NetWitness® Plate-forme

Version 12.5

Notes de mise à jour

NETWITNESS

Platform

Informations de contact

Communauté NetWitness 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

RSA et les autres marques commerciales sont des marques commerciales de RSA Security LLC ou de ses filiales (« RSA »). Pour obtenir une liste des marques commerciales de RSA, accédez à https://www.rsa.com/fr-fr/company/rsa-trademarks. Les autres marques commerciales sont la propriété de leurs détenteurs respectifs.

Contrat de licence

Ce logiciel et la documentation qui l'accompagne sont la propriété de RSA Security LLC ou de ses filiales, 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 sujet à changement sans préavis et ne doit pas être interprété comme un engagement de RSA.

Il est conseillé de ne pas déployer de référentiels tiers, ni d'effectuer des modifications sur le système d'exploitation NetWitness sous-jacent qui ne font pas partie de la version NetWitness prise en charge. Tout changement en dehors de l'image approuvée par NetWitness peut entraîner un conflit de service ou de fonctionnalité et nécessiter une réimage du système NetWitness pour ramener NetWitness à un état fonctionnel optimisé. Si un référentiel tiers est déployé ou si une autre modification non prise en charge est appliquée par le client sans l'approbation de NetWitness, le client assume l'entière responsabilité de tout dysfonctionnement du système jusqu'à la résolution du problème dans le cadre d'une procédure de dépannage ou de création d'une nouvelle image du service.

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

L'utilisation, la copie et la diffusion de tout logiciel RSA Security LLC ou de ses sociétés affiliées (« RSA ») décrit dans cette publication nécessitent une licence logicielle en cours de validité.

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

LES INFORMATIONS CONTENUES DANS CETTE PUBLICATION SONT FOURNIES « EN L'ÉTAT ». RSA NE FOURNIT AUCUNE DÉCLARATION OU GARANTIE D'AUCUNE SORTE CONCERNANT LES INFORMATIONS CONTENUES DANS CETTE PUBLICATION ET REJETTE PLUS SPÉCIALEMENT TOUTE GARANTIE IMPLICITE DE QUALITÉ COMMERCIALE OU D'ADÉQUATION À UNE UTILISATION PARTICULIÈRE.

Divers

Ce produit, ce logiciel, les documentations associées ainsi que le contenu sont soumis aux conditions générales standard de NetWitness en vigueur à la date de publication de cette documentation et qui peuvent être consultées à l'adresse https://www.netwitness.com/standard-form-agreements/.

septembre 2024

Sommaire

Nouveautés de la version 12.5.0.0

Les notes de publication de NetWitness 12.5.0.0 décrivent les nouvelles fonctionnalités, les améliorations, les mises à jour de sécurité, les chemins d'accès aux mises 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 :

- Tableau de bord
- Investigate
- Respond
- Insight
- Analytique comportementale des utilisateurs et des entités
- Fonction SASE
- Endpoint
- Gestion des contenus centralisée, basée sur des règles
- Services Concentrator, Decoder, Log Collector et Archiver
- Intégration des journaux
- Context Hub
- Service Live Cloud

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.

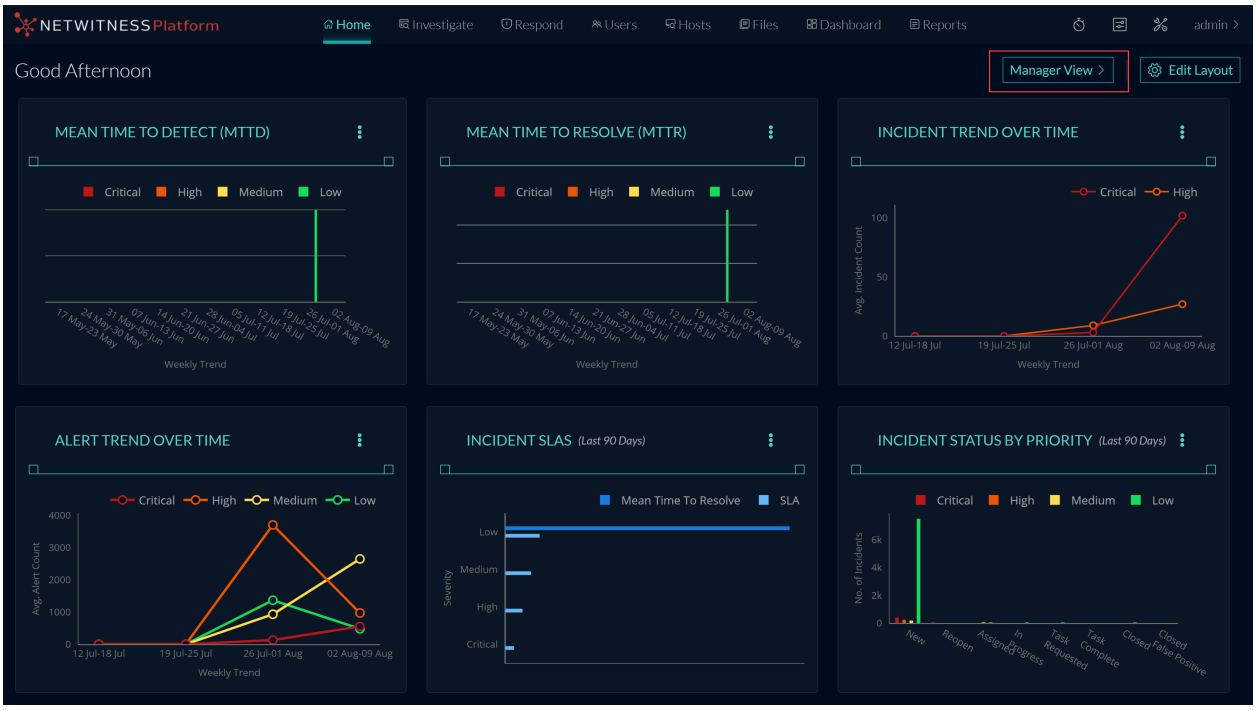
Tableau de bord

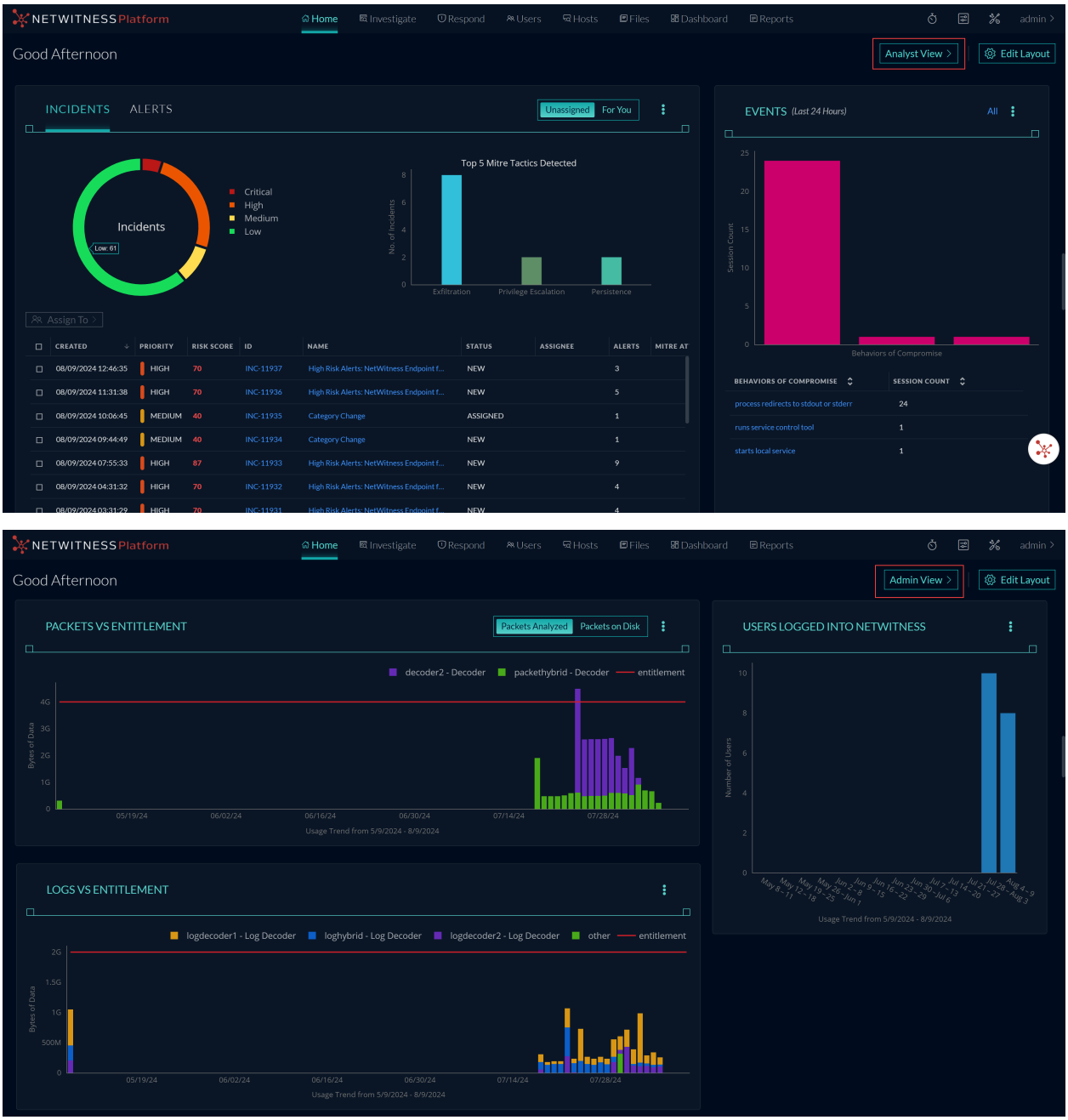
La section suivante décrit les nouvelles améliorations apportées au composant Tableau de bord :

Nouvelles pages d'accueil

NetWitness lance un nouveau menu sur la page d'**Accueil**, composé des vues **Admin**, **Analyste** et **Gestionnaire**. Chaque page d'accueil est composée de plusieurs widgets. Les administrateurs, les analystes et les responsables SOC peuvent accéder aux widgets respectifs qui affichent certaines données sous forme graphique. Les données peuvent être associées à des points de terminaison, des utilisateurs, des ressources, du contenu, des incidents, des alertes, MITRE ATT&CK, la rétention, etc.


