



Guide de déploiement

pour la version 11.0



Informations de contact

RSA Link à l'adresse <https://community.rsa.com> contient une base de connaissances qui répond aux questions courantes et fournit des solutions aux problèmes connus, de la documentation produit, des discussions communautaires et la gestion de dossiers.

Marques commerciales

Pour obtenir la liste des marques commerciales de RSA, rendez-vous à l'adresse suivante : france.emc.com/legal/emc-corporation-trademarks.htm#rsa.

Contrat de licence

Ce logiciel et la documentation qui l'accompagne sont la propriété d'EMC et considérés comme confidentiels. Délivrés sous licence, ils ne peuvent être utilisés et copiés que conformément aux modalités de ladite licence et moyennant l'inclusion de la note de copyright ci-dessous. Ce logiciel et sa documentation, y compris toute copie éventuelle, ne peuvent pas être remis ou mis de quelque façon que ce soit à la disposition d'un tiers.

Aucun droit ou titre de propriété sur le logiciel ou sa documentation ni aucun droit de propriété intellectuelle ne vous est cédé par la présente. Toute utilisation ou reproduction non autorisée de ce logiciel et de sa documentation peut faire l'objet de poursuites civiles et/ou pénales.

Ce logiciel est modifiable sans préavis et ne doit nullement être interprété comme un engagement de la part d'EMC.

Licences tierces

Ce produit peut inclure des logiciels développés par d'autres entreprises que RSA. Le texte des contrats de licence applicables aux logiciels tiers présents dans ce produit peut être consulté sur la page de la documentation produit du site RSA Link. En faisant usage de ce produit, l'utilisateur convient qu'il est pleinement lié par les conditions des contrats de licence.

Remarque sur les technologies de chiffrement

Ce produit peut intégrer une technologie de chiffrement. Étant donné que de nombreux pays interdisent ou limitent l'utilisation, l'importation ou l'exportation des technologies de chiffrement, il convient de respecter les réglementations en vigueur lors de l'utilisation, de l'importation ou de l'exportation de ce produit.

Distribution

EMC estime que les informations figurant dans ce document sont exactes à la date de publication. Ces informations sont modifiables sans préavis.

février 2018

Sommaire

Déploiement de NetWitness Suite	5
Processus basique de déploiement	6
Processus	6
Diagramme de déploiement NetWitness Suite	8
Environnement de l'appliance physique RSA	9
déploiement: Architecture réseau et ports	12
Schéma de l'architecture réseau NetWitness Suite	12
Liste complète des hôtes et des ports de service NetWitness Suite	12
Hôte de serveur NW	13
Hôte Archiver	14
Hôte Broker	14
Hôte Concentrator	15
Hôte Event Stream Analysis (ESA)	16
Hôte Log Collector	18
Hôte de Log Decoder	19
Hôte Log Hybrid	20
Hôte Malware	22
Hôte Packet Decoder	23
Hôte Packet Hybrid	24
Exigences du site et sécurité	25
Usages prévus de l'application	25
Service	25
Informations relatives à la sécurité	25
Sélection de site	25
Pratiques de manipulation de l'équipement	26
Avertissements relatifs à l'alimentation et à l'électricité	26
Avertissements relatifs au montage en rack	26
Refroidissement et circulation de l'air	27
Placement de l'antenne	27

Configurer l'agrégation de groupes	28
Recommandations à propos du déploiement d'agrégation de groupes RSA	28
Avantages de l'utilisation de l'agrégation de groupes	28
Configurer l'agrégation de groupes	30
Conditions préalables	30
	32
Configurer l'agrégation de groupes	32

Déploiement de NetWitness Suite

Ce guide décrit les exigences de base d'un déploiement NetWitness Suite. De plus, il présente des scénarios optionnels pour répondre aux besoins de votre entreprise. Vous pouvez utiliser des réseaux distribués pour installer les composants Broker, Concentrator, Decoder et Log Decoder sur différents sites avant l'installation et la mise en ligne de Serveur NetWitness. Même dans de petits réseaux, une planification peut garantir un déroulement sans accroc une fois que vous êtes prêt à mettre les hôtes en ligne.

Remarque : Ce document fait référence à des documents supplémentaires disponibles sur RSA Link. Accédez à la [Table des matières principale](#) pour la version 11.0 trouver des documents NetWitness Suite 11.0.

Il existe de nombreux facteurs à prendre en compte avant de déployer NetWitness Suite. Les éléments suivants ne sont que quelques-uns de ces facteurs. Vous devez estimer les besoins en matière de croissance et de stockage lorsque vous prenez ces facteurs en considération.

- Taille de votre entreprise (nombre de sites et d'utilisateurs NetWitness Suite).
- Volume de paquets et de logs à traiter.
- Performances dont chaque rôle d'utilisateur NetWitness Suite a besoin pour travailler efficacement.
- Prévention des périodes d'interruption (comment éviter un point unique de défaillance).
- L'environnement dans lequel vous comptez exécuter NetWitness Suite
 - Les appliances RSA (logiciels en cours d'exécution sur le matériel fourni par RSA)
. Reportez-vous au *Guide d'Installation d'hôtes physiques RSA NetWitness® Suite* pour obtenir des instructions détaillées sur la façon de déployer les appliances RSA.
 - Logiciels uniquement fournis par RSA :
 - Hôtes virtuels sur site
 - vCloud :
 - Amazon Web Services (AWS)
 - Azure

Processus basique de déploiement

Avant de pouvoir déployer NetWitness Suite vous devez :

- Prendre en considération les exigences de votre entreprise et comprendre le processus de déploiement.
- Avoir une vue d'ensemble de la complexité et de la portée d'un déploiement NetWitness Suite.

Processus

Les composants et la topologie d'un réseau NetWitness Suite peuvent varier largement d'une installation à une autre et doivent être planifiés soigneusement avant le début du processus. La planification initiale comprend :

- La prise en compte des exigences liées au site et à la sécurité.
- L'examen de l'utilisation de l'architecture réseau et des ports.
- La prise en charge de l'agrégation de groupes sur les Concentrators et les Archivers ainsi que sur les hôtes virtuels .

