
Data_Privacy_ Officers	sys.manage users.manage sdk.meta sdk.content sdk.packets sdk.manage logs.manage database.manage index.manage dpo.manage	データ プライバシー責任者 データ プライバシー責任者はDecoderとLog Decoderでdpo.manage権限を持ちます。

ロール	割り当てられた権限	担当者/アカウント
Operators	sys.manage services.manage connections.manage users.manage logs.manage parsers.manage rules.manage database.manage index.manage sdk.manage decoder.manage archiver.manage concentrator.manage storedproc.manage	オペレーターはサービスの日々の運用に対して責任を負います。

サービス ユーザ権限

NetWitness Platformには、サービス ロールに割り当てることができる権限が多数あります。ユーザは、自分に割り当てられたロールと、各ロールに割り当てられた権限に応じて、各サービスに対する異なる権限を持つことができます。次の表は、ロールに割り当てることができる権限について説明しています。

権限	定義
sys.manage	ユーザがサービス構成設定を編集することを許可します。
services.manage	ユーザが他のサービスへの接続を管理することを許可します。
connections.manage	ユーザがサービスへの接続を管理することを許可します。
users.manage	ユーザが個々のユーザとユーザ ロールを作成し、ユーザ権限を指定することを許可します。
aggregate	ユーザがデータの集計を実行することを許可します。
sdk.meta	ユーザがInvestigationおよびReportingアプリケーションでクエリを実行し、クエリが返したメタデータを表示することを許可します。
sdk.content	ユーザがいずれかのアプリケーション(Investigation、Reporting) からraw/パケットとログにアクセスすることを許可します。
sdk.packets	ユーザがいずれかのアプリケーションからraw/パケットとログにアクセスすることを許可します。
appliance.manage	ユーザがアプライアンス(ホスト) タスクを管理することを許可します。この権限はApplianceサービスで必要です。
decoder. manage	ユーザがDecoderサービスの構成設定を編集することを許可します。

権限	定義
concentrator.manage	ユーザがConcentrator/Brokerサービスの構成設定を編集することを許可します。
logs.manage	ユーザがサービスのログを表示し、特定のサービスのログ構成設定を編集することを許可します。
parsers.manage	ユーザがparsersノードですべての属性を管理することを許可します。
rules.manage	ユーザがすべてのルールを追加および削除することを許可します。
database.manage	ユーザがセッション、メタ、パケット/ログ データベースの場所、サイズ、データベースに関するその他のさまざまな構成を設定することを許可します。
index.manage	ユーザがすべてのインデックス関連属性を管理することを許可します。
sdk.manage	ユーザがすべてのSDK構成項目を表示および設定することを許可します。
storedproc.execute	ユーザがLuaのストアド プロシージャを実行することを許可します。
storedproc.manage	ユーザがLuaのストアド プロシージャを管理することを許可します。
archiver.manage	ユーザがArchiver構成を変更することを許可します。
dpo.manage	ユーザが変換構成と適用可能なキーを管理することを許可します。

Aggregationロール

このトピックではAggregationロールと、サービス ユーザが集計を実行するための権限について説明します。

Aggregationロールはサービス ユーザのロールであり、データの集計のみを意図しています。Aggregationロールは、集計を行うために最小限必要な次の権限を持つロールです。

- aggregate
- sdk.meta
- sdk.packets
- sdk.content

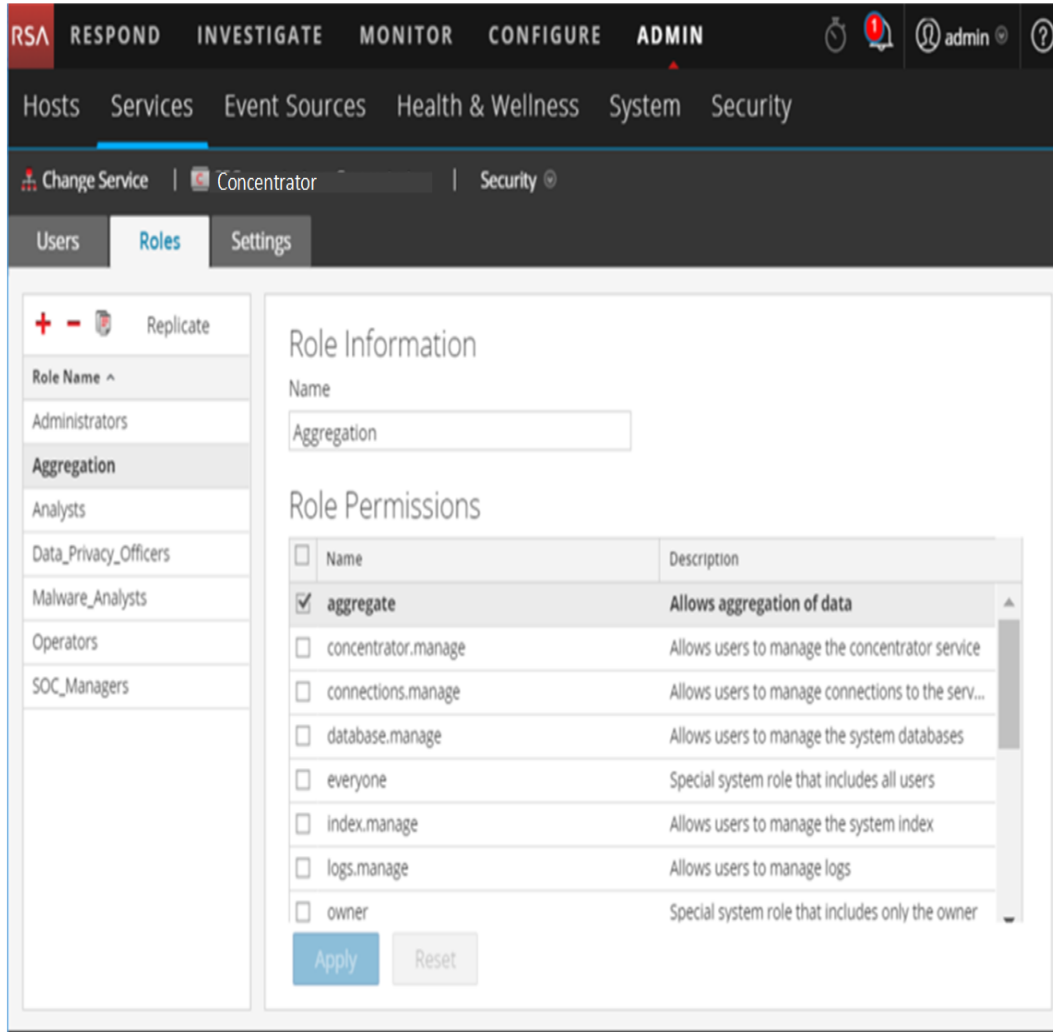
AggregationロールはNetWitness Platform 10.5以降のサービスのみで利用でき、集計アカウントに割り当てることができます。このロールのメンバまたはこれらの権限を持つサービス ユーザは、Decoders、Concentrators、Archivers、Brokersで集計を実行できます。aggregate権限を持つサービス ユーザは、セッションやメタデータの集計、およびRAWパケットやログの集計を実行できます。

引き続きdecoder.manage、concentrator.manage、archiver.manage権限を使用することも可能ですが、Aggregationロールの権限では集計のみが可能であり、その他の操作は禁止されています。

サービス ロールには、[管理] > [サービス] (サービスを1つ選択) > [アクション] > [表示] > [セキュリティ] > [ロール] タブからアクセスできます。

ロールに関連した手順については、「[ホストとサービスの手順](#)」で説明しています。「[サービス ユーザロールと権限](#)」では、事前構成されたロールの詳細な情報を説明しています。

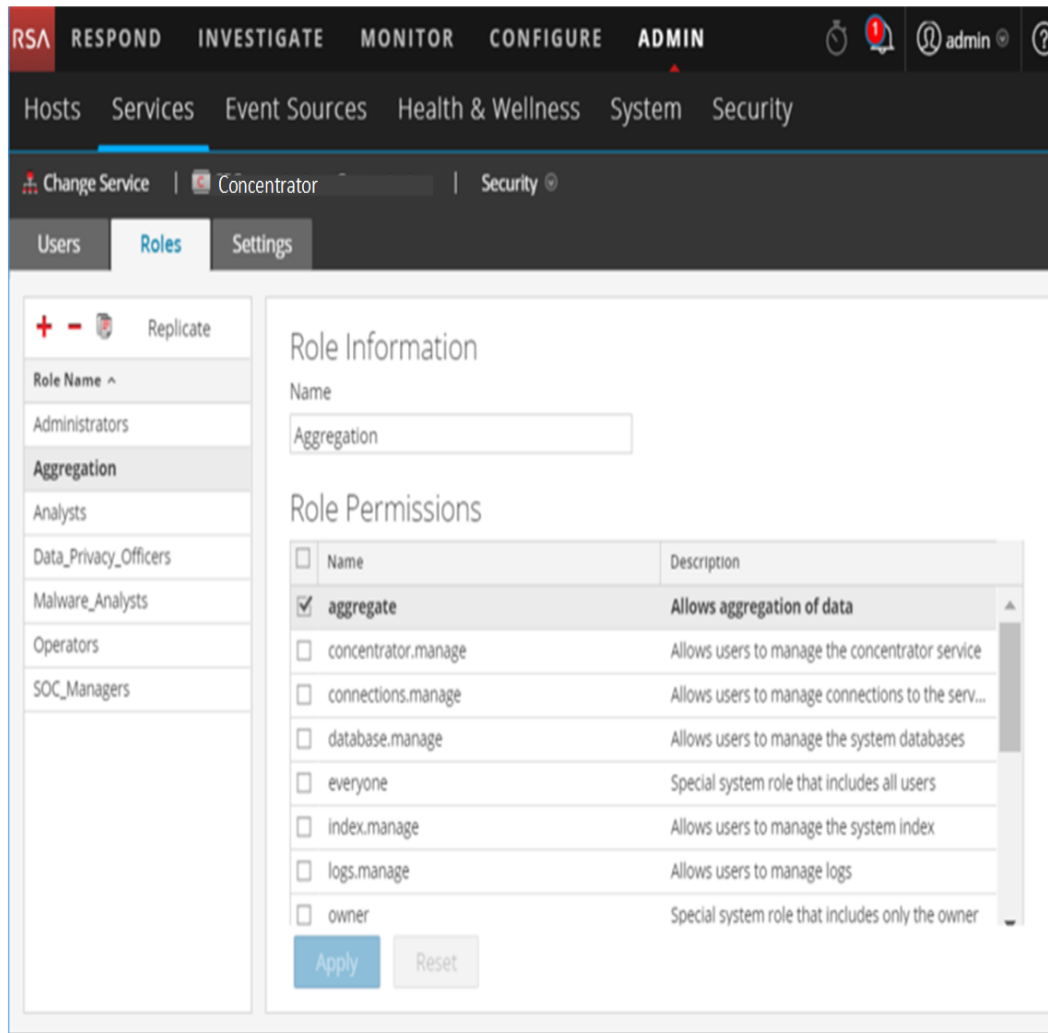
次の図は、Aggregationロールの権限を示しています。



[設定]タブ


このピックでは、[サービス]の[セキュリティ]ビュー> [設定]タブの機能について説明します。

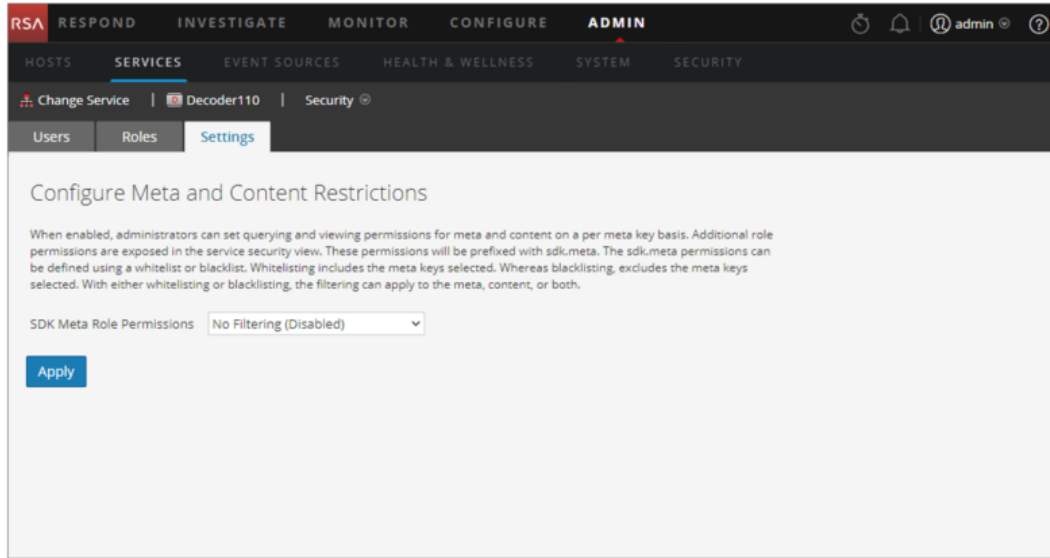
[サービス]の[セキュリティ]ビューにある[設定]タブでは、Brokers、Concentrators、Decoders、Log Decodersに対してメタキー単位の権限を定義するシステムロールを、管理者が有効化および構成できます。この機能を構成すると、メタキーが[サービス]の[セキュリティ]ビュー> [ロール]タブに追加されます。これにより、特定のサービスの特定のロールに個別のメタキーに対する権限を割り当てることができるようになります。次の図は、これを示しています。



この構成は、一般的には、データ プライバシー計画に含まれており、メタ データおよびコンテンツの可視性を特権ユーザだけに制限することで、サービスによって使用または集計されている特定のタイプのコンテンツのセキュリティを確保するために実装されます(「データ プライバシーの管理」を参照してください)。

タブを表示するには次の手順を実行します。

1. NetWitness Platformで、[管理]>[サービス]に移動します。
2. [サービス]グリッドで、DecoderサービスまたはLog Decoderサービスを選択し、 > [表示] > [セキュリティ]を選択して、[設定]タブをクリックします。



機能

タブには2つの機能が含まれます。

機能	説明
[SDKメタ ロール権限] フィールド	メタ キーとコンテンツの制限を無効化または構成するためのオプションを提供します。各オプションの説明は、次の「SDKメタ ロール権限のオプション」を参照してください。
[適用] ボタン	選択した構成をすぐに適用します。無効化以外を選択した場合、[ロール] タブにメタ キーが追加されます。これにより、特定のロールにメタ キー権限を割り当てることができます。

