NetWitness® Plate-forme

Version 12.4.0.0

Notes de mise à jour

NETWITNESS
Platform

Informations de contact

NetWitness Community à l'adresse https://community.netwitness.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

Contrat de licence

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 NetWitness Community. 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

Divers

Mars 2024

Sommaire

Nouveautés de la version 12.4.0.0

Les notes de version NetWitness 12.4.0.0 décrivent les nouvelles fonctionnalités, les améliorations, les correctifs de sécurité, les stratégies de mise à niveau, les problèmes résolus, les problèmes connus, les fonctionnalités de fin de vie, les numéros de build et les ressources d'auto-assistance.

Améliorations

Les sections suivantes constituent une liste complète et une description des améliorations apportées à des fonctionnalités spécifiques :

- Upgrade
- Fonction SASE
- Investigate
- Respond
- Actions de réponse
- Insight
- Analytique comportementale des utilisateurs et des entités
- Endpoint
- Gestion des contenus centralisée, basée sur des règles
- Services Concentrator, Decoder, Log Collector et Archiver
- Intégration des journaux
- Sécurité

Pour localiser les documents mentionnés dans cette section, voir https://community.netwitness.com/t5/netwitness-platform-online/netwitness-platform-all-documents/ta-p/676246.

La section Documentation produit contient des liens vers la documentation de cette version.

Upgrade

La section suivante décrit la nouvelle amélioration pour la mise à niveau :

Migration du système d'exploitation Alma

RedHat a annoncé que CentOS Linux 7 atteindra sa fin de vie (EOL) le 30 juin 2024. Pour s'adapter à ce changement, NetWitness Platform est désormais intégrée à la nouvelle version, AlmaLinux. Lorsque vous effectuez une mise à niveau vers la version NetWitness 12.4, vous serez automatiquement migré de CentOS 7.9 vers AlmaLinux 8.9. Le processus de mise à niveau de NetWitness Platform 12.4 est simple et régulier, comme toutes les autres mises à niveau précédentes. Vous n'avez pas à suivre de procédure spécifique pour la mise à niveau vers le système d'exploitation AlmaLinux.
AlmaLinux offre plusieurs avantages clés et de nouvelles fonctionnalités :

- La mise à niveau vers AlmaLinux est un processus intrinsèquement automatisé sans intervention manuelle.
- Il est livré avec un outil de pré-mise à niveau qui aide les administrateurs à détecter et à atténuer les problèmes avant d'exécuter le processus de mise à niveau proprement dit.
- Gain de temps et d'efforts administratifs.
- Conserve le contrôle sur les applications installées.
- Conserve la plupart des informations de configuration.

NetWitness Platform rationalise le processus de mise à niveau, permet d'économiser du temps et des ressources et maintient le contrôle sur les applications et configurations installées lors de la migration de CentOS 7.9 vers AlmaLinux 8.9.

Fonction SASE

La section suivante décrit la nouvelle amélioration pour SASE :

Intégrations NetWitness SASE

- **Intégration de NetWitness SASE avec Palo Alto Networks** - présente l'intégration de NetWitness avec Palo Alto Prisma SASE pour fournir une visibilité complète du réseau et des journaux. Grâce à cette intégration technique personnalisée, les utilisateurs de NetWitness obtiennent un aperçu du comportement et de la communication entre les appareils et les services dans les réseaux distants et distribués dans le cadre de déploiements sur site, hybrides et cloud. L'intégration NetWitness-Palo Alto SASE permet aux clients de tirer parti de la flexibilité du SASE et de ses avantages inhérents en matière de sécurité tout en conservant une visibilité complète sur la détection et la réponse aux menaces.
- **Intégration de NetWitness SASE avec Symantec par Broadcom (mode aperçu privé)** - présente l'intégration de NetWitness avec Symantec par Broadcom SASE pour fournir une visibilité complète du réseau et des journaux. Grâce à cette intégration technique personnalisée, les utilisateurs de NetWitness obtiennent un aperçu du comportement et de la communication entre les appareils et les services dans les réseaux distants et distribués dans le cadre de déploiements sur site, hybrides et cloud. L'intégration NetWitness-Broadcom SASE permet aux clients de tirer parti de la flexibilité du SASE et de ses avantages inhérents en matière de sécurité tout en conservant une visibilité complète sur la détection et la réponse aux menaces.

  Remarque : Dans la version 12.4, l'intégration de NetWitness SASE avec Symantec par Broadcom est en mode aperçu privé.

Pour en savoir plus, consultez le *Guide de configuration Broadcom SASE pour la version 12.4* et *Guide de configuration Palo Alto Prisma SASE pour la version 12.4*.

Configuration du cloud hybride NetWitness SASE

Les administrateurs peuvent désormais opter pour un modèle de Cloud hybride pour SASE. La configuration de Cloud hybride SASE est une conception basée sur les données. Le Cloud hybride SASE fournit des communications plus efficaces et sécurisées entre les composants de NetWitness Platform. Le serveur d'administration NetWitness contient un script nw-create-cloud-hybrid, qui déploiera le réseau de superposition NetWitness et les nœuds NetWitness définis dans leurs régions respectives dans Google Cloud Platform (GCP). Le réseau NetWitness Peer-to-Peer (nw-ppn) fournit une communication sécurisée, mutuellement authentifiée et basée sur l'infrastructure à clé publique entre les composants NetWitness.

Pour en savoir plus, consultez *Guide d'installation SASE pour la version 12.4*.

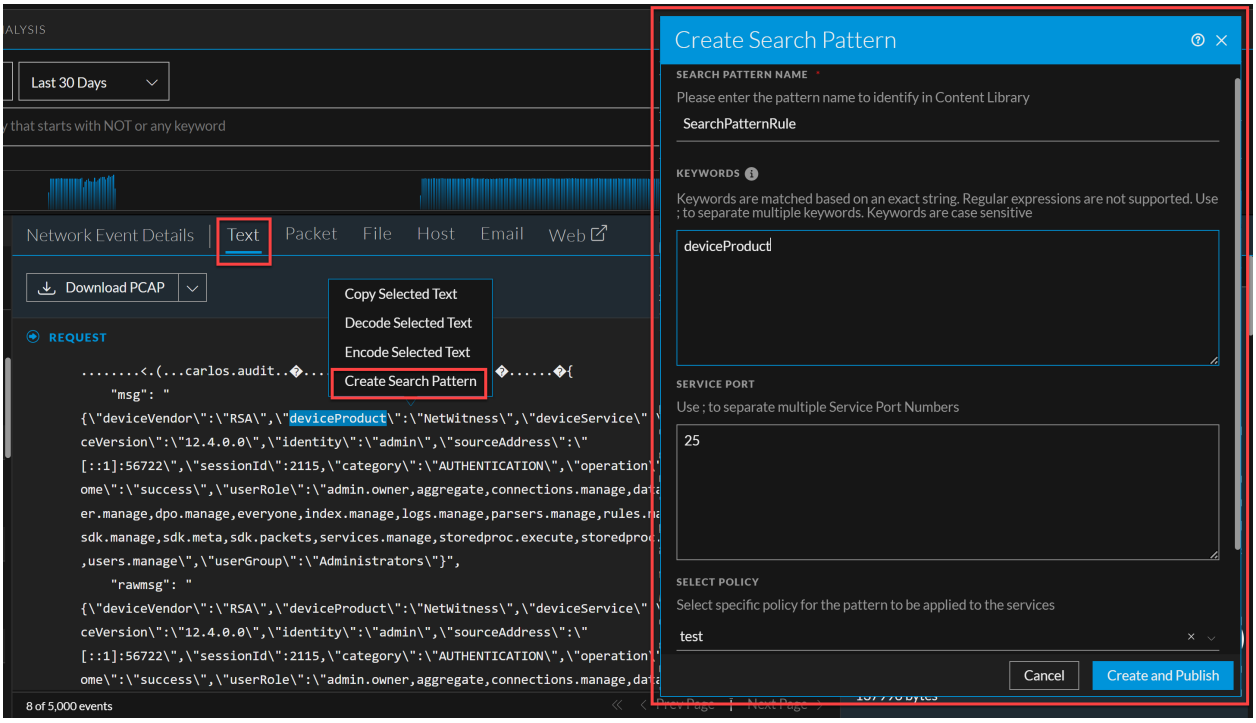
Investigate

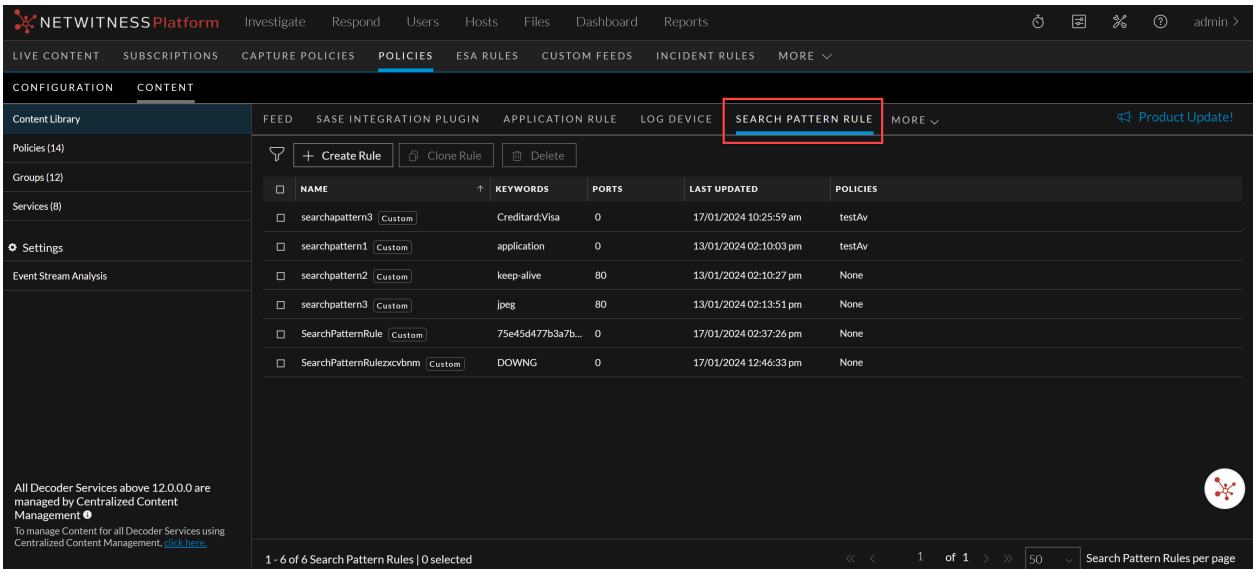
La section suivante décrit les nouvelles améliorations du composant Investigate :