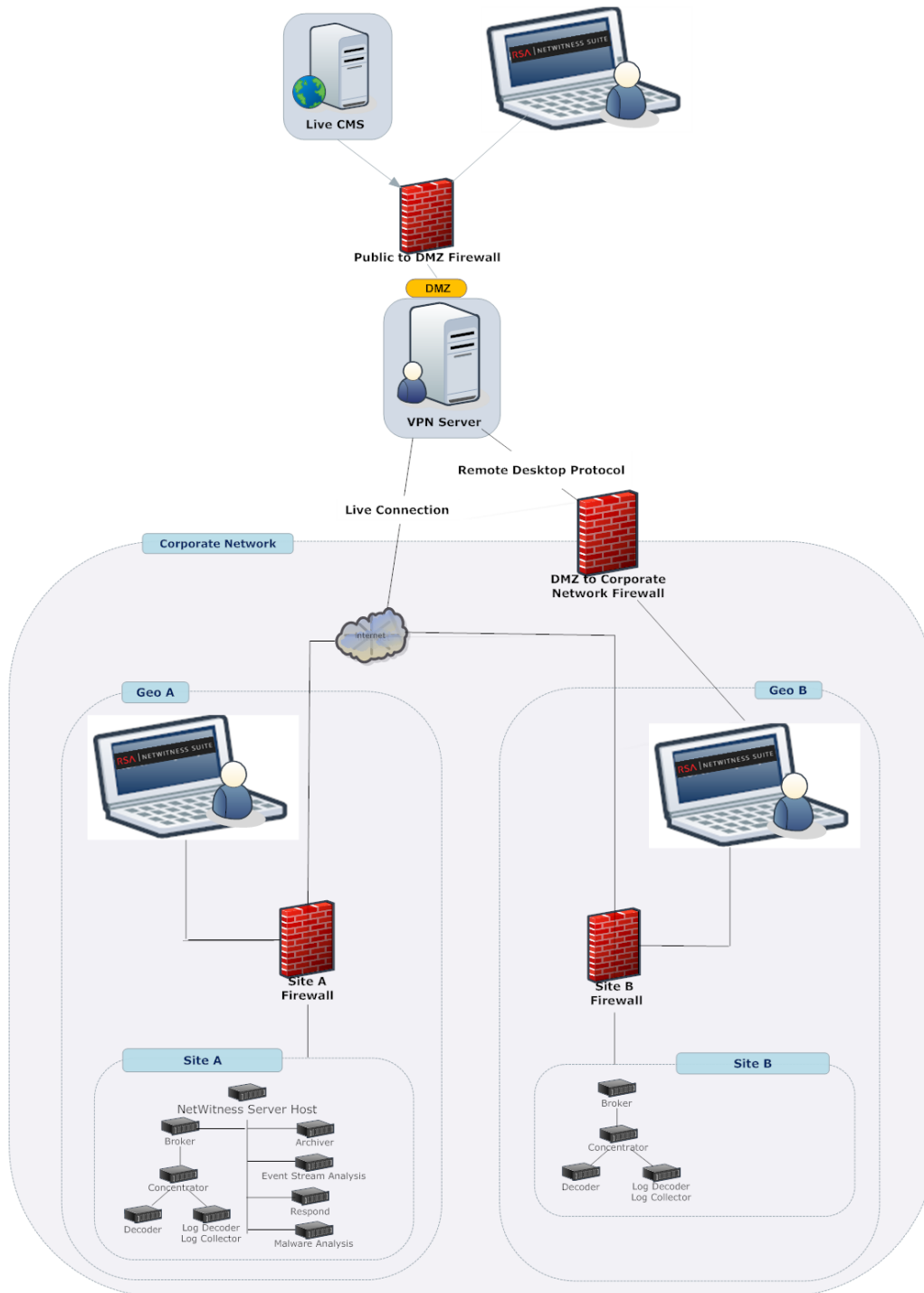
Lorsque vous êtes prêt à commencer le déploiement, la séquence générale est la suivante :

- Pour les appliances RSA :
 1. Installez les appliances et connectez-les au réseau comme décrit dans les Guides de configuration du matériel RSA NetWitness® Suite et le *Guide d'Installation d'hôtes physiques RSA NetWitness® Suite* .
 2. Configurez les licences de NetWitness Suite comme décrit dans le *Guide d'octroi des licences RSA NetWitness® Suite* .
 3. Configurez les différents services et appliances comme décrit dans le *RSA NetWitness® Suite Guide de mise en route de l'hôte et des services*. Ce guide décrit aussi les procédures d'application des mises à jour et de préparation des mises à niveau des versions.
- Pour les hôtes virtuels sur site, suivez les instructions du *Guide de configuration d'hôte virtuel RSA NetWitness® Suite* .
- Pour AWS, suivez les instructions du *Guide de déploiement AWS RSA NetWitness® Suite* .
- Pour Azure, suivez les instructions du *Guide de déploiement Azure RSA NetWitness® Suite* .

Lors de la mise à jour des hôtes et des services, suivez les directives recommandées dans la section « Exécution en mode mixte » dans le *Guide de mise en route de l'hôte et des services RSA NetWitness Suite*.

Diagramme de déploiement NetWitness Suite

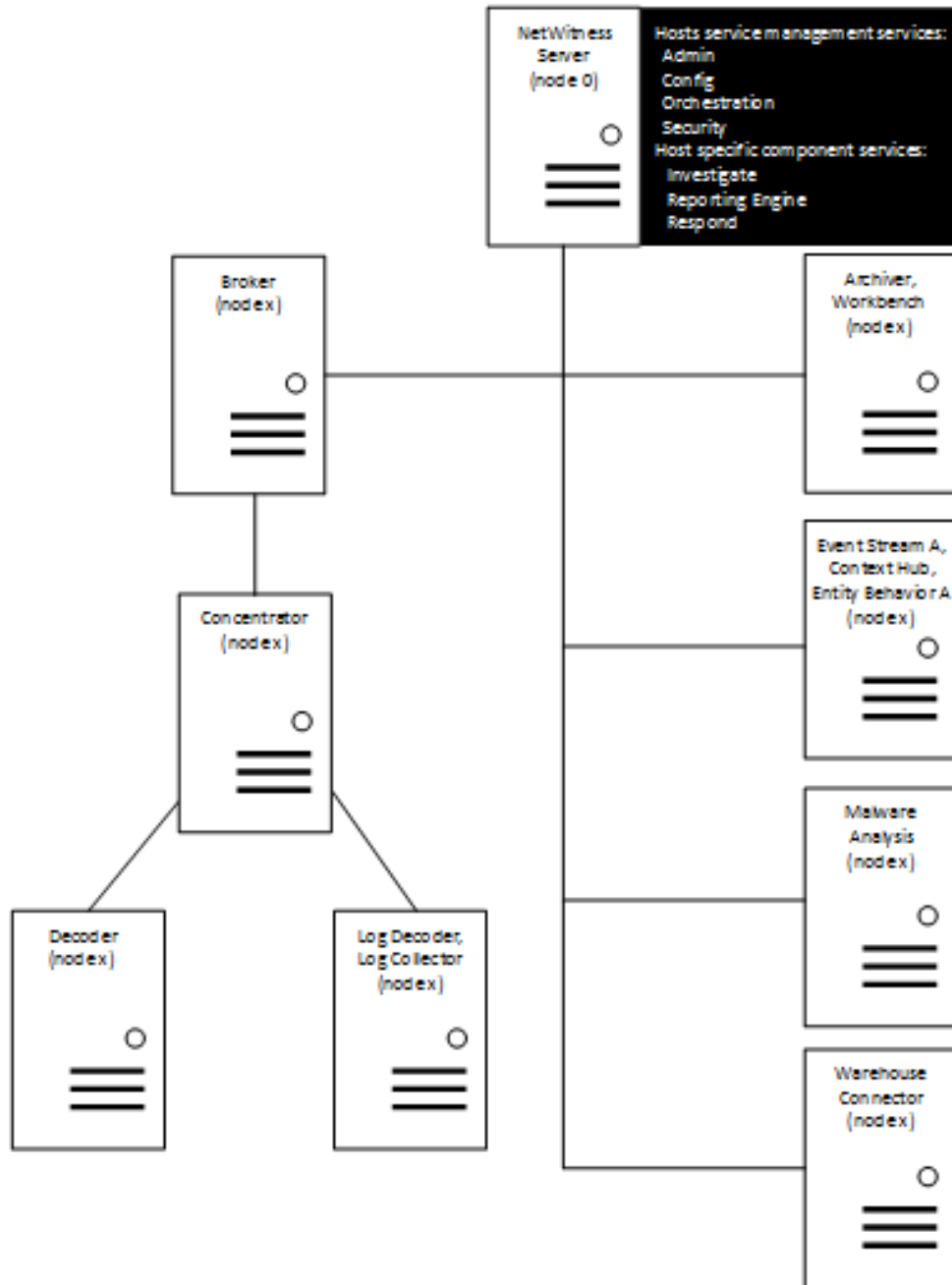
Le diagramme suivant illustre un déploiement NetWitness Suite basique sur plusieurs sites.