SDKメタ ロール権限のオプション

次の表は、SDKメタ ロール権限で選択可能なフィルタ オプションと、それぞれの数値を示しています。数値は、無効(0)、フィルタ タイプ(1~6)です。

注: system.rolesノードを手動で変更してメタおよびコンテンツの可視性を構成する場合を除き、数値を知っておく必要はありません。

system.roles ノード 値	[設定] タブのオプション	説明
0	フィルタなし (無効化)	メタ キーごとに権限を定義するシステム ロールは無効です。
1	メタとコンテンツのホワイトリスト	システム ロールには、SDKメタ ロール権限のホワイトリストを定義し、システム ロールを割り当てられたユーザのみが指定されたメタおよびコンテンツを表示できます。

system.roles ノード 値	[設定]タ ブのオブ ション	説明
2	メタのみの ホワイトリス ト	システム ロールには、SDKメタ ロール権限のホワイトリストを定義し、システム ロールを割り当てられたユーザのみが指定されたメタを表示 できます。
3	コンテンツの みのホワイト トリスト	システム ロールには、SDKメタ ロール権限のホワイトリストを定義し、システム ロールを割り当てられたユーザのみが指定されたコンテンツを 表示 できます。
4	メタとコンテ ンツのブラッ クリスト	システム ロールには、SDKメタ ロール権限のブラックリストを定義し、システム ロールを割り当てられたユーザは指定されたメタおよびコンテ ンツを表示 できません。
5	メタのみの ブラックリス ト	システム ロールには、SDKメタ ロール権限のブラックリストを定義し、システム ロールを割り当てられたユーザは指定されたメタを表示 でき ません。
6	コンテンツの みのブラッ クリスト	システム ロールには、SDKメタ ロール権限のブラックリストを定義し、システム ロールを割り当てられたユーザは指定されたコンテンツを 表示 できません。

[ユーザ]タブ

このピックでは、[サービス]の[セキュリティ]ビュー> [ユーザ]タブの機能について紹介します。

[サービス]の[セキュリティ]ビューにある[ユーザ]タブでは、サービスに対して次の項目を構成できます。

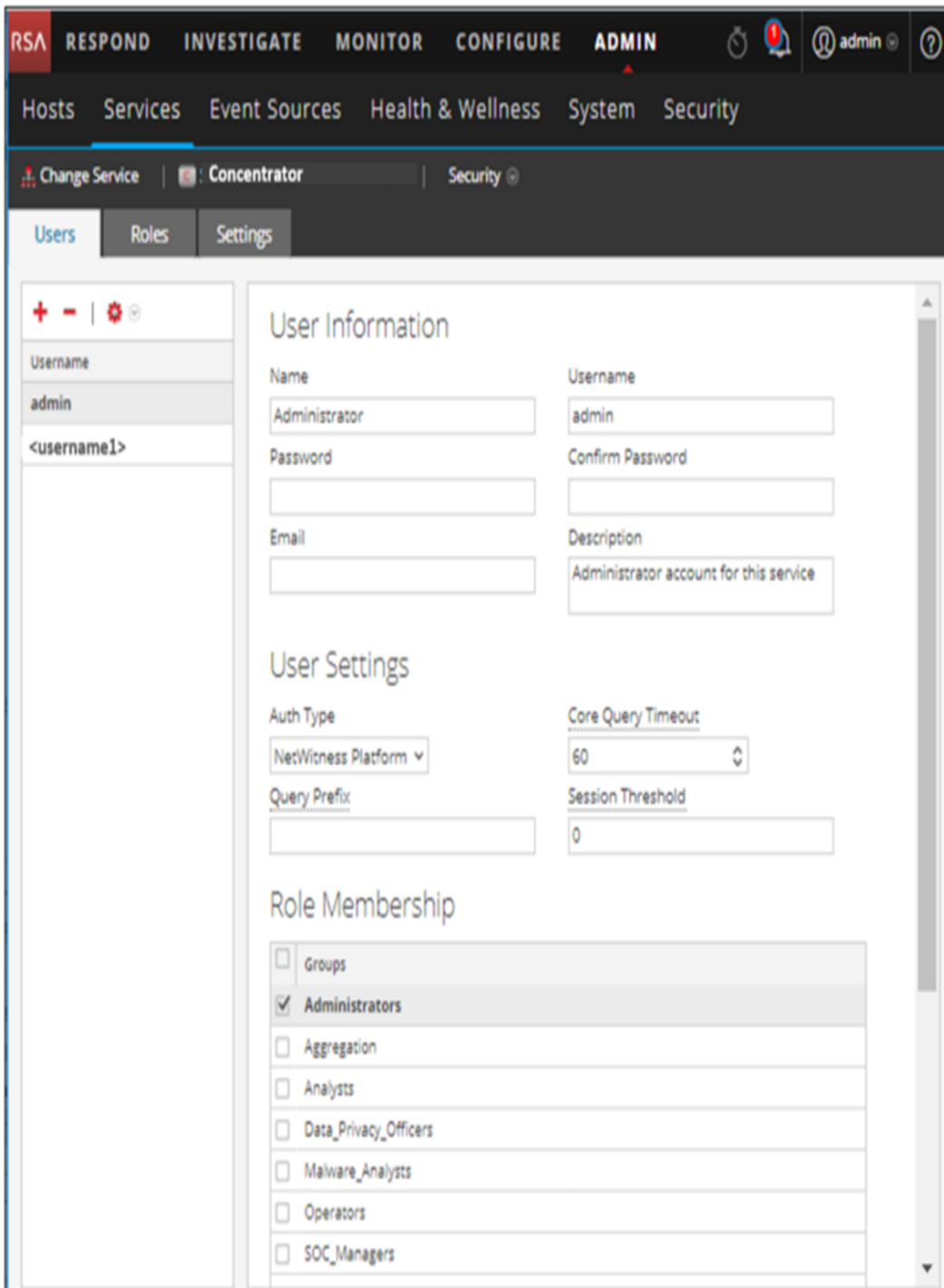
- ユーザアカウントの追加。
- サービスユーザのパスワードの変更。
- サービスユーザの認証プロパティとクエリ処理プロパティの構成。
- ユーザのロールのメンバシップの指定。これによって、選択したサービスに関してユーザが所属する
ロールが指定されます。

注: 信頼接続を使用する10.4以降のNetWitness Platform Coreサービスの場合、Webクライアントから
ログオンするユーザ用にNetWitness Platform Coreユーザアカウントを作成する必要がなくなりました。
NetWitness Platform Coreユーザアカウントを作成する必要があるのは、集計の設定時、シック クラ
イアント、REST APIを使用する場合です。

このタブに関連する手順については、「[ホストとサービスの手順](#)」で説明します。

[サービス]の[セキュリティ]ビュー> [ユーザ]タブにアクセスするには、次の手順を実行します。

1. NetWitness Platformで、[管理]>[サービス]に移動します。
2. ユーザを追加するサービスを選択し、 > [表示]> [セキュリティ]を選択します。






機能

[ユーザ]タブには、左側に[ユーザリスト]パネルがあります。ユーザ名を選択すると、右側の[ユーザ定義]パネルが使用可能になります。

[ユーザリスト]パネル

[ユーザリスト]パネルには次の機能があります。

機能	説明
	現在のサービスに新しいユーザを追加します。
	選択したユーザをサービスから削除します。
	<p>選択したサービス ユーザ アカウントに対し、次のいずれかのアクションを実行します。</p> <ul style="list-style-type: none"> • レプリケート: サービス ユーザ アカウント全体を、選択したサービスにレプリケートします。 • パスワードの変更: サービス ユーザ アカウントのパスワードを変更し、新しいパスワードを、同じ アカウントが定義されている他のコア サービスにレプリケートします。[パスワードの変更]オプションによって選択されたコア サービスにレプリケートされるのは、ユーザ アカウント全体ではなく、パスワードの変更のみです。
ユーザ名	サービスにアクセスするすべてのユーザ アカウントのユーザ名。NetWitness Platformのログインで使うユーザ名と同一にする必要があります。

次の図は、[他のサービスへのユーザのレプリケート]ダイアログを示しています。

Replicate User to other services ✕

Please enter and confirm the service user password. The entire service user account replicates to the selected services. The user password also changes on each selected service.

Password

Confirm Password

<input type="checkbox"/>	Name ^	Address	Type
<input type="checkbox"/>	- Broker		Broker
<input type="checkbox"/>	- Conc...		Concentrator
<input type="checkbox"/>	- Archi...		Archiver
<input type="checkbox"/>	- Work...		Workbench
<input type="checkbox"/>	- Log C...		Log Collector
<input type="checkbox"/>	- Log ...		Log Decoder
<input type="checkbox"/>	- Wareh...		Warehouse C...
	NW - Malware A		Malware A

次の図は、[パスワードの変更]ダイアログを示しています。

Change Password

Please enter and confirm the service user password. Only the user password changes on the selected services. No other user attributes will replicate to the services

Password

Confirm Password

<input type="checkbox"/>	Name ^	Address	Type
<input type="checkbox"/>	S5EndpointLohHyb - Log Decoder		Log Decoder
<input type="checkbox"/>	S5LogDecoder - Log Collector		Log Collector
<input type="checkbox"/>	S5LogDecoder - Log Decoder		Log Decoder
<input type="checkbox"/>	S5LogHybrid - Concentrator		Concentrator
<input type="checkbox"/>	S5LogHybrid - Log Collector		Log Collector
<input type="checkbox"/>	S5LogHybrid - Log Decoder		Log Decoder
<input type="checkbox"/>	S5MalwareAnalysis - Broker		Broker
<input type="checkbox"/>	S5NWDecoder - Decoder		Decoder
<input type="checkbox"/>	S5PacketHybrid - Concentrator		Concentrator
<input type="checkbox"/>	S5PacketHybrid - Decoder		Decoder
<input type="checkbox"/>	VLC2514 - Log Collector		Log Collector

Cancel Change Password

[ユーザ定義]パネル

[ユーザ定義]パネルには3つのセクションがあります。

- [ユーザ情報]では、[管理]の[セキュリティ]ビューで作成されたとおりにユーザを特定します。
- [ユーザ設定]は、このユーザがサービスにアクセスするときに適用されるパラメータを定義します。
- [ロールメンバシップ]は、ユーザが所属するユーザロールを定義します。

ボタンが2つあります。

- [保存]ボタンは、[ユーザ定義]パネルでの変更を保存し、変更はすぐに有効になります。
- [リセット]ボタンは、[ユーザ定義]パネルで変更を保存していない場合、すべてのフィールドと設定を編集前の値にリセットします。

ユーザ情報

[ユーザ情報]セクションには次の機能があります。

フィールド	説明
名前	ユーザの名前。
ユーザ名	サービスにログオンするためにユーザが入力するユーザ名。これは、[管理]の[セキュリティ]ビュー([管理]>[セキュリティ])で、管理者がユーザおよび認証情報を追加したときに指定したNetWitness Platformユーザ名です。

フィールド	説明
パスワード (およびパスワードの確認)	サービスにログオンするためにユーザが入力するパスワード。これは、[管理]の[セキュリティ]ビューで、管理者がユーザおよび認証情報を追加したときに指定したNetWitness Platformパスワードです。ユーザがNetWitness Platform全体のサービスに接続できるようにするため、NetWitness Platformのアカウント パスワードとサービス パスワードは一致する必要があります。
メール	(オプション) ユーザのメール アドレス。
説明	(オプション) このユーザの説明。

ユーザ設定

[ユーザ設定] セクションには次の機能があります。

フィールド	説明
認証タイプ	<p>このユーザの認証スキーム。内部および外部の認証をサポートしています。</p> <ul style="list-style-type: none"> Netwitnessは内部認証で、デフォルトで有効になっています。このモードでは、ユーザは、管理者がNetWitness Platformの[管理]の[セキュリティ]ビュー([管理]>[セキュリティ])でユーザアカウントを作成した際に設定したアカウントとパスワードで認証する必要があります。 外部認証は、ホスト インタフェースでPAM(Pluggable Authentication Modules)を構成した場合に選択できます。詳細については、『システム セキュリティとユーザ管理』ガイドの「PAMログイン機能の構成」を参照してください。
クエリプレフィックス	(オプション) このユーザによるすべてのクエリに必ず付加するクエリを構成します。たとえば、 <code>email != 'ceo@company.com'</code> というクエリプレフィックスを追加すると、指定した一部のメールのセッションが結果に表示されなくなります。
Coreクエリタイムアウト	<div style="border: 1px solid green; padding: 5px;"> <p>注:このフィールドは、NetWitness Platform 10.5以降のサービスで使用され、10.4以前のサービスには表示されません。NetWitness Platform 10.4以前のサービスでは、[Coreクエリタイムアウト]ではなく[クエリレベル]が使用されます。</p> </div> <p>ユーザがサービスに対して1つのクエリを実行できる最長時間を分単位で指定します。この値がゼロ(0)に設定されている場合、クエリタイムアウトはサービス上のユーザには適用されません。</p> <p>NetWitness Platform 10.5以降のサービスからNetWitness Platform 10.4のサービスにユーザをレプリケートすると、クエリタイムアウトは、最も近いレベルのクエリレベルに変換されます。たとえば、ユーザのクエリタイムアウトが15分である場合、ユーザはクエリレベル3を取得します。ユーザのクエリタイムアウトが35分である場合、ユーザはクエリレベル2を取得します。ユーザのクエリタイムアウトが45分である場合、ユーザはクエリレベル2を取得します。</p>

フィールド	説明
セッション閾値	<p>(オプション) メタ値をスキャンする場合のセッション数のカウントについて、アプリケーションの動作を制御します。スキャン時にセッション数が閾値に到達すると、それ以降セッション数はカウントされません。</p> <p>セッション閾値を設定し、実際にスキャン時に閾値に到達した場合、[ナビゲート]ビューには閾値に達したこと、また閾値に達するまでに要したクエリの時間の割合が表示されます。</p>

ロールメンバシップ

[ロールメンバシップ]セクションには、選択したサービスでユーザが所属しているロールが表示されます。

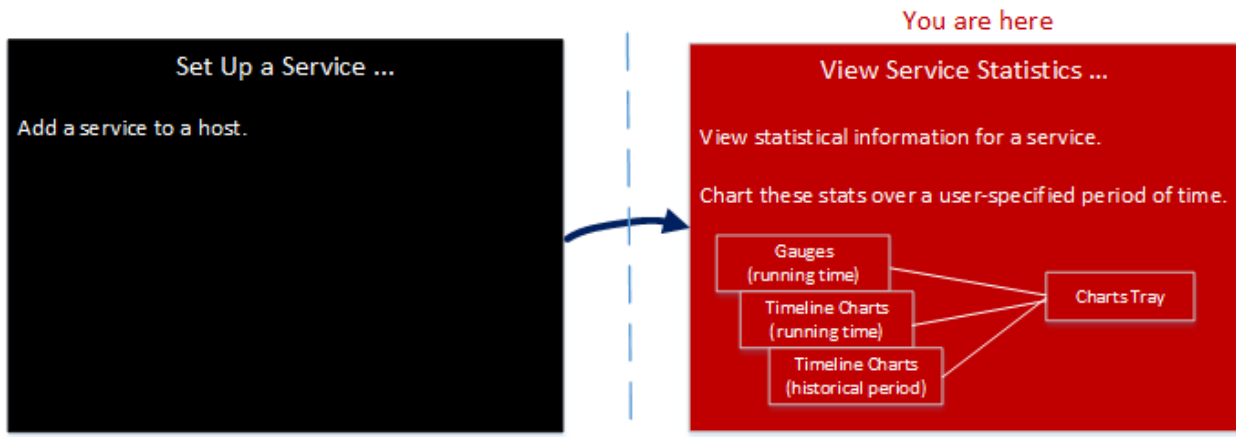
[サービス]の[統計]ビュー

このトピックでは、NetWitness Platformの[サービス]の[統計]ビューで使用できる機能について説明します。

[サービス]の[統計]ビューでは、サービスのステータスと運用状況を監視できます。このビューでは、収集状況、サービスのシステム情報、ホストのシステム情報などが表示されます。さらに、80個を超える統計をゲージやタイムラインチャートで表示できます。履歴チャートには、セッションのサイズ、セッション、パケットの統計情報のみが表示されます。