Création d'un analyseur de réseau interactif

Dans la vue **Investigate** > **Événements**, les utilisateurs peuvent convertir les modèles exacts sélectionnés ou les mots-clés trouvés dans le trafic réseau qu'ils examinent lors de la reconstruction de la session de texte en un analyseur de réseau. Ce processus rationalisé permet à l'utilisateur de générer des méta pour déclencher un incident (par exemple, une détection future) sans qu'il ne soit nécessaire de comprendre comment créer l'analyseur.

Les utilisateurs peuvent également créer un analyseur de réseau à l'aide de mots-clés à partir de la vue **(Configurer)** > **Règles** > **Bibliothèque de contenu** > **Plus** > **Règle de modèle de recherche**.

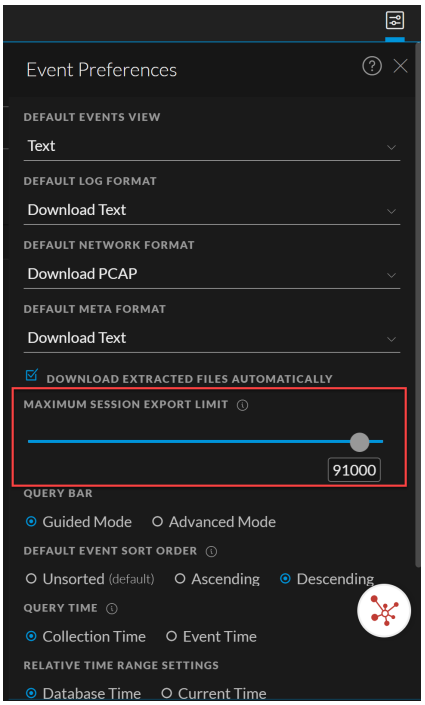




Pour plus d'informations, voir le sujet **Créer un modèle de recherche dans l'onglet Texte** dans le *Guide de l'utilisateur de NetWitness Investigate* et le sujet **Gérer la règle de modèle de recherche** dans le *Guide de gestion de contenu centralisé basé sur des règles*.

Télécharger plus de sessions que ce qui est affiché dans le tableau des événements

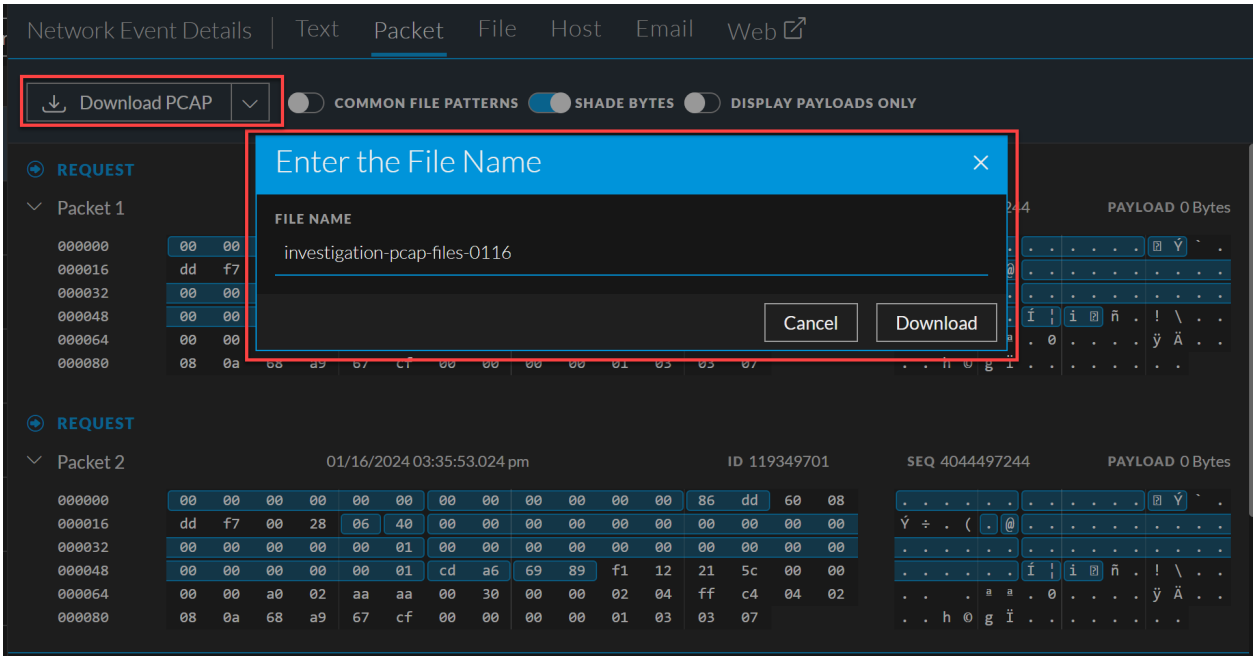
Une nouvelle préférence utilisateur, **Limite maximale d'exportation de session**, a été ajoutée au panneau **Préférences d'événements** dans la vue **Investigate** > **Événements**. Les analystes peuvent utiliser ce paramètre pour ajuster le nombre de sessions disponibles pour l'exportation à l'aide des options du menu **Tout télécharger**. Cette amélioration rend le nombre de sessions exportées indépendant du nombre de sessions affichées dans le tableau Événements.



Pour plus d'informations, voir le sujet **Définir les préférences utilisateur pour la vue Événements** dans le *Guide de l'utilisateur de NetWitness Investigate*.

Option de téléchargement des fichiers avec des noms personnalisés

Les analystes peuvent désormais utiliser des noms personnalisés lors du téléchargement de fichiers d'événements à partir de la vue du panneau **Événements**. Les noms personnalisés facilitent l'organisation et la gestion des fichiers d'événements téléchargés, ce qui permet aux analystes d'économiser du temps et des efforts.



Pour en savoir plus, consultez la rubrique **Télécharger les données dans la vue Événement** du *guide de l'utilisateur NetWitness Investigate*.