Environnement de l'appliance physique RSA

Le schéma suivant illustre un déploiement NetWitness Suite basique hébergé sur un matériel RSA.

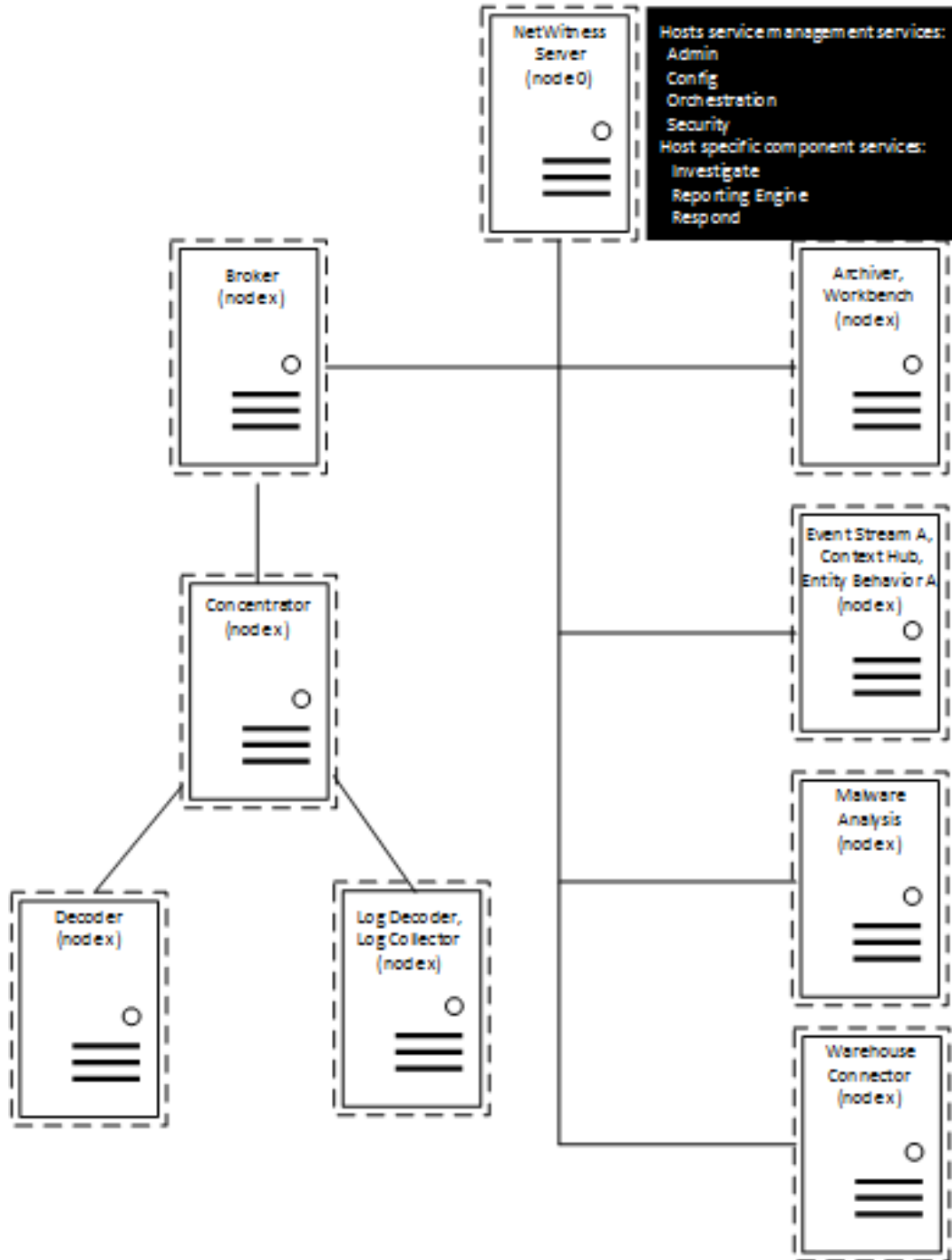
RSA NetWitness® Suite Physical Appliance Deployment



Le schéma suivant illustre un déploiement NetWitness Suite basique hébergé virtuellement. Reportez-vous au RSA NetWitness® Suite Guide de configuration de hôte virtuel sur site pour plus d'informations.

RSA NetWitness® Suite

On-Prem Virtual Deployment



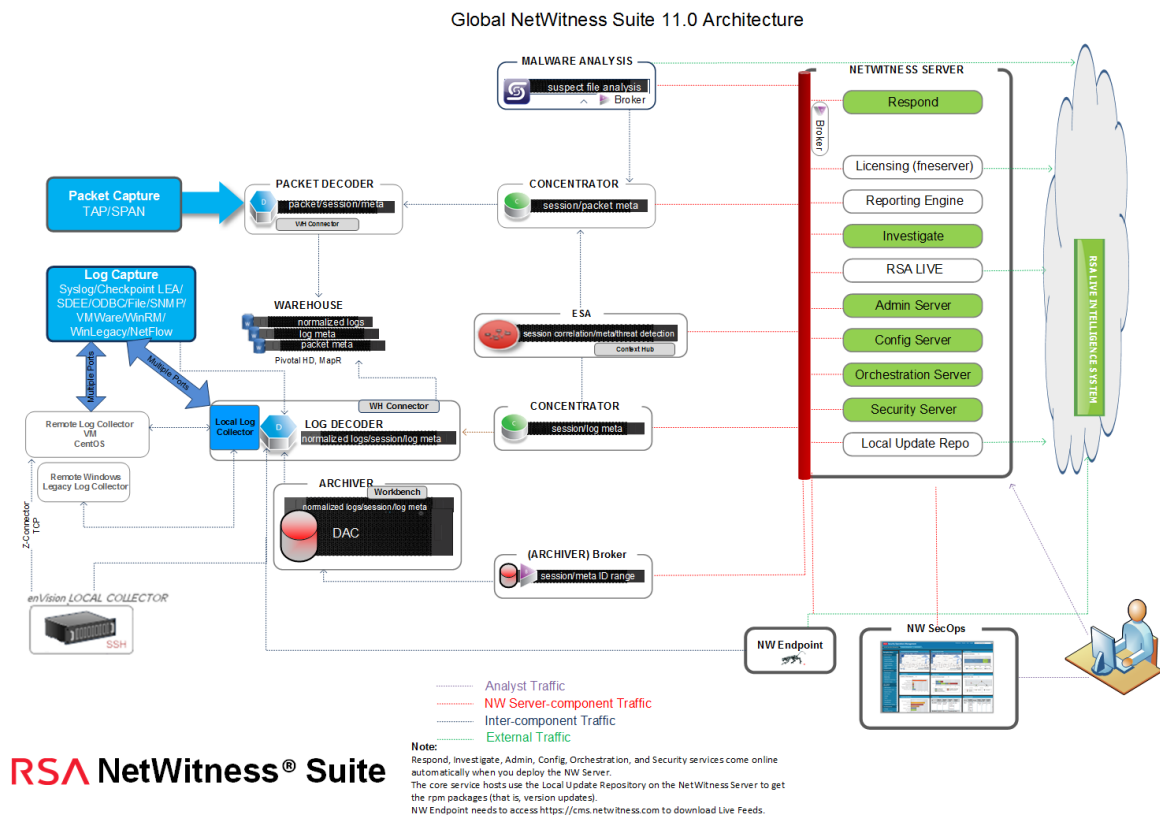
déploiement: Architecture réseau et ports

Reportez-vous au schéma et au tableau des ports suivants pour veiller à ce que tous les ports concernés soient ouverts et que les composants de votre déploiement NetWitness Suite puissent communiquer les uns avec les autres.

