RSA NETWITNESS® PLATFORM

導入ガイド

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

基本情報

このガイドでは、NetWitness Platformの導入に関する基本的な要件および組織のニーズに対応するためのオプション シナリオについて説明します。小規模なネットワークでも、プランニングを実施し、ホストをオンラインにする準備を整えておくことによって、すべての作業を円滑に進めることができます。

注: このドキュメントで参照しているその他のドキュメントは、RSA Linkで入手可能です。NetWitness Plarform Logs & Network 11.xのすべてのドキュメントの一覧は、「マスター目次」で確認できます。

NetWitness Platformを導入する前に、多くの要素について検討する必要があります。次の項目は、これらの要素の一部です。これらの要素を検討するときには、将来の拡張とストレージの要件を予測する必要があります

- 組織の規模(つまり、NetWitness Platformを使用する場所とユーザの数)
- 処理する必要があるネットワーク データとログの量
- NetWitness Platformの各ユーザ ロールがジョブを効率的に実行するために必要なパフォーマンス。
- ダウンタイムの防止(つまり、単一障害点を回避する方法)。
- NetWitness Platformを実行する環境
  - RSA物理ホスト(RSAが提供するハードウェアでソフトウェアを実行)
    RSA物理ホストを導入する方法についての詳細は『*RSA NetWitness® Platform物理ホスト インストール ガイド*』を参照してください。
  - RSAが提供するソフトウェアのみ(ハードウェアなし)
    - オンプレミス仮想ホスト
      オンプレミス仮想ホストを導入する方法についての詳細は、「*RSA NetWitness® Platform仮想ホスト インストール ガイド*」を参照してください。
    - vCloud:
      - AWS(Amazon Web Services)
        AWSに仮想ホストを導入する方法についての詳細は、「*RSA NetWitness® Platform AWS導入ガイド*」を参照してください。
      - Azure
        Azureに仮想ホストを導入する方法についての詳細は、「*RSA NetWitness® Platform Azure導入ガイド*」を参照してください。

導入の基本情報

NetWitness Platformを導入する前に、次の事項を検討する必要があります。

- 組織の要件を検討し、導入プロセスを理解します。
- NetWitness Platformの導入の複雑性と対象範囲の概要を決定します。

プロセス

NetWitness Platformネットワークのコンポーネントとトポロジーは、導入環境によって大きく異なる場合があります。導入プロセスの開始前に慎重に計画を立てるようにしてください。初期計画には、次の項目が含まれます。

- 設置場所の要件と安全性の要件の検討。
- ネットワークアーキテクチャと使用ポートの確認。
- Archiver、Concentratorでのグループ統合および仮想ホストのサポート。

導入を開始する準備ができたら、通常は次の手順に従います。

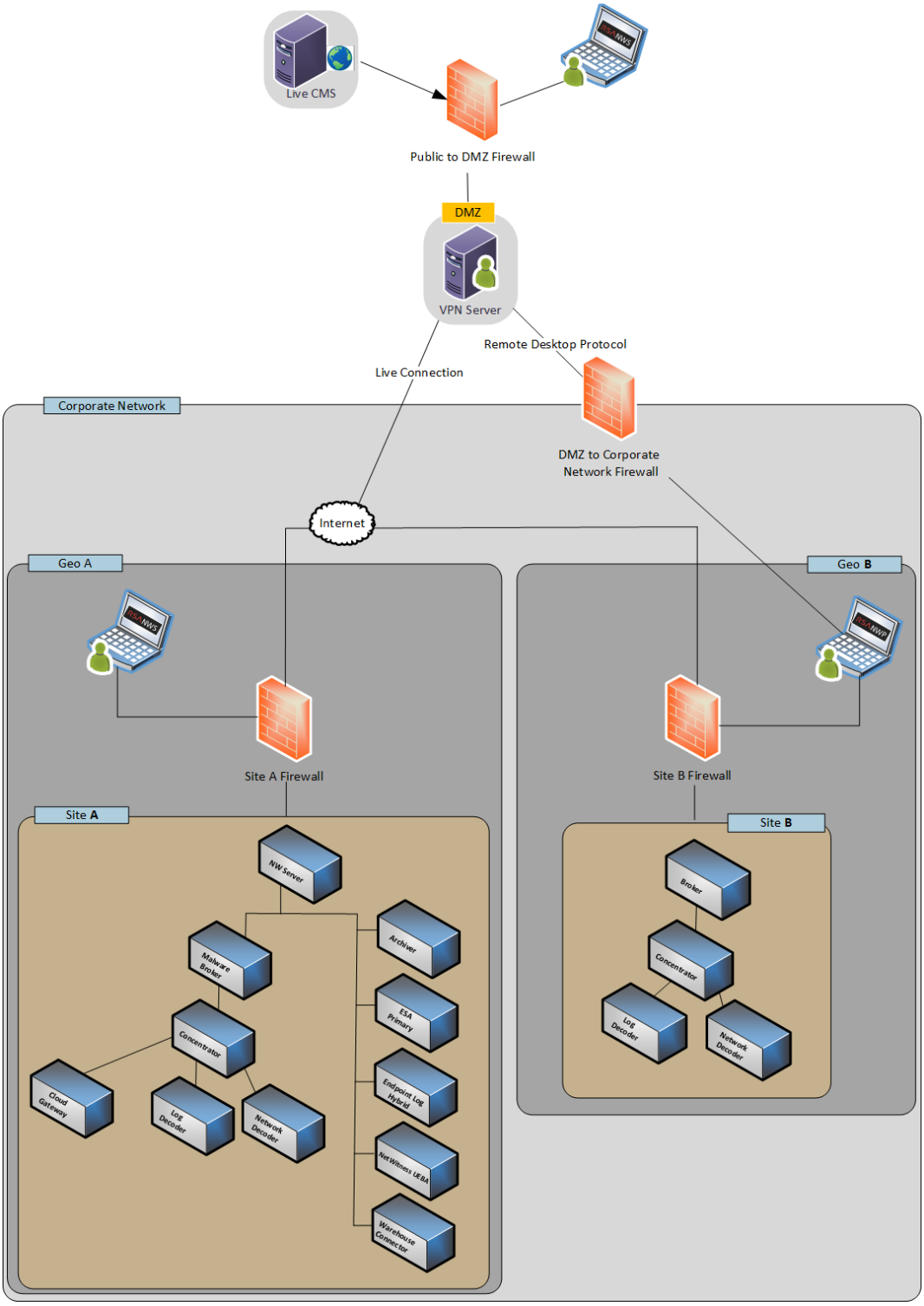
- RSA物理ホストの場合、次の手順に従います。
  1. 物理ホストを設置し、ネットワークに接続します(『RSA NetWitness® Platformハードウェア構成ガイド』および『*RSA NetWitness® Platform物理ホスト インストールガイド*』を参照)。
  2. NetWitness Platformのライセンスを設定します(「*RSA NetWitness® Platformライセンス ガイド*」を参照)。
  3. 個々の物理ホストとサービスを構成します(『*RSA NetWitness® Platformホストおよびサービス スタート ガイド*』を参照)。更新を適用する手順やバージョン アップグレードの準備手順も、このガイドで説明しています。
- オンプレミス仮想ホストの場合は、『*RSA NetWitness® Platform仮想ホスト インストールガイド*』の手順に従います。
- AWSの場合は、『*RSA NetWitness® PlatformAWS導入ガイド*』の手順に従います。
- Azureの場合は、『*RSA NetWitness® Platform Azure導入ガイド*』の手順に従います。