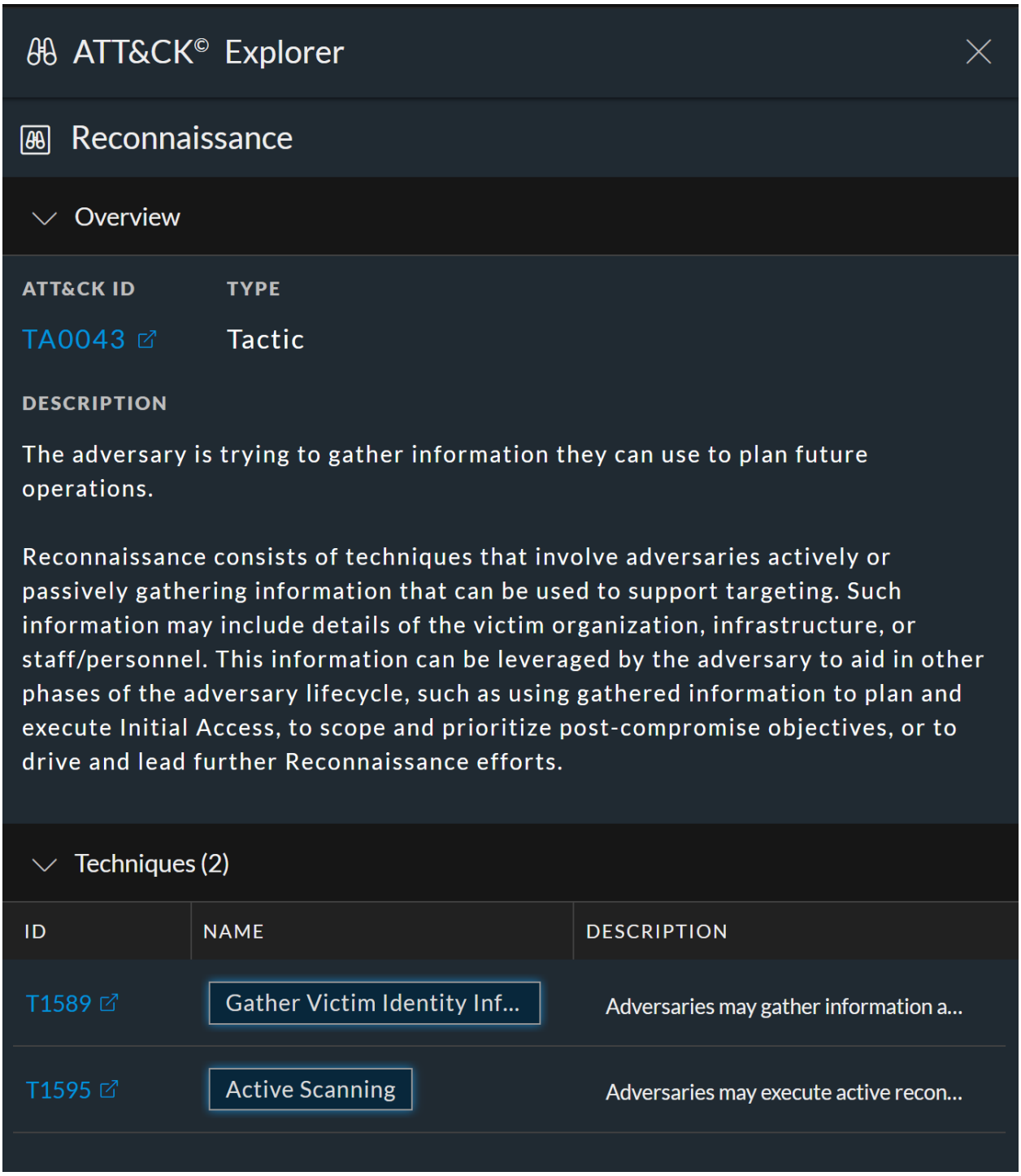
Respond

Les sections suivantes décrivent les nouvelles améliorations du composant Respond :

Intégration de MITRE ATT&CK® avec NetWitness

MITRE ATT&CK® est une base de connaissances organisée sur les techniques et tactiques de l'adversaire. Elle fournit un niveau approprié de catégorisation des actions adverses et des moyens spécifiques de se défendre contre elles. Les analystes peuvent consulter la liste générale des tactiques, techniques et sous-techniques spécifiées, ainsi que leurs détails, et découvrir comment les menaces et vulnérabilités potentielles de leur environnement sont associées au cadre MITRE ATT&CK.

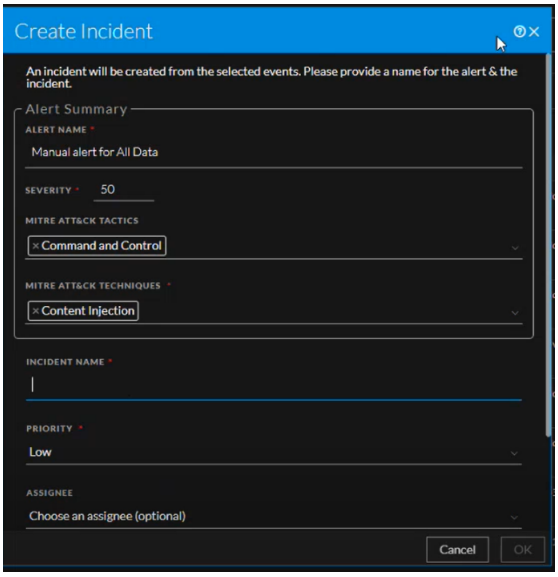
Le nouveau panneau **ATT&CK© Explorer** fournit des informations sur les tactiques et techniques de l'adversaire associées aux incidents dans la vue **Respond**.



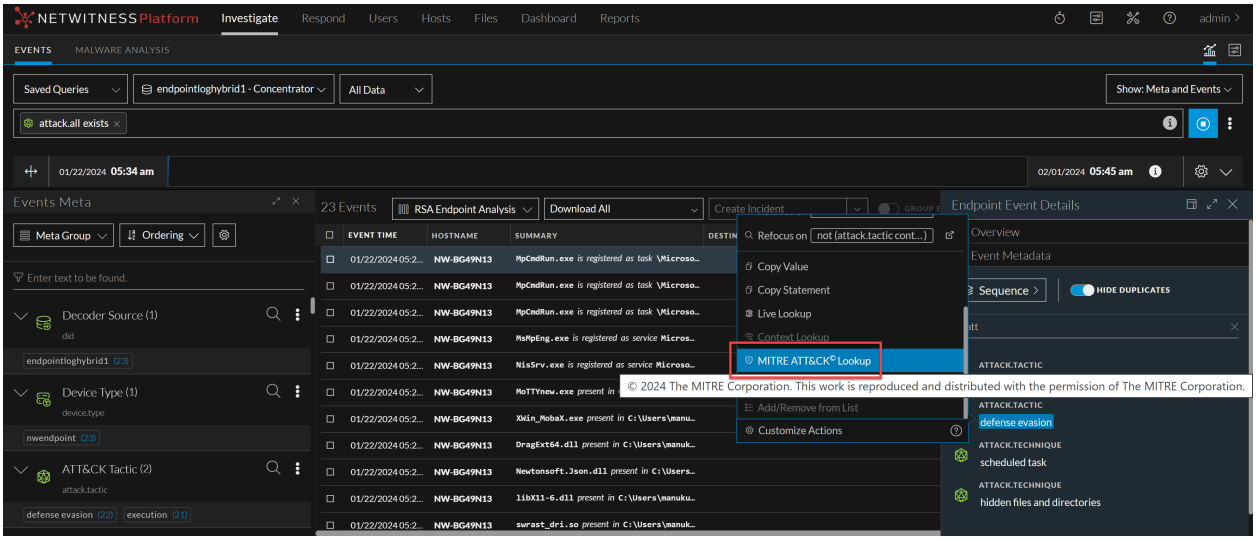
NetWitness Live est intégré au framework MITRE ATT&CK pour aider les analystes à visualiser les tactiques et techniques MITRE ATT&CK associées aux **règles d'application** et aux **règles Event Stream Analysis**. Le panneau droit Détails du service (**(Configurer)** > **Règles** > **Contenu** > **Bibliothèque de contenu** > **Règle d'application** ou **Règle Event Stream Analysis** > cliquez sur une ligne > panneau droit Détails du service) a été amélioré pour fournir des informations sur les tactiques et techniques MITRE ATT&CK.

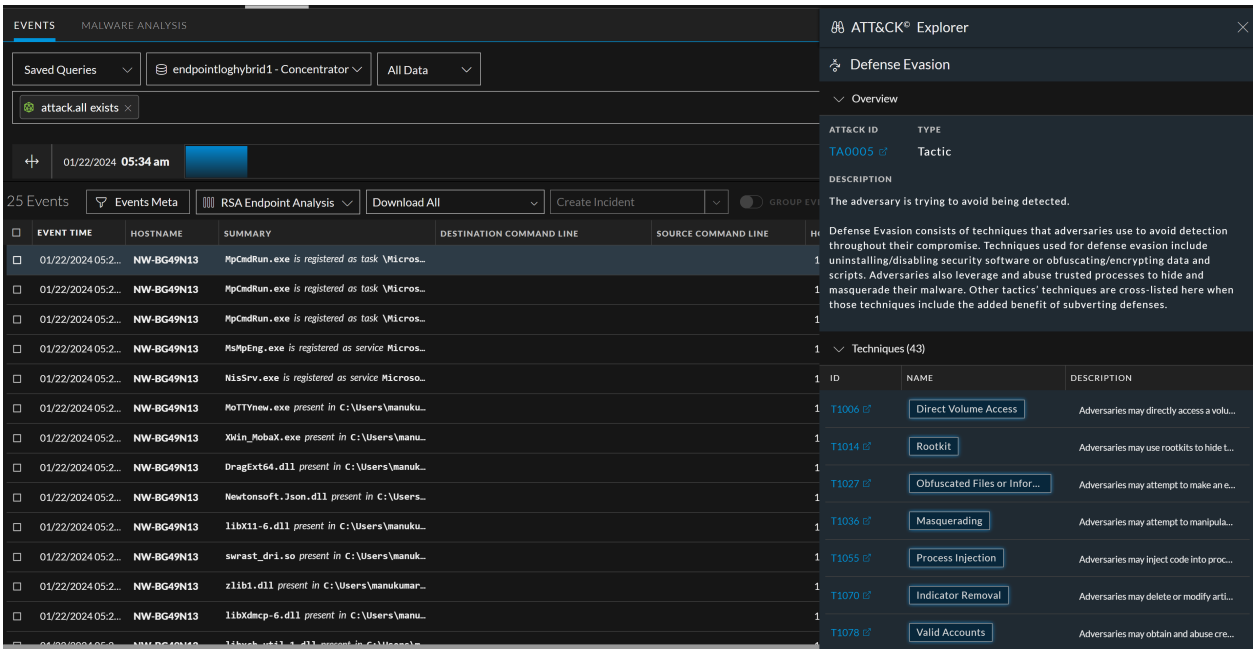
Vous pouvez baliser les tactiques et techniques MITRE ATT&CK tout en créant une **Règle d'application** ou une **Règle Event Stream Analysis** personnalisée.

Vous pouvez également sélectionner les tactiques et techniques MITRE ATT&CK lors de la création d'un incident à partir de la vue **Investigate** > **Événements**.



Ainsi, les clés méta **ATTACK.TACTIC** et **ATTACK.TECHNIQUE** du panneau **Métadonnées des événements** a été amélioré avec l'intégration de **Recherche MITRE ATT&CK©** pour vous aider à obtenir plus d'informations sur la tactique et la technique spécifiques associées à l'événement.