NETWITNESS Platform
Home
Investigate
Respond
Users
Hosts
Files
Dashboard
Reports
admin
Good Afternoon
Manager View
Edit Layout
INCIDENTS
9
NEW INCIDENTS
8
CLOSED INCIDENTS
0
ALERTS
40
MEAN TIME TO RESOLVE
0 Sec
MITRE ATT&CK® OVERVIEW
MEDIUM
CONTENT TYPE
EXPAND ALL SUB TECHNIQUES
Deployed
Partially Deployed
Not Deployed
Unavailable
Reconnaissance
Resource Development
Initial Access
Execution
Persistence
Privilege Escalation
Defense Evasion
Credential Access
Discovery
Lateral Movement
Collection
Command and Control
Exfiltration
5 of 10 techniques
2 of 8 techniques
7 of 10 techniques
7 of 14 techniques
15 of 20 techniques
13 of 14 techniques
25 of 43 techniques
7 of 17 techniques
16 of 32 techniques
3 of 9 techniques
9 of 17 techniques
7 of 17 techniques
6 of 9 techniq


NETWITNESS Platform
Home
Investigate
Respond
Users
Hosts
Files
Dashboard
Reports
admin
Good Afternoon
Manager View
Edit Layout
MEAN TIME TO DETECT (MTTD)
Critical
High
Medium
Low
Weekly Trend
MEAN TIME TO RESOLVE (MTTR)
Critical
High
Medium
Low
Weekly Trend
INCIDENT TREND OVER TIME
Critical
High
Avg. Incident Count
100
50
0
12 Jul-18 Jul
19 Jul-25 Jul
26 Jul-01 Aug
02 Aug-09 Aug
Weekly Trend
ALERT TREND OVER TIME
Critical
High
Medium
Low
Avg. Alert Count
4000
3000
2000
1000
0
12 Jul-18 Jul
19 Jul-25 Jul
26 Jul-01 Aug
02 Aug-09 Aug
Weekly Trend
INCIDENT SLAS (Last 90 Days)
Mean Time To Resolve
SLA
Severity
Low
Medium
High
Critical
INCIDENT STATUS BY PRIORITY (Last 90 Days)
Critical
High
Medium
Low
No. of Incidents
6k
4k
2k
0
New
Reopen
Assigned
In Progress
Task Requested
Task Complete
Closed
Closed False Positive



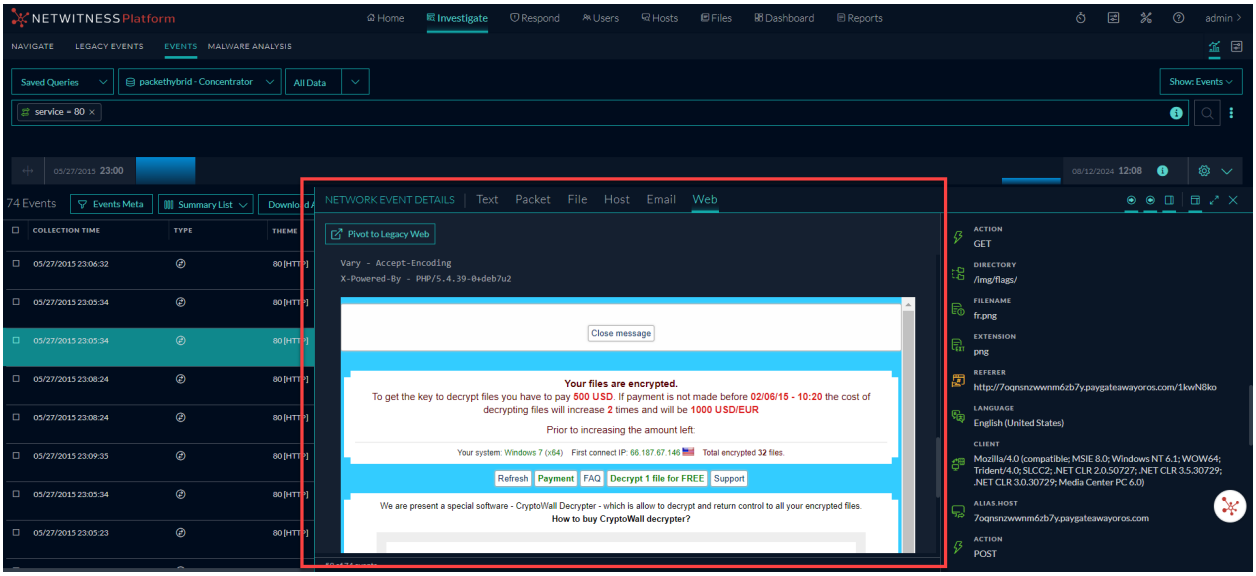
Pour plus d'informations, consultez la rubrique **Gérer les widgets d'accueil** du Guide de démarrage de NetWitness pour 12.5.

Investigate

La section suivante décrit les nouvelles améliorations du composant Investigate :

Reconstruction du Web à partir de la vue Événements

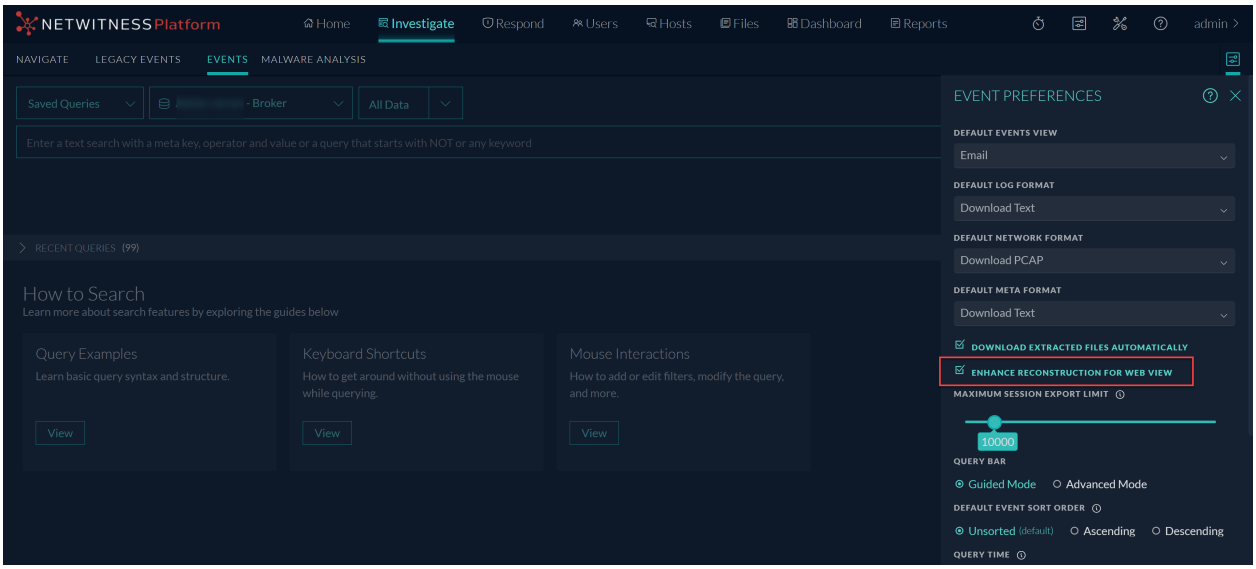
Les analystes peuvent reconstruire en toute sécurité la vue Web de l'événement cible à partir de la vue **Événements > Reconstruction Web** si un utilisateur a visité des pages Web liées à un événement particulier. NetWitness peut reconstruire la même page Web en utilisant les données disponibles dans les paquets, en affichant la page Web et en la reliant aux images et aux styles CSS aussi précisément que possible. Ce processus de reconstruction Web permet aux analystes d'obtenir des informations précieuses sur l'activité Web réalisée, en vue d'une analyse et d'une enquête efficaces.



Pour en savoir plus, consultez la section **Reconstruction Web** de la rubrique **Examiner les détails de l'événement dans la vue Événements** du Guide de l'utilisateur NetWitness Investigate pour la version 12.5.

Amélioration de Reconstruction des événements dans la vue Web

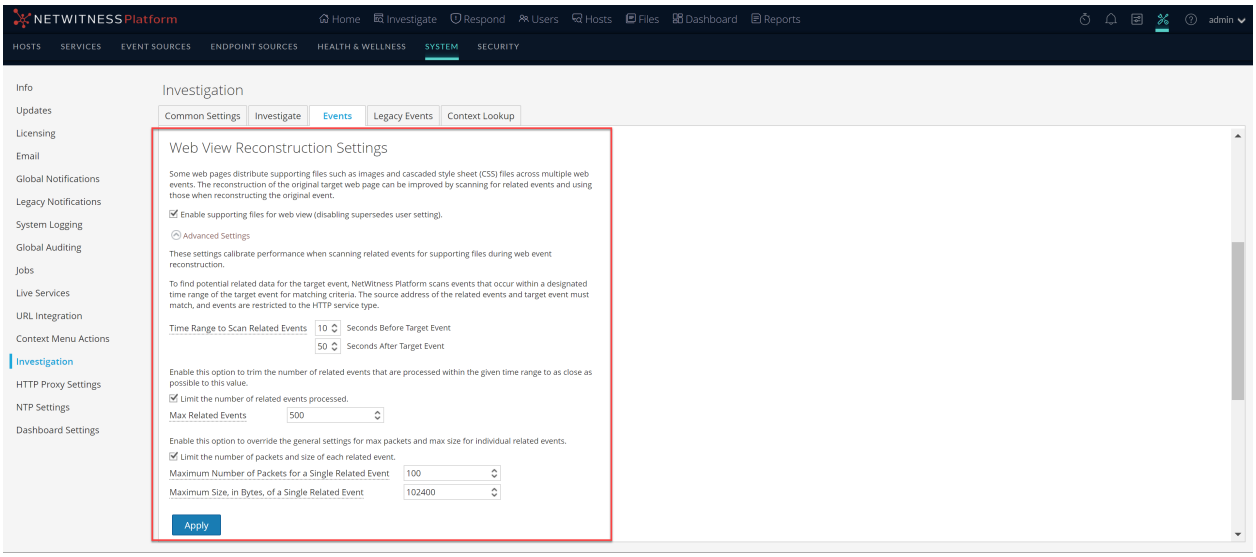
Une nouvelle préférence utilisateur, **Renforcer la reconstruction pour la vue Web**, a été ajoutée au panneau **Préférences d'événements** dans la vue **Investigate** > **Événements**. Cette préférence est activée par défaut pour tous les utilisateurs. Cette option améliore la reconstruction des sites Web qui reconstituent un événement en utilisant CSS, des images et des liens pour formater la vue de manière efficace, permettant ainsi aux analystes de mieux comprendre le contexte et les détails des événements qu'ils reconstituent. Cette amélioration permet aux analystes de mener une analyse plus éclairée et plus précise et de prendre les mesures appropriées.



Pour plus d'informations, consultez la rubrique **Définir les préférences utilisateur pour la vue Événements** du *Guide de l'utilisateur de NetWitness Investigate*.