ホストとサービスを更新するときは、「*RSA NetWitness Platformホストおよびサービス スタート ガイド*」の「混在モードでの実行」トピックにある推奨ガイドラインに従います。

NetWitness Platformで使用されるホスト、ホスト タイプ、サービスについても理解しておく必要があります。「*RSANetWitness Platformホストおよびサービス スタート ガイド*」を参照してください。

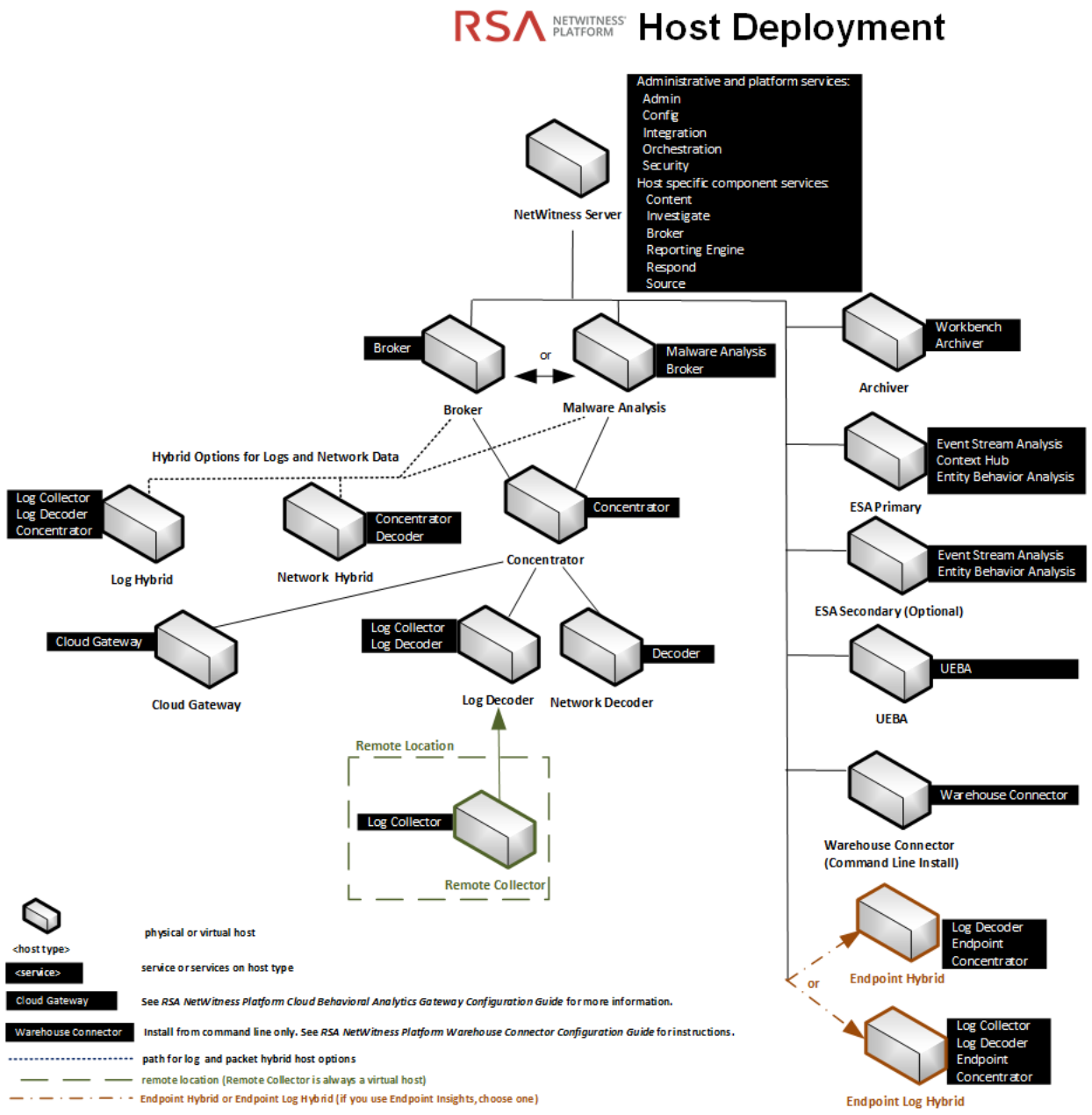
NetWitness Platform導入環境の概要図

次の図は、基本的な複数サイトのNetWitness Platform導入環境を示します。



RSA NetWitness Platform導入環境のホスト詳細図

次の図は、NetWitness Platformの物理マシンまたは仮想マシンを含む導入環境の例です。インストール方法の詳細については、NetWitness Platform「*物理ホスト インストール ガイド*」、「*仮想ホスト インストール ガイド*」、「*AWS導入ガイド*」、「*Azure導入ガイド*」を参照してください。NetWitness Plarform 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。



ネットワーク アーキテクチャとポート

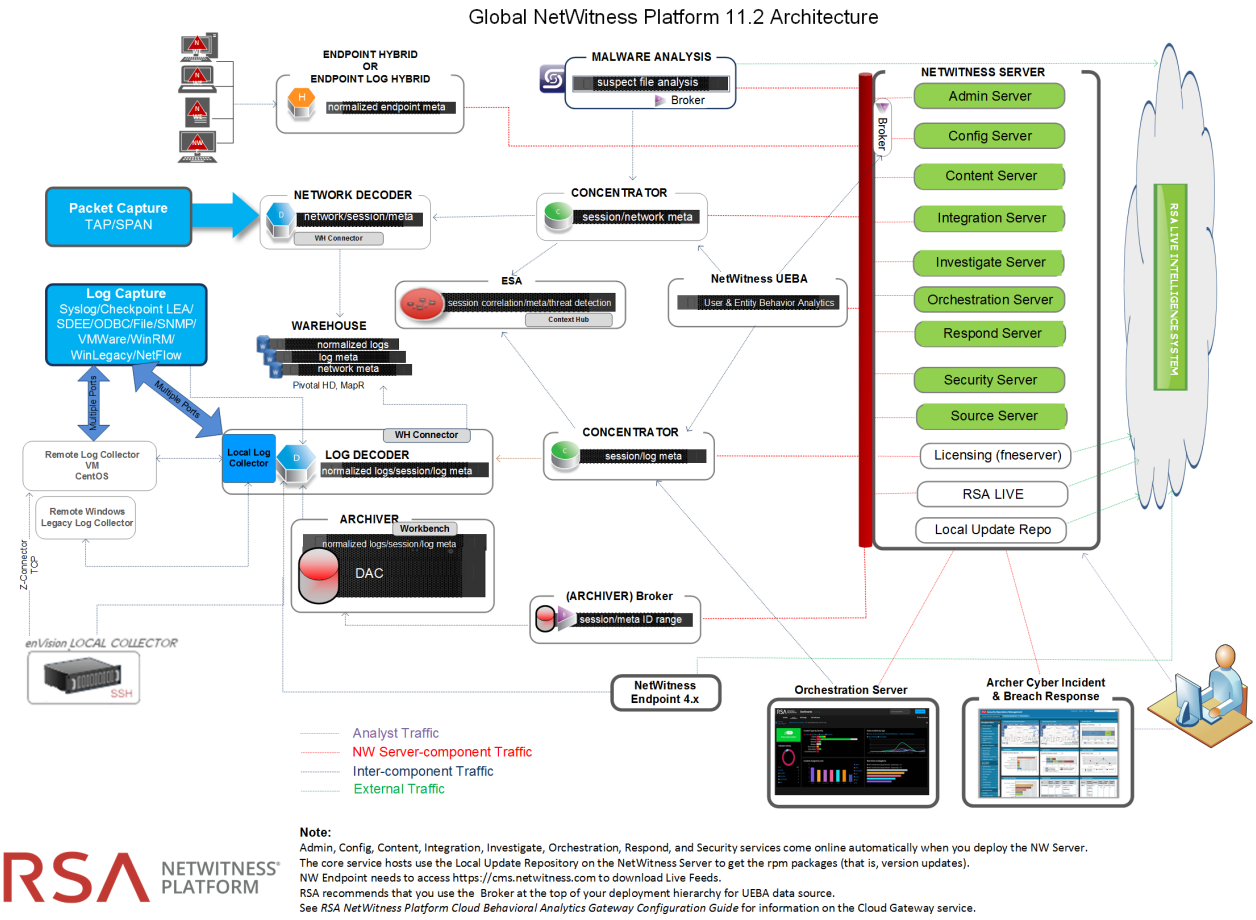
次の図とポートの一覧を参照して、NetWitness Platform導入環境のコンポーネントが相互に通信できるように、関連するすべてのポートを開いてください。

