RSA NETWITNESS® PLATFORM

Guide de démarrage rapide de NetWitness Endpoint

pour la plate-forme RSA NetWitness® 11.3

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, une 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 de Dell 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 de Dell.

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

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

juin 2019

Qu’est-ce que NetWitness Endpoint ?

RSA NetWitness Endpoint est un outil de détection et de réponse qui surveille en continu le comportement de tous les terminaux du réseau pour offrir une visibilité approfondie et une analyse des exécutables et des processus. Il permet de détecter les attaques à la fois nouvelles, inconnues et ciblées, met en évidence les activités suspectes pour la procédure d’enquête, expose des comportements anormaux et détermine le périmètre des compromissions afin d’aider les analystes à répondre plus rapidement aux menaces avancées.

À propos de ce guide

Ce guide fournit des instructions de bout en bout pour configurer NetWitness Platform Endpoint et utiliser les fonctions Endpoint.

Documentation en ligne de RSA NetWitness Platform 11.3 dans RSA Link

La documentation produit de NetWitness Platform s’organise sur des axes fonctionnels. Si vous recherchez un guide ou une version spécifique, accédez à la Table des matières principale de la version 11.x.

Utilisez ces liens pour afficher la documentation de RSA NetWitness Platform 11.3. Les deux liens fournissent la même documentation, dans les deux formats suivants :

- Les guides HTML incluent les dernières informations sur les versions 11.x actuellement prises en charge : Documentation RSA NetWitness Platform 11.x.
- Les guides au format PDF fournissent des informations sur une version spécifique : Documents PDF sur RSA NetWitness Platform 11.3.

Utilisez ces liens pour accéder à la documentation qui n’est pas liée à une version particulière du logiciel :

- Guides de configuration du matériel : https://community.rsa.com/community/products/netwitness/hardware-setup-guides
- Documentation pour le contenu RSA, comme les feeds, les parsers, les règles d’application et les rapports : https://community.rsa.com/community/products/netwitness/rsa-content.

Prise en main

Les tâches suivantes peuvent être exécutées dans n’importe quel ordre.

Description	Références
	
Affichez des informations sur les mises à jour du produit, les améliorations et les problèmes connus.	Notes de mise à jour
Appréhendez NetWitness Endpoint.	Rubrique « Prise en main de NetWitness Platform » et « Investigate » dans le *Guide de mise en route de NetWitness Platform*

Installation et configuration

Nouvelle installation

Les tâches suivantes doivent être exécutées dans l'ordre indiqué.

Description	Références
	
Obtenez une licence pour Endpoint Log Hybrid.	Guide de gestion des licences
Passez en revue le matériel pris en charge.	Rubrique « Matériel pris en charge » dans le *Guide d'installation d'un hôte physique*
Passez en revue l'architecture Endpoint. Planifiez votre déploiement en fonction du nombre de terminaux, de la distribution et de l'emplacement de ces terminaux, puis choisissez l'un des déploiements suivants : • Serveur Endpoint unique • Serveurs Endpoint multiples	Rubrique « Architecture NetWitness Endpoint » dans le *Guide de déploiement*
Configurez les ports sur votre pare-feu.	Rubrique « Architecture réseau et ports » dans le *Guide de déploiement*.

Description	Références
Installez le serveur NetWitness et d'autres composants. Pour un déploiement de serveur Endpoint unique, vous devez installer : NetWitness Server, Endpoint Log Hybrid et ESA. Dans le cas de serveurs Endpoint multiples, en plus des composants ci-dessus, vous devez installer : une instance supplémentaire d'Endpoint Log Hybrid, NetWitness Broker avec Endpoint Broker installé dessus.	- Consultez le *Guide d'installation d'un hôte physique* pour obtenir des instructions sur la configuration des hôtes physiques - Consultez le *Guide d'installation d'un hôte virtuel* pour obtenir des instructions sur la façon de configurer des hôtes virtuels
Installez Endpoint Log Hybrid.	Rubrique « RSA NetWitness Endpoint » dans le *Guide d'installation d'un hôte physique*
Passez en revue les services installés.	*Guide de mise en route des hôtes et des services*
Remarque : Passez en revue les stratégies par défaut et modifiez-les en conséquence. Installez l'agent Endpoint sur les hôtes.	Rubrique « Sources Endpoint » dans le *Guide de configuration Endpoint* *Guide d'installation de l'agent NetWitness Endpoint*

Mise à niveau

Les tâches suivantes doivent être exécutées dans l'ordre indiqué.