Présentation des paramètres de reconstruction de la vue Web à partir de la vue système

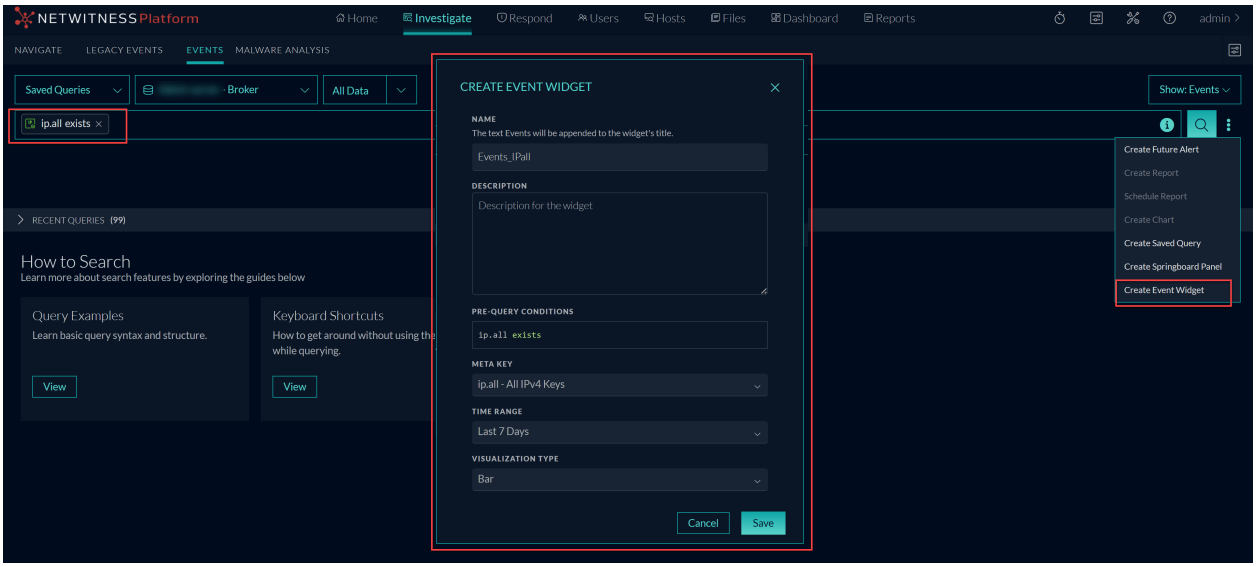
NetWitness présente les nouveaux **Paramètres de reconstruction de la vue Web** de la vue **(Admin)** > **Système** > **Investigation**. Ce paramètre de l'onglet **Événements** permet aux administrateurs d'améliorer la reconstruction des vues Web en analysant et en reconstruisant les événements associés avec les mêmes fichiers de prise en charge. Lors de la reconstruction d'une vue Web couvrant plusieurs événements, le système peut améliorer la reconstruction de l'événement cible en incluant des événements associés contenant des images et des fichiers CSS pertinents. Seuls les événements de type service HTTP avec la même adresse source que l'événement cible et un horodatage dans une plage de temps spécifiée avant et après l'événement cible seront analysés. Les administrateurs peuvent également configurer le nombre maximal d'événements associés à analyser, offrant ainsi une plus grande flexibilité et précision dans la reconstruction de la vue Web. L'option Paramètres avancés affiche tous les paramètres configurables dans cette section.



Pour en savoir plus, consultez la section **Paramètres de reconstruction de la vue Web** de la rubrique **Panneau de configuration d'investigation** du Guide de configuration du système.

Créer un widget Événements personnalisés à partir d'une requête

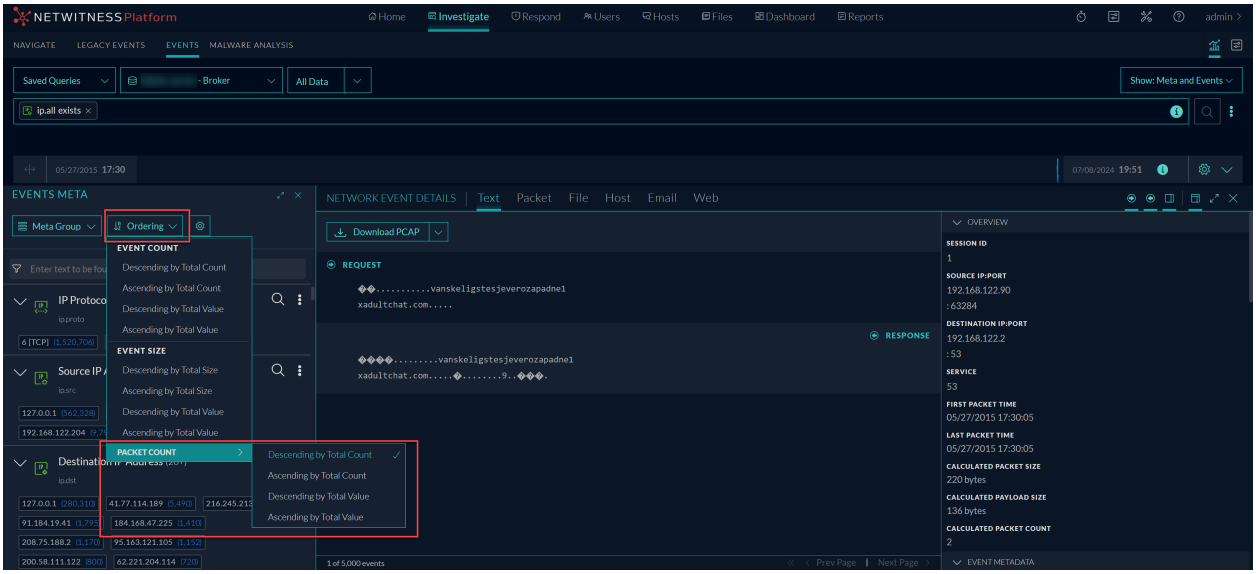
Au cours de l'enquête, les administrateurs et les analystes peuvent désormais créer un widget Événement à partir de la vue **Enquêter** > **Événements** . Les utilisateurs peuvent ajouter n'importe quel nombre de filtres à la barre de recherche de requête et convertir ces recherches en widgets Événement pour une détection et une surveillance améliorées. Le widget nouvellement créé sera enregistré pour un accès rapide dans la bibliothèque de la page d'accueil. Les utilisateurs peuvent ensuite ajouter le widget Événement à la vue Mise en page du tableau de bord (**Admin**, **Analyste** ou **Gestionnaire**) sous la page d'accueil et personnaliser sa configuration selon leurs besoins. Cette fonctionnalité améliore la surveillance et l'analyse des événements, permettant aux utilisateurs de suivre et de surveiller les événements pertinents et importants en temps réel.



Pour en savoir plus, consultez la rubrique **Créer un widget Événement à partir de la vue Investigate** dans le Guide de l'utilisateur de NetWitness Investigate pour la version 12.5.

Trier les résultats de la clé méta par nombre de paquets

Les analystes peuvent désormais trier les résultats de chaque clé méta selon le nombre de paquets présents dans la session sur la page **Investigate** > **Événements**. Vous pouvez trier les résultats par valeur ou par total et par ordre croissant ou décroissant. En triant les résultats des clés méta par nombre de paquets, vous pouvez facilement trouver les valeurs méta les plus ou les moins fréquentes qui se sont produites dans l'environnement utilisateur et peuvent être utilisées pour une enquête ou une analyse plus approfondie.



Pour en savoir plus, consultez la section **Définir la méthode de classement des valeurs méta** de la rubrique **Explorer les métadonnées dans la vue Événements** du Guide de l'utilisateur de NetWitness Investigate pour la version 12.5.

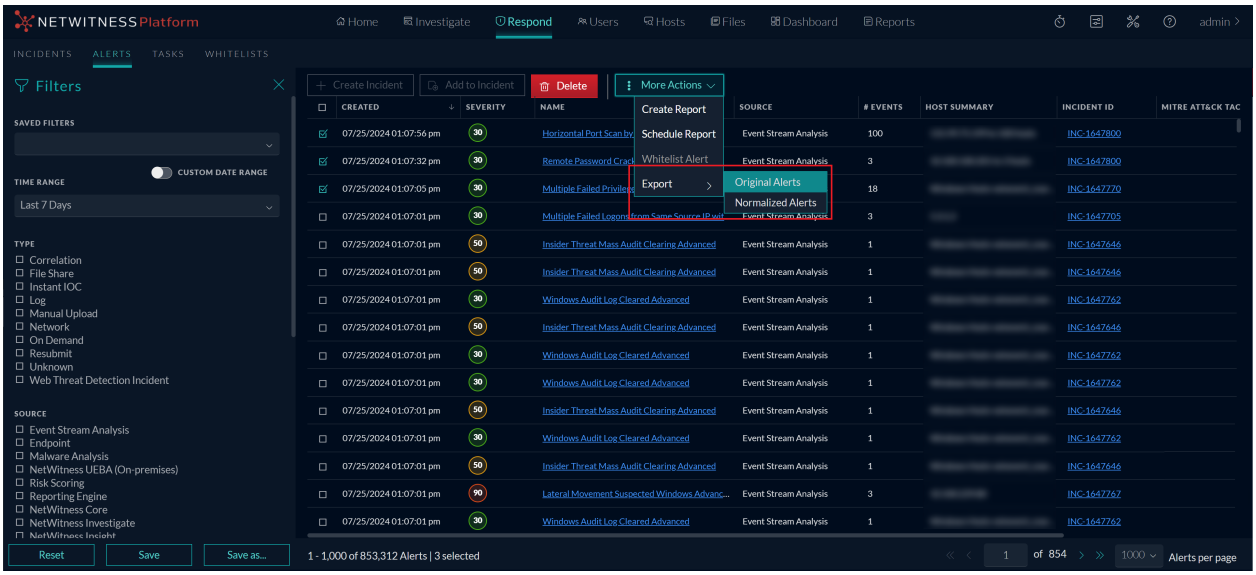
Respond

La section suivante décrit les nouvelles améliorations apportées au composant Respond :

Amélioration de la vue Alertes

L'option **Exportation** dans **Respond** > **Alertes** > Sélectionner une alerte > **Plus d'actions** vous permet d'exporter et de télécharger les alertes originales et normalisées ainsi que les événements au format JSON. NetWitness Platform vous permet d'exporter jusqu'à **1 000** alertes à la fois en vue d'une enquête hors ligne.