Endpointのアーキテクチャ図については、このトピックの終わりにある「NetWitness Endpoint Insightsのアーキテクチャ」を参照してください。

NetWitness Platformネットワーク アーキテクチャ図

次の図は、すべてのコンポーネントを含むNetWitness Platformのネットワーク アーキテクチャを示します。

注：NetWitness Platformコア ホストは、NTP(Network Time Protocol) による時刻同期のために、UDPポート123を通じてNetWitness Server(複数サーバ導入環境ではプライマリ サーバ) と通信する必要があります。



RSA NETWITNESS PLATFORM

Note:
Admin, Config, Content, Integration, Investigate, Orchestration, Respond, and Security services come online automatically when you deploy the NW Server.
The core service hosts use the Local Update Repository on the NetWitness Server to get the rpm packages (that is, version updates).
NW Endpoint needs to access https://cms.netwitness.com to download Live Feeds.
RSA recommends that you use the Broker at the top of your deployment hierarchy for UEBA data source.
See *RSA NetWitness Platform Cloud Behavioral Analytics Gateway Configuration Guide* for information on the Cloud Gateway service.

NetWitness Platformホストおよびサービス ポートの総合リスト

注：NetWitness Logsのイベント収集に使用されるポートについては、「*RSA NetWitness Platformログ収集の構成ガイド*」の「ログ収集の基礎」を参照してください。NetWitness Plarform 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。

このセクションでは、次のホストのポート仕様を説明します。

NW Serverホスト
Archiverホスト
Brokerホスト
Concentratorホスト
Endpoint Hybrid/Endpoint Log Hybridホスト
Event Stream Analysisホスト
Log Collectorホスト
Log Decoderホスト
Log Hybridホスト
Malwareホスト
Network Decoderホスト
Network Hybridホスト
UEBAホスト

NW Serverホスト

ソース ホスト	宛先ホスト	宛先ポート	コメント
管理ワークステーション	NW Server	TCP 443、80	nginx: NetWitness UI
NWホスト	NW Server	TCP 443	RSA更新リポジトリ
管理ワークステーション	NW Server	TCP 15671	RabbitMQ管理UI
NWホスト	NW Server	TCP 15671	RabbitMQ管理UI
管理ワークステーション	NW Server	TCP 22	SSH
NWホスト	NW Server	TCP 4505、4506	Saltマスター ポート
NWホスト	NW Server	TCP 5671	RabbitMQ-amqp
NW Server	NW Server	UDP 50514	監査データ - リモートSyslog
NWホスト	NW Server	UDP 123	NTP
NW Server	NWホスト	UDP 123	NTP
NWホスト	NW Server	TCP 27017	MongoDB
NW Server	NFSサーバ	TCP 111 2049 UDP 111 2049	iDRACインストール
NW Server	NW Endpoint	TCP 443、9443	NW Endpoint 4.x統合用

Archiverホスト

ソース ホスト	宛先ホスト	宛先ポート	コメント
管理ワークステーション	Archiver	TCP 15671	RabbitMQ管理UI
Archiver	NW Server	TCP 15671	RabbitMQ管理UI
Archiver	NW Server	TCP 443	RSA更新リポジトリ
管理ワークステーション	Archiver	TCP 22	SSH
NW Server	Archiver	TCP 56008(SSL) 、50008 (非SSL) 、50108(REST)	Archiverアプリケーション ポート
NW Server	Archiver	TCP 56006(SSL) 、50006 (非SSL) 、50106(REST)	NetWitnessアプライアンス ポート
NW Server	Archiver	TCP 5671	すべてのNWホストへの RabbitMQ(AMQPS) メッセージ バス。
NW Server	Archiver	TCP 514、6514、56007 (SSL) 、50007(非SSL) 、50107(REST) 、UDP 514	Workbenchアプリケーション ポート
Archiver	Archiver	UDP 50514	監査データ - リモートSyslog
Archiver	NFSサーバ	TCP 111 2049 UDP 111 2049	iDRACインストール

Brokerホスト

ソース ホスト	宛先ホスト	宛先ポート	コメント
管理ワークステーション	Broker	TCP 15671	RabbitMQ管理UI
Broker	NW Server	TCP 15671	RabbitMQ管理UI
Broker	NW Server	TCP 443	RSA更新リポジトリ
管理ワークステーション	Broker	TCP 22	SSH
NW Server	Broker	TCP 56003(SSL) 、50003 (非SSL) 、50103(REST)	Brokerアプリケーション ポート
NW Server	Broker	TCP 56006(SSL) 、50006 (非SSL) 、50106(REST)	NetWitnessアプライアンス ポート
NW Server	Broker	TCP 5671	すべてのNWホストへの RabbitMQ(AMQPS) メッセージ バス
Broker	Broker	UDP 50514	監査データ - リモートSyslog
Broker	NW Server	TCP 111 2049 UDP 111 2049	iDRACインストール

Concentratorホスト

ソース ホスト	宛先ホスト	宛先ポート	コメント
管理ワークステーション	Concentrator	TCP 15671	RabbitMQ管理UI
Concentrator	NW Server	TCP 15671	RabbitMQ管理UI
Concentrator	NW Server	TCP 443	RSA更新リポジトリ
管理ワークステーション	Concentrator	TCP 22	SSH
NW Server	Concentrator	TCP 56005(SSL) 、50005(非SSL) 、50105(REST)	Concentratorアプリケーション ポート
Malware	Concentrator	TCP 56005(SSL)	Malware
NW Server	Concentrator	TCP 56006(SSL) 、50006(非SSL) 、50106(REST)	NetWitnessアプライアンス ポート
NW Server	Concentrator	TCP 5671	すべてのNWホストへのRabbitMQ (AMQPS) メッセージ バス。
Concentrator	NFSサーバ	TCP 111 2049 UDP 111 2049	iDRACインストール
Concentrator	Concentrator	UDP 50514	監査データ - リモートSyslog