Le nouveau panneau **ATT&CK© Explorer** s'affiche lorsque vous cliquez sur **MITRE ATT&CK© Lookup**.

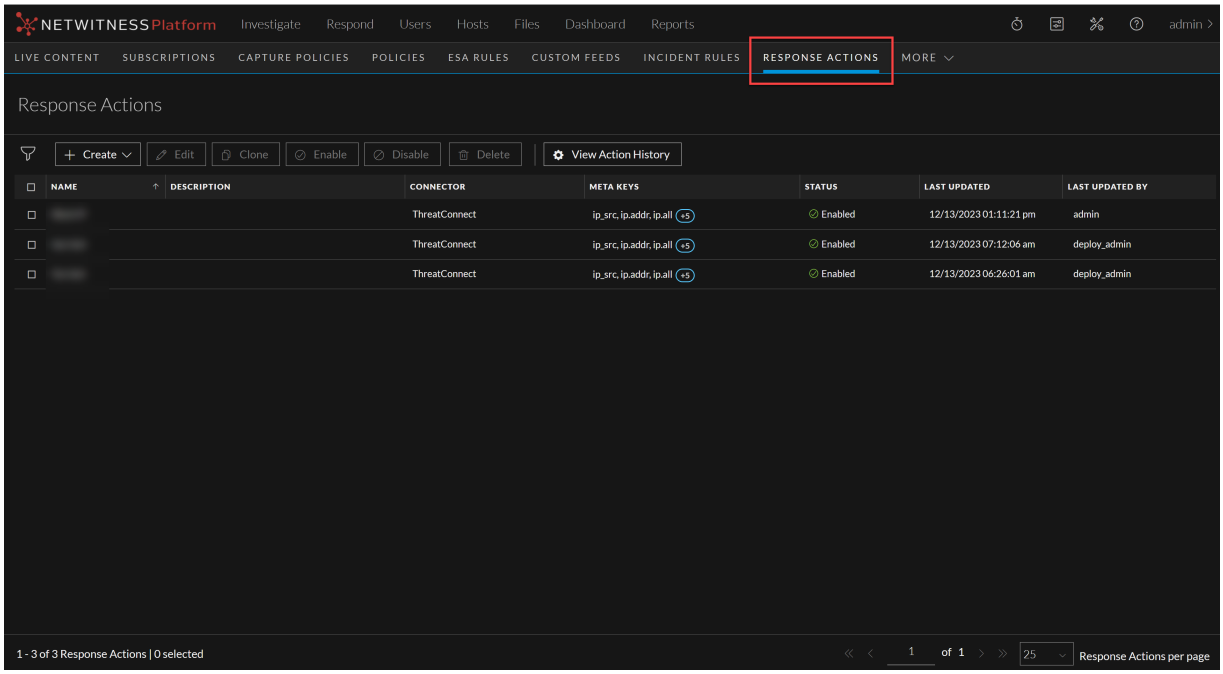
Pour plus d'informations, consultez le Guide de l'utilisateur de NetWitness Respond pour la version 12.4, le *Guide de l'utilisateur de NetWitness Investigate* et le *Guide de gestion de contenu centralisé basé sur des règles*.

Actions de réponse

Les actions de réponse sont les opérations réactives effectuées sur les métas configurées à l'aide d'un outil ou d'un connecteur tiers tel que ThreatConnect après le tri d'un événement. **Actions de réponse**, la nouvelle fonctionnalité ajoutée dans **(CONFIGURER)** > **Plus** vous permet d'effectuer les actions suivantes :

- Créer et gérer des actions de réponse pour les métas prises en charge disponibles dans les vues **Respond**, **Investigate**, **Hôtes** et **Utilisateurs**.
- Effectuez des actions rapides sur la méta configurée et publiez la méta avec des paramètres

supplémentaires sur le connecteur pour effectuer d'autres actions.



Pour plus d'informations, consultez le *Guide de configuration Actions de réponse NetWitness pour la version 12.4*.

Insight

Les sections suivantes décrivent les nouvelles améliorations du composant Insight :

Liste blanche des alertes Insight dans la vue Respond

Les administrateurs et les analystes peuvent désormais ajouter à la liste blanche les alertes Insight indésirables et récurrentes générées dans la vue **Respond** > **Alertes**. Cette amélioration offre la possibilité de sélectionner des valeurs spécifiques, telles que l'adresse IP et le type d'actif, et de définir une condition de liste blanche pour empêcher la génération d'alertes indésirables pour ces valeurs. Grâce à cette amélioration, les analystes peuvent rationaliser le processus de gestion des alertes en excluant des adresses IP ou des types d'actifs spécifiques connus pour être fiables et sécurisés. Cette optimisation minimise les alertes inutiles générées dans la vue **Respond** > **Alertes**, réduisant ainsi le temps et les efforts requis pour examiner et analyser les alertes.

Pour plus d'informations, consultez la section **NetWitness Insight** dans le *Portail de documentation NetWitness*.

Analytique comportementale des utilisateurs et des entités

La section suivante décrit les nouvelles améliorations pour le composant UEBA :

Prise en charge des appareils Cisco Adaptive Security Appliance (ASA) et Fortinet VPN

NetWitness UEBA a ajouté la prise en charge des périphériques VPN Cisco ASA et Fortinet. Grâce à cette amélioration, l'UEBA peut désormais traiter les journaux VPN Cisco ASA et Fortinet, ce qui permet de collecter et d'analyser les informations sur l'activité des utilisateurs.

Pour plus d'informations, consultez la section **Sources prises en charge par l'UEBA par schéma** dans le *Guide de configuration de l'UEBA*.

Améliorations des performances UEBA

Les améliorations de performances suivantes sont apportées pour UEBA dans la version 12.4.0.0 :

- Optimisation des modèles d'agrégation et d'accumulation pour générer et stocker des modèles en parallèle.
- Optimisation de la tâche d'agrégation horaire des scores pour agréger et marquer en parallèle.

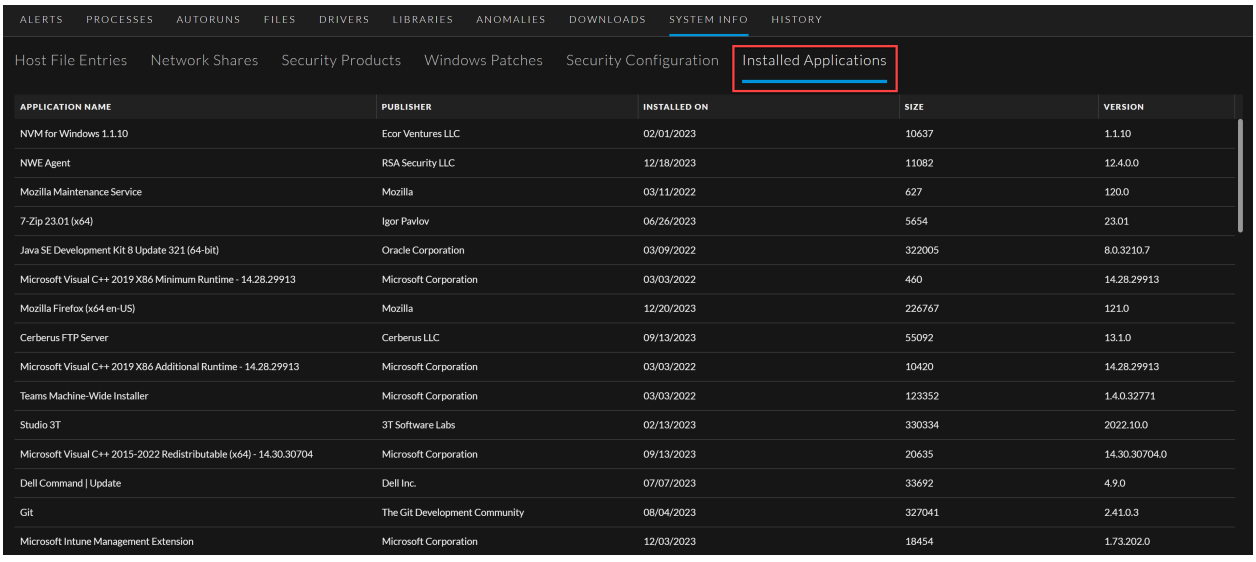
Pour plus d'informations sur l'échelle prise en charge, consultez la rubrique **Période d'apprentissage par échelle pour la version 12.4** dans le *Guide de configuration de l'UEBA*.

Endpoint

La section suivante décrit les nouvelles améliorations pour le composant Endpoint :

Affichage des applications installées

La vue **Détails** des hôtes > **Informations système** a été améliorée pour permettre aux analystes de visualiser les informations sur les différentes applications installées sur une machine Windows.