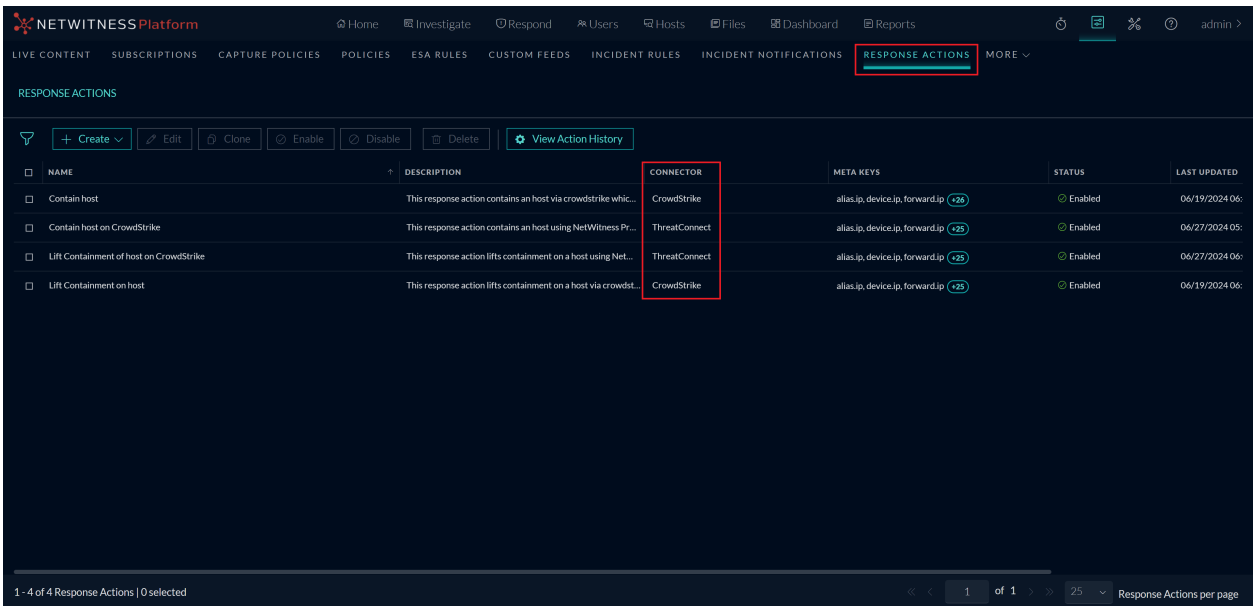
Pour en savoir plus, consultez **Exportation de données d'alertes** dans le *Guide de l'utilisateur de NetWitness Respond pour la version 12.5*.



Actions de réponse OOTB

Introduction des actions prêtes à l'emploi (OOTB) dans le cadre du service Actions de réponse. Les actions OOTB « Contenir l'hôte » et « Lever le confinement sur l'hôte » sont activées pour CrowdStrike et CrowdStrike intégré via NetWitness Orchestrator. Cette amélioration permet aux analystes d'exécuter manuellement des actions de réponse après avoir examiné un incident ou automatiquement dans le cadre d'un incident déclenché. Les actions de réponse avec CrowdStrike sont disponibles directement ou via NetWitness Orchestrator.

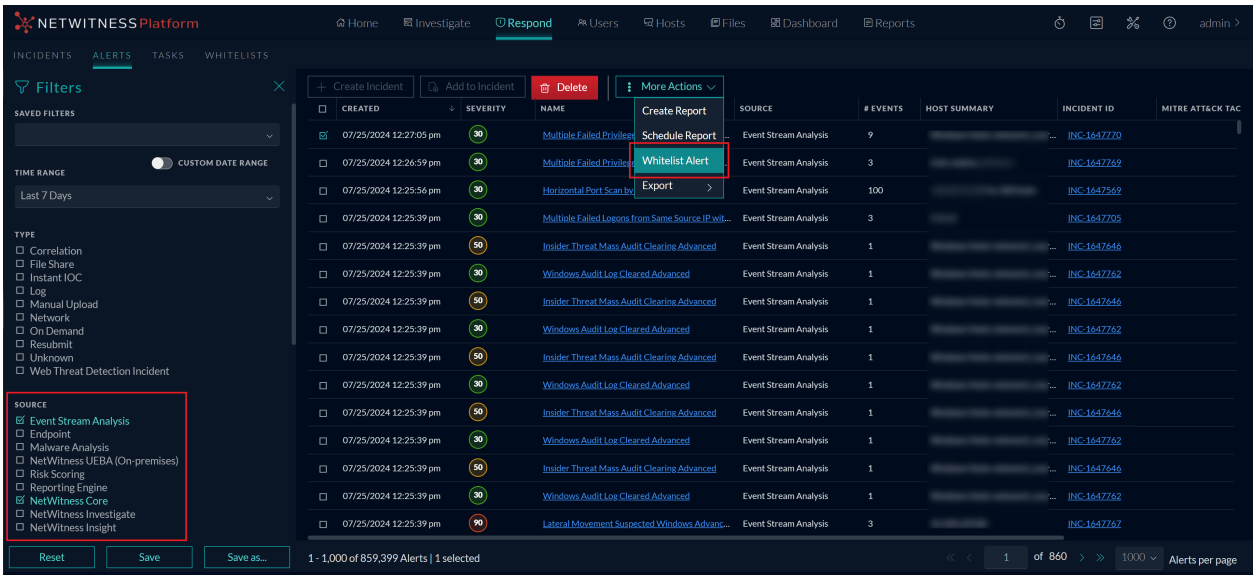
Pour en savoir plus, consultez **Actions de réponse** dans *Guide de configuration Actions de réponse NetWitness pour la version 12.5*.



Amélioration de la fonctionnalité Liste blanche

La fonctionnalité Liste blanche a été améliorée pour inclure des alertes pour les services Event Stream Analysis et NetWitness Core. Vous pouvez désormais ajouter sur liste blanche les alertes indésirables et récurrentes non suspectes pour ces services. Cela vous permet de sélectionner des entités spécifiques et de définir des conditions de liste blanche pour éviter les alertes indésirables pour ces entités.

Pour en savoir plus, consultez **Vue des listes blanches** dans le *Guide de l'utilisateur de NetWitness Respond pour la version 12.5*.

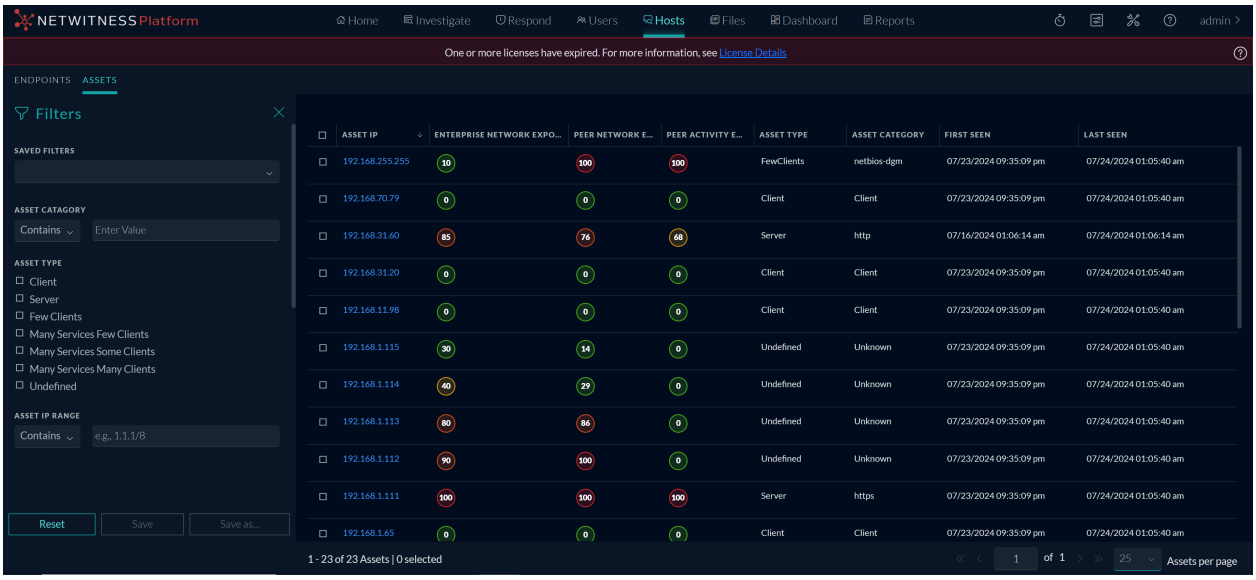


Insight

La section suivante décrit les nouvelles améliorations du composant Insight :

Nouvelle vue Ressources pour la détection et l'investigation des Ressources réseau

NetWitness introduit une nouvelle vue Ressources dans le menu **Hôtes > Ressources**. Cette vue fournit un emplacement centralisé, dans lequel toutes les ressources réseaux sont détectées dans votre environnement avec les détails qui leur sont associés, tels que l'IP de la ressource, le type de ressource, la catégorie de ressource, l'exposition du réseau de l'entreprise, l'exposition du réseau pair, l'exposition de l'activité pair, la première connexion et la dernière connexion. Vous pouvez utiliser des filtres pour affiner les ressources selon différents critères. Cette vue aide les analystes à identifier et à hiérarchiser facilement les actifs se comportant de manière anormale ou les actifs inconnus, afin qu'ils puissent prendre des mesures immédiates pour atténuer tout risque de sécurité potentiel.



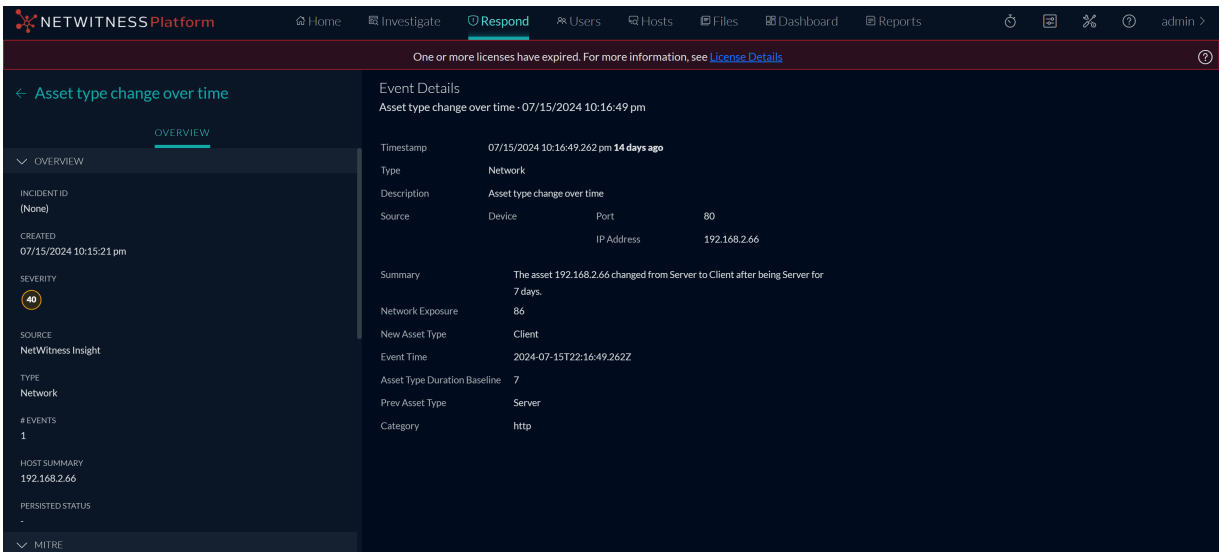
Nouvelles alertes Insight pour Ressources réseau