Schéma de l'architecture réseau NetWitness Suite

Le schéma suivant illustre l'architecture réseau NetWitness Suite, y compris tous ses produits composants.

Remarque : Les hôtes de base NetWitness Suite doivent être en mesure de communiquer avec Serveur NetWitness (serveur primaire dans un déploiement avec plusieurs serveurs) via le port UDP 123 pour la synchronisation horaire Network Time Protocol (NTP).



Liste complète des hôtes et des ports de service NetWitness Suite

Remarque : 1.) Pour les ports utilisés dans la collecte des événements via les NetWitness Logs, reportez-vous à la section [Les bases](#) du *Guide de déploiement de Log Collection*.

Cette section contient les spécifications de port pour les hôtes suivants.

[Hôte de serveur NW](#)

[Hôte Log Decoder](#)

[Hôte Archiver](#)

[Hôte Log Hybrid](#)

[Hôte Broker](#)

[Hôte Malware](#)

[Hôte Concentrator](#)

[Hôte Packet Decoder](#)

[Hôte Event Stream Analysis](#)

[Hôte Packet Hybrid](#)

[Hôte Log Collector](#)

Hôte de serveur NW

Hôte source	Hôte de destination	Ports de destination	Commentaires
Station de travail de l'administrateur	Serveur NW	TCP 443, 80	nginx - IU NetWitness
Station de travail Admin	Serveur NW	TCP 15671	Interface utilisateur de gestion RabbitMQ
Station de travail Admin	Serveur NW	TCP 22	SSH
Hôtes NW	Serveur NW	TCP 4505, 4506	Ports Salt Master
Hôtes NW	Serveur NW	UDP 123	NTP
Hôtes NW	Serveur NW	TCP 27017	MongoDB
Serveur NW	Serveur NW	UDP 123	NTP
Serveur NW	Serveur NFS	TCP 111 2049 UDP 111 204	Installations iDRAC
Serveur NW	NW Endpoint	TCP 443, 9443	

Hôte Archiver

Hôte source	Hôte de destination	Ports de destination	Commentaires
Station de travail Admin	Archiver	TCP 15671	Interface utilisateur de gestion RabbitMQ
Station de travail Admin	Archiver	TCP 22	SSH
Serveur NW	Archiver	TCP 56008 (SSL), 50008 (Non SSL), 50108 (REST)	Ports d'application Archiver
Serveur NW	Archiver	TCP 56006 (SSL), 50006 (Non SSL), 50106 (REST)	Ports d'appliance NetWitness
Serveur NW	Archiver	TCP 5671	Bus de messages RabbitMQ (AMQPS) pour tous les hôtes NW.
Serveur NW	Archiver	TCP 514, 6514, 56007 (SSL), 50007 (Non SSL), 50107 (REST), UDP 514	Ports d'application Workbench
Archiver	Serveur NFS	TCP 111 2049 UDP 111 204	Installations iDRAC

Hôte Broker

Hôte source	Hôte de destination	Ports de destination	Commentaires
Station de travail Admin	Broker	TCP 15671	Interface utilisateur de gestion RabbitMQ

Hôte source	Hôte de destination	Ports de destination	Commentaires
Station de travail Admin	Broker	TCP 22	SSH
Serveur NW	Broker	TCP 56003 (SSL), 50003 (Non SSL), 50103 (REST)	Ports d'application Broker
Serveur NW	Broker	TCP 56006 (SSL), 50006 (Non SSL), 50106 (REST)	Ports d'appliance NetWitness
Serveur NW	Broker	TCP 5671	Bus de messages RabbitMQ (AMQPS) pour tous les hôtes NW.
Broker	Serveur NW	TCP 111 2049 UDP 111 2049	Installations iDRAC

Hôte Concentrator

Hôte source	Hôte de destination	Ports de destination	Commentaires
Station de travail Admin	Concentrator	TCP 15671	Interface utilisateur de gestion RabbitMQ
Station de travail Admin	Concentrator	TCP 22	SSH
Serveur NW	Concentrator	TCP 56005 (SSL), 50005 (Non SSL), 50105 (REST)	Ports d'application Concentrator
Malware	Concentrator	TCP 56005 (SSL)	Malware

Hôte source	Hôte de destination	Ports de destination	Commentaires
Serveur NW	Concentrator	TCP 56006 (SSL), 50006 (Non SSL), 50106 (REST)	Ports d'appliance NetWitness
Serveur NW	Concentrator	TCP 5671	Bus de messages RabbitMQ (AMQPS) pour tous les hôtes NW.
Concentrator	Serveur NFS	TCP 111 2049 UDP 111 204	Installations iDRAC

Hôte Event Stream Analysis (ESA)

Hôte source	Hôte de destination	Ports de destination	Commentaires
Station de travail Admin	ESA	TCP 15671	Interface utilisateur de gestion RabbitMQ
Station de travail Admin	ESA	TCP 22	SSH
Serveur NW, NW Endpoint, ESA secondaire	ESA primaire	TCP 27017	MongoDB
Serveur NW	ESA primaire	TCP 7005	Port de lancement Context Hub - (ESA primaire)

Hôte source	Hôte de destination	Ports de destination	Commentaires
Serveur NW	ESA	TCP 50030 (SSL)	Port d'application ESA
Serveur NW	ESA	TCP 50035 (SSL)	Port d'application ESA
Serveur NW	ESA	TCP 50036 (SSL)	Port d'application ESA
Serveur NW	ESA	TCP 5671	Bus de messages RabbitMQ (AMQPS) pour tous les hôtes NW.
ESA	cms.netwitness.com	TCP 443	Live
ESA	Serveur NFS	TCP 111 2049 UDP 111 2049	NTP
ESA	Active Directory	636 (SSL)/389 (Non SSL)	
Serveur NW	ESA	80 (HTTP)/ 443 (HTTPS) (REST)	
ESA primaire	Archer	443 (SSL)/80 (Non SSL)	

Hôte Log Collector

Hôte source	Hôte de destination	Ports de destination	Commentaires
Station de travail Admin	Log Collector	TCP 15671	Interface utilisateur de gestion RabbitMQ
Station de travail Admin	Log Collector	TCP 22	SSH
Log Collector	Source d'événements de Log	Voir le <i>Guide de configuration de Log Collection</i> . Accédez à la Table des matières principale pour la version 11.0 trouver des documents NetWitness Suite 11.0.	
Source d'événements de Log	Log Collector	TCP 514 (Syslog) UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)"	Ports de Log Collection
Source d'événements de Log	Log Collector	TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008,64009	Ports de Log Collection FTP/S
Serveur NW	Log Collector	TCP 56001 (SSL), 50001 (Non SSL), 50101 (REST)	Ports d'application de Log Collector
Serveur NW	Log Collector	TCP 56006 (SSL), 50006 (Non SSL), 50106 (REST)	Ports d'appliance NetWitness

Hôte source	Hôte de destination	Ports de destination	Commentaires
Serveur NW	Log Collector	TCP 5671	Bus de messages RabbitMQ (AMQPS) pour tous les hôtes NW.
Log Collector	Serveur NFS	TCP 111 2049 UDP 111 2049	Installations iDRAC