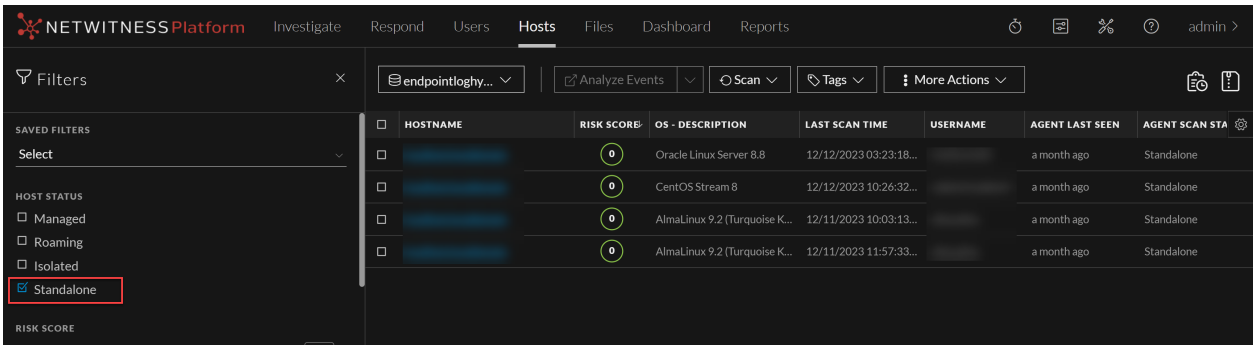


APPLICATION NAME	PUBLISHER	INSTALLED ON	SIZE	VERSION
NVM for Windows 1.1.10	Ecor Ventures LLC	02/01/2023	10637	1.1.10
NWE Agent	RSA Security LLC	12/18/2023	11082	12.4.0.0
Mozilla Maintenance Service	Mozilla	03/11/2022	627	120.0
7-Zip 23.01 (x64)	Igor Pavlov	06/26/2023	5654	23.01
Java SE Development Kit 8 Update 321 (64-bit)	Oracle Corporation	03/09/2022	322005	8.0.3210.7
Microsoft Visual C++ 2019 X86 Minimum Runtime - 14.28.29913	Microsoft Corporation	03/03/2022	460	14.28.29913
Mozilla Firefox (x64 en-US)	Mozilla	12/20/2023	226767	121.0
Cerberus FTP Server	Cerberus LLC	09/13/2023	55092	13.1.0
Microsoft Visual C++ 2019 X86 Additional Runtime - 14.28.29913	Microsoft Corporation	03/03/2022	10420	14.28.29913
Teams Machine-Wide Installer	Microsoft Corporation	03/03/2022	123352	1.4.0.32771
Studio 3T	3T Software Labs	02/13/2023	330334	2022.10.0
Microsoft Visual C++ 2015-2022 Redistributable (x64) - 14.30.30704	Microsoft Corporation	09/13/2023	20635	14.30.30704.0
Dell Command | Update	Dell Inc.	07/07/2023	33692	4.9.0
Git	The Git Development Community	08/04/2023	327041	2.41.0.3
Microsoft Intune Management Extension	Microsoft Corporation	12/03/2023	18454	1.73.202.0

Pour plus d'informations, consultez le *Guide d'utilisation de NetWitness Endpoint pour la version 12.4*.

Analyse autonome pour les agents Linux

Les administrateurs peuvent exécuter des analyses hors ligne ou autonomes sur les hôtes Linux pour effectuer une analyse des menaces sur les machines Linux avec Air Gap.



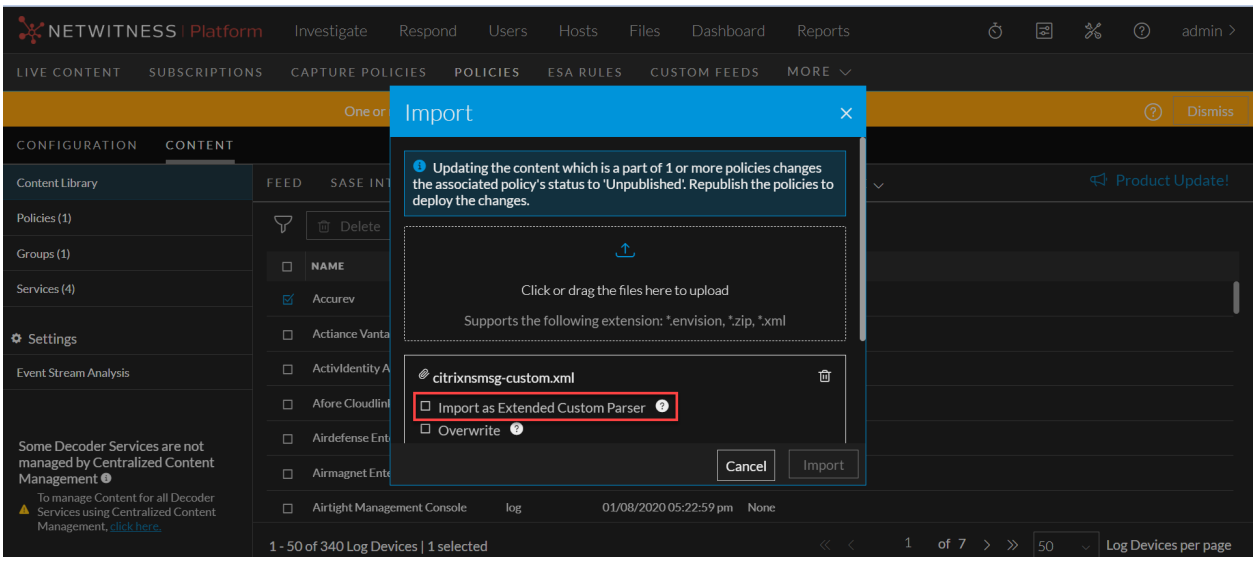
Pour plus d'informations, consultez le *Guide d'utilisation de NetWitness Endpoint pour la version 12.4*.

Gestion des contenus centralisée, basée sur des règles

Les améliorations suivantes sont apportées pour CCM dans la version 12.4.0.0 :

Améliorations pour le bon fonctionnement et le déploiement d'analyseurs personnalisés dans les services via CCM

Introduction de la possibilité d'importer du XML individuel (type de contenu Log Device) dans la bibliothèque de contenu. Vous pouvez télécharger les analyseurs de base ou les analyseurs étendus sous forme de fichier XML autonome. Lors de l'importation de fichiers XML, vous pouvez éventuellement l'associer à son analyseur de base correspondant, le traitant ainsi comme un analyseur d'extension. Pour importer un XML autonome en tant qu'analyseur étendu, sélectionnez **Importer en tant qu'analyseur personnalisé étendu** dans l'écran **Importer**.



La bibliothèque de contenu affiche désormais les analyseurs de base et les analyseurs d'extension comme des éléments distincts, offrant ainsi une vue claire et organisée aux utilisateurs. Cette séparation garantit que les utilisateurs peuvent facilement identifier et gérer les deux types d'analyseurs au sein de la bibliothèque. De plus, lorsqu'un analyseur d'extension est ajouté à une règle, l'analyseur de base correspondant est également automatiquement inclus dans la règle. Cette intégration rationalisée simplifie le processus pour les utilisateurs, éliminant le besoin de lier manuellement les analyseurs de base et d'extension lors de la création ou de la modification de règles.

Pour plus d'informations, consultez la section **Importer du contenu dans la bibliothèque de contenu** dans le *Guide de gestion de contenu centralisé basé sur des règles*.

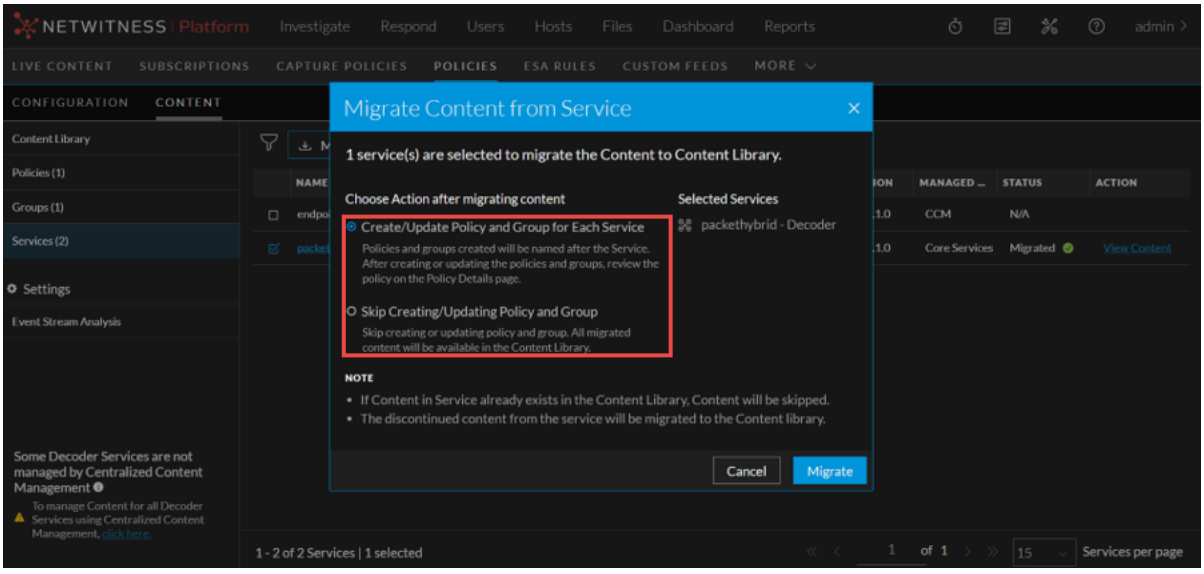
Améliorations lors de la suppression d'un service du groupe

Lors de la suppression d'un service du groupe, vous pouvez choisir soit de supprimer le contenu du service, puis de supprimer le service du groupe, soit de supprimer le service du groupe sans supprimer le contenu.