ワークフロー


このワークフローは、[統計]ビューから実行するタスクを示します。

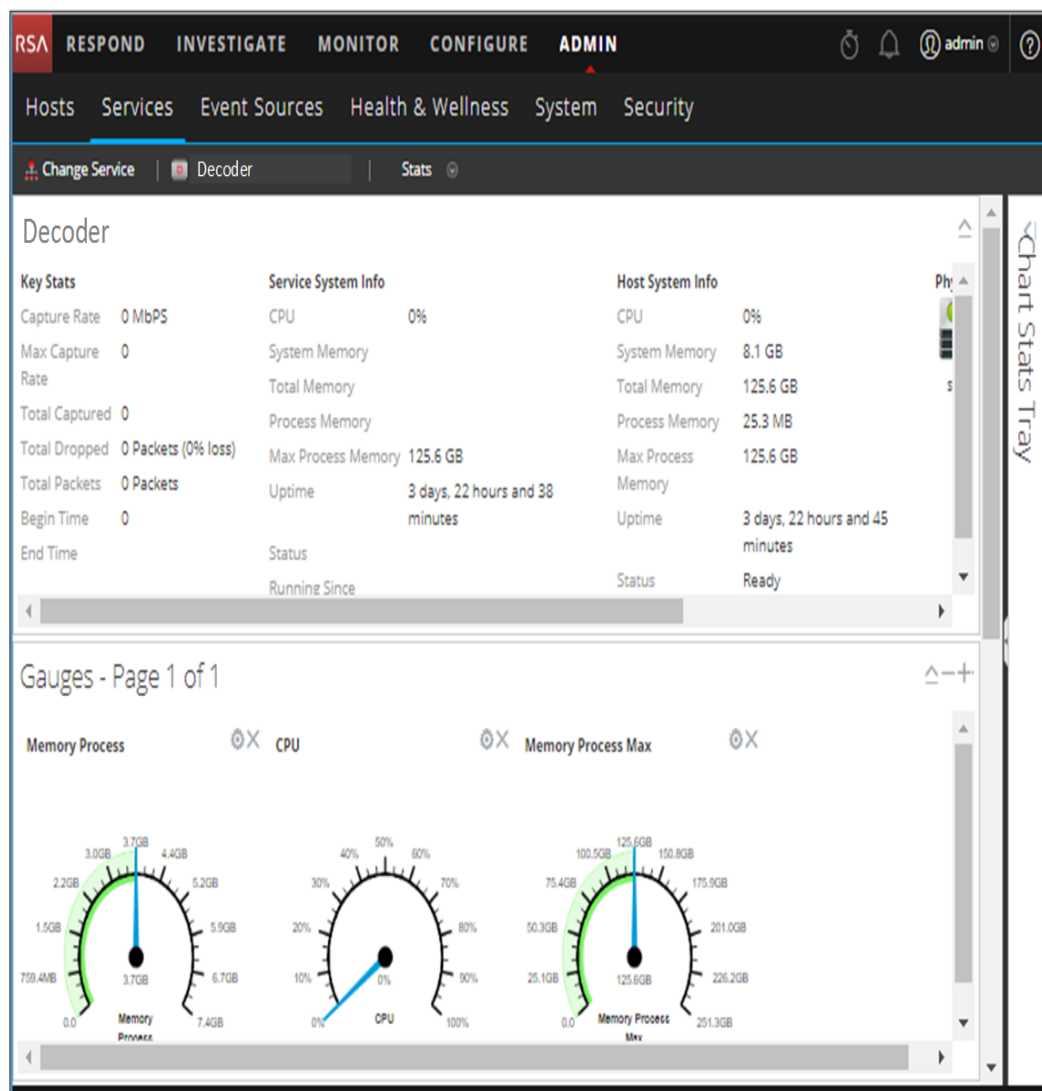


[統計]ビューでは、サービスごとに、監視する統計情報をカスタマイズすることができます。

次の例は、Decoderの[統計]ビューを使用する方法を示します。すべてのサービスの[統計]ビューで、各サービスの同様の情報が表示されます。

[サービス]の[統計]ビューにアクセスするには、次の手順を実行します。

1. NetWitness Platformで、[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. サービスを選択し、 > [表示]> [統計]の順に選択します。



機能

サービスのタイプに応じて異なる統計が使用できますが、次に示す要素はどのコア サービスにも共通しています。

- [サマリ統計]セクション
- [ゲージ]セクション
- [タイムライン]セクション
- [履歴]セクション
- 統計チャートトレイ

[サマリ統計]セクション

[サマリ統計]セクションは、デフォルト ビューの上部にあり、編集可能なフィールドはありません。

[サマリ統計]セクションには5つのパネルがあります。[収集状況]パネルには、サービスのタイプに応じて異なる統計が表示されます。[サマリ統計]セクションのそれ以外のパネルは、どのタイプのサービスでも同じです。

収集状況

[収集状況]パネルには、サービスのタイプに応じて異なる統計が表示されます。

- DecoderまたはLog Decoderの場合、収集状況には、収集レート、収集されたパケットやログの合計、ドロップされたパケットやログの合計、データ収集の開始時刻と終了時刻など、収集に関する統計が含まれます。

Key Stats	
Capture Rate	0 MBPS
Max Capture Rate	33 MBPS
Total Captured	8.2 Million Packets
Total Dropped	0 Packets (0% loss)
Total Packets	271,941 Packets
Begin Time	2008-Feb-13 16:55:19
End Time	2015-Jan-23 05:15:47

- BrokerまたはConcentratorは、複数のサービスからデータを集計します。そのため、収集状況のグリッドにはすべてのサービスからのデータの集計状況が示されます。グリッドの列では、サービス名、収集レート、最大収集レート、未処理セッション数、サービスステータスが示されます。

Key Stats				
Key Stats	Rate	Max	Behind	Status
[REDACTED]	0	2346	0	consumir
[REDACTED]	0	0	0	consumir
[REDACTED]	0	26	0	consumir

サービスシステム情報

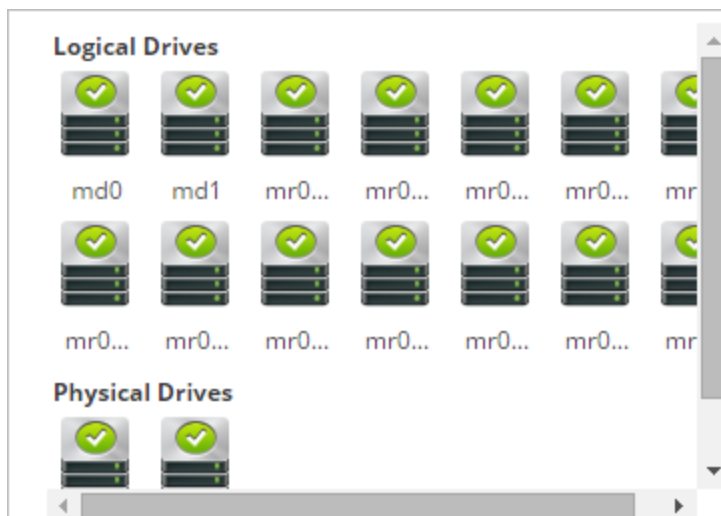
[サービスシステム情報]パネルには、サービスのCPU使用率、メモリ使用量の統計(システム、合計、処理メモリ、最大処理メモリ)、サービスの稼働時間、ステータス、起動日時、現在の日時が含まれます。

Service System Info	
CPU	7%
System Memory	14.9 GB
Total Memory	15.6 GB
Process Memory	111.4 MB
Max Process Memory	15.6 GB
Uptime	1 week, 6 days, 3 hours and 25 minutes
Status	Ready
Running Since	2015-Jan-23 09:29:11

[ホスト システム情報]には、ホストが使用するCPU使用率、メモリ使用量の統計(システム、合計、処理メモリ、最大処理メモリ)、ホストの稼働時間、ステータス、起動日時、現在の日時が含まれます。

Host System Info	
CPU	0%
System Memory	31.2 GB
Total Memory	31.4 GB
Process Memory	22.9 MB
Max Process Memory	31.4 GB
Uptime	5 weeks, 1 day, 19 hours and 57 minutes
Status	Ready

[論理ドライブ]と[物理ドライブ]には、ドライブ名と状態を表すアイコンが表示されます。ドライブ名で使用するタイプとドライブ ステータスのオプションは、次のリストに示されています。



ドライブ タイプとステータス

ドライブタイプ	説明	コメント	ステータス オプション
sd	SCSIブロック デバイス	直接接続されたSAS、SATA MegaRAIDボリューム	OK(緑) FAIL(赤)
ld	MegaRAID論理ボリューム	BIOSまたはMegaCLIツールで定義	OK(緑) DEGRADED (黄) BUILDING(黄色) FAIL(赤)
pd	MegaRAID物理 ディスク	Linuxにボリュームが作成されていない物理ディスク	OK(緑) FAIL(赤)
md	LinuxソフトウェアRAIDボリューム		OK(緑) DEGRADED (黄) BUILDING(黄色) FAIL(赤)

ゲージ

[統計]ビューの[ゲージ]セクションでは、統計情報がアナログ ゲージ形式で表示されます。ゲージの構成の詳細については、「[機能](#)」を参照してください。

タイムライン

タイムライン チャートは、現在の時間を中心に選択した項目の実行中の統計をタイムラインで表示します。これはすべてのタイプのサービスで同じで、タイムラインの表示名だけが編集可能です。タイムラインの構成に詳細については、[タイムライン チャート](#)を参照してください。

履歴タイムライン

履歴チャートは、セッション サイズ、セッション、パケットの統計情報を履歴タイムラインで表示します。これはすべてのタイプのサービスで同じで、表示名、開始日、終了日を編集できます。タイムラインの構成に詳細については、[タイムライン チャート](#)を参照してください。

注:履歴タイムライン チャートは、Log Collector、VLC(Virtual Log Collector)、Windows Legacy Collectorサービスでは廃止されています。

統計チャートトレイ

[統計チャートトレイ]には、選択したサービスタイプで利用可能なすべての統計情報が一覧表示されます。サービスによって監視する統計情報が異なります。詳細については、「[コンポーネント](#)」を参照してください。

トピック



- [コンポーネント](#)
- [機能](#)
- [タイムライン チャート](#)

統計チャートトレイ

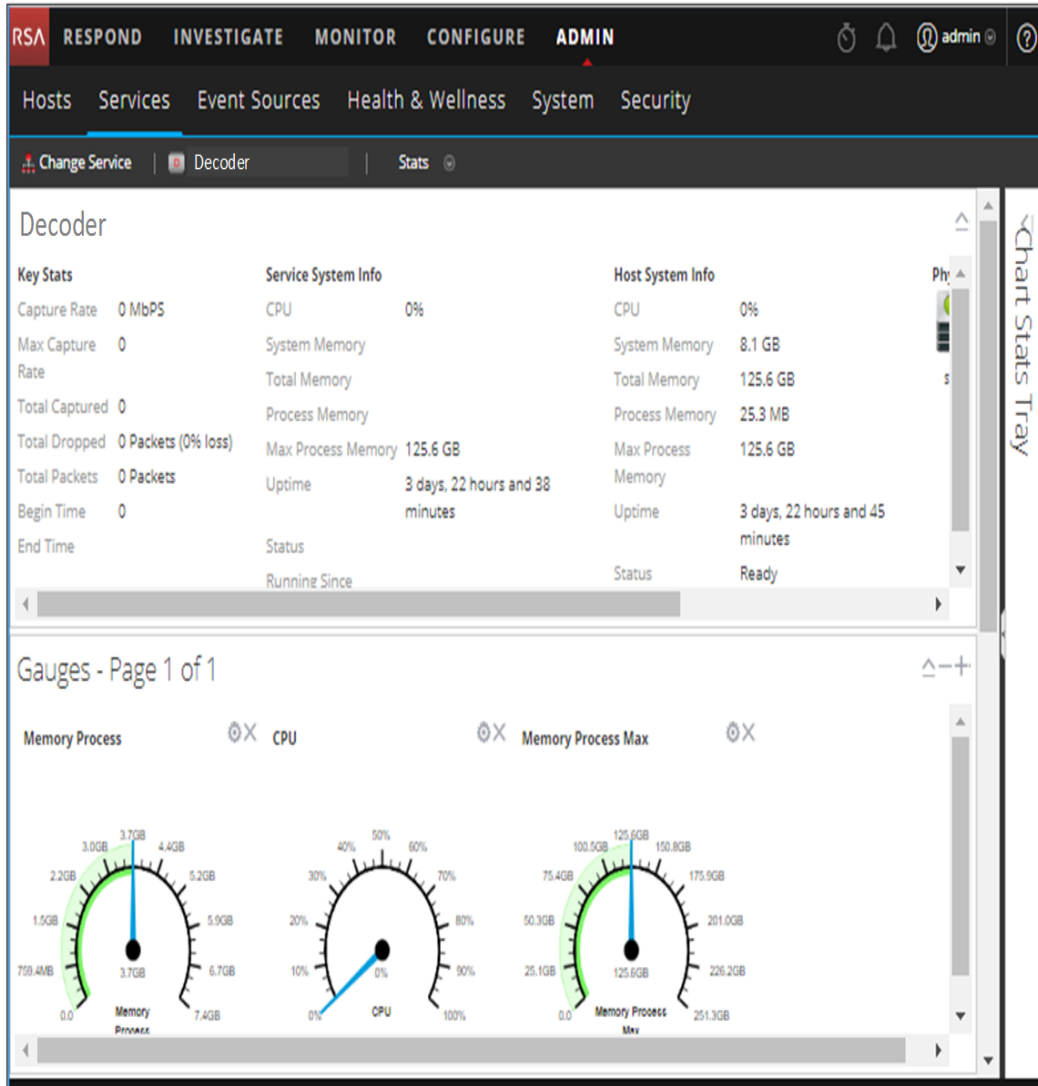
このピックでは、[サービス]の[統計]ビューにある[統計チャートトレイ]について説明します。