Endpoint HybridまたはEndpoint Log Hybrid

ソース ホスト	宛先ホスト	宛先ポート	コメント
Endpoint 11.2エージェント	Endpoint HybridまたはEndpoint Log Hybrid	TCP 443	NGINX HTTPS
Endpoint 11.2エージェント	Log Decoderまたは仮想Log Collector	TCP 514 (Syslog) UDP 514 (Syslog) TLS 6514	Windowsログ収集
Endpoint Server	Log Decoder(外部)	TCP 50102、56202、50202	メタを外部Log Decoderに転送
Endpoint Server	NW Server	TCP 443	RSA更新リポジトリ
NW Server	Endpoint HybridまたはEndpoint Log Hybrid	TCP 7050	UI Webトラフィック
Endpoint HybridまたはEndpoint Log Hybrid	NW Server	TCP 5671	メッセージ バス
Endpoint Server	NW Server	TCP 27017	MongoDB

Endpoint HybridまたはEndpoint Log HybridとNetWitness Endpoint 4.4

ソース ホスト	宛先ホスト	宛先ポート	コメント
NW Console Server (4.4.0.2以降)	Endpoint Hybrid	TCP 443	NGINX HTTPS
メタ サービス	Log Decoder	TCP 50102、56202、50202	NGINX HTTPS メタをLog Decoderに転送 Endpoint HybridまたはEndpoint Log HybridとNWE 4.4

ESA(Event Stream Analysis) ホスト

ソース ホスト	宛先ホスト	宛先ポート	コメント
管理ワークステーション	ESA	TCP 15671	RabbitMQ管理UI
ESAプライマリおよびセカンダリ	NW Server	TCP 15671	RabbitMQ管理UI
ESAプライマリおよびセカンダリ	NW Server	TCP 443	RSA更新リポジトリ
管理ワークステーション	ESA	TCP 22	SSH
NW Server、ESAセカンダリ	ESAプライマリ	TCP 27017	MongoDB
NW Server	ESAプライマリ	TCP 7005	Context Hub起動ポート : (ESAプライマリ)
NW Server	ESA	TCP 50030(SSL)	ESAアプリケーション ポート
NW Server	ESA	TCP 50035(SSL)	ESAアプリケーション ポート
NW Server	ESA	TCP 50036(SSL)	ESAアプリケーション ポート
NW Server	ESA	TCP 5671	すべてのNWホストへのRabbitMQ (AMQPS) メッセージ バス。
ESAプライマリおよびセカンダリ	cms.netwitness.com	TCP 443	Live
ESAプライマリおよびセカンダリ	NFSサーバ	TCP 111 2049 UDP 111 2049	iDRACインストール
ESAプライマリおよびセカンダリ	Active Directory	636(SSL) /389(非SSL)	
NW Server	ESA	80(HTTP) /443 (HTTPS) (REST)	
ESAプライマリ	Archer	443(SSL) /80(非SSL)	
ESAプライマリ	ESAプライマリ	TCP 7007	起動ポート
ESAプライマリ	ESAプライマリ	UDP 50514	監査データ - リモートSyslog

Log Collectorホスト

ソース ホスト	宛先ホスト	宛先ポート	コメント
管理ワークステーション	Log Collector	TCP 15671	RabbitMQ管理UI
Log Collector	NW Server	TCP 15671	RabbitMQ管理UI
Log Collector	NW Server	TCP 443	RSA更新リポジトリ
管理ワークステーション	Log Collector	TCP 22	SSH
Log Collector	ログ イベント ソース	「*ログ収集の構成ガイド*」を参照してください。NetWitness Plarform 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。	
ログ イベント ソース	Log Collector	TCP 514(Syslog) UDP 162(SNMP) 、514 (Syslog) 、2055(NetFlow) 4739(NetFlow) 、6343 (NetFlow) 、9995(NetFlow)	ログ収集ポート
ログ イベント ソース	Log Collector	TCP 21、64000、64001、64002、64003、64004、64005、64006、64007、64008、64009	ログ収集FTP/Sポート
NW Server	Log Collector	TCP 56001(SSL) 、50001 (非SSL) 、50101(REST)	Log Collectorアプリケーションポート
NW Server	Log Collector	TCP 56006(SSL) 、50006 (非SSL) 、50106(REST)	NetWitnessアプライアンスポート
NW Server	Log Collector	TCP 5671	すべてのNWホストへのRabbitMQ(AMQPS) メッセージ バス
Log Collector	Log Collector	UDP 50514	監査データ - リモートSyslog
Log Collector	NFSサーバ	TCP 111 2049 UDP 111 2049	iDRACインストール
Log Collector	仮想Log Collector	TCP 5671	プル モード
仮想Log Collector	Log Collector	TCP 5671	プッシュ モード

Log Decoderホスト

ソース ホスト	宛先ホスト	宛先ポート	コメント
管理ワークステーション	Log Decoder	TCP 15671	RabbitMQ管理UI
Log Decoder	NW Server	TCP 15671	RabbitMQ管理UI
Log Decoder	NW Server	TCP 443	RSA更新リポジトリ
管理ワークステーション	Log Decoder	TCP 22	SSH
Log Decoder	ログ イベント ソース	「*ログ収集の構成ガイド*」を参照してください。NetWitness Plarform 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。	
ログ イベント ソース	Log Decoder	TCP 514(Syslog) 、UDP 162 (SNMP) 、514(Syslog) 、2055(NetFlow) 、4739 (NetFlow) 、6343 (NetFlow) 、9995(NetFlow)	ログ収集ポート
ログ イベント ソース	Log Decoder	TCP 21、64000、64001、64002、64003、64004、64005、64006、64007、64008、64009	ログ収集FTP/Sポート
NW Server	Log Decoder	TCP 56001(SSL) 、50001 (非SSL) 、50101(REST)	Log Collectorアプリケーション ポート
NW Server	Log Decoder	TCP 56002(SSL) 、50002 (非SSL) 、56202 (Endpoint) 、50102(REST)	Log Decoderアプリケーション ポート
NW Server	Log Decoder	TCP 56006(SSL) 、50006 (非SSL) 、50106(REST)	NetWitnessアプライアンス ポート
NW Server	Log Decoder	TCP 5671	すべてのNWホストへの RabbitMQ(AMQPS) メッセージ バス
Log Decoder	Log Decoder	UDP 50514	監査データ - リモートSyslog
Log Decoder	Log Collector	TCP 6514	
Log Decoder	NFSサーバ	TCP 111 2049 UDP 111 2049	iDRACインストール

Log Hybridホスト

ソースホスト	宛先ホスト	宛先ポート	コメント
管理ワークステーション	Log Hybrid	TCP 15671	RabbitMQ管理UI
Log Hybrid	NW Server	TCP 15671	RabbitMQ管理UI
Log Hybrid	NW Server	TCP 443	RSA更新リポジトリ
管理ワークステーション	Log Hybrid	TCP 22	SSH
Log Collector	ログイベントソース	「*ログ収集の構成ガイド*」を参照してください。NetWitness Plarform 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。	
ログイベントソース	Log Hybrid	TCP 514(Syslog) 、UDP 162 (SNMP) 、514(Syslog) 、2055(NetFlow) 、4739 (NetFlow) 、6343 (NetFlow) 、9995(NetFlow)	ログ収集ポート
ログイベントソース	Log Hybrid	TCP 21、64000、64001、64002、64003、64004、64005、64006、64007、64008、64009	ログ収集FTP/Sポート
NW Server	Log Hybrid	TCP 56001(SSL) 、50001 (非SSL) 、50101(REST)	Log Collectorアプリケーションポート
NW Server	Log Hybrid	TCP 56002(SSL) 、50002 (非SSL) 、56202 (Endpoint) 、50102(REST)	Log Decoderアプリケーションポート
NW Server	Log Hybrid	TCP 56005(SSL) 、50005 (非SSL) 、50105(REST)	Concentratorアプリケーションポート
NW Server	Log Hybrid	TCP 56006(SSL) 、50006 (非SSL) 、50106(REST)	NetWitnessアプライアンスポート
NW Server	Log Hybrid	TCP 5671	すべてのNWホストへのRabbitMQ(AMQPS) メッセージバス
Log Hybrid	NFSサーバ	TCP 111 2049 UDP 111 2049	iDRACインストール