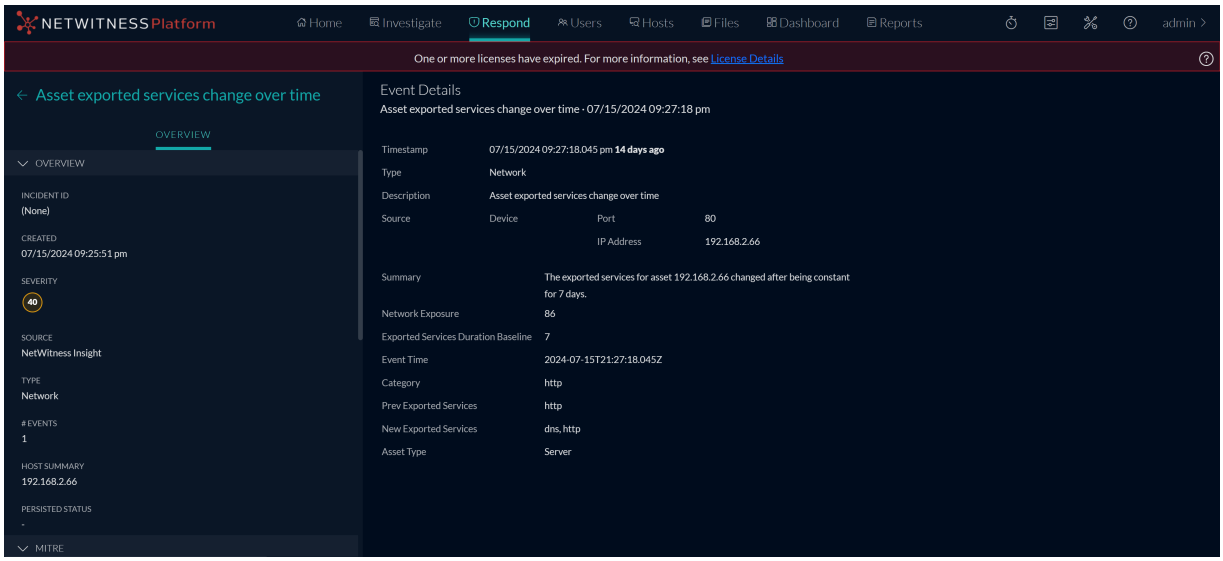
NetWitness présente deux nouvelles alertes Insight pour vous aider à surveiller et à réagir en cas de changement dans vos ressources réseaux. Ces alertes sont disponibles dans la vue **Respond** > **Alertes** et sont basées sur le type de ressource et les services exportés de chaque ressource.

- **Changement du type de ressource au fil du temps** : Cette alerte est générée en cas de changement de type d'un actif (par exemple, client vers serveur) après que le même type a été observé pendant 7 jours consécutifs.

- **Les services de ressources exportées évoluent au fil du temps** : Cette alerte est générée en cas de changement du nombre de services exportés par une ressource après que le même nombre de services a été observé pendant 7 jours consécutifs, même si la catégorie de la ressource demeure inchangée.

  Ces alertes aident les analystes à identifier et à enquêter sur toute anomalie ou menace potentielle dans leur environnement.





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

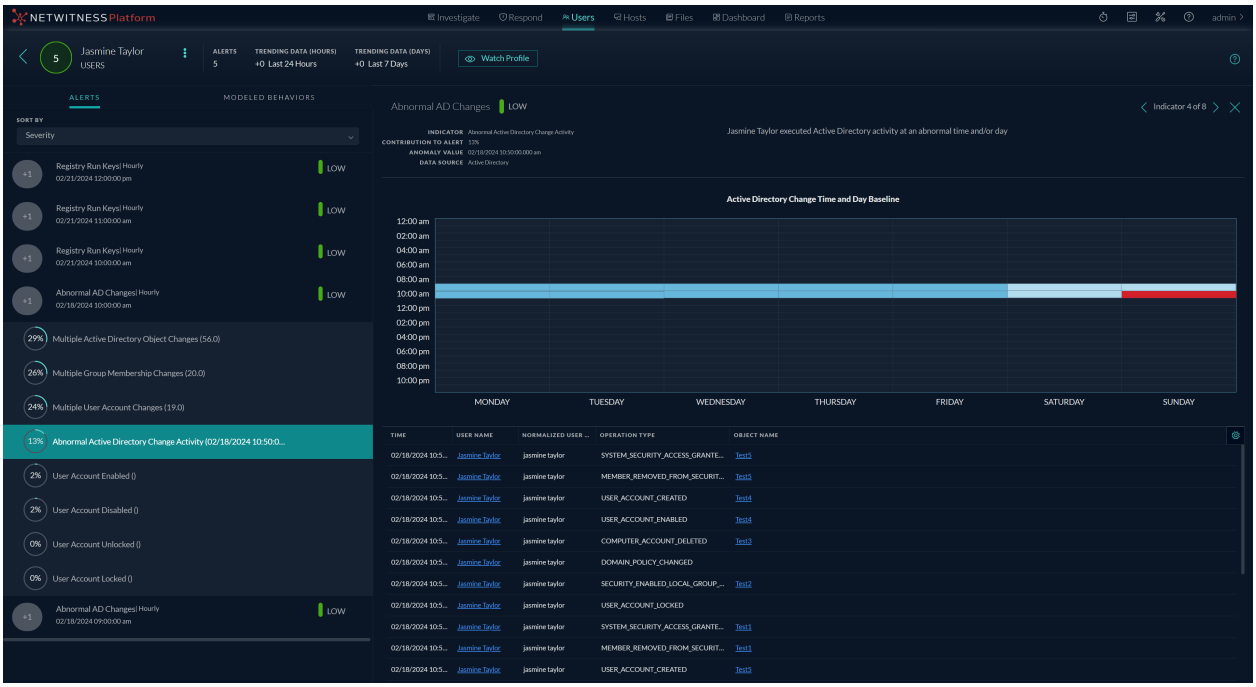
Analytique comportementale des utilisateurs et des entités

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

Détection d'anomalies UEBA à l'aide de la fonctionnalité Jour de la semaine

NetWitness UEBA améliore ses capacités de détection d'anomalies en introduisant la fonctionnalité Jour de la semaine. Cette fonctionnalité permet de détecter des modèles d'accès non standard qui peuvent indiquer qu'un compte est compromis, ou qu'il existe une menace interne. Lorsque l'activité d'un utilisateur surveillé ou d'une entité du réseau au cours d'un jour spécifique de la semaine diffère de son niveau de référence habituel, UEBA la signale comme une anomalie, génère une alerte d'accès non standard ou d'activité non standard et informe les analystes pour qu'ils procèdent à une enquête et à une vérification plus approfondies. Pour plus d'informations sur les activités surveillées pour l'accès non standard et l'activité non standard, veuillez consulter la rubrique **Types d'alertes** dans le *Guide de l'utilisateur NetWitness UEBA*.

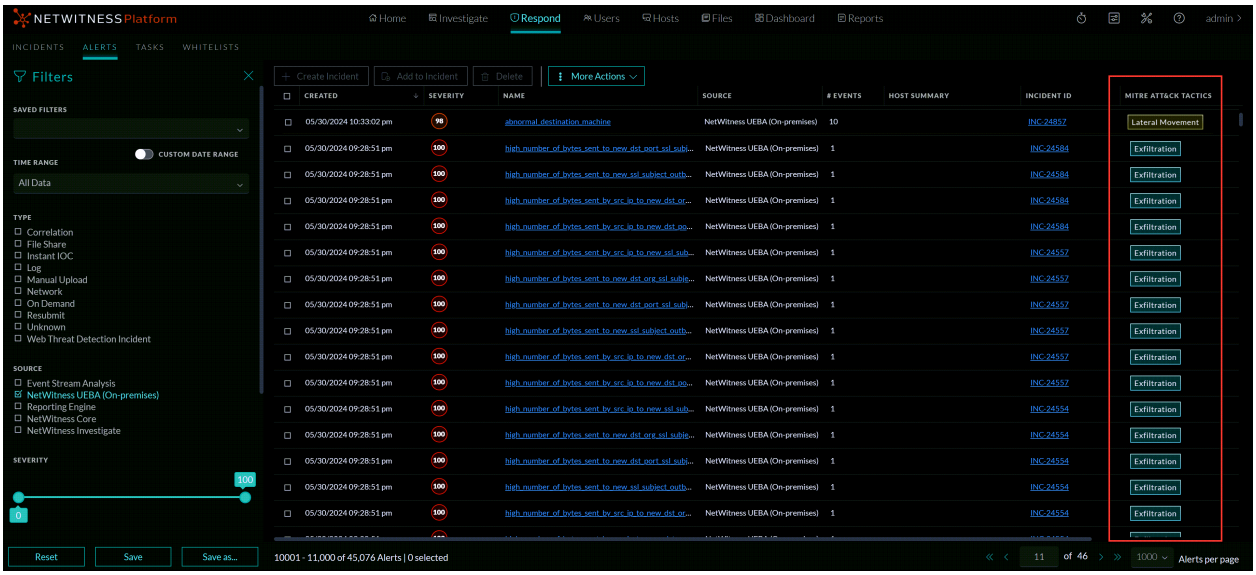
Par exemple, l'utilisateur a accédé à Active Directory un jour inhabituel. L'utilisateur travaille généralement du lundi au vendredi, mais il s'est connecté un dimanche et a effectué des modifications dans Active Directory. Ce comportement a été détecté comme étant une anomalie par NetWitness UEBA grâce à l'amélioration de la fonctionnalité d'analyse basée sur le jour de la semaine, laquelle indique que cet utilisateur effectue des modifications dans AD durant un jour inhabituel, ce qui génère une alerte afin que les analystes examinent l'incident.



Mappage MITRE ATT&CK pour UEBA

NetWitness intègre désormais le mappage du framework MITRE ATT&CK pour les alertes et incidents UEBA. Ce mappage aide les analystes à comprendre les tactiques, techniques et sous-techniques potentielles de l'attaquant à l'origine des activités détectées en les corrélant avec des comportements connus. Lors de l’enquête sur les alertes et les incidents UEBA, les analystes peuvent voir une liste de tactiques et de techniques mappées à partir de la vue **Respond**, ainsi qu’un panneau **ATT&CK Explorer** dédié, qui fournit un contexte supplémentaire et des informations connexes ; ainsi, il n’est plus nécessaire de consulter le site Web de MITRE afin d’obtenir des informations sur ATT&CK. Cette amélioration fournit des informations précieuses sur la gravité et la nature des menaces, afin de prendre rapidement des décisions plus éclairées en conséquence.