[サービス]の[統計]ビューでは、[統計チャートトレイ]を使用して個別のサービスで監視する統計をカスタマイズすることができます。[統計チャートトレイ]には、サービスで利用可能なすべての統計情報が一覧表示されます。統計情報は、監視されるサービスのタイプに応じて異なります。[統計チャートトレイ]内の統計情報は、ゲージまたはタイムラインチャートで表示できます。セッション サイズ、セッション、パケットの統計情報については、履歴タイムラインチャートで表示できます。

[サービス]の[統計]ビューにアクセスする方法




1. NetWitness Platformメニューで、[管理]>[サービス]を選択します。
[管理]の[サービス]ビューが表示されます。
2. サービスを選択し、 > [表示]> [統計]の順に選択します。
[統計チャートトレイ]が右側に表示されます。
3. トレイが折りたたまれている場合、 をクリックすると、使用可能な統計情報のリストが表示されます。





次の例は、Decoderの[サービス]の[統計]ビューを示しています。統計チャートトレイが折りたたまれています。



コンポーネント

[統計チャートトレイ]には、サービスのタイプに応じて異なる統計情報があります。上の例では、Decoderに関して111件の統計情報を使用できます。次の表に、[統計チャートトレイ]の機能を説明します。

機能	説明
	クリックすると、パネルが水平に展開します。
	クリックすると、パネルが水平に折りたたまれます。
検索	フィールドに検索する用語を入力します。合致する統計が表示され、一致する単語が強調表示されます。
	クリックすると、最初のページに移動します。


機能	説明
	クリックすると、前のページに移動します。
Page <input type="text" value="5"/> of 200	[ページ]フィールドに、ページ番号を入力します。
	クリックすると、次のページに移動します。
	クリックすると、最後のページに移動します。
	クリックすると、ビューが更新されます。
Stats 1 - 12 of 111	表示される統計の範囲を示します。統計情報の数はサービスタイプによって異なります。

ゲージ

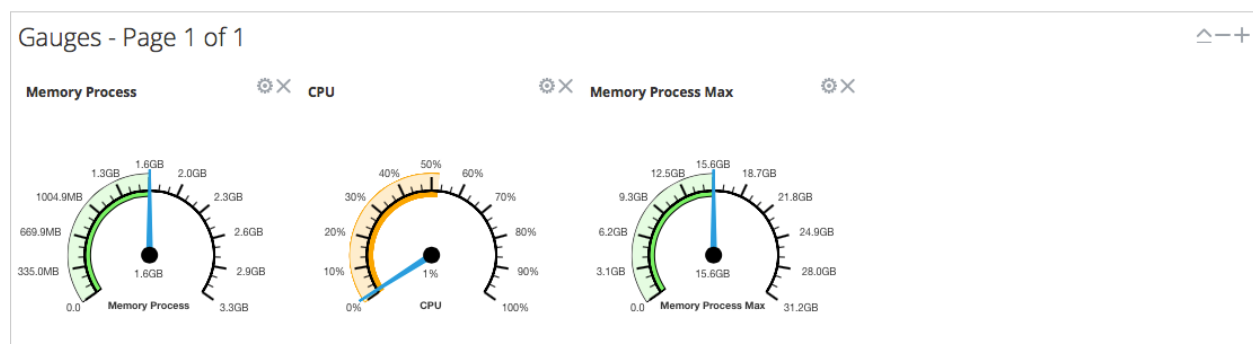
このトピックでは、[サービス]の[統計]ビューにある[ゲージ]セクションの機能について説明します。

[サービス]の[統計]ビューの[ゲージ]セクションでは、統計情報がアナログゲージ形式で表示されます。[統計チャートトレイ]にある使用可能な統計はどれも[ゲージ]セクションにドラッグできます。個々のゲージのプロパティは編集可能です。すべてのゲージでタイトルを編集できます。さらに編集可能なプロパティがあるものもあります。

[サービス]の[統計]ビューにアクセスする方法

1. NetWitness Platformメニューで、[管理]>[サービス]を選択します。
[管理]の[サービス]ビューが表示されます。
2. サービスを選択し、 > [表示]> [統計]の順に選択します。
[サービス]の[統計]ビューには[ゲージ]セクションが含まれます。

次の図は、Log Decoderの[サービス]の[統計]ビューにあるデフォルトのゲージを表しています。



機能

デフォルトのゲージでは次の統計が表示されます。

- 処理メモリの使用量
- CPUの使用率
- 処理メモリの使用量の最大値

ゲージ タイトル バーと各ゲージにあるコントロールは、標準ダッシュレット コントロールです。

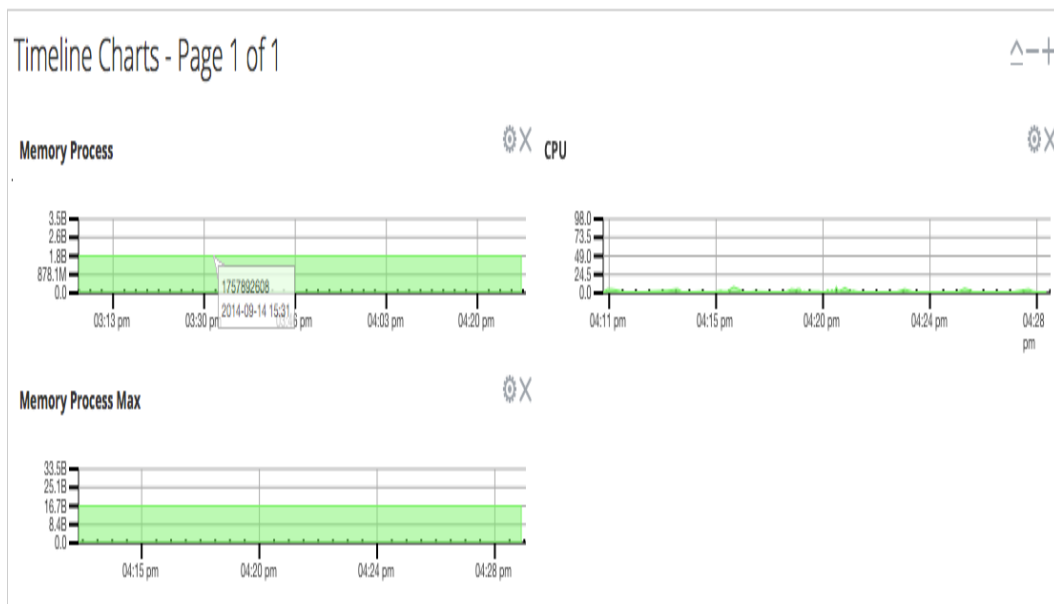
- ゲージ タイトル バーでは、セクションを展開または折りたたみ表示をしたり、ページを前後に移動できます。
- 各ゲージでは、プロパティを編集(⚙️)したり、ゲージを削除(✖️)したりすることができます。

タイムライン チャート

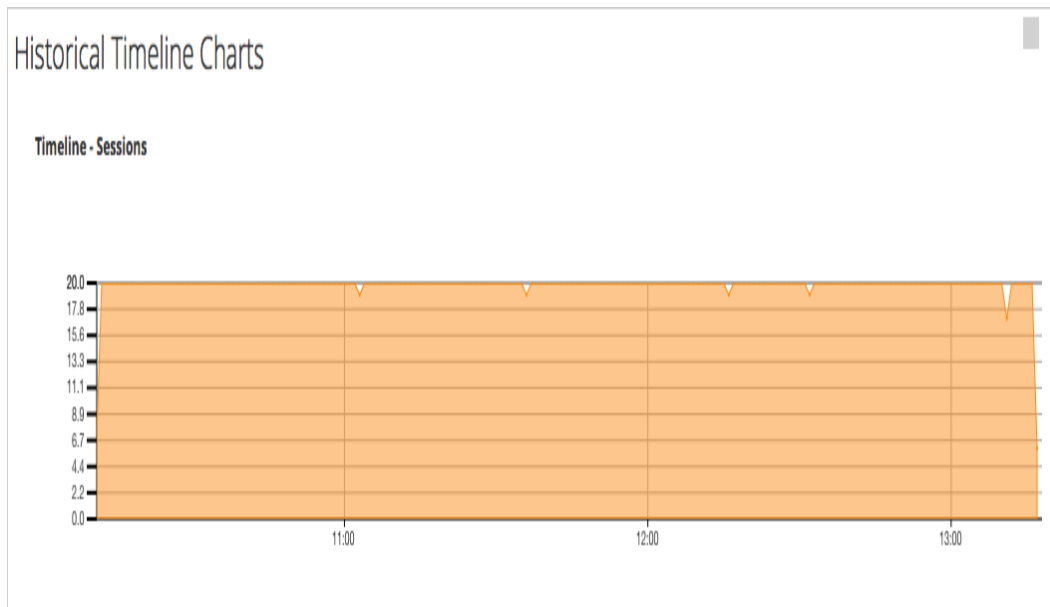
このトピックでは、[サービス]の[統計]ビューにあるタイムライン チャートの機能について説明します。

タイムライン チャートには、実行中の統計がタイムラインに表示されます。[サービス]の[統計]ビューには、リアルタイムと履歴という2種類のタイムラインがあります。[統計チャートトレイ]にある統計は[タイムライン チャート]セクションにドラッグできます。セッション サイズ、セッション、パケットの統計情報については、履歴タイムライン チャートで表示できます。個々のタイムライン チャートのプロパティは編集可能です。すべてのタイムライン チャートでタイトルを編集できます。さらに編集可能なプロパティがある統計もあります。

次の図は、データ ポイントの値とタイム スタンプを示した、リアルタイムのタイムラインの例です。



次の図は履歴チャートの例です。



リアルタイムのタイムライン チャートはデフォルトで以下の統計を表しています。

- 処理メモリ
- CPU
- 最大処理メモリ

履歴チャートは以下の統計を表しています。

- セッション
- パケット
- セッション サイズ

タイムライン チャート タイトル バーと各タイムラインにあるコントロールは、標準ダッシュレット コントロールです。

- タイムライン チャート タイトル バーでは、セクションを展開または折りたたみ表示をしたり、ページを前後に移動したりすることができます。
- 各タイムラインでは、プロパティを編集(⚙)したり、タイムラインを削除(✕)したりすることができます。
- チャートのデータ ポイントの上にカーソルを置くと、選択したポイントの値とタイム スタンプが表示されます。

システムビュー

このトピックでは、例としてDecoderやLog Decoderを使用して[システム]ビューの機能について説明します。[管理]>[サービス]>[システム]ビューの詳細については、構成ガイド(『RSA NetWitness® PlatformBrokerおよびConcentrator構成ガイド』など)の個々のサービスを参照してください。

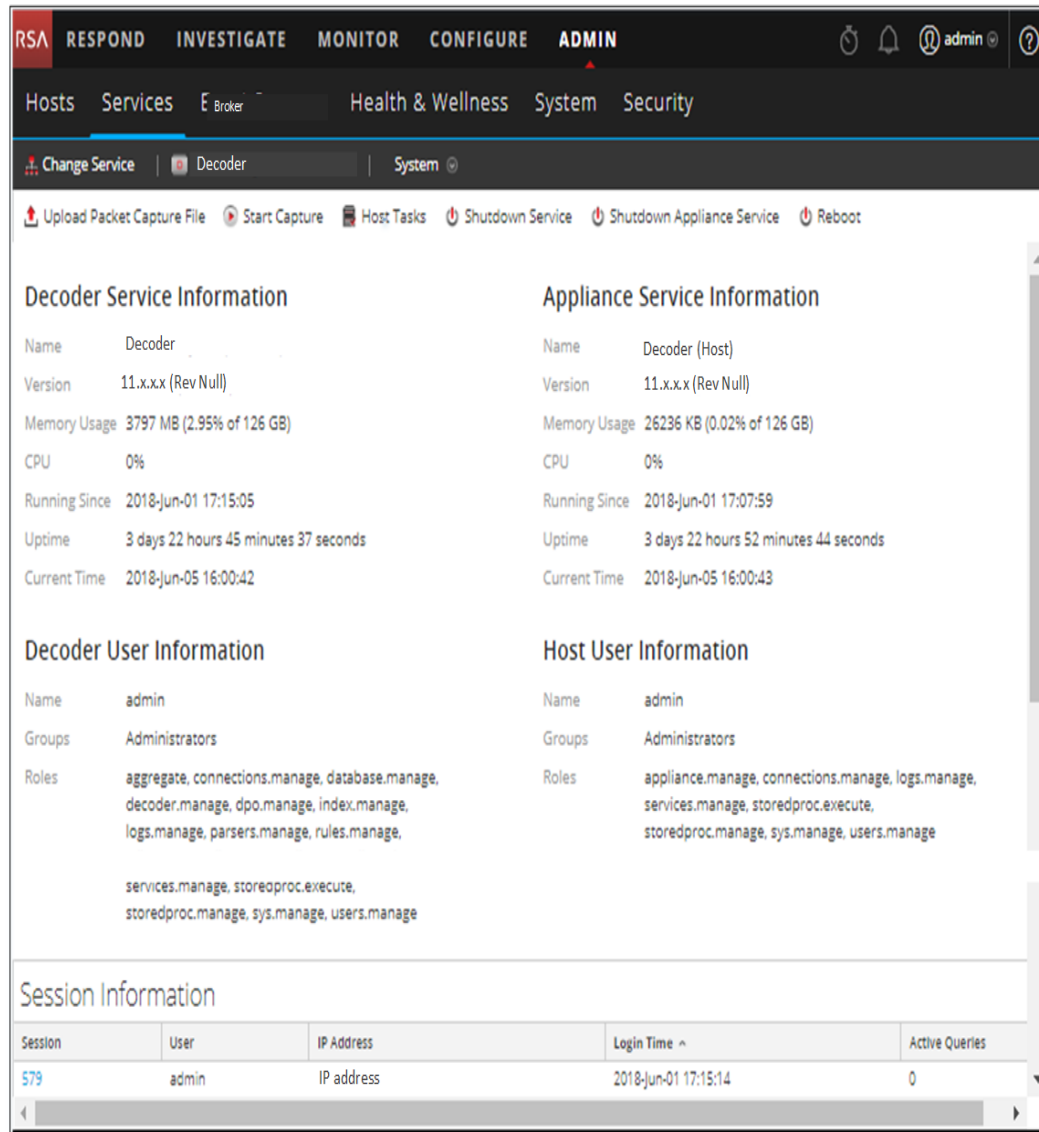
Log Decoderは特殊なタイプのDecoderで、Decoderと同様に構成および管理されます。そのため、このセクションのほとんどの情報は、両方のタイプのDecoderについてあてはまります。違いがある場合には個別に記載があります。