Pour plus d'informations, consultez les sections **Modifier un groupe**, **Modifier une règle** et **Supprimer une règle** dans le *Guide de gestion de contenu centralisé basé sur des règles*.

Possibilité de migrer le contenu du service

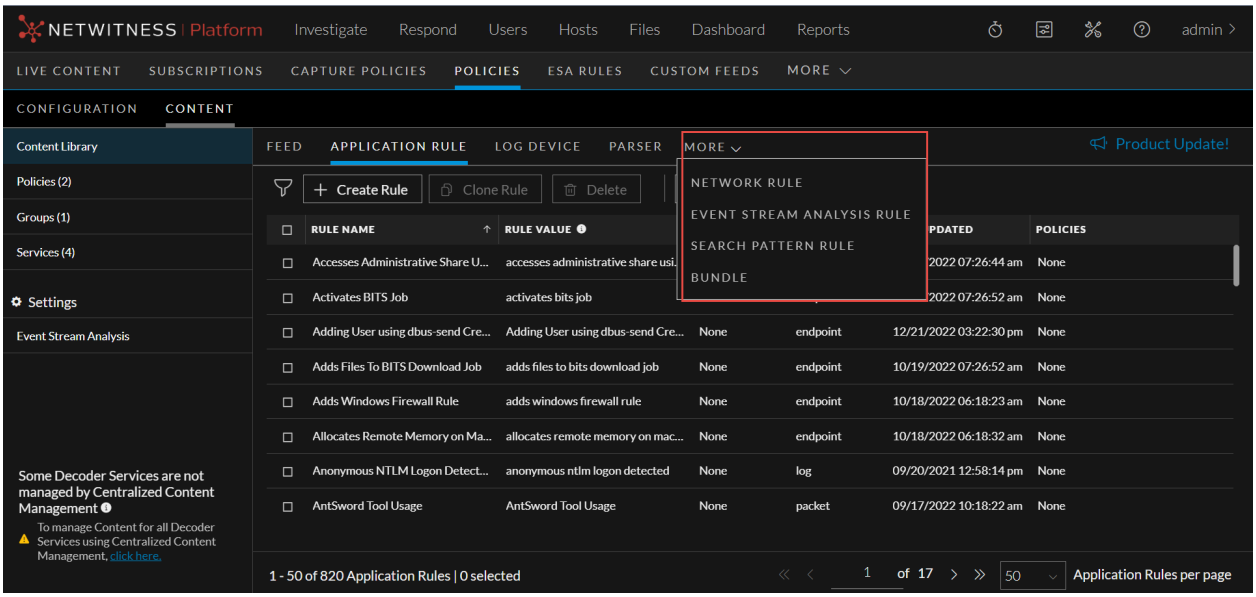
CCM est amélioré pour migrer à nouveau le contenu d'un service même s'il est déjà migré et/ou attribué à des groupes et des règles. Lors de la migration du contenu d'un service déjà associé à une règle, vous pouvez éventuellement mettre à jour la règle associée avec le contenu migré. Pour mettre à jour la règle et le groupe existants pour le service après la remigration du service, les options disponibles sur la page **Migrer le contenu à partir du service** sont mises à jour pour **Créer/ Mettre à jour la règle et le groupe pour chaque service** et **Ignorer la création/mise à jour d'une règle et d'un groupe**.



Pour plus d'informations, consultez la section **Migrer le contenu du service** dans le *Guide de gestion de contenu centralisé basé sur des règles*.

Améliorations de l’interface utilisateur

Le menu de navigation **PLUS** est ajouté à l’interface utilisateur du CCM pour afficher les offres groupées, les modèles de recherche et les intégrations par défaut. Lorsque vous sélectionnez le type de contenu dans le menu **PLUS**, ce type de contenu apparaît à gauche du menu **PLUS**.

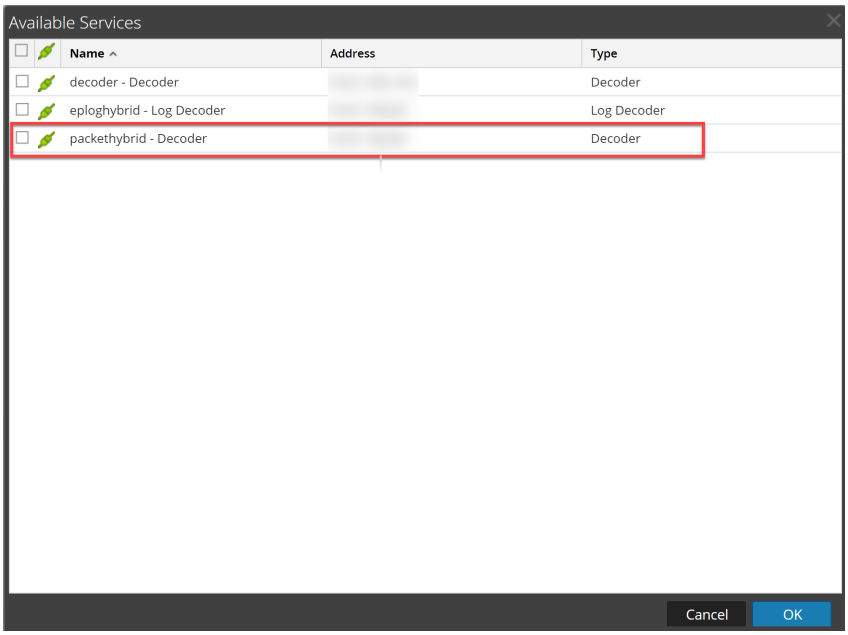


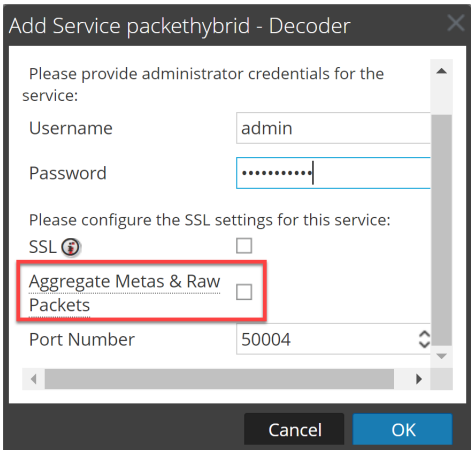
Services Concentrator, Decoder, Log Collector et Archiver

Les améliorations suivantes sont apportées aux services Concentrator, Decoder, Log Collector et Archiver dans la version 12.4.0.0 :

Rétention sélective pour Packet Decoder

Cette version offre une option de rétention sélective aux clients NDR, leur permettant de réduire de manière efficace les exigences de rétention requises tout en conservant des preuves importantes pour continuer à être leader en matière de capacités d’investigation et de chasse aux menaces. Ceci est possible car les administrateurs peuvent désormais configurer l’hôte Packet Decoder pour Archiver en tant que source de données de manière transparente à partir de l’onglet  **(Admin)** > **Services** > Vue **Config** > **Général**. De plus, les administrateurs peuvent désormais sélectionner le type d’agrégation souhaité à l’aide de la nouvelle option **Agréger les métas et les paquets bruts**. De cette manière, les administrateurs peuvent choisir d’agréger le service Décoder uniquement en fonction des valeurs de métadonnées ou à la fois en fonction des valeurs de métadonnées et des paquets bruts.





Pour plus d'informations, consultez la section **Ajouter un Packet Decoder en tant que source de données à Archiver** dans le *Guide de configuration Archiver*.

Possibilité de déprécier l'utilisation de l'adresse IP pour l'authentification de base

Netwitness a déconseillé l'utilisation de l'adresse IP pour l'authentification de base de Windows Collection. Vous devez désormais utiliser le FQDN dans l'adresse source de l'événement et ajouter une entrée du même FQDN dans « /etc/hosts » lors de la configuration de l'authentification de base.

Nouvel utilitaire pour diffuser des méta depuis des décodeurs vers des outils tiers

Introduction d'un utilitaire bêta pour diffuser des méta depuis des décodeurs réseau vers d'autres outils tiers, facilitant ainsi l'intégration de NetWitness Platform à d'autres produits. Tout ou un sous-ensemble des métadonnées peut être diffusé en continu pour limiter la quantité envoyée à l'outil tiers en fonction du cas d'utilisation.

Pour plus d'informations, consultez le *Guide d'installation et de configuration des exportations méta*.

Intégration des journaux

NetWitness Platform prend en charge l'intégration des sources d'événements suivantes pour collecter et analyser les journaux. Sauf indication contraire, ces services sont pris en charge sur NetWitness Platform 12.2.0.0 ou version ultérieure.