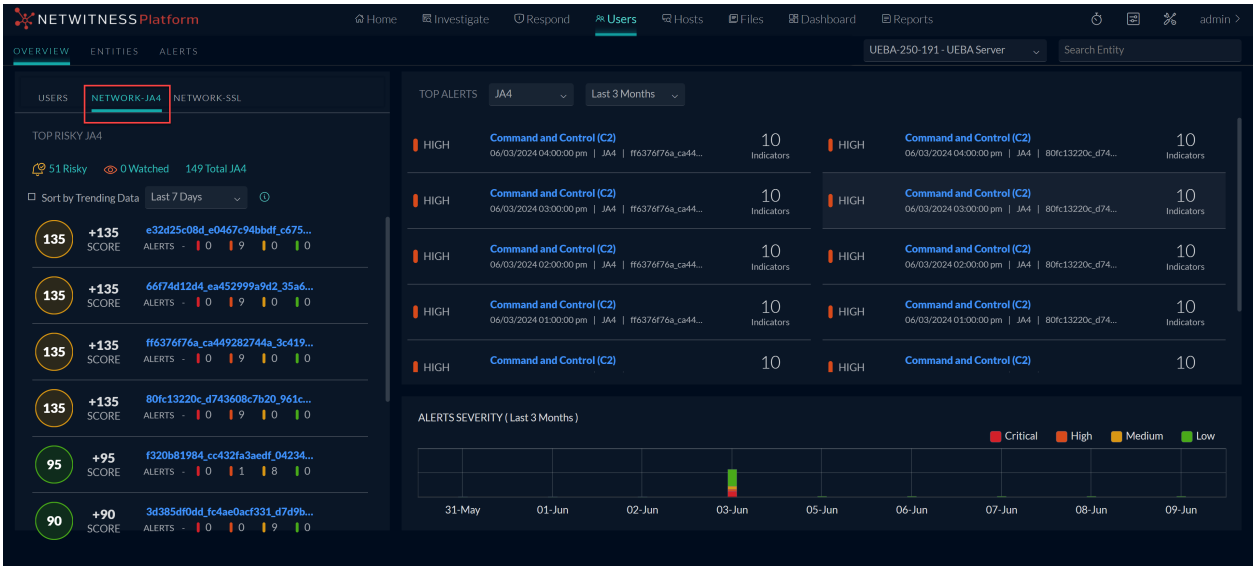
Par exemple, une alerte UEBA a identifié un comportement d’accès à distance suspect à partir d’un compte utilisateur. Ce comportement est conforme à la tactique MITRE ATT&CK de **mouvement latéral** et à la technique utilisant **Services à distance**, qui alertent les analystes pour qu'ils enquêtent sur une éventuelle tentative d'usurpation des données et prennent les mesures nécessaires.



Pour en savoir plus sur l'utilisation du framework Mitre ATT&CK pour UEBA, consultez la rubrique **Utiliser le framework MITRE ATT&CK®** dans le Guide NetWitness Respond 12.5.

Ajout de la prise en charge JA4 dans UEBA pour une meilleure identification des clients et une meilleure détection des menaces

NetWitness a ajouté la prise en charge de l'empreinte JA4 et est la valeur par défaut pour UEBA à partir de la version 12.5. Cette modification est appliquée car l'empreinte JA4 est considérée comme la méthode d'identification client la plus fiable et la plus optimisée. JA4 exploite les paquets TLS Client Hello pour identifier les modèles de trafic spécifiques à l'application et créer des empreintes digitales uniques pour chaque application. Cela réduit le nombre total d'empreintes uniques pour les navigateurs modernes. Par conséquent, un seul client n'aura qu'une seule empreinte digitale JA4 au lieu de plusieurs, ce qui facilitera le suivi et la surveillance. Cette amélioration d'UEBA avec la prise en charge de l'empreinte JA4 permet d'identifier les empreintes digitales des applications malveillantes et aide les analystes à détecter et à atténuer proactivement les menaces de sécurité qui se dissimulent dans le trafic chiffré.

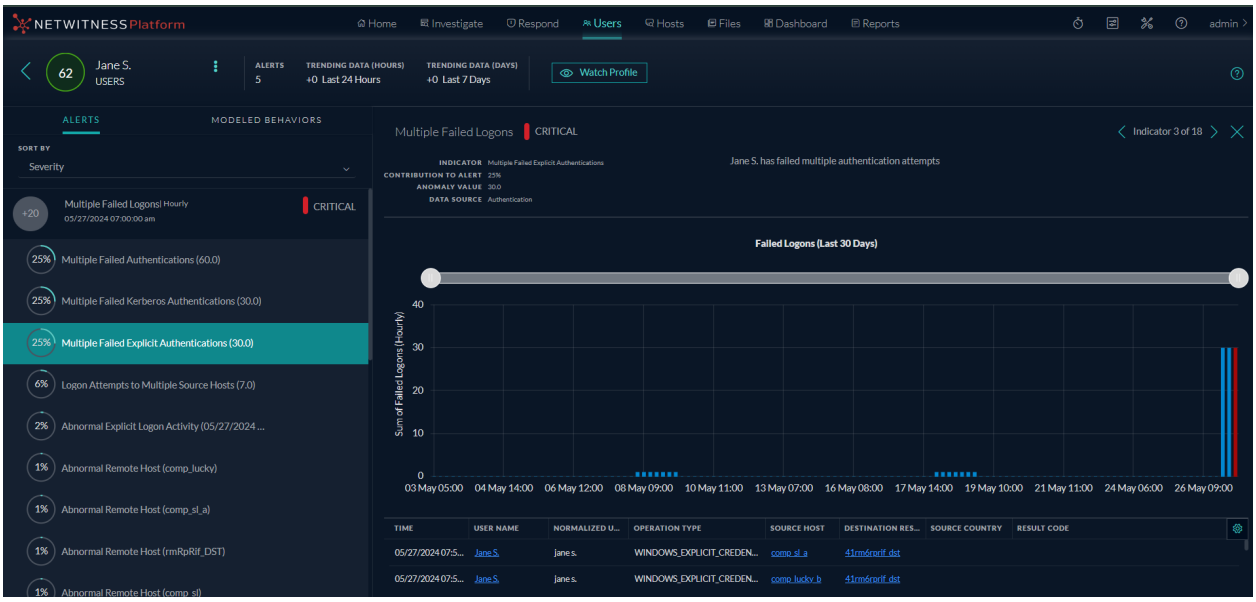


Pour plus d'informations sur la prise en charge de JA4, consultez le Guide de l'utilisateur NetWitness UEBA pour la version 12.5.

UEBA améliorée pour la détection des activités Kerberos et d'ouvertures de session explicites

NetWitness UEBA a amélioré ses capacités de détection dans les activités d'ouverture de session en introduisant deux nouveaux indicateurs et comportements modélisés spécifiquement pour les ouvertures de session **Kerberos** et **Explicit**. Cette amélioration permet de différencier plus précisément les divers événements d'ouverture de session au sein de votre environnement, ce qui réduit considérablement les faux positifs et les incohérences liées aux activités d'ouvertures de session Kerberos et Explicit. En séparant ces types d'ouverture de session, les analystes peuvent détecter plus efficacement les comportements d'ouverture de session anormaux et protéger leur environnement contre d'éventuelles menaces. Ces nouveaux indicateurs fournissent des informations plus précises sur les activités d'ouverture de session, ce qui aide les analystes à surveiller et à examiner efficacement tout comportement suspect ou malveillant.

Par exemple, une alerte **Plusieurs ouvertures de session échouées** peut être déclenchée lorsqu'une activité anormale est détectée lors de plusieurs ouvertures de session échouées, dans **Kerberos** et dans **Explicit**.



Pour en savoir plus, consultez la section **Indicateurs d'activité d'ouverture de connexion** de la rubrique **Cas d'utilisation de NetWitness UEBA** du Guide de l'utilisateur de NetWitness UEBA pour la version 12.5.

Fonction SASE

La section suivante décrit la nouvelle amélioration pour SASE :

Intégration de NetWitness SASE avec Netskope (mode d'aperçu privé)

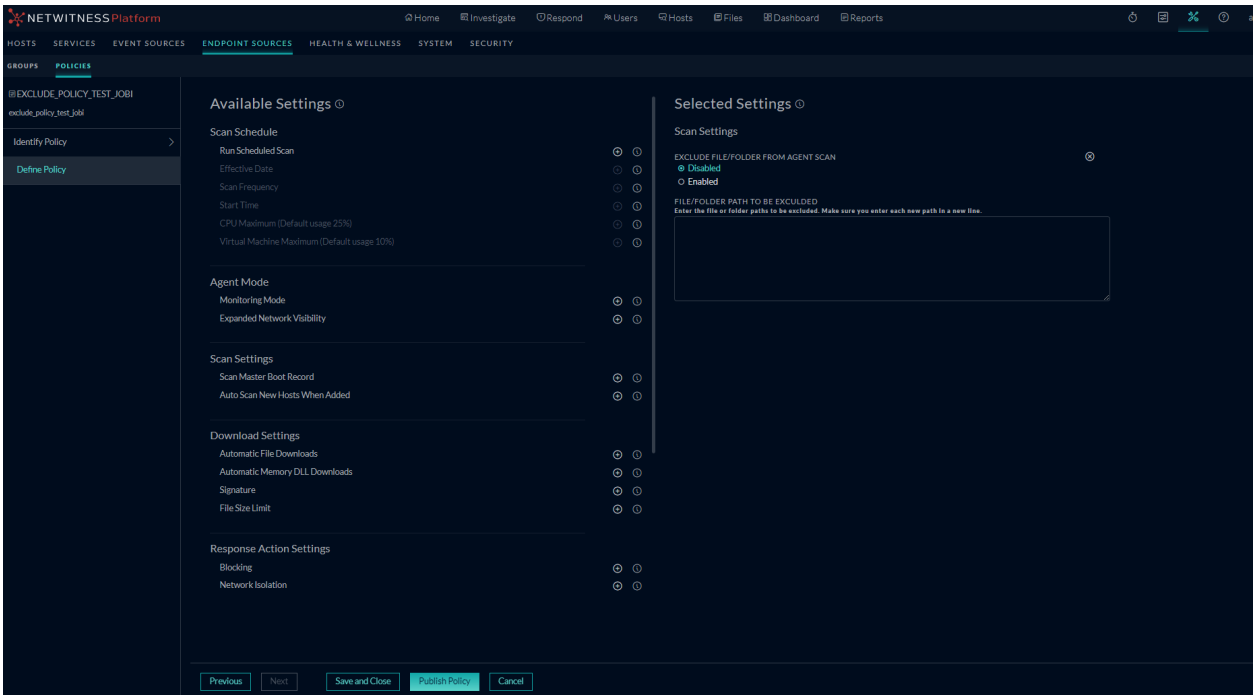
Présente l'intégration de NetWitness avec Netskope SASE pour fournir une visibilité complète du réseau et des fichiers journaux. Grâce à cette intégration technique personnalisée, les utilisateurs de NetWitness obtiennent un aperçu du comportement et de la communication entre les appareils et les services dans les réseaux distants et distribués dans le cadre de déploiements sur site, hybrides et cloud. L'intégration NetWitness-Netskope SASE permet aux clients de tirer parti de la flexibilité SASE et de ses avantages inhérents en matière de sécurité, tout en conservant une visibilité complète sur la détection et la réponse aux menaces. Dans la version 12.5, l'intégration de NetWitness SASE avec Netskope est en mode Aperçu privé.