Decoderサービスの[システム]ビューにアクセスするには、次の手順を実行します。

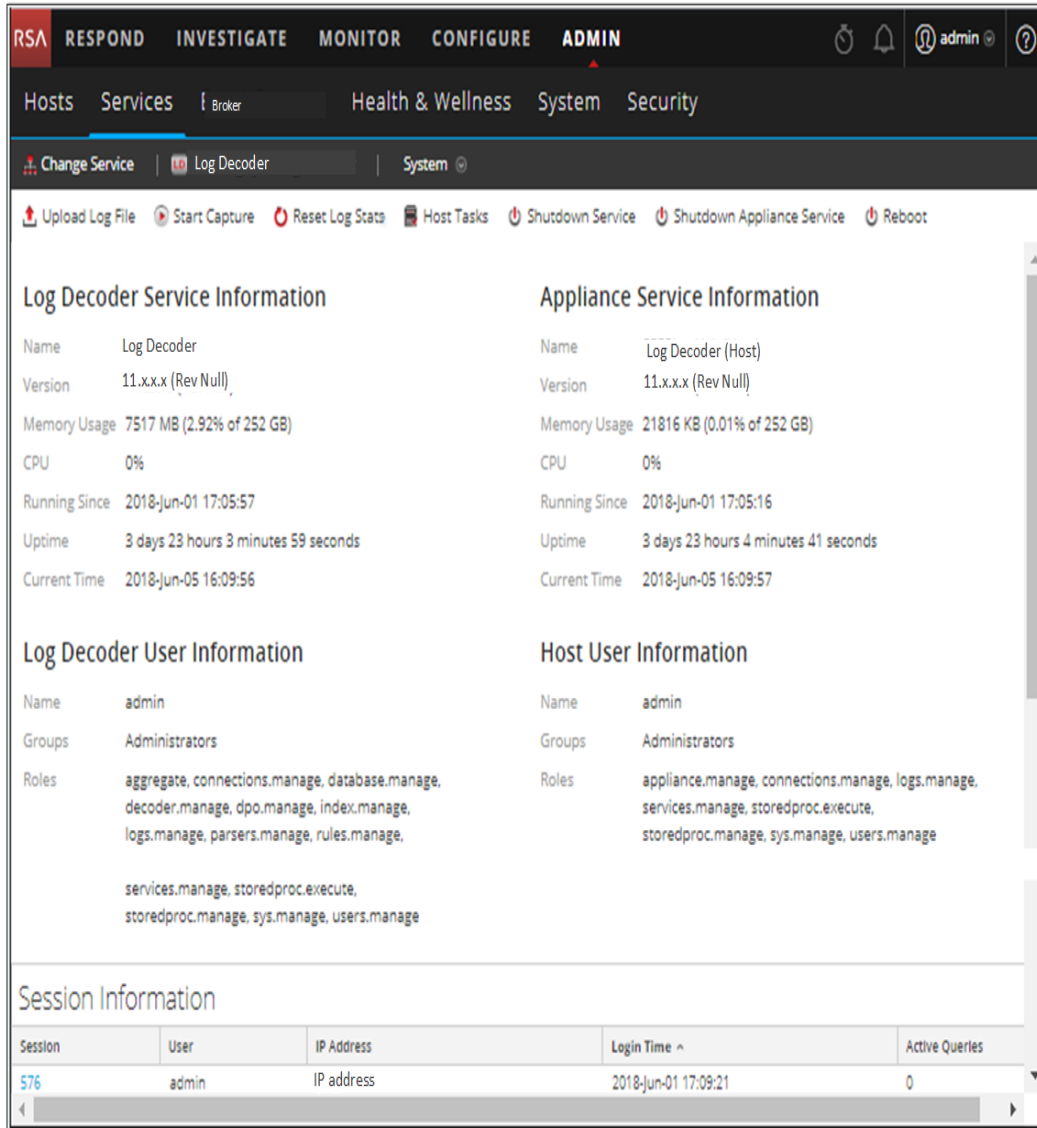
1. NetWitness Platformメニューで、[管理]>[サービス]に移動します。
[サービス]ビューが表示されます。

2. サービスを選択し、 > [表示]> [システム]を選択します。

次の図は、Decoderの[サービス]の[システム]ビューを示しています。



次の図は、Log Decoderの[サービス]の[システム]ビューを示しています。



機能

[サービス情報] ツールバー

次のツールバーは、Log DecoderおよびDecoderに固有のオプションを示します。



[サービス]の[システム]ビューのツールバーにある共通オプションに加え、パケット収集やログ収集の開始と停止も実行できます。ファイルのアップロード オプションは、Decoder(パケット キャプチャ ファイル)と Log Decoder(ログ ファイル)で異なります。


アクション	説明
パケット キャプチャファイルのアップロード	<p>選択されたDecoderにアップロードするパケット キャプチャ(.pcap)ファイルを選択するためのダイアログを表示します。詳細については、『<i>DecoderおよびLog Decoder構成ガイド</i>』の「パケット キャプチャファイルのアップロード」を参照してください。</p> <div style="border: 1px solid green; padding: 5px; margin-top: 10px;"> <p>注: このオプションはLog Decoderにはありません。</p> </div>
ログファイルのアップロード	<p>選択されたLog Decoderにアップロードするログ(.log)ファイルを選択するためのダイアログを表示します。詳細については、『<i>DecoderおよびLog Decoder構成ガイド</i>』の「Log Decoderへのログファイルのアップロード」を参照してください。</p>
収集の開始/停止	<p>選択されたDecoder(またはLog Decoder)で、パケットやログの収集を開始します。パケットの収集が実行中の場合、ツールバーのこのオプションは[収集の停止]になります。また、収集の実行中はファイルのアップロードのオプションは使用できません。</p>

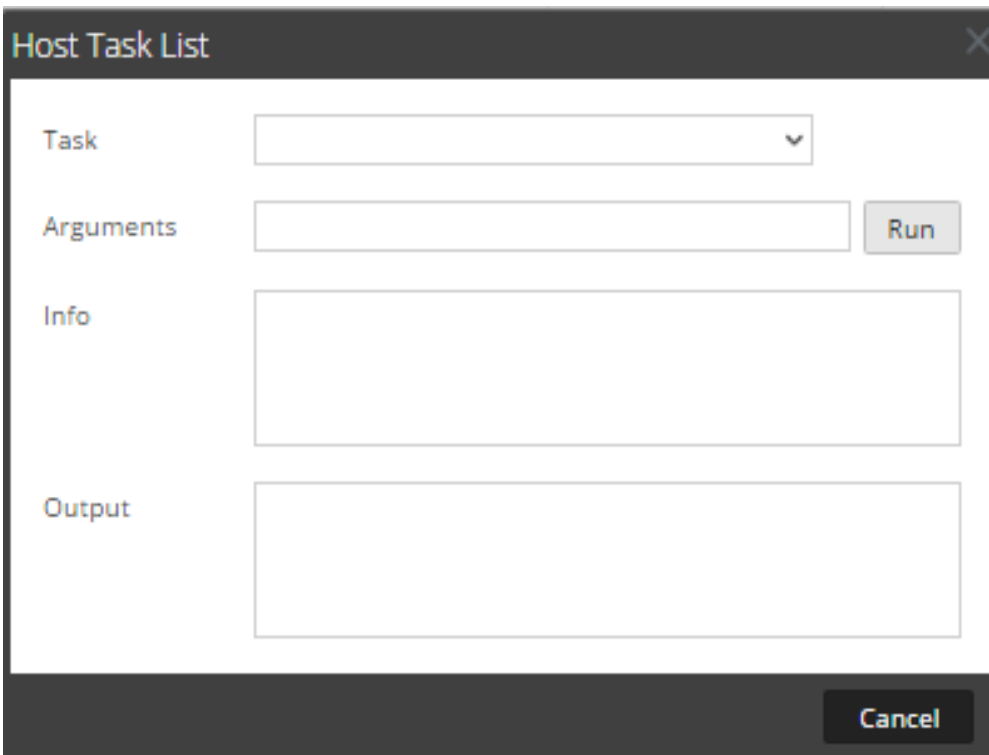
[ホスト タスク リスト]ダイアログ

このトピックでは、サービスの[システム]ビュー> [ホスト タスク リスト]ダイアログについて説明します。

RSA NetWitness Platformサービスの[システム]ビューでは、[ホスト タスク]オプションを使用して、ホストに関連するタスクおよびネットワークとの通信を管理できます。コア サービスに対して、複数のサービスおよびホストの構成オプションが使用できます。

[ホスト タスク]ダイアログにアクセスするには、次の手順を実行します。

1. NetWitness Platformで、[管理]> [サービス]を選択します。
2. サービスを選択し、> [ 表示]> [システム]を選択します。
サービスの[システム]ビューが表示されます。
3. サービスの[システム]ビューのツールバーで、[ホスト タスク]をクリックします。
[ホスト タスク リスト]ダイアログが表示されます。タスク リストは、このホストでサポートされているタスクのリストを提供します。



機能

下の表はダイアログの機能について説明しています。

フィールド	説明
タスク	コア ホストのタスクを入力するか選択するためのフィールドです。このフィールドをクリックすると、使用可能なホスト タスクのドロップダウン リストが表示されます。

フィールド	説明
引数	メッセージの引数(ある場合)を入力する入力フィールドです。
実行	タスクを実行します。
情報	タスクの情報や構文を表示します。
出力	実行されたタスクの出力または結果です。
キャンセル	[ホスト タスク リスト]ダイアログを閉じます。

ホスト タスク選択リスト

これらのタスクは、[タスク]フィールドのドロップダウン リストとして表示されます。使用可能なオプションは、オプションを実行するのに必要なセキュリティ ロールによって制限されます。

タスク	説明
ファイル システム 監視の追加	指定されたファイル システムが格納されたストレージ サービスのモニタリングを開始します(ファイル システム監視の追加と削除 を参照)。
ファイル システム 監視の削除	指定されたファイル システムが格納されたストレージ サービスのモニタリングを停止します。
ホストの再起動	ホストをシャットダウンし、リスタートします(ホストの再起動 を参照)。
ホスト内蔵クロックの設定	ホストのローカル クロックを設定します(ホスト内蔵クロックの設定 を参照)。
ホストのホスト名の設定	ホスト名を変更するためのこの方法は、NetWitness Platform 10.6では廃止されました。「 ホストとサービスの手順 」で説明されている手順に置き換えられました。
ネットワーク構成の設定	ネットワーク アドレス パラメータを設定します(ネットワーク構成の設定 を参照)。
ネットワーク タイムソースの設定	このホストのタイム ソースを設定します(ネットワーク タイムソースの設定 を参照)。
Syslog転送の設定	リモート サーバから、選択されたサービスへのSyslog転送を有効化または無効化します。(「 Syslog転送の設定 」を参照)。
ネットワーク ポート ステータスの表示	ホストのネットワーク インタフェース情報を表示します(ネットワーク ポート ステータスの表示 を参照)。
シリアル番号の表示	ホストのシリアル番号を表示します(シリアル番号の表示 を参照)。
ホストのシャットダウン	物理ホストをシャットダウンし、ホストの電源をオフにします(ホストのシャットダウン を参照)。
サービスの開始	このホストでサービスを開始します(「 サービスの起動、停止、再起動 」を参照)。
サービスの停止	このホストでサービスを停止します。

タスク	説明
SNMPの設定	ホスト上でSNMPサービスを有効化または無効化します(「 SNMPの設定 」を参照)。

サービス構成設定

このトピックでは、RSA NetWitness Platformコア サービスで利用可能なサービス構成設定について説明します。

NetWitness Platformコア サービスには、Brokers、Concentrator、Decoder、Log Decoder、Archiver、Applianceサービスが含まれています。これらの表には、表示および構成可能なサービス構成パラメータがすべて示されています。一部のパラメータは、NetWitness Platformユーザ インタフェースのさまざまな部分で構成できますが、中には[サービス]の[エクスプローラ]ビューでしか表示または構成できないパラメータもあります。

Applianceサービスの構成パラメータ

このトピックでは、NetWitness Platform Core Applianceサービスで利用可能な構成パラメータのリストと説明を示します。

NetWitness Platform Core Applianceサービスでは、従来のNetWitnessハードウェアのハードウェア モニタリングを提供します。

次の表は、Applianceの構成パラメータについて説明しています。

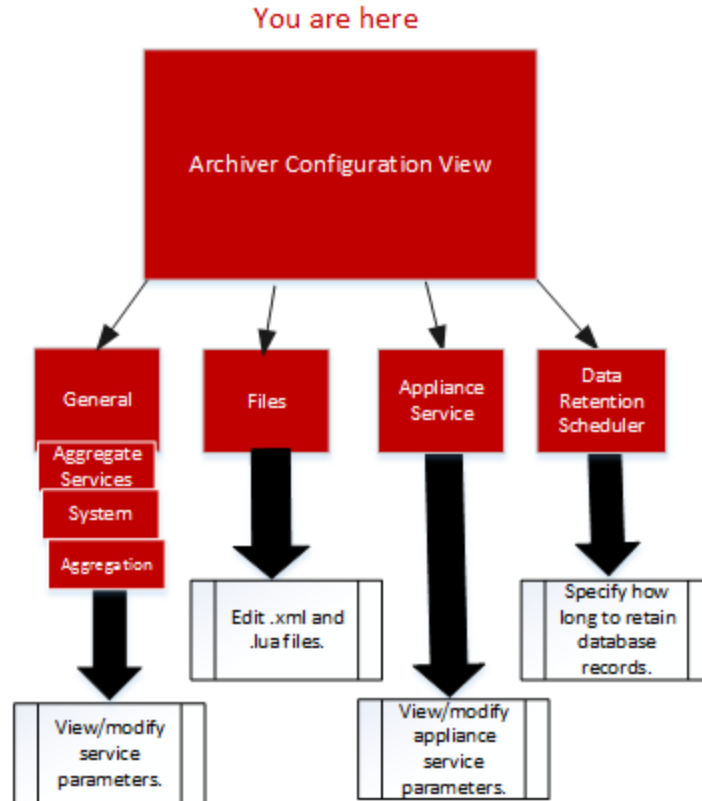
Applianceのパラメータ フィールド	説明
Logs	/logs/config。 「コア サービスのログ構成パラメータ」 を参照してください
REST	/rest/config。 「RESTインタフェースの構成パラメータ」 を参照してください
Services	/services/<service name>/config。 「コア サービス間接続の構成パラメータ」 を参照してください
System	/sys/config。 「コア サービスのシステム構成パラメータ」 を参照してください