Malwareホスト

ソース ホスト	宛先ホスト	宛先ポート	コメント
管理ワークステーション	Malware	TCP 15671	RabbitMQ管理UI
Malware	NW Server	TCP 15671	RabbitMQ管理UI
Malware	NW Server	TCP 443	RSA更新リポジトリ
管理ワークステーション	Malware	TCP 22	SSH
NW Server	Malware	TCP 60007	Malwareアプリケーション ポート
NW Server	Malware	TCP 56006(SSL) 、50006 (非SSL) 、50106(REST)	NetWitnessアプライアンス ポート
NW Server	Malware	TCP 5671	すべてのNWホストへの RabbitMQ(AMQPS) メッセージバス。
NW Server	Malware	TCP 5432	Postgresql
NW Server	Malware	TCP 56003(SSL) 、50003 (非SSL) 、50103(REST)	Brokerアプリケーション ポート
Malware	panacea.threatgrid.com	TCP 443	ThreatGRID
Malware	cloud.netwitness.com	TCP 443	コミュニティの評価/OPSWAT
Malware	Malware	UDP 50514	監査データ - リモートSyslog
Malware	NFSサーバ	TCP 111 2049 UDP 111 2049	iDRACインストール

Network Decoderホスト

ソース ホスト	宛先ホスト	宛先ポート	コメント
管理ワークステーション	Network Decoder	TCP 15671	RabbitMQ管理UI
Network Decoder	NW Server	TCP 15671	RabbitMQ管理UI
Network Decoder	NW Server	TCP 443	RSA更新リポジトリ
管理ワークステーション	Network Decoder	TCP 22	SSH
NW Server	Network Decoder	TCP 56004(SSL) 、50004 (非SSL) 、50104(REST)	Network Decoderアプリケーション ポート
NW Server	Network Decoder	TCP 56006(SSL) 、50006 (非SSL) 、50106(REST)	NetWitnessアプライアンス ポート
NW Server	Network Decoder	TCP 5671	すべてのNWホストへの RabbitMQ(AMQPS) メッセージ バス
Network Decoder	Network Decoder	UDP 50514	監査データ - リモートSyslog
Network Decoder	NFSサーバ	TCP 111 2049 UDP 111 2049	iDRACインストール

Network Hybridホスト

ソース ホスト	宛先ホスト	宛先ポート	コメント
管理ワークステーション	Network Hybrid	TCP 15671	RabbitMQ管理UI
Network Hybrid	NW Server	TCP 15671	RabbitMQ管理UI
Network Hybrid	NW Server	TCP 443	RSA更新リポジトリ
管理ワークステーション	Network Hybrid	TCP 22	SSH
NW Server	Network Hybrid	TCP 56004(SSL) 、50004 (非SSL) 、50104(REST)	Network Decoderアプリケーション ポート
NW Server	Network Hybrid	TCP 56005(SSL) 、50005 (非SSL) 、50105(REST)	Concentratorアプリケーション ポート[512]
NW Server	Network Hybrid	TCP 56006(SSL) 、50006 (非SSL) 、50106(REST)	NetWitnessアプライアンス ポート
NW Server	Network Hybrid	TCP 5671	すべてのNWホストへの RabbitMQ(AMQPS) メッセージ バス
Network Hybrid	NFSサーバ	TCP 111 2049 UDP 111 2049	iDRACインストール

