RSA NETWITNESS® PLATFORM

Guide de démarrage rapide NetWitness UEBA

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 UEBA ?

RSA NetWitness UEBA (Analytique comportementale de l'entité et de l’utilisateur) est une solution d'analyse avancée pour découvrir, étudier et surveiller les comportements à risque pour tous les utilisateurs et entités de votre environnement réseau. NetWitness UEBA est utilisé pour :

- Détecter des utilisateurs malveillants et non autorisés
- Pointer les comportements à haut risque
- Découvrir des attaques
- Enquêter sur des menaces émergentes en matière de sécurité
- Identifier une activité malveillante potentielle

À propos de ce guide

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

Documentation 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
Comprendre NetWitness UEBA	*Guide de l'utilisateur de RSA NetWitness UEBA*

Installation et configuration

Installation standard

Les tâches suivantes doivent être exécutées dans l'ordre qui suit.

Description	Références
	
Passez en revue le matériel pris en charge.	Rubrique « Configuration matérielle » du *Guide d'installation autonome de UEBA*
Passez en revue le déploiement de UEBA.	Rubrique « Installation autonome de RSA NetWitness UEBA » dans le *Guide d'installation autonome d'UEBA*
Configurer les ports sur votre pare-feu.	Rubrique « Installation autonome de RSA NetWitness UEBA » dans le *Guide d'installation autonome d'UEBA*
Installez l'hôte du serveur NetWitness	Rubrique « Tâches d'installation » du *Guide d'installation autonome de UEBA*
Installez l'hôte 11.3 Log Hybrid.	Rubrique « Tâches d'installation » du *Guide d'installation autonome de UEBA*
Installez et configurez NetWitness UEBA.	Rubrique « Tâches d'installation » du *Guide d'installation autonome de UEBA*
Attribuez les rôles Analystes_UEBA et Analystes aux utilisateurs UEBA.	Rubrique « Autorisations des rôles » dans le Guide de la sécurité du système et de la gestion des utilisateurs

Nouvelle installation

Les tâches suivantes doivent être exécutées dans l'ordre qui suit.

Description	Références
	
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 UEBA.	Rubrique « Schéma de l'architecture réseau de NetWitness Platform » dans le *Guide de déploiement*
Configurer les ports sur votre pare-feu.	Rubrique « Architecture réseau et ports » dans le *Guide de déploiement*
Installez l'hôte du serveur NetWitness et d'autres composants.	« Tâche 1 - Installation de la version 11.3 sur l'hôte du serveur NetWitness (serveur NW) » et « Tâche 2 - Installation de la version 11.3 sur tous les autres composants hôtes » dans le *Guide d'installation de l'hôte physique* Rubrique « Installer l'hôte virtuel NetWitness Platform dans l'environnement virtuel » du *Guide d'installation d'un hôte virtuel*
Installez UEBA.	Rubrique « RSA NetWitness® UEBA » dans le *Guide d'installation d'un hôte physique*
Attribuez les rôles Analystes_UEBA et Analystes aux utilisateurs UEBA.	Rubrique « Autorisations des rôles » dans le *Guide de la sécurité du système et de la gestion des utilisateurs*

Mise à jour

Les tâches suivantes doivent être exécutées dans l'ordre qui suit.

Description	Références
	
Déployez le Pack Endpoint à partir de RSA Live, qui contient l'analyseur Lua de catégorie de fichier pour l'intégration de UEBA avec Endpoint.	Lors du déploiement, vous devez spécifier le service Log Decoder Endpoint Log Hybrid. Dans le cas de plusieurs serveurs Endpoint, sélectionnez tous les services Log Decoder Endpoint Log Hybrid

Description	Références
Activez les sources de données Endpoint (Processus et Registre, par exemple) pour générer des alertes dans UEBA.	« Activer les sources de données Endpoint » dans les *Instructions de mise à jour*
Activez le transfert d'indicateur UEBA pour transférer les Indicateurs UEBA sur le serveur NetWitness Respond et sur le serveur de corrélation pour créer un incident.	Rubrique « Activer le transfert d'indicateur UEBA » dans les *Instructions de mise à jour*
Après la mise à jour vers NetWitness Platform 11.3, l'UUID du Broker ou du Concentrator change. Vous devez mettre à jour les services Core de NetWitness Platform et mettre à jour l'UUID du Broker ou du Concentrateur.	Rubrique « Mettre à jour l'UUID du Broker ou du Concentrator » dans les *Instructions de mise à jour*
Mettez à jour la configuration du flux d'air.	Rubrique «Mettre à jour la configuration du flux d'air » dans les *Instructions de mise à jour*
Redémarrez le service de l'ordonnanceur du flux d'air après la réussite de la DAG presidio_upgrade.	« Redémarrez le service de l'ordonnanceur du flux d'air » dans les *Instructions de mise à jour*

Investigation

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

Description	Références
	
Enquêtez sur les utilisateurs à haut risque.	Rubrique « Enquêter sur les utilisateurs à haut risque » dans le *Guide de l'utilisateur de RSA NetWitness UEBA*
Enquêtez sur les alertes principales.	Rubrique « Enquêter sur les alertes principales » dans le *Guide de l'utilisateur de RSA NetWitness UEBA*

Monitoring

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

Description	Références
	

Description	Références
Affichez les metrics NetWitness UEBA dans Intégrité.	Rubrique « Voir les mesures NetWitness UEBA dans Intégrité » dans le Guide de l'utilisateur de RSA NetWitness UEBA
Surveillez l'intégrité d'UEBA.	Rubrique « Surveiller l'intégrité d'UEBA » dans le Guide de l'utilisateur de RSA NetWitness UEBA