Hôte de Log Decoder

Hôte source	Hôte de destination	Ports de destination	Commentaires
Station de travail Admin	Log Decoder	TCP 15671	Interface utilisateur de gestion RabbitMQ
Station de travail Admin	Log Decoder	TCP 22	SSH
Log Decoder	Source d'événements de Log	Voir le <i>Guide de configuration de Log Collection</i> . Accédez à la Table des matières principale pour la version 11.0 trouver des documents NetWitness Suite 11.0.	
Source d'événements de Log	Log Decoder	TCP 514 (Syslog), UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)	Ports de Log Collection

Hôte source	Hôte de destination	Ports de destination	Commentaires
Source d'événements de Log	Log Decoder	TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008, 64009	Ports de Log Collection FTP/S
Serveur NW	Log Decoder	TCP 56001 (SSL), 50001 (Non SSL), 50101 (REST)	Ports d'application de Log Collector
Serveur NW	Log Decoder	TCP 56002 (SSL), 50002 (Non SSL), 56202 (Endpoint), 50102 (REST)	Ports d'application Log Decoder
Serveur NW	Log Decoder	TCP 56006 (SSL), 50006 (Non SSL), 50106 (REST)	Ports d'appliance NetWitness
Serveur NW	Log Decoder	TCP 5671	Bus de messages RabbitMQ (AMQPS) pour tous les hôtes NW.
Log Decoder	Serveur NFS	TCP 111 2049 UDP 111 204	Installations iDRAC

Hôte Log Hybrid

Hôte source	Hôte de destination	Ports de destination	Commentaires
Station de travail Admin	Log Hybrid	TCP 15671	Interface utilisateur de gestion RabbitMQ

Hôte source	Hôte de destination	Ports de destination	Commentaires
Station de travail Admin	Log Hybrid	TCP 22	SSH
Log Collector	Source d'événements de Log	Voir le <i>Guide de configuration de Log Collection</i> . Accédez à la Table des matières principale pour la version 11.0 trouver des documents NetWitness Suite 11.0.	
Source d'événements de Log	Log Hybrid	TCP 514 (Syslog), UDP 162 (SNMP), 514 (Syslog), 2055 (NetFlow), 4739 (NetFlow), 6343 (NetFlow), 9995 (NetFlow)	Ports de Log Collection
Source d'événements de Log	Log Hybrid	TCP 21, 64000, 64001, 64002, 64003, 64004, 64005, 64006, 64007, 64008, 64009	Ports de Log Collection FTP/S
Serveur NW	Log Hybrid	TCP 56001 (SSL), 50001 (Non SSL), 50101 (REST)	Ports d'application de Log Collector
Serveur NW	Log Hybrid	TCP 56002 (SSL), 50002 (Non SSL), 56202 (Endpoint), 50102 (REST)	Ports d'application Log Decoder
Serveur NW	Log Hybrid	TCP 56005 (SSL), 50005 (Non SSL), 50105 (REST)	Ports d'application Concentrator
Serveur NW	Log Hybrid	TCP 56006 (SSL), 50006 (Non SSL), 50106 (REST)	Ports d'appliance NetWitness

Hôte source	Hôte de destination	Ports de destination	Commentaires
Serveur NW	Log Hybrid	TCP 5671	Bus de messages RabbitMQ (AMQPS) pour tous les hôtes NW.
Log Hybrid	Serveur NFS	TCP 111 2049 UDP 111 204	Installations iDRAC

Hôte Malware

Hôte source	Hôte de destination	Ports de destination	Commentaires
Station de travail Admin	Malware	TCP 15671	Interface utilisateur de gestion RabbitMQ
Station de travail Admin	Malware	TCP 22	SSH
Serveur NW	Malware	TCP 60007	Ports d'application Malware
Serveur NW	Malware	TCP 56006 (SSL), 50006 (Non SSL), 50106 (REST)	Ports d'appliance NetWitness
Serveur NW	Malware	TCP 5671	Bus de messages RabbitMQ (AMQPS) pour tous les hôtes NW.
Serveur NW	Malware	TCP 5432	Postgresql

Hôte source	Hôte de destination	Ports de destination	Commentaires
Serveur NW	Malware	TCP 56003 (SSL), 50003 (Non SSL), 50103 (REST)	Ports d'application Broker
Malware	panacea.threatgrid.com	TCP 443	Threatgrid
Malware	cloud.netwitness.com	TCP 443	Évaluation de la Communauté / Opswat
Malware	Serveur NFS	TCP 111 2049 UDP 111 204	Installations iDRAC

Hôte Packet Decoder

Hôte source	Hôte de destination	Ports de destination	Commentaires
Station de travail Admin	Packet Decoder	TCP 15671	Interface utilisateur de gestion RabbitMQ
Station de travail Admin	Packet Decoder	TCP 22	SSH
Serveur NW	Packet Decoder	TCP 56004 (SSL), 50004 (Non SSL), 50104 (REST)	Ports d'application Log Decoder
Serveur NW	Packet Decoder	TCP 56006 (SSL), 50006 (Non SSL), 50106 (REST)	Ports d'appliance NetWitness
Serveur NW	Packet Decoder	TCP 5671	Bus de messages RabbitMQ (AMQPS) pour tous les hôtes NW.
Packet Decoder	Serveur NFS	TCP 111 2049 UDP 111 204	Installations iDRAC

Hôte Packet Hybrid

Hôte source	Hôte de destination	Ports de destination	Commentaires
Station de travail Admin	Packet Hybrid	TCP 15671	Interface utilisateur de gestion RabbitMQ
Station de travail Admin	Packet Hybrid	TCP 22	SSH
Serveur NW	Packet Hybrid	TCP 56004 (SSL), 50004 (Non SSL), 50104 (REST)	Ports d'application Log Decoder
Serveur NW	Packet Hybrid	TCP 56005 (SSL), 50005 (Non SSL), 50105 (REST)	Ports d'application Concentrator
Serveur NW	Packet Hybrid	TCP 56006 (SSL), 50006 (Non SSL), 50106 (REST)	Ports d'appliance NetWitness
Serveur NW	Packet Hybrid	TCP 5671	Bus de messages RabbitMQ (AMQPS) pour tous les hôtes NW.
Packet Hybrid	Serveur NFS	TCP 111 2049 UDP 111 204	Installations iDRAC

Exigences du site et sécurité

Lisez soigneusement et respectez tous les avertissements et précautions avant d'installer ou d'effectuer la maintenance de vos appareils RSA.

Usages prévus de l'application

Ce produit a été évalué comme équipement IT (ITE) pouvant être installé à l'intérieur d'un bureau, d'une école, d'une salle informatique ou d'un emplacement commercial. Ce périphérique n'est pas destiné à être branché à un câble de type extérieur.

Service

Aucun composant réparable par l'utilisateur n'est présent à l'intérieur de cet appareil. Veuillez contacter le support client en cas de dysfonctionnement. En cas de défaillance, une température élevée peut survenir à l'intérieur du système provoquant un signal d'alarme. Si l'alarme se déclenche, débranchez immédiatement l'appareil de la source d'alimentation et contactez le support client. Un fonctionnement prolongé du périphérique serait dangereux et pourrait causer des blessures ou des dommages matériels.

Informations relatives à la sécurité

Sélection de site

Le système est conçu pour fonctionner dans un environnement de bureau classique. Choisissez un site avec les caractéristiques suivantes :

- Être propre, sec et exempt de particules en suspension dans l'air (sans compter la poussière que l'on peut s'attendre à trouver normalement dans une pièce).
- Bénéficier d'une bonne ventilation et ne pas être exposé à une source de chaleur, y compris à la lumière directe du soleil et
- à la chaleur de radiateurs.
- Ne pas être exposé à des sources de vibrations ou de chocs physiques.
- Être éloigné des champs magnétiques puissants produits par les appareils électriques.
- Dans les régions qui sont sensibles aux orages électriques, nous vous recommandons de brancher le système à un parasurtenseur.
- Être doté d'une prise murale avec mise à la terre.