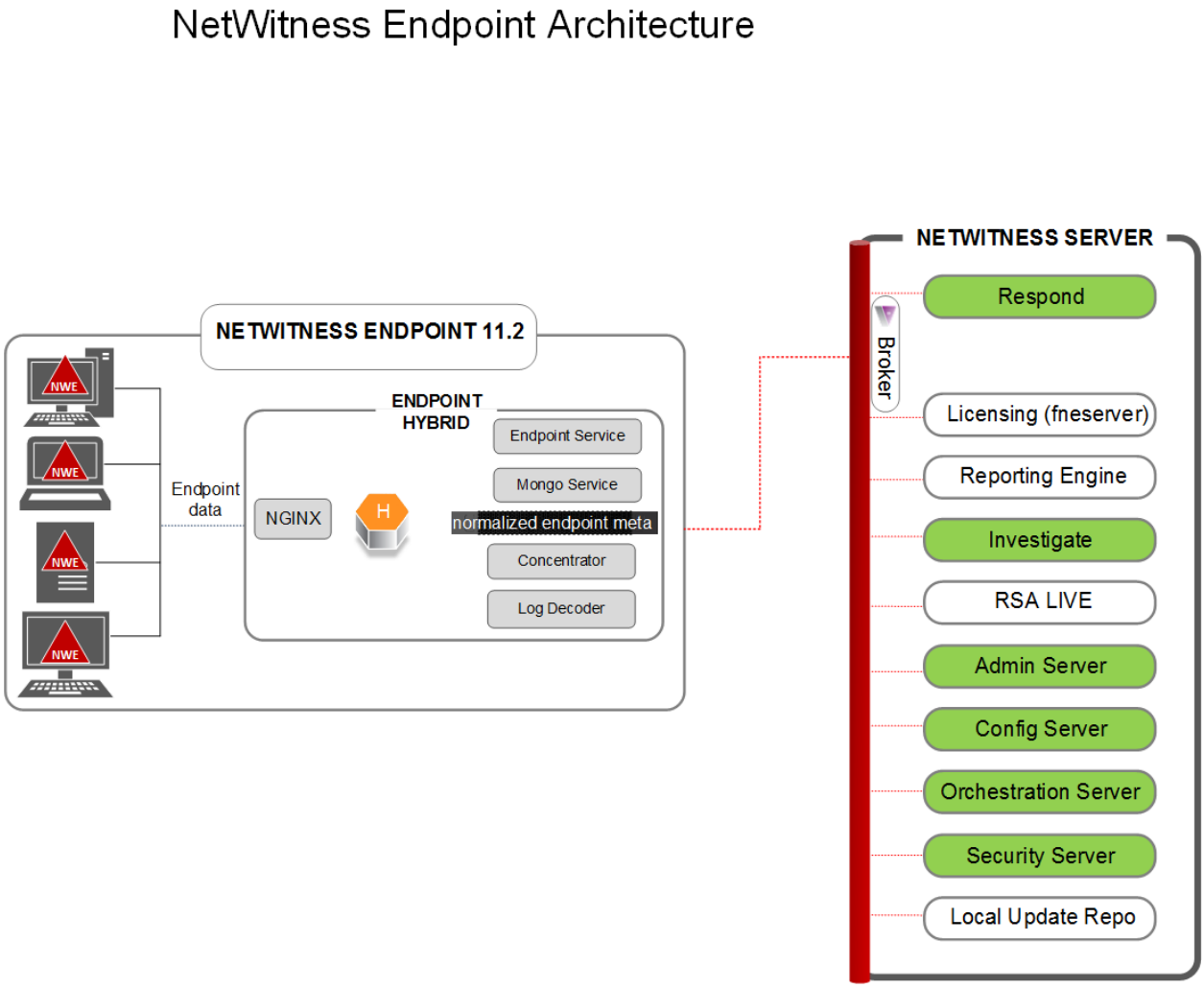
UEBAホスト

ソース ホスト	宛先ホスト	宛先ポート	コメント
UEBAサーバ	NW Server	TCP 443	RSA更新リポジトリ
UEBAサーバ	NW Server	TCP 56003(SSL) 、50003 (非SSL) 、50103(REST)	Brokerアプリケーション ポート
UEBAサーバ	NW Server	TCP 56005(SSL) 、50005 (非SSL) 、50105(REST)	Concentratorアプリケーション ポート
管理ワークステーション	UEBAサーバ	443	UEBAモニタリング
管理ワークステーション	UEBAサーバ	22	SSH
UEBAサーバ	NW Server	15671	UEBAアラートをRespondに転送

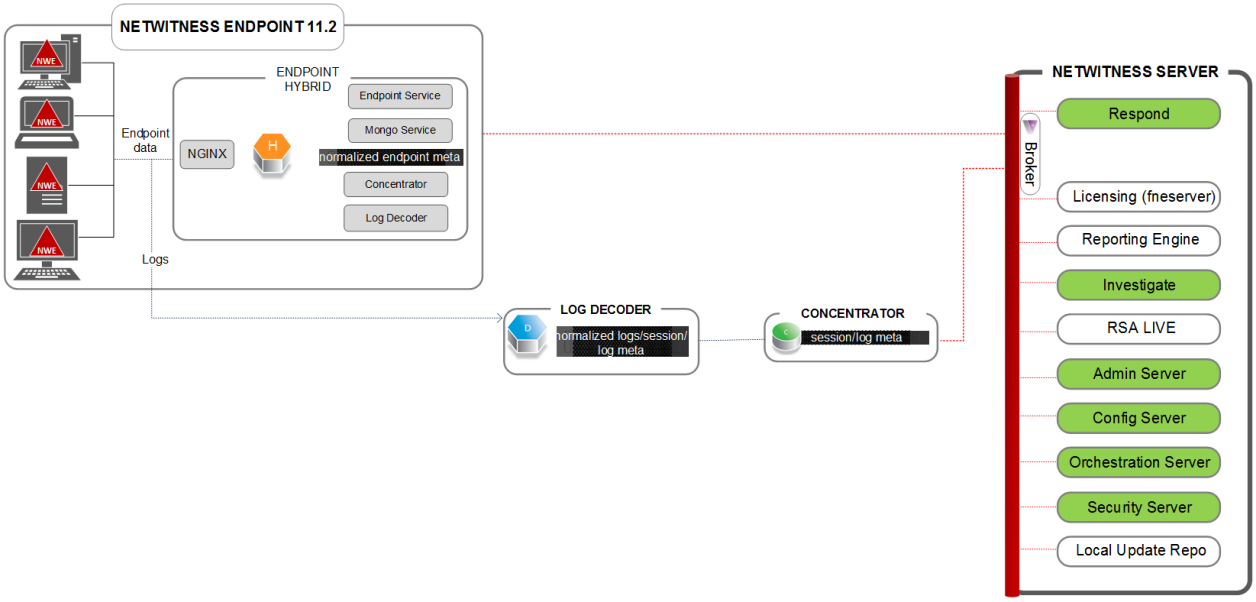
NetWitness Endpoint Insightsのアーキテクチャ

次の図は、NetWitness Endpoint Insightsのネットワーク アーキテクチャを示しています。

NetWitness Endpoint Insights 11.2

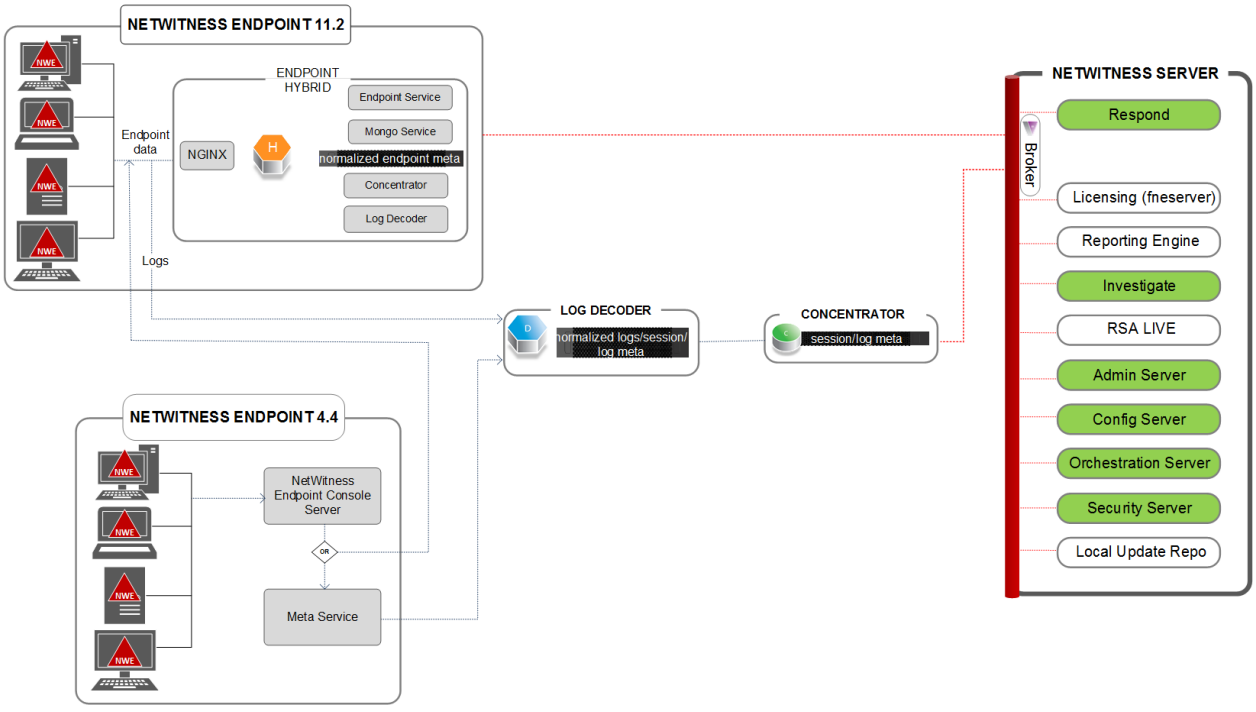


NetWitness Endpoint Insights 11.2とLog Decoder



NetWitness Endpoint 4.4とNetWitness Endpoint Insights 11.2の統合

NetWitness Endpoint Architecture



Endpoint Hybridで実行されるサービスの詳細については、「*RSA NetWitness Endpoint Insights*構成ガイド」を参照してください。NetWitness Plarform 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。

設置場所の要件と安全性

RSAデバイスの設置や保守を行う前に、このガイドを良くお読みの上、すべての警告や予防措置にご注意ください。

意図されている使用方法

この製品は、オフィス、学校、コンピュータ室、あるいはそれらと同等の商業的な屋内施設に設置可能な情報技術機器(ITE)として評価されています。このデバイスは、屋外タイプのケーブルに接続することは意図されていません。