Description	Références
	
Mise à niveau de la version 10.6.5 vers la version 11.3 Après la mise à niveau NetWitness Platform 11.3, installez Endpoint Log Hybrid puis les autres composants de Endpoint.	- Consultez le *Guide de mise à niveau d'un hôte physique* pour obtenir des instructions sur la mise à niveau des hôtes physiques - Consultez le *Guide de mise à niveau d'un hôte virtuel* pour obtenir des instructions sur la mise à niveau des hôtes virtuels
Mise à jour de la version 11.x vers la version 11.3 Mettez à jour le serveur Endpoint et les agents.	*Guide de mise à jour*

Description	Références
Mettez à niveau les agents Endpoint des versions 11.1. x et 11.2.x vers la version 11.3.	Rubrique « Mise à niveau des agents » dans le *Guide d'installation de l'agent Endpoint*
Migrer NetWitness Endpoint 4.4.0.x vers NetWitness Platform.	*Guide de migration de NetWitness Endpoint 4.4.0.x vers RSA NetWitness Platform 11.3*

Configuration

Les tâches suivantes peuvent être exécutées dans n'importe quel ordre.

Description	Références
	
Comprendre NetWitness Endpoint et les tâches générales requises pour sa configuration.	Rubrique « Présentation de NetWitness Endpoint et configuration du Serveur Endpoint » dans le *Guide de configuration Endpoint*
Passez en revue les groupes et les politiques pour les agents.	Rubrique « Sources Endpoint » dans le *Guide de configuration Endpoint*
Configurez le compte RSA Live et vérifiez si le contenu ESA et les Règles d'application pour Endpoint sont disponibles. **Remarque :** Le service de réputation de fichiers est automatiquement activé sur RSA Live.	*Guide de gestion des services Live*
Créez un contrôle d'accès basé sur les rôles (RBAC).	Rubrique « Autorisations des rôles » dans le Guide de la sécurité du système et de la gestion des utilisateurs
Configurez la politique de rétention des données.	Rubrique « Configurer la rétention des données » dans le *Guide de configuration Endpoint*
Gérez les agents inactifs.	Rubrique « Gérer les agents inactifs » dans le *Guide de configuration Endoint*

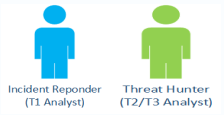
Procédure d'enquête

Les tâches suivantes peuvent être exécutées dans n'importe quel ordre.

Description	Références
	
Découvrez comment fonctionne Investigation.	Rubrique « Fonctionnement de NetWitness Investigate » dans le *Guide de l'utilisateur de NetWitness Investigate*
Configurez les vues Investigate.	Rubrique « Configuration des vues et des préférences NetWitness Investigate » dans le *Guide d'utilisation de NetWitness Investigate*
Commencez une procédure d'enquête dans différentes vues Investigate.	Rubrique « Commencer une procédure d'enquête » dans le *Guide d'utilisation de NetWitness Investigate*
Passez en revue les bonnes pratiques en matière de fichiers et d'hôtes et configurez votre vue Investigate pour la procédure d'enquête.	Rubrique « Bonnes pratiques », sous Procédure d'enquête sur les fichiers et Procédure d'enquête sur les hôtes du *Guide d'utilisation de NetWitness Endpoint*
Lancez une procédure d'enquête sur les fichiers.	Rubrique « Procédure d'enquête sur les fichiers » dans le *Guide de l'utilisateur NetWitness Endpoint*
Lancez une procédure d'enquête sur les hôtes.	Rubrique « Procédure d'enquête sur les hôtes » dans le *Guide de l'utilisateur NetWitness Endpoint*
Lancez une procédure d'enquête sur le processus.	Rubrique « Procédure d'enquête sur les hôtes » dans le *Guide de l'utilisateur NetWitness Endpoint*
Analysez les fichiers téléchargés.	Rubrique « Analyse des fichiers téléchargés » dans le *Guide d'utilisation de NetWitness Endpoint*
Modifiez l'état et corrigez les fichiers.	Rubrique « Modification de l'état ou correction d'un fichier » dans le *Guide de l'utilisateur NetWitness*
Analysez les événements.	Rubrique « Analyse des événements » dans le *Guide de l'utilisateur NetWitness Endpoint* Rubriques « Analyse des données brutes et des métadonnées dans la vue Analyse d'événements », « Procédure d'enquête relative aux métadonnées dans la vue Naviguer » et « Examen des événements bruts dans la vue Événements » du *Guide de l'utilisateur NetWitness Investigate*

Réponse et Reporting

Les tâches suivantes peuvent être exécutées dans n'importe quel ordre.

Description	Références
	
Répondez aux incidents Endpoint.	*Guide de l'utilisateur de NetWitness Respond*
Affichez les rapports relatifs aux données Endpoint.	*Guide de l'utilisateur de Reporting*

Maintenance

Les tâches suivantes peuvent être exécutées dans n'importe quel ordre.

Description	Références
	
Surveillez l'intégrité.	Guide de maintenance du système

Intégration (pour NetWitness Endpoint existant)

Les tâches suivantes peuvent être exécutées dans n'importe quel ordre.

Description	Références
	
Configurez les métadonnées NetWitness Endpoint 4.4.x avec NetWitness Platform.	Rubrique « Intégration de NetWitness Endpoint 4.4.0.2 ou version ultérieure avec NetWitness Platform » dans le *Guide de configuration Endpoint*
Configurez le fonctionnement intégré de NetWitness Endpoint 4.4.x avec NetWitness Platform.	*Guide d'intégration de RSA NetWitness Endpoint*