Endpoint

La section suivante décrit les nouvelles améliorations du composant Endpoint

Exclusion de fichiers et de dossiers spécifiques des analyses complètes du système de l'agent

Vous pouvez configurer NetWitness Platform de sorte à exclure des fichiers et des dossiers spécifiques des analyses complètes du système de l'agent NetWitness Endpoint. Lorsque vous excluez des fichiers ou des dossiers, l'agent NetWitness Endpoint les ignore lorsqu'il recherche des risques de sécurité. Si vous excluez les fichiers et les dossiers de grande taille, vous constaterez peut-être que le temps d'analyse de l'agent Endpoint est réduit. L'exclusion d'un fichier ou d'un dossier des analyses de l'agent NetWitness Endpoint réduit le niveau de protection des hôtes de votre réseau. Une telle exclusion ne doit être appliquée que si vous avez un besoin spécifique et que vous avez la certitude que les éléments ne sont pas infectés. Vous ne pouvez exclure que des fichiers et des dossiers d'une analyse complète du système.



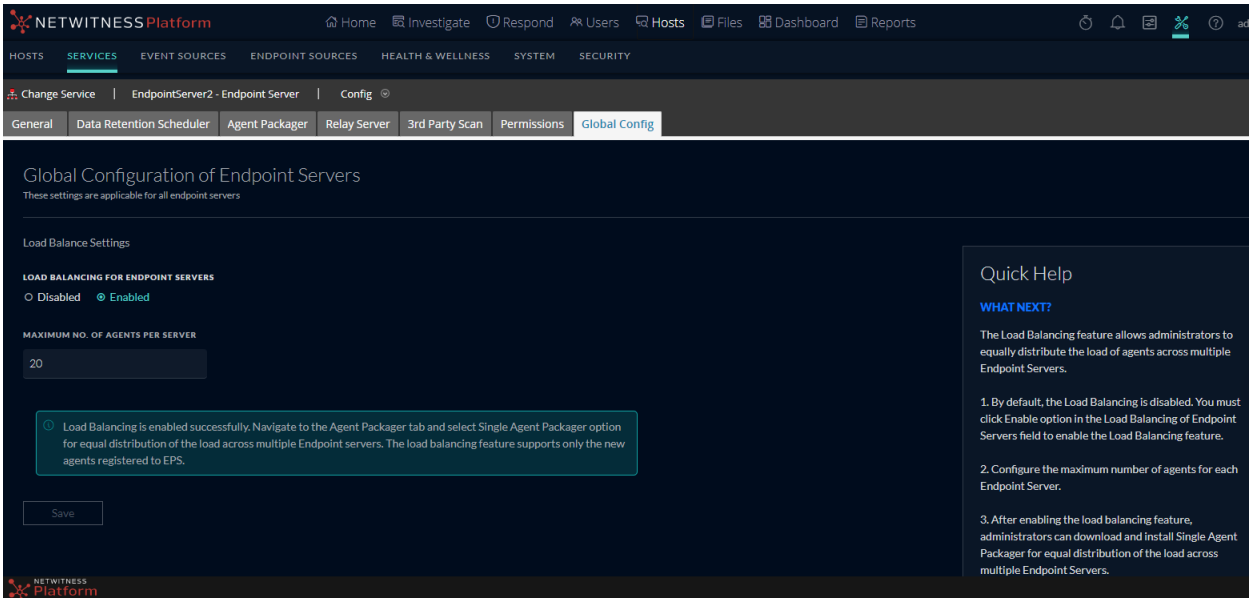
Pour en savoir plus sur la manière d'exclure des fichiers et des dossiers de l'analyse complète du système de l'agent NetWitness, consultez le Guide de configuration de NetWitness Endpoint.

Optimisation des performances : Capacités d'équilibrage de charge dans les serveurs Endpoint

Grâce à la nouvelle fonctionnalité d'équilibrage de charge, les administrateurs peuvent répartir les charges des agents de manière égale sur les serveurs Endpoint de l'environnement.

À mesure que les organisations se développent, de nouveaux agents doivent être ajoutés pour les déploiements et il devient de plus en plus difficile de les répartir sur les serveurs Endpoint. Les administrateurs doivent télécharger un Packager distinct pour chaque serveur Endpoint et appliquer des stratégies afin de répartir la charge en fonction des conditions. Grâce à la fonctionnalité d'équilibrage de charge, les clients ont seulement besoin de télécharger un package d'agent et de le transmettre à tous les agents Endpoint. Selon la charge et les paramètres définis, les agents seront répartis de manière égale sur les serveurs Endpoint.

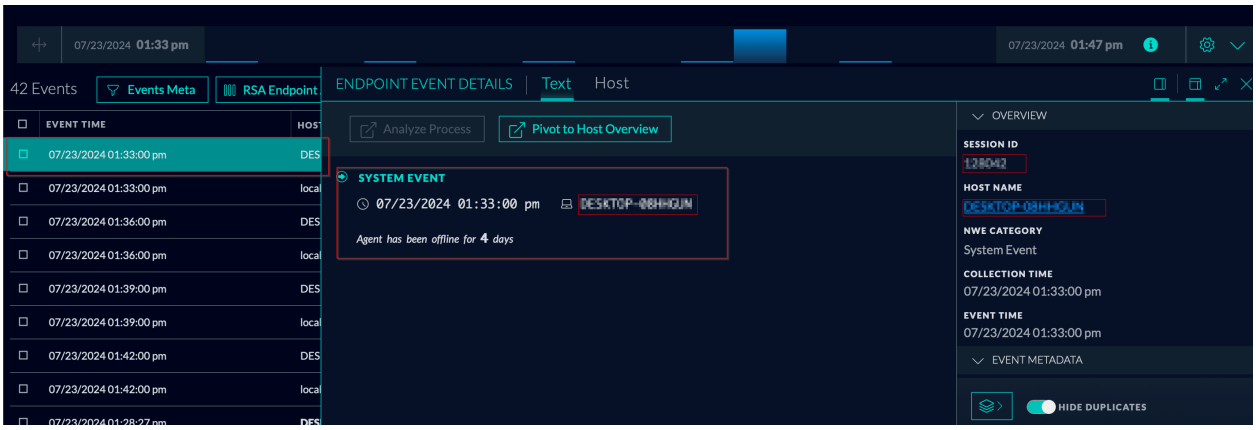
La mise en œuvre de l'équilibrage de charge permet aux entreprises de s'assurer que leur déploiement évolue efficacement, en réduisant le risque de surcharge d'un seul serveur Endpoint et en assurant des performances optimales sur l'ensemble du réseau. Pour utiliser la fonctionnalité d'équilibrage de charge, vous devez activer l'équilibrage de charge.



Pour en savoir plus sur l'équilibrage de charge, consultez les rubriques « À propos de l'équilibrage de charge » et « Activation de l'équilibrage de charge » dans le *Guide de l'utilisateur de NetWitness Endpoint.*

Capacité à surveiller les détails Dernière connexion des agents Endpoint

NetWitness Platform permet aux administrateurs et aux analystes de créer régulièrement des rapports détaillant le nombre d'agents Endpoint qui n'ont pas émis de rapport pendant un nombre de jours spécifié, ce qui garantit ainsi la conformité et la gouvernance au sein de l'organisation. Le fait de savoir à quand remonte la dernière connexion de l'agent Endpoint fournit des informations sur les performances globales des points de terminaison. Le suivi des dernières connexions des agents Endpoint est crucial pour garantir la sécurité, la conformité, l'efficacité opérationnelle et la gestion des ressources au sein d'une organisation.



Pour en savoir plus, consultez la rubrique « Suivi des dernières connexions des agents Endpoint » dans le Guide de l'utilisateur de NetWitness Endpoint.

Améliorations apportées aux systèmes d'exploitation pris en charge

Les administrateurs ont la possibilité de déployer des agents Endpoint sur la version suivante du système d'exploitation Windows :

- **Windows 11 (jusqu'à la version 23H2)**

Pour en savoir plus, consultez la rubrique **Introduction à l'installation de l'agent Endpoint** du *Guide d'installation de l'agent NetWitness Endpoint*.

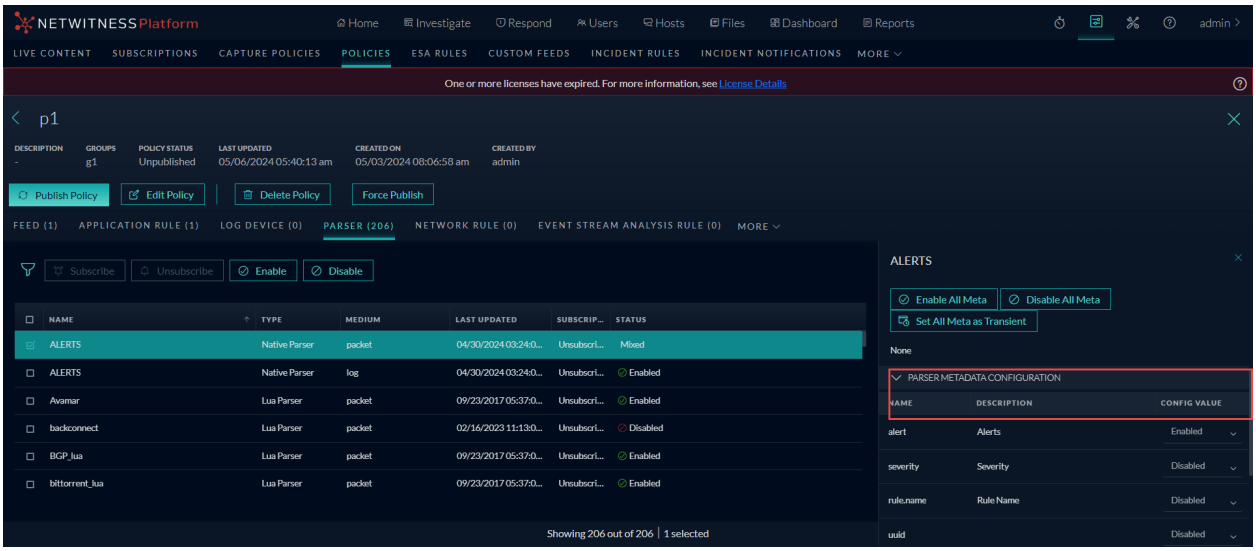
Gestion des contenus centralisée, basée sur des règles

Les améliorations suivantes sont apportées pour CCM dans la version 12.5.0.0 :

Prise en charge des parsers natifs

Afficher la configuration des métadonnées des parsers

La vue **Détails de la stratégie** > **Parser** a été améliorée pour afficher la **Configuration des métadonnées des parsers** sur le panneau de droite, avec toutes les métadonnées du parser sélectionné.