サービス

このデバイスの内部には、ユーザによる保守が可能なコンポーネントは含まれていません。異常が発生した場合は、RSAにお問い合わせください。故障状態になると、システム内部が高温になることがあり、アラーム信号が発せられる場合があります。アラーム信号が発せられた場合は、すぐにデバイスを電源から外し、RSAまでご連絡ください。それ以上のデバイス操作は安全ではありません。負傷や資産の破損を招くおそれがあります。

安全に関する情報

サイトの選択

このシステムは、一般的なオフィス環境で運用するように設計されています。以下のような場所で使用してください。

- 清潔で乾燥し、空気中に浮遊する微粒子(通常の室内の粉塵以外)がない場所。
- 十分に換気され、直射日光やラジエータを含む熱源から離れた場所。
- 振動や物理的衝撃の発生源から離れた場所。
- 電気装置により発生する強力な電磁場から隔離されている場所。
- 雷雨の影響を受ける地域では、システムをサージ抑制器に接続することを推奨します。
- 適切に接地されたコンセントがある場所。
- 電源ケーブルを取り扱うのに十分なスペースがある場所。製品の主電源は切断された状態で提供されるため、電源に接続する必要があります。

機器の取り扱い方法

負傷や機器の損傷のリスクを減らすために:

- 機器を移動させたり持ち上げたりするときは、所在地の労働衛生および安全性に関する要件に従ってください。

- 機器を移動させたり持ち上げたりするときは、機械的補助またはその他の適切な補助を使用してください。
- 取り扱いが容易になるように、簡単に取り外しできるコンポーネントは取り外して重量を減らしてください。

電源および電気に関する警告

注意：予備電源のマークが付いている電源ボタンでは、システムのAC電源は完全にはオフになりません。システムが電源に接続されているときは常に5Vの予備電源がアクティブになっています。システムから電源を切断するには、AC電源ケーブルをコンセントから抜く必要があります。

- AC電源ケーブルを改造したり、または規格外のケーブルを使用したりしないでください。ACケーブルは、システムの各電源に1つずつ必要です。
- この製品には、ユーザによる保守が可能な部品は含まれていません。システムの内部を開かないようにしてください。
- ホットプラグの電源を交換するときは、サーバから取り外す前に、交換する電源に接続されている電源ケーブルを抜いてください。

ラックマウントに関する警告

- サーバや機器を引き出しているときにラックが倒れないように、しっかりと固定してください。ラックはメーカーの指示に従って取り付けてください。
- 機器をラックにマウントするときは、不均等な荷重によって危険な状態にならないように注意してください。
- ラックから機器を引き出すときは、一度に1つの機器のみ引き出します。
- 感電の危険を避けるため、ラックおよびラックに設置した各機器には、適切な保安用接地を行う必要があります。

冷却およびエアフロー

機器を設置するときは、機器の安全な運用に必要なエアフローを維持する必要があります。

アンテナを設置する場合

この機器は、ラジエータおよび人体から7cm以上離れて設置および運用する必要があります。このトランスミッターに使用するアンテナは、他のアンテナまたはトランスミッターと同じ場所に設置したり、一緒に使用したりしないでください。

グループ集計の構成

グループ集計を使用すると、複数のArchiverサービスまたはConcentratorサービスを1つのグループとして構成して、これらのサービス間で集計タスクを分担できます。複数のArchiverサービスまたはConcentratorサービスで複数のLog Decoderサービスからのデータを効率的に集計するように構成して、次のようなデータに対するクエリのパフォーマンスを向上させることができます。

- Archiverに格納されているデータ。
- Concentratorで処理されるデータ。

グループ集計導入に関するRSAの推奨事項

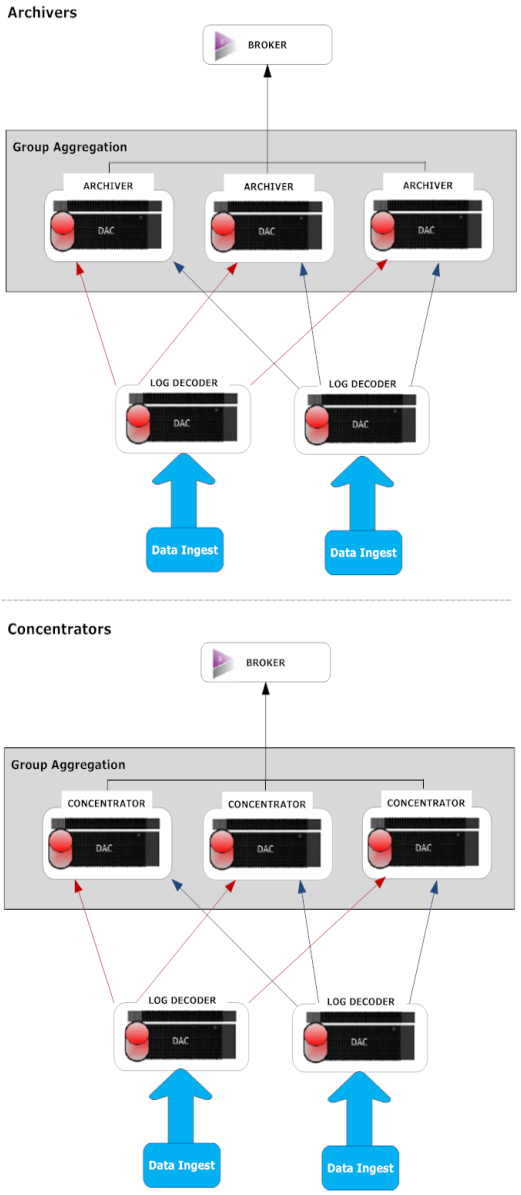
RSAでは、グループ集計の導入環境として次のような構成を奨しています。

- 1～ 2個のLog Decoder
- 3～5個のArchiverまたはConcentrator

グループ集計を使用するメリット

- RSA NetWitness® Platformのクエリの速度が向上します。
- 集計クエリ(件数と合計) のパフォーマンスが向上します。
- 調査のパフォーマンスが向上します。
- 調査目的で、データをより長い期間格納するオプションを使用できます。

次の図はグループ集計の構成を示しています。



任意の数のArchiverまたはConcentratorをまとめて、1つの集計グループを形成できます。すべての集計対象のセッションは、Aggregate Max Sessionsパラメータで定義したセッション数に基づいて、グループ内のArchiverまたはConcentratorサービスに分割されます。

たとえば、集計グループが2つのArchiverサービスまたは2つのConcentratorサービスで構成され、Aggregate Max Sessionsパラメータが10,000に設定されている場合は、サービス間でセッションが次の表で示すように分割されます。

