



Guide de démarrage rapide de NetWitness Investigate

pour la plate-forme RSA NetWitness® 11.3



Copyright © 1994-2019 Dell Inc. or its subsidiaries. All Rights Reserved.

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® Investigate ?

NetWitness Platform audite et surveille l'ensemble du trafic sur un réseau. Un seul type de service, un Decoder, acquiert, analyse et stocke les données de paquets, logs et terminaux transitant sur le réseau. Les analyseurs et feeds configurés sur le Decoder créent des *métadonnées* que les analystes peuvent utiliser pour enquêter sur les logs et paquets acquis. Un autre type de service, nommé Concentrator, indexe et stocke les métadonnées. NetWitness Investigate offre aux analystes la possibilité d'analyser des données dans RSA NetWitness® Platform et d'analyser des données de paquet, de log et de point de terminaison, ainsi que d'identifier d'éventuelles menaces internes ou externes à la sécurité et à l'infrastructure IP.

À propos de ce guide

Ce guide fournit des instructions de bout en bout pour tous les membres de l'équipe du SOC afin de configurer NetWitness Investigate et d'examiner les événements de log et de réseau. Des documents distincts donnent des instructions de bout en bout sur les procédures d'enquête relatives aux terminaux et au comportement des entités utilisateur à l'aide de NetWitness Investigate :

- [Guide de démarrage rapide de NetWitness Endpoint](#)
- [Guide de démarrage rapide NetWitness UEBA](#)

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 et concernent l'intégralité de l'équipe du SOC.

Description	Références
	
Affichez des informations sur les mises à jour du produit, les améliorations et les problèmes connus	Notes de mise à jour sur NetWitness Platform 11.3
Comprendre le fonctionnement de NetWitness Investigate	Rubrique « Fonctionnement de NetWitness Investigate » dans le Guide de l'utilisateur de NetWitness Investigate


Installation, configuration ou mise à niveau

Aucune tâche de configuration, d'installation ou de mise à niveau spéciale n'est requise pour Investigate qui fait partie de NetWitness Platform pour les logs et le réseau. Toutefois, la configuration est nécessaire pour plusieurs composants avec lesquels NetWitness Investigate fonctionne si vous envisagez d'effectuer ce type d'analyse. Ces tâches sont destinées à l'administrateur, et au responsable du SOC qui peut souhaiter comprendre la configuration.

Description	Références
	
Installez et configurez Malware Analysis (autonome ou service)	Guide de configuration de Malware Analysis
Installez et configurez NetWitness Endpoint (autonome ou service)	Guide de démarrage rapide de NetWitness Endpoint
Installez et configurez NetWitness UEBA (autonome ou service)	Guide de démarrage rapide NetWitness UEBA

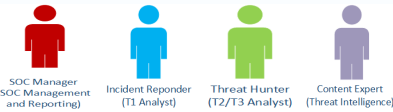
Configuration système

Les administrateurs configurent des préférences au niveau de NetWitness Enquêteur. Les tâches suivantes concernent l'administrateur, et les tâches peuvent être effectuées dans n'importe quel ordre. Les responsables du SOC doivent comprendre les options de configuration possibles.

Description	Références
	
<p>Configurez le contrôle d'accès basé sur les rôles (RBAC) pour les analystes qui utiliseront Investigate. Ces composants ont des autorisations liées à la procédure d'enquête : Investigate (vue Naviguer et vue Événements), investigate-server (vue Analyse d'événements), Malware (vue Analyse de malware), Endpoint-broker-server et Endpoint-server.</p>	<p>Rubrique « Autorisations des rôles » dans le Guide de la sécurité du système et de la gestion des utilisateurs</p>
<p>Configurez Investigate afin de limiter le contenu disponible pour différents rôles d'utilisateur (preQueries).</p>	<p>Rubrique « Vérifier les attributs Requête (Query) et Session par rôle » dans le Guide de sécurité du système et de gestion des utilisateurs</p>
<p>Configurez les paramètres par défaut et les limites de NetWitness Investigate au niveau du système.</p>	<p>Rubrique « Configurer les paramètres Investigation dans le Guide de configuration du système</p>

Configuration des préférences utilisateur

Les tâches suivantes concernent les responsables de la recherche des menaces, les experts en contenu, les responsables de la réponse aux incidents et les responsables du SOC. Les tâches peuvent être exécutées dans n'importe quel ordre.


Description	Références
	
<p>Configurez les préférences de la vue Naviguer et de la vue Événements.</p>	<p>Rubrique « Configurer la vue Naviguer et la vue Événements » du Guide de l'utilisateur NetWitness Investigate.</p>

Description	Références
Configurez les préférences de la vue Analyse d'événements.	Rubrique « Configurer la vue Analyse d'événements » du Guide de l'utilisateur NetWitness Investigate .
Configurez les préférences de la vue Analyse d'événements.	Rubrique « Configurer l'Analyse de malware » dans le Guide de l'utilisateur Malware Analysis .

Procédure d'enquête



Les analystes peuvent mener différents types de procédures d'enquête, avec des niveaux de compétences et des objectifs divers.

- Les responsables de la réponse aux incidents (Analystes T1) se tournent généralement vers Investigate à partir de NetWitness Respond pour trouver des informations détaillées sur un incident afin d'y répondre et d'y remédier.
- Les responsables de la recherche des menaces (Analystes T2/T3) examinent généralement les événements, les métadonnées et le contenu brut afin de recommander des problèmes à corriger.
- Les experts en contenu (renseignements sur les menaces) examinent généralement les événements, les métadonnées, le contenu brut, les données des utilisateurs et des hôtes, et les données UEBA afin de pouvoir analyser de nouveaux renseignements sur les menaces, évaluer et créer de nouveaux feeds et créer des règles de corrélation pour signaler des indicateurs de compromission.
- Les responsables du SOC doivent comprendre les exemples d'utilisation.

Description	Références
 <p>SOC Manager (SOC Management and Reporting) Incident Responder (T1 Analyst) Threat Hunter (T2/T3 Analyst) Content Expert (Threat Intelligence)</p>	
Découvrez des exemples d'utilisation pratiques	Rubrique « Exemples d'utilisation pour NetWitness Investigate » dans le Guide de l'utilisateur NetWitness Investigate
Examinez les métadonnées et les événements bruts dans les logs et le trafic réseau	Rubrique « Commencer une procédure d'enquête » dans le Guide de l'utilisateur de NetWitness Investigate
Enquêtez sur les logiciels malveillants éventuels	Guide d'utilisation de l'analyse de logiciel malveillant
Examinez les terminaux	Guide de l'utilisateur de NetWitness Endpoint
Exécutez une analyse comportementale de l'entité et de l'utilisateur	Guide de l'utilisateur de NetWitness UEBA

Maintenance

L'administrateur peut exécuter les tâches suivantes dans n'importe quel ordre.

Description	Références
 System Administrator  Content Expert (Threat Intelligence)	
Gérez la liste des requêtes et analysez les modèles de requête des autres utilisateurs du système NetWitness Platform.	Rubrique « Gérer les requêtes à l'aide de l'intégration d'URL » dans le Guide de maintenance du système
Ajustez les paramètres de configuration au niveau du système pour améliorer les performances ou limiter l'accès aux données.	Rubrique « Vérifier les attributs Requête (Query) et Session par rôle » dans le Guide de sécurité du système et de gestion des utilisateurs Rubrique « Configurer les paramètres Investigation » dans le Guide de configuration du système