- Accès Palo Alto Prisma
- VMware vSphere
- Inspection approfondie
- Journaux de VM Windows GCP (via le plug-in GCP)

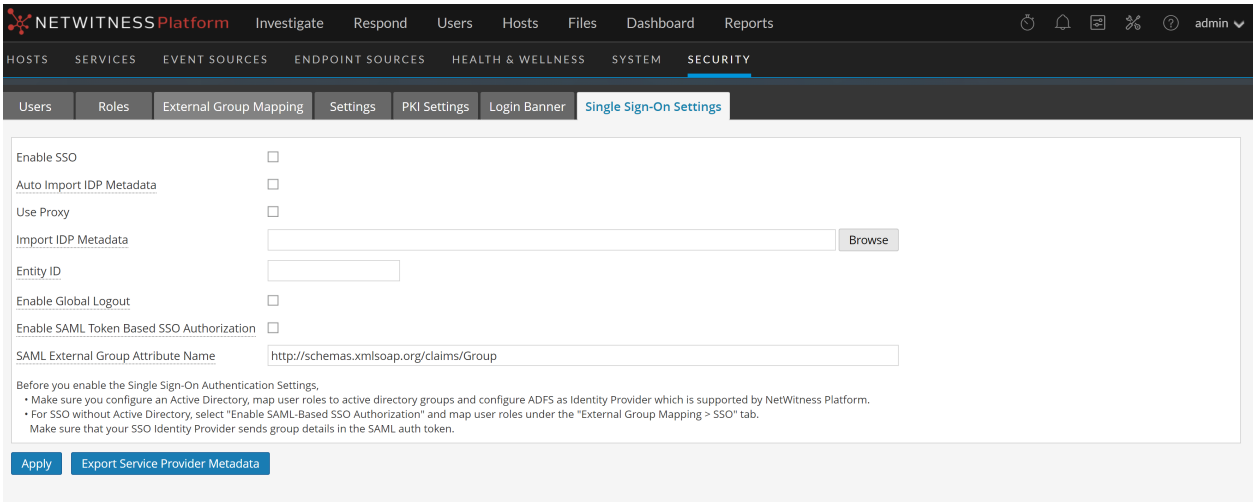
Remarque : À partir de la version 12.4, le plug-in VMWare est également disponible pour la collection d'événements et de tâches VMWare.

Pour plus d'informations sur l'intégration des services d'analyseur, consultez le Guide d'intégration de NetWitness Platform.

Sécurité

Authentification par authentification unique (SSO) indépendante de la configuration d'Active Directory (AD) dans NetWitness

À partir de NetWitness Platform version 12.4, NetWitness propose une authentification unique indépendante de la configuration AD dans NetWitness. Cela permet l'autorisation des utilisateurs via la liste des groupes d'utilisateurs intégrée dans le jeton d'authentification SAML reçu d'ADFS et leur vérification par rapport aux groupes d'utilisateurs déjà configurés dans NetWitness. Cela élimine le besoin pour les utilisateurs de configurer ou de s'appuyer sur les paramètres Active Directory dans NetWitness pour l'authentification. NetWitness prend désormais en charge Azure ADFS et Microsoft ADFS.



Pour plus d'informations, consultez la rubrique **Configurer l'authentification par authentification unique** dans le *Guide de sécurité du système et de gestion des utilisateurs*.

Correctifs relatifs à la sécurité

Pour plus d'informations sur les correctifs de sécurité, consultez https://community.netwitness.com/t5/netwitness-platform-advisories/ct-p/netwitness-advisories#security.

Mettre à niveau les chemins

Les stratégies de mise à niveau suivantes sont prises en charge par NetWitness 12.4.0.0

- NetWitness 12.3.1.0 vers 12.4.0.0
- NetWitness 12.3.0.0 vers 12.4.0.0
- NetWitness 12.2.0.1 vers 12.4.0.0
- NetWitness 12.2.0.0 vers 12.4.0.0

Pour plus d'informations sur la mise à niveau vers 12.4.0.0, consultez le Guide de mise à niveau pour NetWitness 12.4.0.0

IMPORTANT : Si vous souhaitez mettre à niveau les versions 11.7.x ou 11.7.x.x vers la version 12.4.0.0, vous devez d'abord effectuer une mise à niveau vers la version 12.2.0.0 ou 12.3.0.0 avant de passer à la version 12.4.

Cycle de vie de la version du produit pour NetWitness Platform

Consultez le Cycle de vie des versions du produit pour NetWitness Platform une liste des versions qui atteignent la fin de la période de support initial (EOPS).

Nouveautés dans les versions précédentes (11.7 à 12.3.1.0)

La section fournit de nouvelles fonctionnalités et améliorations pour toutes les versions précédentes prises en charge.

Pour plus d'informations, consultez https://community.netwitness.com/t5/netwitness-platform-online/what-s-new-in-previous-releases-11-7-to-12-1-1/ta-p/695650.

Problèmes corrigés dans la version 12.4.0.0

Cette section répertorie les problèmes résolus dans la version 12.4.0.0.

Pour plus d'informations sur les problèmes résolus, consultez la colonne Version corrigée dans la liste des problèmes connus de NetWitness® Platform (https://community.netwitness.com/t5/netwitness-platform-known-issues/netwitness-platform-known-issues/ta-p/571872) sur le portail NetWitness Community.

Correctifs de gestion des contenus centralisée, basée sur des règles

Numéro de suivi	Description
ASOC-142018	Le contenu Log Device publié à partir de CCM n'est pas désactivé lorsque le contenu est supprimé pour un service.
ASOC-141524	Les règles ESA n'ont pas pu être enregistrées en modifiant ou en mettant à jour la règle ESA. Les journaux de l'interface utilisateur NetWitness et de SA ont montré une exception d'exécution lors de l'enregistrement de la règle. De plus, lors du dépannage, le **flux Intel de menace non-IP RSA OSINT** n'avait pas d'ID unique associé à la règle et se produisait dans plusieurs documents des collections de règles de contenu.

Problèmes connus dans la version 12.4.0.0

Les problèmes qui restent non résolus dans cette version sont documentés dans la liste des problèmes connus de NetWitness® Platform sur le portail de NetWitness Community : https://community.netwitness.com/t5/netwitness-platform-known-issues/netwitness-platform-known-issues/ta-p/571872

Numéros de build pour les composants 12.4.0.0

Le tableau suivant répertorie les numéros de build des différents composants de NetWitness 12.4.0.0

Composant	Numéro de version
Serveur admin NetWitness	rsa-nw-admin-server-12.4.0.0-240117024246.5.165a1f70.el8.alma.noarch.rpm
NetWitness Contenu d'analyse avancée	rsa-nw-advanced-analytics-content-12.4.0.0-231212110357.5.9b3b362.el8.alma.noarch.rpm
NetWitness Serveur d'analyse avancée	rsa-nw-advanced-analytics-server-12.4.0.0-231212110325.5.9b3b362.el8.alma.noarch.rpm
NetWitness Appliance	rsa-nw-appliance-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Archiver	rsa-nw-archiver-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Plugin d'audit	rsa-audit-plugins-12.4.0.0-4892.5.9d0750b41.el8.noarch.rpm
NetWitness Audit RT	rsa-audit-rt-12.4.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitness Démarrage	rsa-nw-bootstrap-12.4.0.0-2401240926.5.a3d68ef.el8.noarch.rpm
NetWitness Broker	rsa-nw-broker-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Carlos RT	rsa-carlos-rt-12.4.0.0-2787.5.721a8daa7.el7.x86_64.rpm
NetWitness Cloud	rsa-nw-cloud-12.4.0.0-12867.5.957818c84.el8.x86_64.rpm
NetWitness Serveur Cloud Connector	rsa-nw-cloud-connector-server-12.4.0.0-240116135943.5.4220688.el8.alma.noarch.rpm
NetWitness Serveur de lien Cloud	rsa-nw-cloud-link-server-12.4.0.0-240117032857.5.d4a8422.el8.alma.noarch.rpm
NetWitness Collectd	rsa-collectd-12.4.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitness Collectd SMS	rsa-collectd-sms-12.4.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitness Description du composant	rsa-nw-component-descriptor-12.4.0.0-2402080831.5.a403c19.el8.noarch.rpm
NetWitness Concentrator	rsa-nw-concentrator-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Gestion de la configuration	rsa-nw-config-management-12.4.0.0-2402050947.5.b7e9f64.el8.noarch.rpm
NetWitness Serveur de configuration	rsa-nw-config-server-12.4.0.0-240109020724.5.dc657b7.el8.alma.noarch.rpm
Console NetWitness	rsa-nw-console-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm

NetWitness Serveur de contenu	rsa-nw-content-server-12.4.0.0-240109040529.5.314fc043.el8.alma.noarch.rpm
NetWitness Serveur ContextHub	rsa-nw-contexthub-server-12.4.0.0-240122010054.5.d98d0ac61.el8.alma.noarch.rpm
NetWitness Serveur de corrélation (ESA)	rsa-nw-correlation-server-12.4.0.0-240117103632.5.61d080a9.el8.alma.noarch.rpm
NetWitness Contenu du tableau de bord	rsa-nw-dashboard-content-20231220155210-5.noarch.rpm
NetWitness Decoder	rsa-nw-decoder-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Contenu analytique Decoder	rsa-nw-decoder-analytics-content-20231220155210-5.noarch.rpm
NetWitness Contenu Decoder	rsa-nw-decodercontent-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Déploiement de mise à niveau	rsa-nw-deployment-upgrade-12.4.0.0-2402050945.5.1903a3b.el8.noarch.rpm
Agents NetWitness Endpoint	rsa-nw-endpoint-agents-12.4.0.0-2402061657.5.db93b9a.el8.x86_64.rpm
NetWitness Serveur Endpoint Broker	rsa-nw-endpoint-broker-server-12.4.0.0-240103053136.5.8430874.el8.alma.noarch.rpm
NetWitness Contenu analytique Endpoint Decoder	rsa-nw-endpointdecoder-analytics-content-20231220155210-5.noarch.rpm
Serveur NetWitness Endpoint	rsa-nw-endpoint-server-12.4.0.0-240125030031.5.12c246114.el8.alma.noarch.rpm
NetWitness Esper Enterprise	rsa-nw-esper-enterprise-12.4.0.0-2311071130.5.04c15de.el8.alma.noarch.rpm
NetWitness Serveur d’intégration	rsa-nw-integration-server-12.4.0.0-240117101347.5.0ed5cc33.el8.alma.noarch.rpm
Serveur NetWitness Investigate	rsa-nw-investigate-server-12.4.0.0-240109023320.5.2a0d2764.el8.alma.noarch.rpm
Serveur Web existant NetWitness	rsa-nw-legacy-web-server-12.4.0.0-240122162503.5.40628dd.el8.almalinux.noarch.rpm
NetWitnessServeur de licences	rsa-nw-license-server-12.4.0.0-240111044400.5.a6108af.el8.alma.noarch.rpm
NetWitness Log Collector	rsa-nw-logcollector-12.4.0.0-15127.5.527ec7727.el8.x86_64.rpm
NetWitness Contenu Log Collector	rsa-nw-logcollectorcontent-20240105141144-5.x86_64.rpm
NetWitness Log Collector Perl	rsa-nw-logcollector-perl-12.4.0.0-15127.5.527ec7727.el8.x86_64.rpm