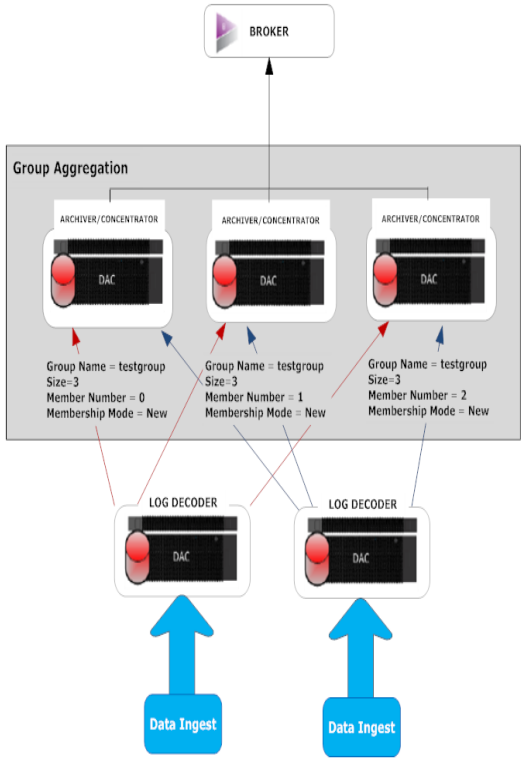
Archiver 0またはConcentrator 0	Archiver 1またはConcentrator 1
1 - 9,999	10,000 - 19,999
20,000 - 29,999	30,000 - 39,999
40,000 - 49,999	50,000 - 59,999

グループ集計の構成

複数のArchiverサービスまたはConcentratorサービスを1つのグループとして構成し、これらのサービス間で集計タスクを分担するには、この手順を実行します。

前提条件

グループ集計用のネットワーク設計を計画します。次の図にグループ集計の設定の例を示します。



次の表にあるグループ集計パラメータを理解し、グループ集計のプランを作成します。

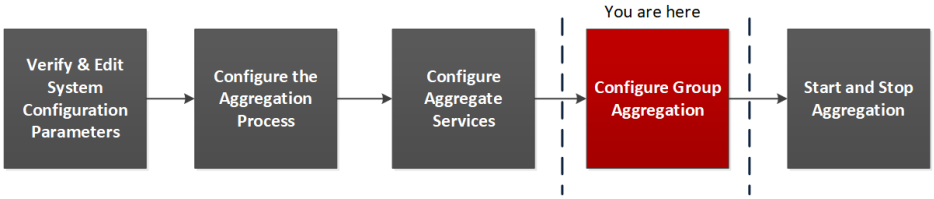
パラメータ	説明
グループ名	ArchiverまたはConcentratorが属するグループを指定します。 Log Decoderからデータを集計するグループは、任意の数だけ追加できます。Log Decoderは、[グループ名]パラメータによりどのArchiverまたはConcentratorサービスが連携しているかを特定します。グループ内のすべてのArchiverまたはConcentratorサービスで、同じグループ名が使用されます。
サイズ	集計グループ内のArchiverまたはConcentratorサービスの数を指定します。
メンバ番号	集計グループ内でのArchiverまたはConcentratorの番号を指定します。サイズがNのグループの場合、集計グループ内のArchiverまたはConcentratorサービスごとに、メンバ番号を0からN-1の間で設定する必要があります。 たとえば、集計グループのサイズが2の場合、1つのArchiverまたはConcentratorサービスのメンバ番号を0に指定し、もう1つのArchiverまたはConcentratorのメンバ番号を1に指定する必要があります。

パラメータ	説明
メンバシップ モード	2つのメンバシップ モードがあります。 • 新規 : 新しいArchiverまたはConcentratorサービスをメンバとして既存の集計グループに追加するか、または新しい集計グループを作成します。Archiverまたはconcentratorサービスは、集計対象サービスの既存のセッションを集計しません。グループ内の他のメンバにより、既存のすべてのセッションが集計済みであるとみなします。このArchiverまたはConcentratorサービスが集計するのは、新しいセッションのみです。 • 置換 : 既存の集計グループのメンバを置換します。Archiverまたは Concentratorサービスは、集計対象サービスで使用可能なセッションのうち、最も古いセッションから集計を開始します。

注 : メンバシップ モード パラメータが有効になるのは、集計対象のサービスのセッションが全く集計されていない場合のみです。セッションの一部でも集計されていれば、このパラメータは機能しません。

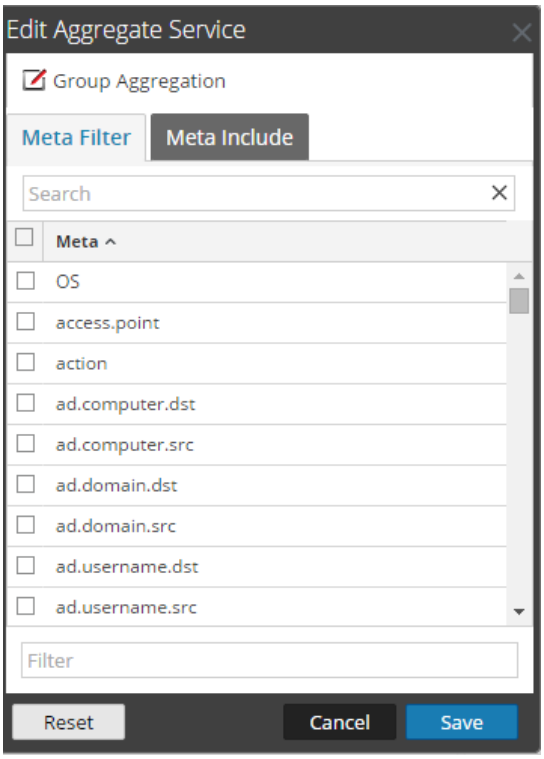
グループ集計の設定

次のワークフローは、グループ集計の構成の手順を示しています。



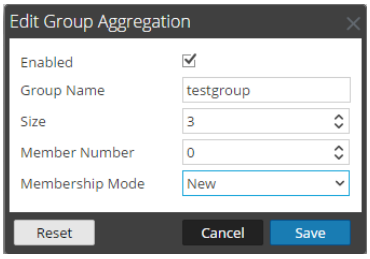
グループ集計を構成するには、次の手順を実行します。

1. ご使用の環境で複数のArchiverサービスまたはConcentratorサービスを構成します。すべてのサービスに必ず同じLog Decoderをデータソースとして追加してください。
2. 集計グループに含めるすべてのArchiverサービスまたはConcentratorサービスで次の手順を実行します。
   a. **[管理]＞[サービス]**に移動します。
   b. ArchiverサービスまたはConcentratorサービスを選択し、さらに[**アクション**]列で[**表示**]＞[**構成**]を選択します。
      ArchiverまたはConcentratorの[サービス]の[構成]ビューが表示されます。
   c. [**サービスの集計**]セクションで、[**Log Decoder**]を選択します。
   d. Log Decoderのステータスがオンラインの場合は、Toggle Service をクリックして、ステータスをオフラインに変更します。
   e. をクリックします。
      [**サービス集計の編集**]ダイアログが表示されます。



f. Group Aggregation をクリックします。

[**グループ集計の編集**]ダイアログが表示されます。



g. [**有効**]チェックボックスをオンにし、次のパラメータを設定します。

- [**グループ名**]フィールドに、グループ名を入力します。
- [**サイズ**]フィールドで、集計グループに含めるArchiverまたはConcentratorサービスの数を選択します。
- [**メンバ番号**]フィールドで、集計グループ内でのArchiverまたはConcentratorの番号を選択します。
- [**メンバシップモード**]ドロップダウンメニューでモードを選択します。

h. [**保存**]をクリックします。

i. [サービス]の[構成]ビューで、[**適用**]をクリックします。

j. 集計グループに追加するその他すべてのArchiverサービスまたはConcentratorサービスで、**ステップb**から**ステップi**を実行します。

3. ［**集計の構成**］セクションで、［**Aggregate Max Sessions**］パラメータを［**10000**］に設定します。