Archiverサービスの構成ビュー

このトピックでは、NetWitness Platform Archiverで利用可能な構成設定のリストと説明を示します。

ワークフロー


次のワークフローは、Archiverサービスの構成タスクを示します。



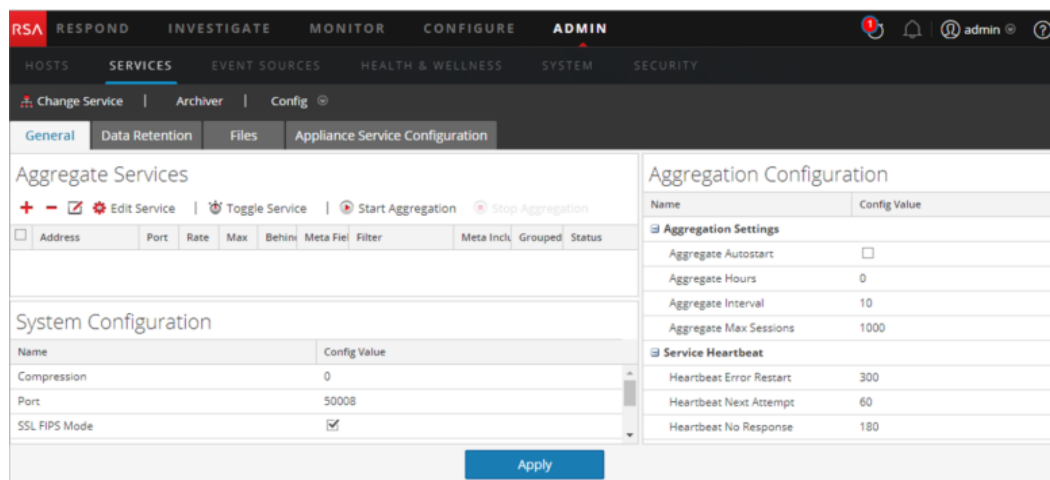
ロール	実行したいこと
管理者	集計用メタフィルタを構成する。手順については、「 <i>RSA NetWitness Platform Archiver構成ガイド</i> 」の「(オプション)集計用メタフィルタの構成」を参照してください。
管理者	グループ集計を構成する。手順については、「 <i>RSA NetWitness Platform導入ガイド</i> 」の「グループ集計の構成」を参照してください。

簡単な説明

[サービス]の[構成]ビューにアクセスするには、次の手順を実行します。

1. NetWitness Platformで、[管理]>[サービス]を選択します。
[管理]の[サービス]ビューが表示されます。
2. Archiverサービスを選択し、 > [表示]> [構成]を選択します。
Archiverサービスの[構成]ビューが表示されます。

これは、Archiverの[サービス]の[構成]ビューの例です。



Brokerサービスの構成パラメータ

このトピックでは、NetWitness Platform Brokerの構成パラメータについて説明します。次の表に、Broker構成パラメータのリストと説明を示します。

Brokerのパラメータフィールド	説明
Broker	/broker/config について「 集計の構成パラメータ 」を参照
aggregate.interval.behind	Brokerの処理が遅れている場合に集計の別のラウンドが要求されるまでの最小間隔(ミリ秒単位)。変更は即座に有効になります。
Database	/database/config について『 <i>NetWitness Platform</i> コア サービス データベース チューニングガイド』の「 データベース構成ノード 」を参照
Index	/index/config
index.dir	Brokerのデバイス マッピング ファイルが格納されるディレクトリ。サービスを再起動すると変更が有効になります。
language.filename	起動時にロードされるインデックスの言語仕様(XML)。変更を反映するには、サービスを再起動する必要があります。
Logs	/logs/config について「 コアサービスのログ構成パラメータ 」を参照
REST	/rest/config について「 RESTインタフェースの構成パラメータ 」を参照
SDK	/sdk/config について『 <i>NetWitness Platform</i> コア サービス データベース チューニングガイド』の「 SDK構成ノード 」のトピックと「 NetWitness Platformコアサービスのsystem.rolesモード 」を参照
Services	/services/<service name>/config について「 コアサービス間接続の構成パラメータ 」を参照
System	/sys/config について「 コアサービスのシステム構成パラメータ 」を参照

集計の構成パラメータ

このトピックでは、NetWitness PlatformのConcentratorやArchiverなど、集計を実行するサービスに共通して使用できる構成設定パラメータとその説明を示します。

この表は、集計サービスで集計を制御するパラメータとその説明を示しています。

構成パス	/concentrator/configまたは/archiver/config
aggregate.autostart	有効にした場合、サービスの再起動後、集計が自動的に開始されず。変更は即座に有効になります。
aggregate.buffer.size	1回の集計に使用されるバッファのサイズ(デフォルトの単位はKB)を表示します。バッファを大きくすることによって集計のパフォーマンスは向上しますが、クエリのパフォーマンスは低下する可能性があります。変更は集計の再開後に有効になります。
aggregate.crc	有効にした場合、すべての集計ストリームでCRC検査が適用されます。変更は即座に有効になります。
aggregate.hours	各サービスの統合の開始時に、どれだけ前の時点から集計を実行するかを時間で指定します。変更は即座に有効になります。
aggregate.interval	次の集計ラウンドがリクエストされるまでの最小時間(ミリ秒)を示します。変更は即座に有効になります。
aggregate.meta.page.factor	集計に使用されるセッションあたりの割り当て済みメタページ数を示します。サービスを再起動すると変更が有効になります。
aggregate.meta.perpage	データの1ページに格納されるメタの割り当て数を示します。サービスを再起動すると変更が有効になります。
aggregate.precache	Concentratorがアップストリーム サービスに対して次のラウンドの統合を事前キャッシュするかどうかを決定します。集計のパフォーマンスは向上しますが、クエリのパフォーマンスは低下する可能性があります。変更は即座に有効になります。
aggregate.sessions.max	各ラウンドで集計するセッションの数を示します。変更は集計の再開後に有効になります。
aggregate.sessions.perpage	データの1ページに格納されるセッション数を示します。サービスを再起動すると変更が有効になります。
aggregate.time.window	次の統合ラウンドがリクエストされるまでのすべてのサービスにおける最大の+/-タイム ウィンドウ(秒)が表示されます。ゼロに指定した場合、タイム ウィンドウがオフになります。変更は即座に有効になります。
consume.mode	ライセンスの制限に基づいて、Concentratorがローカルでのみ集計可能か、またはネットワーク経由で集計可能かを指定します。サービスを再起動すると変更が有効になります。
export.enabled	有効にした場合、セッション データのエクスポートが許可されます。サービスを再起動すると変更が有効になります。
export.expire.minutes	エクスポート キャッシュ ファイルが期限切れとなってフラッシュされるまでの時間(分)を表示します。変更は即座に有効になります。

構成パス	/concentrator/configまたは/archiver/config
export.format	データのエクスポート時に使用するファイル形式を指定します。サービスを再起動すると変更が有効になります。
export.local.path	エクスポート データをキャッシュするローカルの場所を表示します。オプションで割り当てられた最大サイズ(=#単位)を表示します。単位は、tがTB、gがGB、mがMBです。サービスを再起動すると変更が有効になります。
export.meta.fields	エクスポート対象のメタフィールドを指定します。複数のフィールドを指定する場合、カンマで区切って指定します。すべてのフィールドを指定する場合、アスタリスクを使用します。アスタリスクとフィールド リストを組み合わせて指定した場合、リストしたフィールドを除くすべてのフィールドが対象になります。フィールド リストのみの場合、それらのフィールドのみが対象となります。変更は即座に有効になります。
export.remote.path	リモート プロトコル(nfs://)とデータのエクスポート先を表示します。サービスを再起動すると変更が有効になります。
export.rollup	エクスポート ファイルのロールアップ間隔を指定します。サービスを再起動すると変更が有効になります。
export.session.max	エクスポート ファイルごとの最大セッション数を表示します。キャッシュを使用するエクスポート ファイルタイプの場合、この設定によってキャッシュメモリのサイズが決まります。ゼロに設定すると無制限になります。変更は即座に有効になります。
export.size.max	エクスポート ファイルごとの最大バイト数を表示します。キャッシュを使用するエクスポート ファイルタイプの場合、この設定によってキャッシュメモリのサイズが決まります。ゼロに設定すると無制限になります。変更は即座に有効になります。
export.usage.max	集計が停止される分岐点となる最大の使用済みキャッシュ領域の割合(%)を表示します。ゼロに設定すると無制限になります。変更は即座に有効になります。
heartbeat.error	サービス エラーの後、サービスへの再接続を試行する前に待機する秒数を表示します。変更は即座に有効になります。
heartbeat.interval	サービスへのハートビート間隔をミリ秒で示します。変更は即座に有効になります。
heartbeat.next.attempt	サービスへの再接続を試行する前に待機する秒数を示します。変更は即座に有効になります。
heartbeat.no.response	応答しないサービスをオフラインにする前に待機する秒数を示します。変更は即座に有効になります。

Concentratorサービスの構成パラメータ

このトピックでは、NetWitness Platform Concentratorで利用可能な構成パラメータについて説明します。

次の表に、Concentrator構成パラメータのリストと説明を示します。

Concentrator のパラメータ フィールド	説明
Concentrator	/concentrator/configについて「 集計の構成パラメータ 」を参照
Database	/database/configについて「 <i>NetWitness Platform</i> コア データベース チューニングガイド」の「データベース構成ノード」を参照
Index	/index/configについて「 <i>NetWitness Platform</i> コア データベース チューニングガイド」の「インデックス構成ノード」を参照
Logs	/logs/configについて「 コア サービスのログ構成パラメータ 」を参照
REST	/rest/configについて「 REST インタフェースの構成パラメータ 」を参照
SDK	/sdk/configについて「 <i>NetWitness Platform</i> コア データベース チューニングガイド」の「SDK構成ノード」および「 NetWitness Platform コア サービスのsystem.rolesモード」を参照
Services	/services/<service name>/configについて「 コア サービス間接続の構成パラメータ 」を参照
System	/sys/configについて「 コア サービスのシステム構成パラメータ 」を参照

コア サービスのログ構成パラメータ

このピックでは、すべての*NetWitness Platform* コア サービスに共通のログ構成パラメータについて説明します。

ログ構成はどの*NetWitness Platform* コア サービスでも同じです。

次の表に、ログ構成パラメータの説明を示します。

ログ構成フォルダ	/logs/config
log.dir	ログ データベースが格納されるディレクトリを表示します。オプションの最大割り当てサイズ(=#)の単位はMBです。サービスを再起動すると変更が有効になります。
log.levels	格納されるログ メッセージのタイプを制御します(カンマ区切り)。モジュール固有の設定は、次のように定義されます。<Module>=[debug info audit warning failure all none]。変更は即座に有効になります。
log.snmp.agent	SNMPトラップを受信するリモートのエージェントを設定します。
snmp.trap.version	取得およびトラップに使用するSNMPのバージョンを設定します(2cまたは3)。
snmpv3.engine.boots	SNMPv3エンジンの起動回数を表示します。このフィールドは、起動時に自動インクリメントされます。通常、ユーザが設定する必要はありません。

ログ構成フォルダ	/logs/config
snmpv3.engine.id	SNMPv3エンジンのIDを設定します。IDは、10～64桁の16進数になります。必要に応じて先頭に0xを付けることができます。同じホストで動作する各SAコアサービスについて、エンジンIDの末尾にサフィックス値を追加することができます。たとえば、SAコアホストに生成されたエンジンIDが0x1234512345である場合、Decoderサービスには0x123451234501を、Applianceサービスには0x123451234504のエンジンIDを設定することができます。
snmpv3.trap.auth.local.key	SNMPv3トラップの認証に使用するローカルキーを設定します。16桁または20桁の16進数(使用する認証プロトコルプロトコルによる)で、先頭に0xが付きます。MD5の場合は16桁の16進数に、SHAの場合は20桁の16進数になります。任意のアルゴリズムを使用してローカルキーを生成することができます。キーの値は手動で選択せずに、無作為な値を生成することを推奨します。
snmpv3.trap.auth.protocol	SNMPv3トラップ認証プロトコルプロトコル(なし、MD5、SHA)を表示します
snmpv3.trap.priv.local.key	SNMPv3トラップのプライバシーローカルキーを設定します。キーは16桁の16進数で、先頭に0xが付きます。
snmpv3.trap.priv.protocol	SNMPv3トラッププライバシープロトコル(なし、またはAES)を表示します
snmpv3.trap.security.level	SNMPv3トラップのセキュリティレベルを表示します。セキュリティレベルは、認証とプライバシーの使用の有無を示します。指定できる値はnoAuthNoPriv、authNoPriv、authPrivです。
snmpv3.trap.security.name	SNMPv3トラップ認証で使用するSNMPv3トラップのセキュリティ名を設定します。
syslog.size.max	Syslogに送信されるログの最大サイズを表示します(一部のSyslogデーモンでは、メッセージのサイズが大きすぎる場合に問題が発生することがあります)。ゼロに設定すると無制限になります。変更は即座に有効になります。

コアサービス間接続の構成パラメータ

このトピックでは、コアサービスが別のコアサービスに接続する方法を制御する構成パラメータについて説明します。たとえば、ConcentratorがDecoderに接続する場合、その接続はこれらの構成パラメータの設定によって制御されます。

コアサービスが別のコアサービスへの接続を確立する場合は常に、クライアントとして機能するサービスが、構成ツリーの/servicesフォルダに新しいサブフォルダを作成します。サブフォルダの名前はサービスの名前を反映し、host:portの形式をとります。たとえば、ConcentratorサービスからDecoderサービスへの接続のフォルダは、/services/reston-va-decoder:50004のようになります。各サービス接続フォルダ内には、構成パラメータを保存するconfigサブフォルダがあります。

次の表に、/services/host:port/configの構成パラメータの説明を示します。

構成パラメータ	説明
---------	----

構成パラメータ	説明
allow.nonssl.to.ssl	trueに設定した場合、非SSL接続からSSLサービスへの接続が許可されます。falseの場合、非SSLからSSLへの接続は拒否されます。変更は即座に有効になります。
compression	データ送信時に圧縮するかどうかを決定するconfigノードを表示します。圧縮が適用されるかどうかの分岐点となる送信バイト数を正の値で指定します。ゼロの場合、圧縮されません。
crc.checksum	データストリームをCRCチェックサムで検査するかどうかを決定するconfigノードを表示します。CRC検査が適用されるかどうかの分岐点となる送信バイト数を正の値で指定します。ゼロの場合、CRC検査は行われません。
ssl	接続のSSL暗号化を有効化または無効化するconfigノードを表示します。