- Laisser suffisamment d'espace pour accéder aux câbles d'alimentation servant de dispositifs principaux de coupure du courant pour le produit.

Pratiques de manipulation de l'équipement

Réduisez le risque de blessures ou de dommages matériels par les actions suivantes :

- Se conformer aux exigences de santé et de sécurité au travail lors du déplacement ou du soulèvement du périphérique.
- Utiliser une aide mécanique ou toute autre assistance appropriée lors du déplacement ou du soulèvement du périphérique.
- Réduire le poids de l'appareil pour faciliter la manipulation en supprimant tous les composants facilement détachables.

Avertissements relatifs à l'alimentation et à l'électricité

Attention : Le bouton d'alimentation désigné par la marque d'alimentation de secours, n'éteint PAS complètement l'alimentation secteur du système. Une alimentation de secours de 5 V est active lorsque le système est branché. Pour couper l'alimentation du système, vous devez débrancher le cordon d'alimentation secteur de la prise murale.

- N'essayez pas de modifier ni d'utiliser un cordon d'alimentation s'il ne s'agit pas du type exact requis. Un autre cordon d'alimentation est requis pour chaque alimentation du système.
- Ce produit ne contient aucune pièce réparable par l'utilisateur. N'ouvrez pas le système.
- Lorsque vous remplacez une alimentation remplaçable à chaud, débranchez le câble de l'alimentation à remplacer, avant de la retirer du serveur.

Avertissements relatifs au montage en rack

- Le rack doit être fixé à un support inamovible pour l'empêcher de basculer lorsque vous sortez le serveur ou un élément. Le rack doit être installé conformément aux instructions du fabricant du rack.
- Le montage de l'équipement dans le rack doit être effectué soigneusement afin d'éviter tout danger lié à une charge mécanique inégale.
- Ne sortez qu'un seul élément du rack à la fois.
- Pour éviter tout choc électrique, vous devez disposer d'une mise à la terre de sécurité pour le rack et pour chaque équipement qui y est installé.

Refroidissement et circulation de l'air

L'installation de l'équipement ne doit pas compromettre la quantité d'aération nécessaire au fonctionnement sûr de l'équipement.

Placement de l'antenne

Cet équipement doit être installé et utilisé à une distance minimale de 7 cm entre le radiateur et votre corps. Les antennes utilisées pour cet émetteur ne doivent pas être situées ni fonctionner conjointement avec une autre antenne ou un autre émetteur.

Configurer l'agrégation de groupes

Utilisez l'agrégation de groupes pour configurer plusieurs services Archiver ou Concentrator en tant que groupe et partager les tâches d'agrégation entre eux. Vous pouvez configurer plusieurs services Archiver or Concentrator pour agréger de manière efficace plusieurs services Log Decoder et améliorer les performances des requêtes sur les données :

- Stockées dans l'Archiver.
- Traitées par le biais du Concentrator.

Recommandations à propos du déploiement d'agrégation de groupes RSA

RSA recommande le déploiement suivant pour l'agrégation de groupes.

- 1 - 2 Log Decoders
- 3 - 5 Archivers ou Concentrators

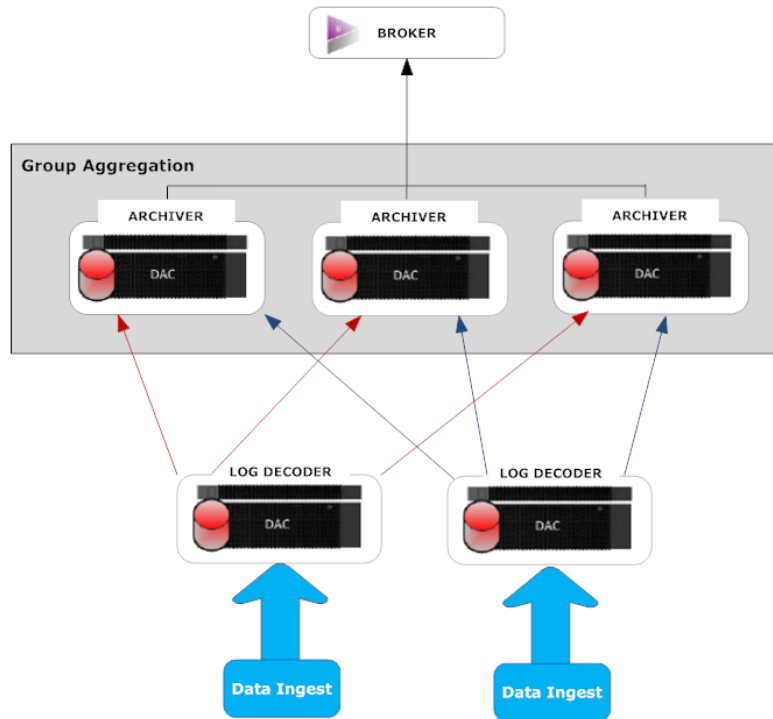
Avantages de l'utilisation de l'agrégation de groupes

Agrégation de groupes :

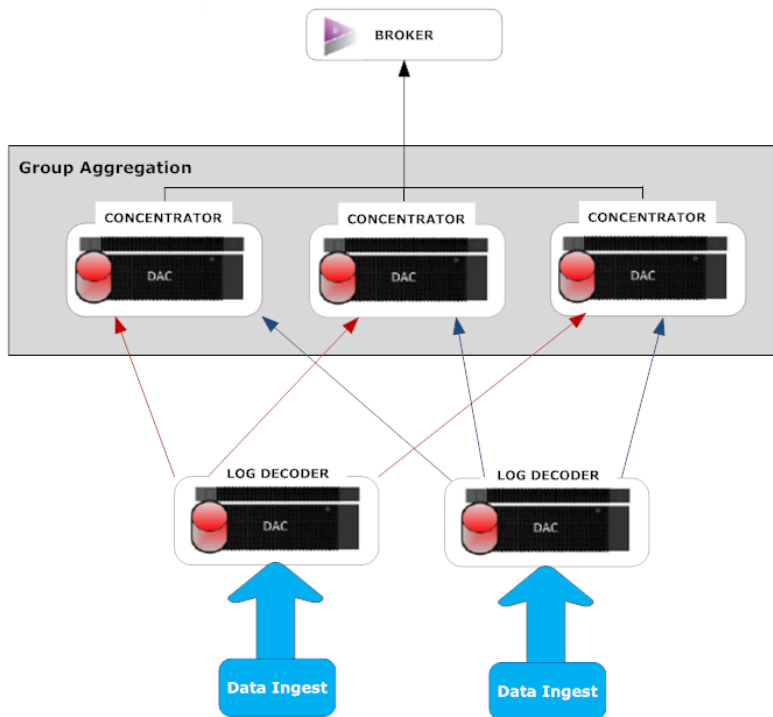
- Augmente la vitesse des requêtes Security Analytics.
- Améliore les performances des requêtes d'agrégation (nombre et somme) sur l'environnement.
- Améliore les performances du service de procédure d'enquête.
- Vous permet de stocker des données pour une durée plus longue à des fins de procédure d'enquête.

Le schéma suivant illustre l'agrégation de groupes.

Archivers



Concentrators



Vous pouvez avoir un nombre quelconque de modules Archivers ou Concentrators regroupés qui forment un groupe d'agrégation. Les services Archiver or Concentrator du groupe divisent toute la session agrégée entre eux sur la base du nombre de sessions définies dans le paramètre Sessions d'agrégation maximum.