NetWitness Outils Log Collector	rsa-nw-logcollector-tools-12.4.0.0-15127.5.527ec7727.el8.x86_64.rpm
NetWitness Log Decoder	rsa-nw-logdecoder-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Contenu analytique Log Decoder	rsa-nw-logdecoder-analytics-content-20231220155210-5.noarch.rpm
NetWitness Contenu de base Log Decoder	rsa-nw-logdecoder-base-content-20240124060008-5.x86_64.rpm
NetWitness Log Player	rsa-nw-logplayer-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Serveur Malware Analytics	rsa-nw-malware-analytics-server-12.4.0.0-240207115909.5.1511622.el8.almalinux.x86_64.rpm
NetWitness Utilitaire de méta-exportation	rsa-nw-metaexport-utility-12.4.0.0-110124.5.el8.x86_64.rpm
NetWitness Serveur de metrics	rsa-nw-metrics-server-12.4.0.0-240109050254.5.c078db1.el8.alma.noarch.rpm
NetWitness Serveur infrarouge de nœud	rsa-nw-node-infra-server-12.4.0.0-240116091133.5.70861f6.el8.alma.noarch.rpm
NetWitness Interface de ligne de commande Orchestration	rsa-nw-orchestration-cli-12.4.0.0-2401091103.5.7317baa.el8.noarch.rpm
Serveur NetWitness Orchestration	rsa-nw-orchestration-server-12.4.0.0-240119064852.5.a87bb81f.el8.alma.noarch.rpm
NetWitness Espace réservé	rsa-nw-placeholder-12.4.0.0-2310040926.5.cebd204.el8.noarch.rpm
NetWitness Presidio Airflow	rsa-nw-presidio-airflow-12.4.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Serveur de configuration Presidio	rsa-nw-presidio-configserver-12.4.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Presidio Core	rsa-nw-presidio-core-12.4.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Initialisation de la recherche Presidio Elastic	rsa-nw-presidio-elasticsearch-init-12.4.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Presidio Ext NetWitness	rsa-nw-presidio-ext-netwitness-12.4.0.0-2401151152.5.18bd06b.el8.noarch.rpm
NetWitness Presidio Manager	rsa-nw-presidio-manager-12.4.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Sortie Presidio	rsa-nw-presidio-output-12.4.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Interface utilisateur Presidio	rsa-nw-presidio-ui-12.4.0.0-2402270745.5.0844250.el8.noarch.rpm

NetWitness Protobufs	rsa-protobufs-rt-12.4.0.0-928.5.6254aabd8.el8.x86_64.rpm
NetWitness Outils de récupération	rsa-nw-recovery-tool-12.4.0.0-2401230435.5.f34a9fd.el8.noarch.rpm
NetWitness Serveur relais	rsa-nw-relay-server-12.4.0.0-240112083607.5.6d41796.el8.alma.noarch.rpm
NetWitness Serveur Reporting Engine	rsa-nw-re-server-12.4.0.0-5996.5.b76234be4.el8.x86_64.rpm
Serveur NetWitness Respond	rsa-nw-respond-server-12.4.0.0-240110052505.5.1eda6132f.el8.alma.noarch.rpm
NetWitness Serveur d'actions de réponse	rsa-nw-response-actions-server-12.4.0.0-240116034125.5.0af5d71.el8.alma.noarch.rpm
NetWitness Mise à jour de l'autorité de certification racine	rsa-nw-root-ca-update-12.4.0.0-2401221231.5.96cd15b.el8.noarch.rpm
NetWitness Outils SA	rsa-sa-tools-12.4.0.0-2401251338.5.89600eb.el8.noarch.rpm
NetWitness Interface de ligne de commande de sécurité	rsa-nw-security-cli-12.4.0.0-2401091103.5.18ab320.el8.noarch.rpm
NetWitness Serveur de sécurité	rsa-nw-security-server-12.4.0.0-240123034132.5.11d93f41.el8.alma.noarch.rpm
NetWitness Shell	rsa-nw-shell-12.4.0.0-240108140410.5.0b0d73f5.el8.alma.noarch.rpm
NetWitness Plugins de rapport SOS	rsa-nw-sosreport-plugins-12.4.0.0-2401162235.5.af21a76.el8.noarch.rpm
NetWitness SMS Runtime RT	rsa-sms-runtime-rt-12.4.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitness Serveur SMS	rsa-sms-server-12.4.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitness Serveur source	rsa-nw-source-server-12.4.0.0-240207074107.5.4b84868b1.el8.alma.noarch.rpm
NetWitness Contenu du serveur source	rsa-nw-sourceserver-content-20240105141144-5.x86_64.rpm
Interface utilisateur NetWitness	rsa-nw-ui-12.4.0.0-240131063757.5.d1b137ecbc.el8.alma.noarch.rpm
NetWitness Workbench	rsa-nw-workbench-12.4.0.0-12866.5.1aefe557c.el8.x86_64.rpm

Obtenir de l'aide avec NetWitness Platform

Documentation produit

Cette version est fournie avec la documentation suivante :

Documentation	URL d'emplacement
Table des matières principale de NetWitness Platform	https://community.netwitness.com/t5/netwitness-platform-online/tkb-p/netwitness-online-documentation
Documentation produit de NetWitness Platform 12.4.0.0	https://community.netwitness.com/t5/netwitness-platform-online/tkb-p/netwitness-online-documentation
Guide de mise à niveau de NetWitness Platform 12.4.0.0	https://community.netwitness.com/t5/rsa-netwitness-platform-staged/upgrade-guide-for-12-4/ta-p/709308
NetWitness Analytics sur le cloud	Pour en savoir plus sur les nouvelles fonctionnalités et améliorations des versions de NetWitness Analytics sur le Cloud, consultez la section Nouveautés suivante : Pour UEBA Cloud, voir https://docs.netwitness.com/netwitnessueba/release_information/whats_new/. Pour Insight, voir https://docs.netwitness.com/netwitnessinsight/release-information/insight_whatsnew/.

Ressources d'assistance en libre-service

Il existe plusieurs options qui vous fournissent de l'aide lorsque vous en avez besoin pour l'installation et l'utilisation de NetWitness :

- Consultez la documentation pour tous les aspects de NetWitness ici : https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation
- Utilisez les champs **Recherche** et **Créer une publication** du portail NetWitness Community pour trouver des informations spécifiques ici : https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions
- Voir la base de connaissances NetWitness : https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base
- Reportez-vous à la section Dépannage dans les guides.

- Voir également Articles de blog sur NetWitness® Platform.
- Si vous avez besoin d'une aide supplémentaire, contactez le support NetWitness.

Contactez le support NetWitness

Si vous contactez le support NetWitness, vous devrez vous trouver devant votre ordinateur. Soyez prêt à fournir les informations suivantes :

- Le numéro de version du produit ou de l'application NetWitness Platform que vous utilisez.
- Le type de matériel que vous utilisez.

Utilisez les informations de contact suivantes si vous avez des questions ou si vous avez besoin d'aide.

Portail NetWitness Community	https://community.netwitness.com Dans le menu principal, cliquez sur **Support > Portail de demandes > Afficher mes demandes**.
Contacts internationaux (contacter le support NetWitness)	https://community.netwitness.com/t5/support/ct-p/support
Communauté	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions
Mise à jour NW	https://update.netwitness.com/
Interface utilisateur Live	https://live.netwitness.com

Services éducatifs NetWitness

Inscrivez-vous pour accéder aux cours NetWitness et à des ressources supplémentaires sur les services éducatifs et la formation NetWitness.

Portail de formation NetWitness	https://netwitness.sabacloud.com/Saba/Web_spf/NA10P2PRD088/guestapp/home;spf-url=guest%2Fguestlearningcatalog
Catalogue de cours des services éducatifs NetWitness	https://community.netwitness.com/t5/netwitness-education-courses/tkb-p/netwitness-training
Programme de formation des services éducatifs NetWitness	https://community.netwitness.com/t5/netwitness-education-blog/netwitness-instructor-led-training-schedule/ba-p/655826
Contact de l'assistance des services éducatifs NetWitness	education.support@netwitness.com

Réactions sur la documentation du produit

Vous pouvez envoyer un e-mail à l'adresse feedbacknwdocs@netwitness.com pour faire part de vos réactions sur la documentation RSA NetWitness Platform.