コアサービスのシステム構成パラメータ

このトピックでは、すべてのNetWitness Platformコア サービスに共通する構成パラメータについて説明します。

次の表に、システム構成パラメータの説明を示します。

システム構成フォルダ	/sys/config
compression	正の値が設定されている場合、メッセージが圧縮される分岐点となる最小バイト数を表示します。ゼロの場合、メッセージは圧縮されません。変更は、次の接続時に反映されます。
crc.checksum	正の値が設定されている場合、ネットワークを介して送信されるメッセージにCRCチェックサム(クライアントによって検証)が付加される分岐点となる最小のバイト数を表示します。ゼロの場合、メッセージに対するCRCチェックサムの検査は実行されません。変更は、次の接続時に反映されます。
drives	使用率の統計を取得する監視対象ドライブを表示します。サービスを再起動すると変更が有効になります。
port	このサービスがリッスンするポートを表示します。サービスを再起動すると変更が有効になります。
scheduler	スケジュール設定されたタスクのフォルダを表示します。
service.name.override	集計を実行するアップストリーム サービスがホスト名の代わりに使用するオプションのサービス名を表示します。
ssl	有効にした場合、すべてのトラフィックがSSLで暗号化されます。サービスを再起動すると変更が有効になります。
stat.compression	有効にした場合、統計情報がデータベースに書き込まれる際に圧縮されます。サービスを再起動すると変更が有効になります。

システム構成フォルダ	/sys/config
stat.dir	履歴統計データベースが格納されるディレクトリを表示します。複数のディレクトリを指定する場合、セミコロンで区切ります。オプションで割り当てられた最大サイズ(=#単位)を表示します。単位は、tがTB、gがGB、mがMBです。サービスを再起動すると変更が有効になります。
stat.exclude	統計データベースから除外する統計のパス名を表示します。値を指定する場合、ワイルドカードを使用することができます。「?」は任意の1文字と一致します。「*」は、区切り文字(/)までのゼロ個以上の文字と一致します。「**」は、区切り文字を含むゼロ個以上の文字と一致します。変更は即座に有効になります。
stat.interval	システムで統計ノードが更新される頻度(ミリ秒単位)を指定します。変更は即座に有効になります。
threads	着信リクエストを処理するスレッド プール内のスレッド 数を表示します。変更は即座に有効になります。

Decoderサービスの構成パラメータ

このトピックでは、NetWitness Platform Decoderで利用可能な構成パラメータについて説明します。

Decoderのパラメータフィールド	説明
Decoder	/decoder/configについて「 DecoderおよびLog Decoderの構成パラメータ 」を参照
Database	/database/configについて「 <i>NetWitness Platform</i> コア データベース チューニング ガイド」の「データベース構成ノード」を参照
Index	/index/configについて「 <i>NetWitness Platform</i> コア データベース チューニング ガイド」の「インデックス構成ノード」を参照
Logs	/logs/configについて「 コアサービスのログ構成パラメータ 」を参照
REST	/rest/configについて「 RESTインタフェースの構成パラメータ 」を参照
SDK	/sdk/configについて「 <i>NetWitness Platform</i> コア データベース チューニング ガイド」の「SDK構成ノード」および「 NetWitness Platformコアサービスのsystem.rolesモード 」を参照
System	/sys/configについて「 コアサービスのシステム構成パラメータ 」を参照

DecoderおよびLog Decoderの構成パラメータ

このトピックは、DecoderサービスとLog Decoderサービスの両方に共通の構成パラメータのリストと、各構成パラメータの説明です。

構成パス	<service>/config
aggregate.buffer.size	1回の集計に使用されるバッファのサイズ(デフォルトの単位はKB)を表示します。バッファを大きくすることによって集計のパフォーマンスは向上しますが、収集のパフォーマンスは低下する可能性があります。変更は収集の再開後に有効になります。
aggregate.precache	Decoderがアップストリーム サービスに対して次のラウンドの集計を事前キャッシュするかどうかを決定します。集計のパフォーマンスは向上しますが、収集のパフォーマンスは低下する可能性があります。変更は即座に有効になります。
assembler.pool.ratio	アセンブラがアセンブリプロセスのために管理および使用するプールページの割合(%)を表示します。サービスを再起動すると変更が有効になります。
assembler.session.flush	完了した場合にセッションをフラッシュ(1)、またはパースされた場合にセッションをフラッシュ(2)します。サービスを再起動すると変更が有効になります。
assembler.session.pool	セッション プールのエントリーの数を表示します。サービスを再起動すると変更が有効になります。
assembler.size.max	セッションが取得する最大サイズを表示します。0に設定すると、セッションサイズの制限がなくなります。変更は即座に有効になります。
assembler.size.min	セッションが存続するために必要な最小サイズを表示します。変更は即座に有効になります。
assembler.timeout.packet	パケットがタイムアウトになるまでの秒数を表示します。変更は即座に有効になります。
assembler.timeout.session	セッションがタイムアウトになるまでの秒数を表示します。変更は即座に有効になります。
assembler.voting.weights	クライアントおよびサーバにマークされるセッション ストリームを決定するために使用される重み付け。変更は即座に有効になります。
capture.autostart	サービスが開始されたときに収集を自動的に開始するかどうかを指定します。サービスを再起動すると変更が有効になります。
capture.buffer.size	収集メモリバッファの割り当てサイズ(デフォルトの単位はMB)を表示します。サービスを再起動すると変更が有効になります。

構成パス	<service>/config
capture.device.params	<p>収集サービス固有のパラメータを表示します。サービスを再起動すると変更が有効になります。</p> <p>このフィールドで認識されるパラメータは、現在選択されている収集デバイスに固有です。パラメータのいずれかが現在の収集デバイスで認識されない場合、そのパラメータは無視されます。</p> <p>Log Decoderには、ログ イベント収集デバイスのみがあります。これは、いくつかのオプションのパラメータを受け入れます。</p> <ul style="list-style-type: none"> • use-envision-time: 1に設定すると、各イベントのtimeメタは、Log Collectorストリームからインポートされます。0である場合または設定しない場合は、インポートされたイベント時刻はevent.timeメタに格納されます。 • port: このパラメータは、デフォルト Syslogポート リスナー514を上書きする数値に設定できます。
capture.selected	現在の収集サービスとインタフェースを表示します。変更は即座に有効になります。
export.expire.minutes	エクスポート キャッシュ ファイルが期限切れとなってフラッシュされるまでの時間(分)を表示します。変更は即座に有効になります。
export.packet.enabled	有効にした場合、パケット データのエクスポートが許可されます。サービスを再起動すると変更が有効になります。
export.packet.local.path	パケットのエクスポート データをキャッシュするローカルの場所を表示します。オプションで割り当てられた最大サイズ(=#単位)を表します。単位は、tがTB、gがGB、mがMBです。サービスを再起動すると変更が有効になります。
export.packet.max	エクスポート ファイルごとの最大パケット数を表示します。キャッシュを使用するエクスポート ファイルタイプの場合、この設定によってキャッシュメモリのサイズが決まります。ゼロに設定すると無制限になります。変更は即座に有効になります。
export.packet.remote.path	リモート プロトコル(nfs://)とデータのエクスポート先を表示します。サービスを再起動すると変更が有効になります。
export.packet.size.max	エクスポート ファイルごとのパケットの最大バイト数を表示します。キャッシュを使用するエクスポート ファイルタイプの場合、この設定によってキャッシュメモリのサイズが決まります。ゼロに設定すると無制限になります。変更は即座に有効になります。
export.rollup	エクスポート ファイルのロールアップ間隔を指定します。サービスを再起動すると変更が有効になります。
export.session.enabled	有効にした場合、セッション データのエクスポートが許可されます。サービスを再起動すると変更が有効になります。
export.session.format	セッションのエクスポート時に使用するファイル形式を指定します。サービスを再起動すると変更が有効になります。

構成パス	<service>/config
export.session.local.path	セッションのエクスポート データをキャッシュするローカルの場所を表示します。オプションで割り当てられた最大サイズ(=#単位)を表示します。単位は、tがTB、gがGB、mがMBです。サービスを再起動すると変更が有効になります。
export.session.max	エクスポート ファイルごとの最大セッション数を表示します。キャッシュを使用するエクスポート ファイルタイプの場合、この設定によってキャッシュメモリのサイズが決まります。ゼロに設定すると無制限になります。変更は即座に有効になります。
export.session.meta.fields	エクスポート対象のメタフィールドを指定します。複数のフィールドを指定する場合、カンマで区切って指定します。すべてのフィールドを指定する場合、アスタリスクを使用します。アスタリスクとフィールド リストを組み合わせで指定した場合、リストしたフィールドを除くすべてのフィールドが対象になります。フィールド リストのみの場合、それらのフィールドのみが対象となります。変更は即座に有効になります。
export.session.remote.path	リモート プロトコル(nfs://)とデータのエクスポート先を表示します。サービスを再起動すると変更が有効になります。
export.session.size.max	エクスポート ファイルごとのセッションの最大バイト数を表示します。キャッシュを使用するエクスポート ファイルタイプの場合、この設定によってキャッシュメモリのサイズが決まります。ゼロに設定すると無制限になります。変更は即座に有効になります。
export.usage.max	エクスポート ファイルごとのセッションの最大バイト数を表示します。キャッシュを使用するエクスポート ファイルタイプの場合、この設定によってキャッシュメモリのサイズが決まります。ゼロに設定すると無制限になります。変更は即座に有効になります。
parse.threads	セッションの解析に使用するParserスレッドの数を表示します。ゼロに設定した場合、サーバによって値が決定されます。サービスを再起動すると変更が有効になります。
pool.packet.page.size	パケット ページのサイズを表示します(デフォルトはKB)。サービスを再起動すると変更が有効になります。
pool.packet.pages	Decoderが割り当てて使用するパケットのページ数を表示します。サービスを再起動すると変更が有効になります。
pool.session.page.size	セッション ページのサイズを表示します(デフォルトはKB)。サービスを再起動すると変更が有効になります。
pool.session.pages	Decoderが割り当てて使用するセッションのページ数を表示します。サービスを再起動すると変更が有効になります。

Log Decoderサービスの構成パラメータ

このトピックでは、RSA NetWitness Platform Log Decoderで利用可能な構成パラメータについて説明します。

Log Decoderの構成設定

次の表に、Log Decoderの構成設定のリストと説明を示します。

Log Decoder の設定フィールド	説明
Database	/database/config について「 <i>NetWitness Platform</i> コア データベース チューニング ガイド」の「データベース構成ノード」を参照
Decoder	/decoder/config について「 DecoderおよびLog Decoderの構成パラメータ 」を参照
Index	/index/config について「 <i>NetWitness Platform</i> コア データベース チューニング ガイド」の「インデックス構成ノード」を参照
Logs	/logs/config について「コア サービスのログ構成」を参照
REST	/rest/config について「REST インタフェースの構成」を参照
SDK	/sdk/config について「 <i>NetWitness Platform</i> コア サービス データベース チューニング ガイド」の「SDK構成ノード」および「コア サービスのsystem.rolesモード」を参照
System	/sys/config について「コア サービスのシステム構成」を参照

ログトークナイザーの構成設定

Log Decoderには、自動ログトークナイザーが未解析ログからメタ アイテムを作成する方法を制御する構成アイテムのセットがあります。ログトークナイザーは、認識可能なトークンのサブセットに対してそれぞれがスキャンする組み込み型のParserのセットとして実行されます。これらの各ネイティブParserの機能について、次の表に示します。これらのwordアイテムは、ConcentratorおよびArchiverのインデックス作成エンジンに取り込まれたときに、フルテキスト インデックスを形成します。parsers.disabled構成エントリを操作して、有効にするログトークナイザーを制御できます。

Parser名	説明	構成パラメータ
ログトークン	「word」メタ アイテムを生成する連続する文字の実行をスキャンします。	token.device.types、 token.char.classes、 token.max.length、 token.min.length、 token.unicode
IPSCAN	「ip.addr」メタ アイテムを生成するIPv4アドレスの可能性のあるテキストをスキャンします。	token.device.types
IPV6SCAN	「ipv6」メタ アイテムを生成するIPv6アドレスの可能性のあるテキストをスキャンします。	token.device.types
URLSCAN	「alias.host」、「filename」、「username」、「password」メタ アイテムを生成するURIの可能性のあるテキストをスキャンします。	token.device.types

Parser名	説明	構成パラメータ
DOMAINSCAN	「alias.host」、「tld」、「cctld」、「sld」メタアイテムを生成するドメイン名を表示するテキストをスキャンします。	token.device.types
EMAILSCAN	「email」および「username」メタを生成する可能性があるメールアドレスのテキストをスキャンします。	token.device.types
SYSLOGTIMESTAMPSCAN	Syslog形式のタイムスタンプである可能性のあるテキストをスキャンします。Syslogには、年とタイムゾーンが存在しません。このようなテキストが検出されると、UTC時間に正規化されて「event.time」メタアイテムが作成されます。	token.device.types
INTERNETTIMESTAMPSCAN	「event.time」メタアイテムを生成するRFC 3339形式のタイムスタンプの可能性のあるテキストをスキャンします。	token.device.types

これらは、ログトークナイザーの構成パラメータです。

Log DecoderのParser設定フィールド	説明
token.device.types	<p>rawテキストのトークンをスキャンする対象デバイスタイプのセットです。デフォルトでは、unknownに設定されており、パースされなかったログについてのみ、rawテキストがスキャンされます。ここでログタイプを追加することにより、パース済みログにテキストトークン情報を付加することができます。</p> <p>このフィールドが空の場合、ログのトークン化は無効です。</p>
token.char.classes	<p>このフィールドは、生成されるトークンのタイプを制御します。alpha、digit、space、punctの値を任意に組み合わせることができます。デフォルト値はalphaです。</p> <ul style="list-style-type: none"> • alpha: トークンに英文字を含めることができます。 • digit: トークンに数字を含めることができます。 • space: トークンにスペースやタブを含めることができます。 • punct: トークンに句読点を含めることができます。
token.max.length	<p>このフィールドは、トークンの長さに制限を設定します。デフォルト値は5文字です。最大文字数の設定により、Log Decoderでwordメタを格納するために必要な領域を制限できます。長いトークンを使用すると、メタデータベースでより多くの領域が必要になりますが、rawテキストの検索が若干高速になる場合があります。短いトークンを使用すると、検索時に、テキストクエリリゾルバーはrawログからより多くの読み取りを実行する必要がありますが、metadbとインデックスで使用する領域は大幅に削減されます。</p>

Log DecoderのParser設定フィールド	説明
token.min.length	これは、検索可能なテキストトークンの最小長です。トークンの最小長は、ユーザが検索ボックスに入力したときに結果を得ることができる最小文字数に対応します。推奨値はデフォルト値の3です。
token.unicode	このブール値の設定は、token.char.classes設定に従って文字を分類するときに、Unicode分類規則を適用するかどうかを制御します。trueに設定した場合、各ログはUTF-8でエンコードされたコードポイントのシーケンスとして処理され、UTF-8のデコードが実行された後に分類が実行されます。falseに設定した場合、各ログはASCII文字として処理され、ASCII文字の分類のみが実行されます。Unicode文字の分類には、Log Decoderでより多くのCPUリソースが必要です。非英語テキストのインデックス作成が不要な場合、この設定を無効にすることにより、Log DecoderのCPU使用率を削減できます。デフォルトでは有効になっています。