Par exemple, dans un groupe d'agrégation contenant 2 services Archiver ou 2 services Concentrator avec le paramètre Sessions d'agrégation maximum défini sur 10 000, les services divisent la session entre eux tel qu'illustré dans le tableau ci-dessous.

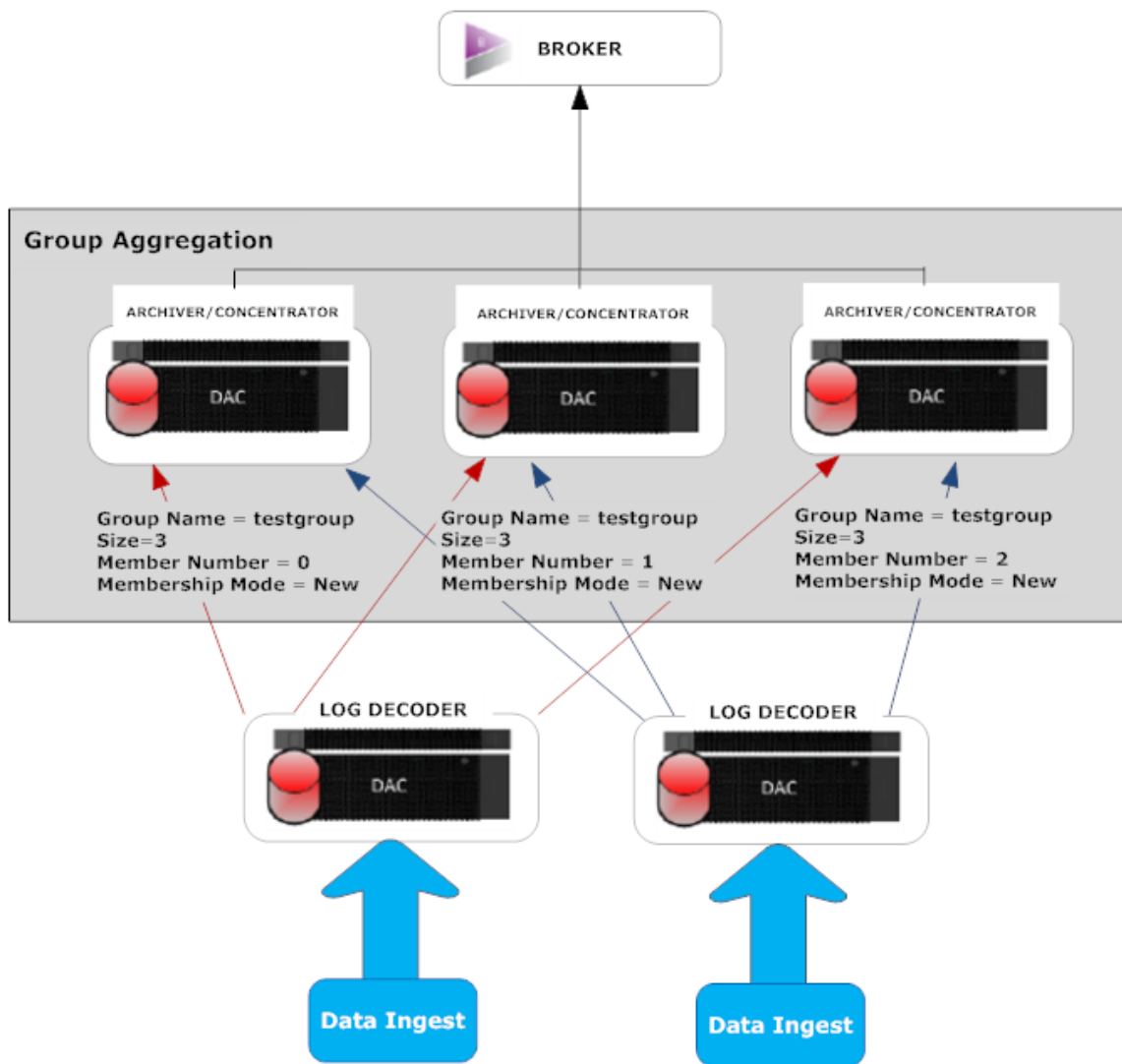
Archiver 0 ou Concentrator 0	Archiver 1 ou Concentrator 1
1 à 9 999	10 000 à 19 999
20 000 à 29 999	30 000 à 39 999
40 000 à 49 999	50 000 à 59 999

Configurer l'agrégation de groupes

Exécutez cette procédure pour configurer plusieurs services Archiver ou Concentrator sous la forme de groupes et partagez les tâches d'agrégation entre eux.

Conditions préalables

Planifiez la conception du réseau pour l'agrégation de groupes. La figure ci-après présente un exemple de configuration d'agrégation de groupes.

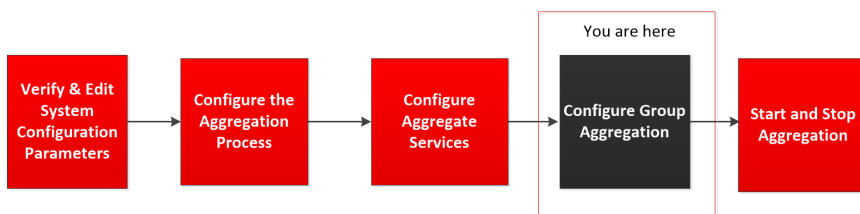


Veillez à bien examiner les paramètres d'agrégation de groupes dans le tableau suivant avant de créer un plan d'agrégation de groupes.

Paramètre	Description
Nom de groupe	Détermine le groupe auquel appartient l'Archiver ou le Concentrator. Vous pouvez ajouter autant de données d'agrégation de groupes d'un Log Decoder que voulu. Le paramètre Nom du groupe est utilisé par le Log Decoder pour identifier les services Archiver ou Concentrator qui interagissent. Tous les services Archiver ou Concentrators du groupe doivent porter le même nom de groupe.

Taille	Détermine le nombre de services Archiver ou Concentrator du groupe d'agrégation.
Numéro de membre	Détermine la position des services Archiver ou Concentrator dans le groupe d'agrégation. Pour un groupe de taille N, vous devez définir un numéro de membre de 0 à N-1 sur chaque service Archiver ou Concentrators dans le groupe d'agrégation. Par exemple : Si la taille du groupe d'agrégation est de 2, le numéro de membre de l'un des services Archiver ou Concentrator doit être défini sur 0 et le numéro de membre de l'autre Archiver ou Concentrator doit être défini sur 1.
Mode Adhésion	Il existe deux modes d'adhésion : Nouveau et Remplacer. Nouveau : Permet d'ajouter un nouveau service Archiver ou Concentrator en tant que membre au groupe d'agrégation actuel ou de créer un tel groupe. Le service Archiver ou Concentrator n'agrège aucune session du service car les autres membres du groupe auraient déjà agrégé toutes les sessions sur le service. Ce service Archiver ou Concentrator n'agrègera que les nouvelles sessions telles qu'elles apparaissent sur le service. Remplacer : Remplace un membre d'un groupe d'agrégation. Le service Archiver ou Concentrator lance l'agrégation à partir de la session la plus ancienne sur le service à partir duquel l'agrégation a lieu.

Remarque : Ce paramètre a une incidence uniquement quand aucune session n'a été agrégée à partir du service. Après l'agrégation de certaines sessions, ce paramètre n'a aucun effet.