RESTインターフェースの構成パラメータ

このトピックでは、すべてのNetWitness Platformコア サービスに組み込まれているRESTインターフェースに使用できる構成パラメータをリストし、説明します。

設定

次の表に、REST構成パラメータのリストと説明を示します。

REST構成パス	/rest/config
cache.dir	一時ファイル用のホスト ディレクトリを表示します。サービスを再起動すると変更が有効になります。
cache.size	キャッシュ ディレクトリに格納される全てのファイルの合計の最大サイズ(デフォルトの単位はMB)を表示します。このサイズを超えると、古いファイルから削除されます。サービスを再起動すると変更が有効になります。
enabled	RESTサービスの有効と無効を切り替えます(1=オン、0=オフ)。サービスを再起動すると変更が有効になります。
port	RESTサービスがリッスンするポートを表示します。サービスを再起動すると変更が有効になります。
ssl	有効にした場合、すべてのRESTトラフィックがSSLで暗号化されます。デフォルトの「system」を指定した場合、/sys/config/sslでの設定が使用されます。サービスを再起動すると変更が有効になります。

NetWitness Platformコア サービスのsystem.rolesモード

すべてのNetWitness Platformコア サービスはロールベースの認証モードを提供します。このトピックでは、使用可能なモードと、各サービス内での構成方法について説明します。

`/sdk/config/system.roles` 構成ノードでは、メタおよびコンテンツに対するクエリと閲覧の権限をキー単位で設定します。このパラメータはデータ プライバシー管理機能をサポートします。ゼロ以外のいずれか1つの値を指定して有効化することにより、データ プライバシー責任者が特定のメタ キーとコンテンツへのアクセスを制御することができます。このパラメータは、NetWitness Platform ユーザー インタフェースから構成可能です(詳細については、「データ プライバシー管理ガイド」の「[データ プライバシー] タブ」を参照してください)。値を編集すると、変更がすぐに反映されます。

0の場合、SDKメタ キーに基づくサービス権限は無効化されます。

- 0: 無効

ゼロ以外の値を指定すると、データ プライバシー責任者はメタ キーを選択して、サービスの特定のユーザー ロールに対して表示するメタまたはコンテンツまたはその両方をフィルタするための、ホワイトリストまたはブラックリストとして使用できます。

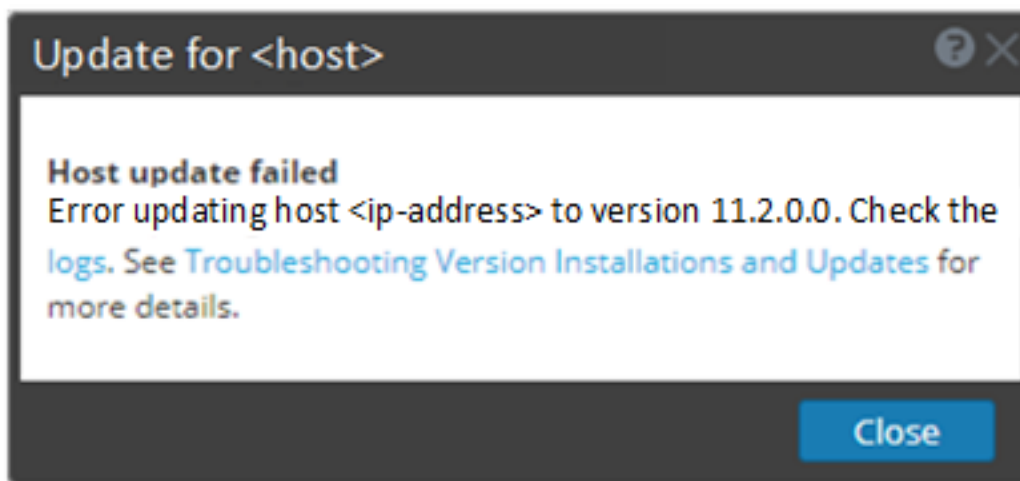
- 1: メタおよびコンテンツのホワイトリスト
- 2: メタのホワイトリスト
- 3: コンテンツのホワイトリスト
- 4: メタおよびコンテンツのブラックリスト
- 5: メタのブラックリスト
- 6: コンテンツのブラックリスト

インストールと更新のトラブルシューティング

このセクションでは、[ホスト]ビューでのホスト バージョンの更新およびホストへのサービスのインストールで問題が発生した場合に、[ホスト]ビューに表示されるエラー メッセージについて説明します。次のトラブルシューティングの解決策で解決できない更新またはインストール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。

ホストの更新失敗

エラー
メッセ
ージ



問題

更新バージョンを選択し、[更新]>[ホストの更新]をクリックすると、ダウンロード プロセスは成功しますが、更新プロセスは失敗します。

解決策

1. ホストへのバージョン更新の適用をもう一度試行します。
多くの場合、これで問題は解決します。
2. それでも新しいバージョンに更新できない場合は、次の手順を実行してください。
 - a. 実行時にNW Server上の次のログを監視します(たとえば、コマンドラインからtail -f コマンドを実行します)。


```

/var/netwitness/uax/logs/sa.log
/var/log/netwitness/orchestration-server/orchestration-server.log
/var/log/netwitness/deployment-upgrade/chef-solo.log
/var/log/netwitness/config-management/chef-solo.log
/var/lib/netwitness/config-management/cache/chef-stacktrace.out
                    
```

 これらのログの1つ以上にエラーが表示されます。
 - b. その問題を解決して、バージョンの更新を再度実行してください。
 - 原因1: deploy_adminのパスワードの有効期限が切れている。
解決策: deploy_adminのパスワードをリセットします。deploy_adminのパスワードをリセットするには、後述の「[deploy_admin/パスワードの有効期限切れ](#)」の解決策の手順を参照してください。
 - 原因2: deploy_adminのパスワードがNW Serverホストで変更されたが、非NW

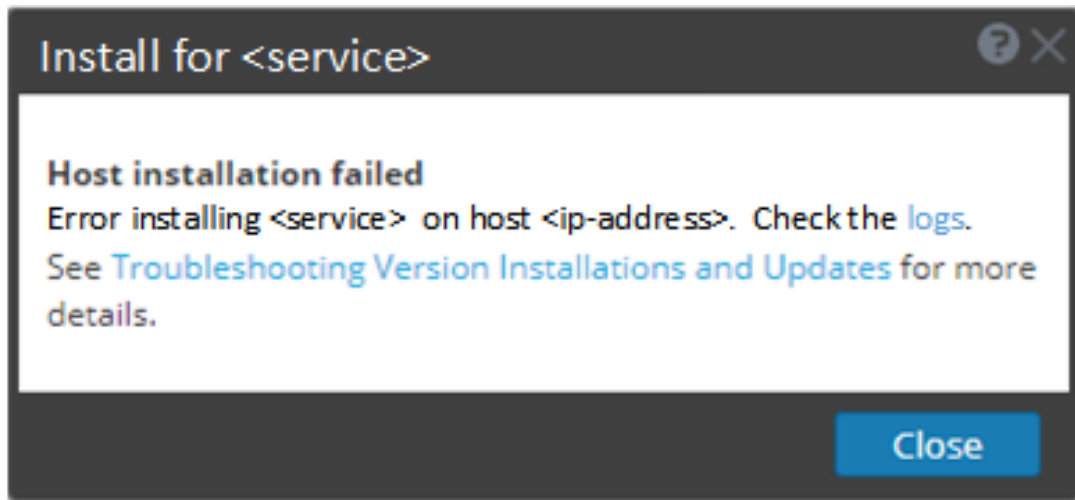
Serverホストでは変更されていない。この場合は、11.xのすべての非NW Serverホストで次のコマンドを実行し、NW Serverと同じ`deploy_admin`のパスワードを指定します。

```
/opt/rsa/saTools/bin/set-deploy-admin-password
```

- それでも更新を適用できない場合は、ステップ2のログを収集して、カスタマー サポートにお問い合わせください。

サービスの更新失敗

エラー
メッ
セージ



問題

ホストを選択して[インストール]をクリックすると、サービスのインストールプロセスが失敗します。

解決
策

- サービスのインストールを再度試行します。
多くの場合、これで問題は解決します。
- それでもサービスをインストールできない場合は、次の操作を試してください。
 - 実行時にNW Server上の次のログを監視します(たとえば、コマンドラインから`tail -f`コマンドを実行します)。


```
/var/netwitness/uax/logs/sa.log
/var/log/netwitness/orchestration-server/orchestration-server.log
/var/log/netwitness/deployment-upgrade/chef-solo.log
/var/log/netwitness/config-management/chef-solo.log
/var/lib/netwitness/config-management/cache/chef-stacktrace.out
```

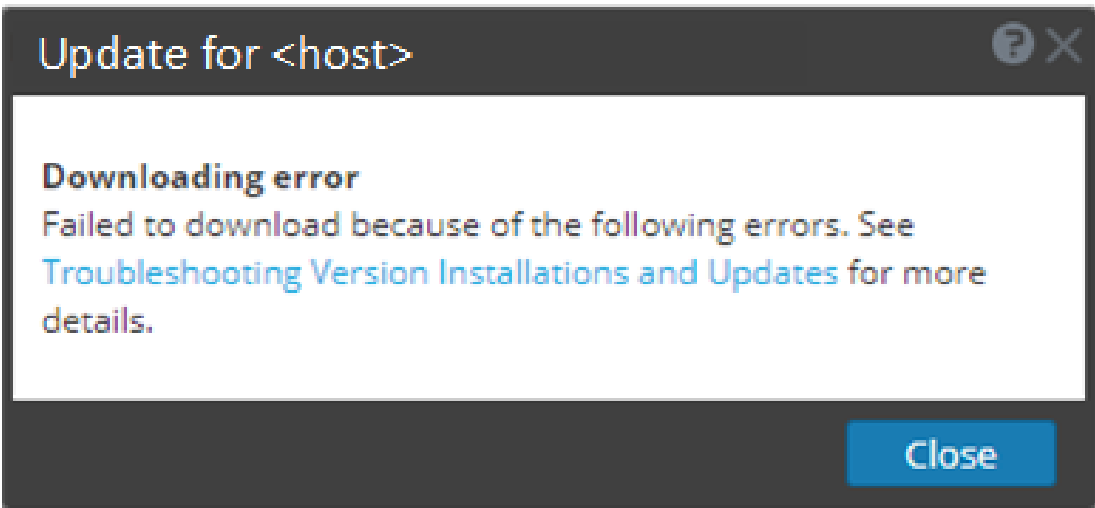
 これらのログの1つ以上にエラーが表示されます。
 - 問題を解決し、サービスを再度適用します。
 - 原因1: `nwsetup-tui`で誤った`deploy_admin`のパスワードを指定した。
解決策: `deploy_admin`のパスワードを復旧します。
`deploy_admin`のパスワードを復旧するには、次の手順を実行します。

1. NetWitness Platformのメニューで、[管理] > [セキュリティ] > [ユーザ] タブの順に選択します。
2. `deploy_admin`を選択し、[パスワードのリセット]をクリックします。
3. (オプション) [パスワードのリセット]ダイアログで、有効期限が切れた`deploy_admin`のパスワードを入力し、NetWitness Platformが再使用を拒否する場合は、次の手順を実行します。
 - a. SSHでNW Serverホストに接続し、次のコマンドを実行します。


```
security-cli-client --get-config-prop --prop-hierarchy
nw.security-client --prop-name
platform.deployment.password -quiet
```
 - b. インストール/オーケストレーションに失敗したホストにSSHで接続します。
 - c. 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。
- 原因2:`deploy_admin`パスワードの有効期限が切れている。

解決策: `deploy_admin`のパスワードをリセットします。`deploy_admin`のパスワードをリセットするには、後述の「[deploy_adminパスワードの有効期限切れ](#)」の解決策の手順を参照してください。
3. それでも更新を適用できない場合は、ステップ2のログを収集して、カスタマー サポートにお問い合わせください。

ホストの更新ダウンロード エラー

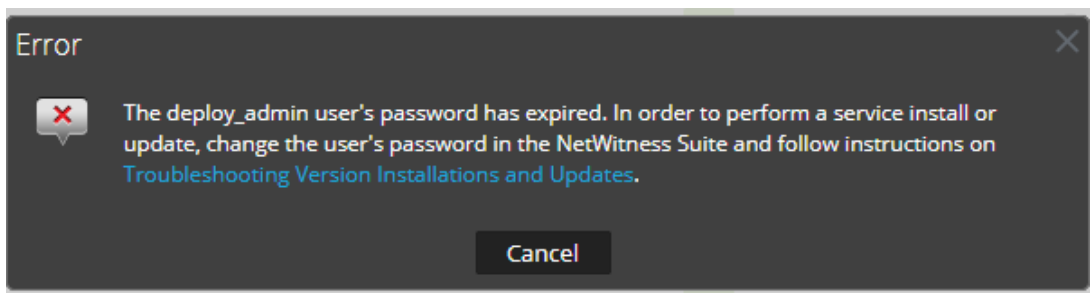
エラー メッ セージ	
問題	更新バージョンを選択し、[更新] > [ホストの更新]をクリックすると、ダウンロードが開始されますが異常終了します。
原因	バージョンのダウンロード ファイルのサイズが大きく、ダウンロードに時間がかかる場合があります。ダウンロード中に通信の問題が発生すると、ダウンロードは失敗します。

解決策

1. 再度ダウンロードしてください。
2. それでもダウンロードが失敗する場合は、「[コマンド ラインから更新を適用する\(Webアクセスなし\)](#)」の説明に従って、NetWitness Platform以外からのダウンロードを試みてください。
3. それでもアップロード ファイルをダウンロードできない場合は、カスタマー サポートにお問い合わせください。

deploy_admin/パスワードの有効期限切れ

エラーメッセージ



原因

deploy_adminユーザのパスワードの有効期限が切れている。

deploy_adminのパスワードをリセットします。

解決策

1. NetWitness Platformのメニューで、[管理] > [セキュリティ] > [ユーザ] タブの順に選択します。
2. deploy_adminを選択し、[パスワードのリセット]をクリックします。
 - [パスワードのリセット]ダイアログで有効期限切れのパスワードを入力し、deploy_adminが再使用を拒否しない場合、次の手順を実行します。
 - a. 期限が切れたdeploy_adminのパスワードを入力します。
 - b. [次回ログイン時にパスワードの変更を強制]チェックボックスをオフにします。
 - c. [保存]をクリックします。
 - [パスワードのリセット]ダイアログで有効期限切れのパスワードを入力し、deploy_adminが再使用を拒否する場合は、次の手順を実行します。
 - a. 11.xのNW Serverホストとそれ以外のすべてのホストで、次のコマンドを実行し、新しいdeploy_adminのパスワードを指定します。
`/opt/rsa/saTools/bin/set-deploy-admin-password`
 - b. インストール/オーケストレーションに失敗したホストで、nwsetup-tuiを実行し、新しいdeploy_adminのパスワードを指定します。