Configurer l'agrégation de groupes

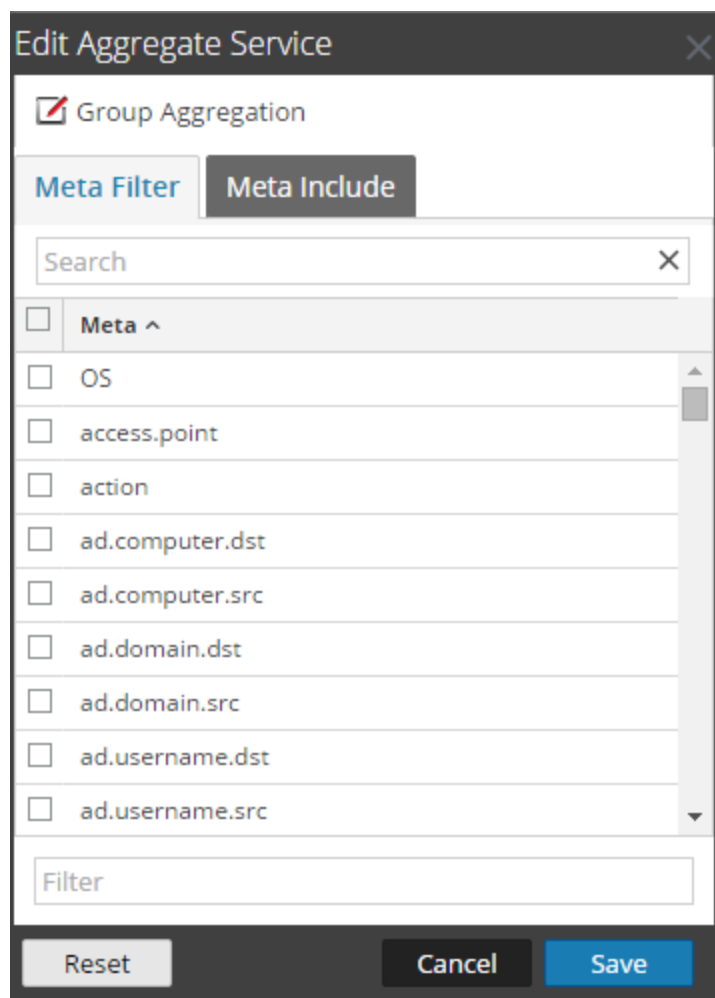
Effectuez la procédure suivante pour configurer l'agrégation de groupes.

1. Configurez plusieurs services Archiver ou Concentrator dans votre environnement. Veillez à ajouter le même Log Decoder en tant que source de données à tous les services.
2. Procédez comme suit sur tous les services Archiver ou Concentrator que vous voulez ajouter

au groupe d'agrégation :

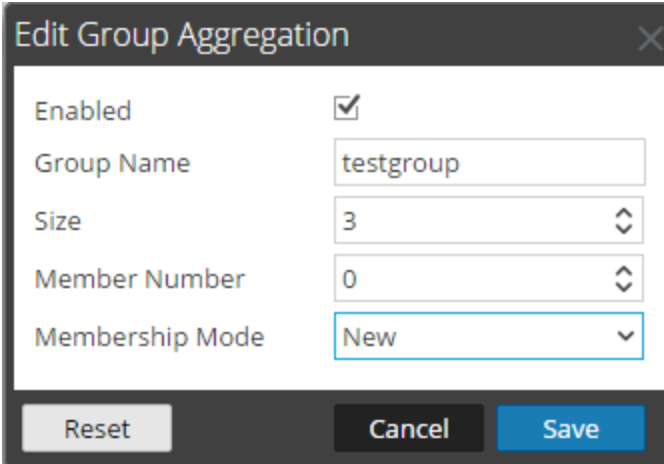
- a. Dans le **Menu principal**, sélectionnez **ADMIN > Services**.
- b. Sélectionnez le service Archiver ou Concentrator, puis dans la colonne **Actions**, sélectionnez **Vue > Config**.
La vue Configuration du périphérique du service Archiver ou Concentrator s'affiche.
- c. Dans la section **Services agrégés**, sélectionnez le périphérique Log Decoder.
- d. Cliquez sur  **Toggle Service** pour modifier le statut de Log Decoder sur hors ligne s'il est en ligne.
- e. Cliquez sur .

La boîte de dialogue **Modifier le service agrégé** s'affiche.



- f. Cliquez sur  **Group Aggregation**.

La boîte de dialogue **Modifier l'agrégation des groupes** s'affiche.



The screenshot shows a dialog box titled "Edit Group Aggregation". It contains the following fields and controls:

- Enabled:** A checkbox that is checked.
- Group Name:** A text input field containing the value "testgroup".
- Size:** A spinner control set to the value 3.
- Member Number:** A spinner control set to the value 0.
- Membership Mode:** A dropdown menu with "New" selected.

At the bottom of the dialog, there are three buttons: "Reset", "Cancel", and "Save".

- g. Sélectionnez la case à cocher **Activé** et définissez les paramètres suivants :
 - Dans le champ **Nom du groupe**, saisissez le nom du groupe.
 - Dans le champ **Taille**, sélectionnez le nombre de services Archiver ou Concentrator du groupe d'agrégation.
 - Dans le champ **Numéro de membre**, sélectionnez la position d'Archiver ou Concentrator dans le groupe d'agrégation.
 - Dans le menu déroulant **Mode Adhésion**, sélectionnez le mode.
 - h. Cliquez sur **Save**.
 - i. Dans la page de la vue Configuration du périphérique, cliquez sur **Appliquer**.
 - j. Effectuez l'**étape b** à l'**étape i** sur tous les autres services Archiver ou Concentrator qui doivent faire partie de l'agrégation de groupe.
3. Dans la section **Configuration de l'agrégation**, définissez le paramètre **Sessions d'agrégation max.** sur **10000**.

The screenshot displays the RSA NetWitness Suite Admin console. The top navigation bar includes 'RESPOND', 'INVESTIGATE', 'MONITOR', 'CONFIGURE', and 'ADMIN'. The 'ADMIN' section is active, showing a breadcrumb trail: 'HOSTS > SERVICES > EVENT SOURCES > HEALTH & WELLNESS > SYSTEM > SECURITY'. Below this, there are tabs for 'Change Service', 'Concentrator', and 'Config'. The 'Config' tab is selected, and the 'Appliance Service Configuration' sub-tab is active.

The main content area is divided into three sections:

- Aggregate Services:** A table with columns for Address, Port, Rate, Max, Behind, Meta Fields, Filter, Meta Include, Grouped, and Status. Two services are listed:

Address	Port	Rate	Max	Behind	Meta Fields	Filter	Meta Include	Grouped	Status
<input type="checkbox"/> 10.31.125.245	5004	0	0	0				no	consuming
<input checked="" type="checkbox"/> 10.31.125.246	5002	0	0	0				yes	offline
- System Configuration:** A table with columns for Name and Config Value.

Name	Config Value
Compression	0
Port	5005
SSL FIPS Mode	<input checked="" type="checkbox"/>
SSL Port	5605
Stat Update Interval	1000
Threads	20
- Aggregation Configuration:** A table with columns for Name and Config Value.

Name	Config Value
Aggregation Settings	
Aggregate Autostart	<input checked="" type="checkbox"/>
Aggregate Hours	0
Aggregate Interval	10
Aggregate Max Sessions	
Aggregate Max Sessions	10000
Service Heartbeat	
Heartbeat Error Restart	300
Heartbeat Next Attempt	60
Heartbeat No Response	180

An 'Apply' button is located at the bottom center of the configuration area. The footer of the console shows 'RSA | NETWITNESS SUITE' on the left and the version number '11.0.0.0-17079005430.1.912748d' on the right.