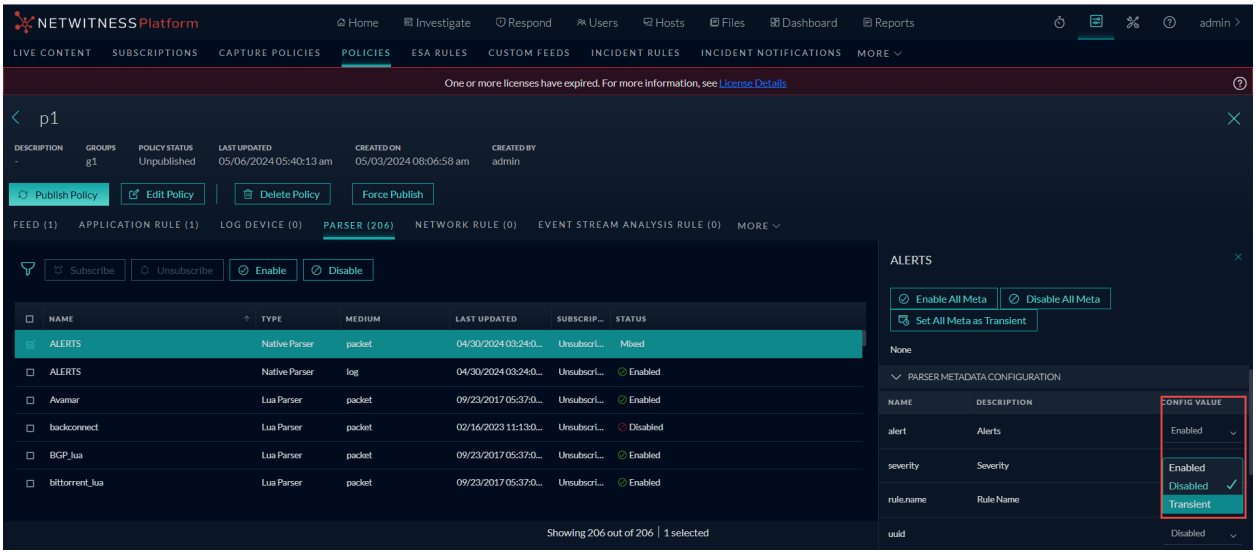


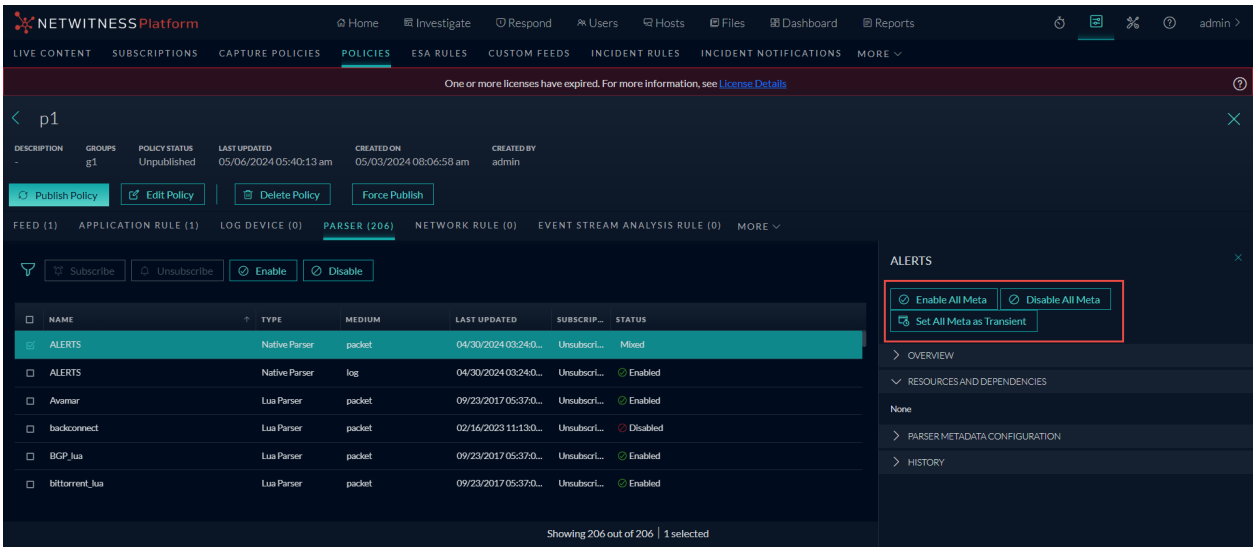
Pour en savoir plus, consultez la rubrique **Afficher une stratégie** du *Guide de gestion centralisée du contenu basée sur des stratégies*.

Activer ou désactiver les métadonnées des parsers

La vue **Détails de la stratégie** > **Parser** a été améliorée pour activer ou désactiver des métadonnées du parser spécifiques, afin que vous ayez la possibilité de décider d'utiliser ou non des parsers natifs. Vous pouvez :

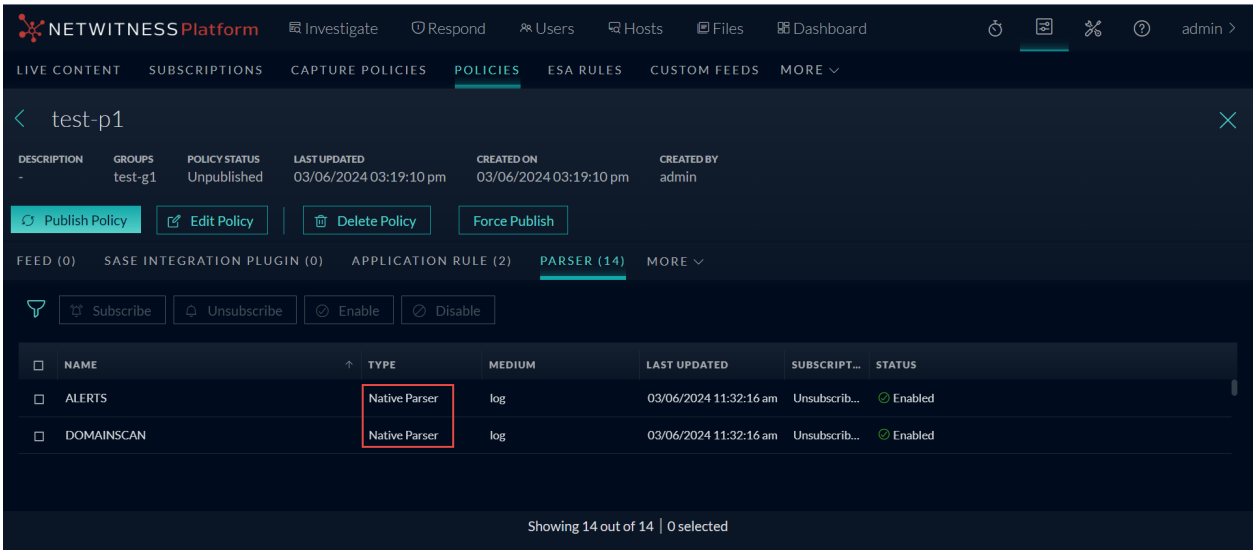
- Activer toutes les métadonnées
- Désactiver toutes les métadonnées
- Rendre toutes les métadonnées transitoires
- Activer les métadonnées individuelles
- Désactiver les métadonnées individuelles
- Rendre les métadonnées individuelles transitoires





Afficher les parsers natifs activés pour les services et éléments associés à la stratégie

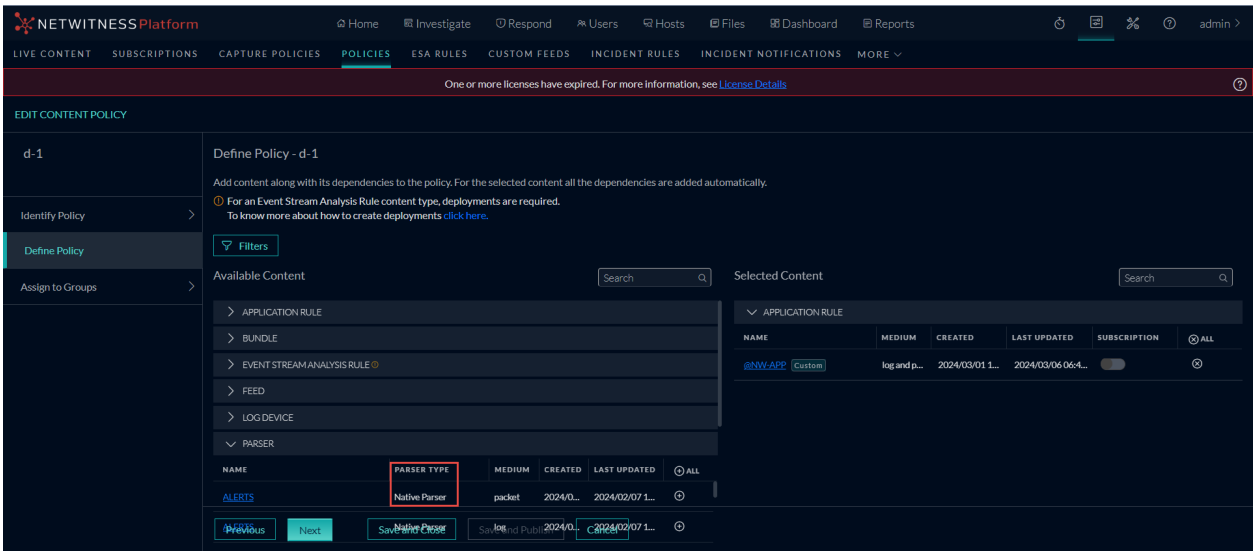
Vous pouvez facilement afficher les parsers natifs activés pour les services et éléments associés à une stratégie car ils s'affichent automatiquement dans la page **Détails de la stratégie**.



Pour en savoir plus, consultez la rubrique **Afficher une stratégie** du *Guide de gestion centralisée du contenu basée sur des stratégies*.

Distinguer les parsers natifs des parsers LUA lors de la création d'une stratégie

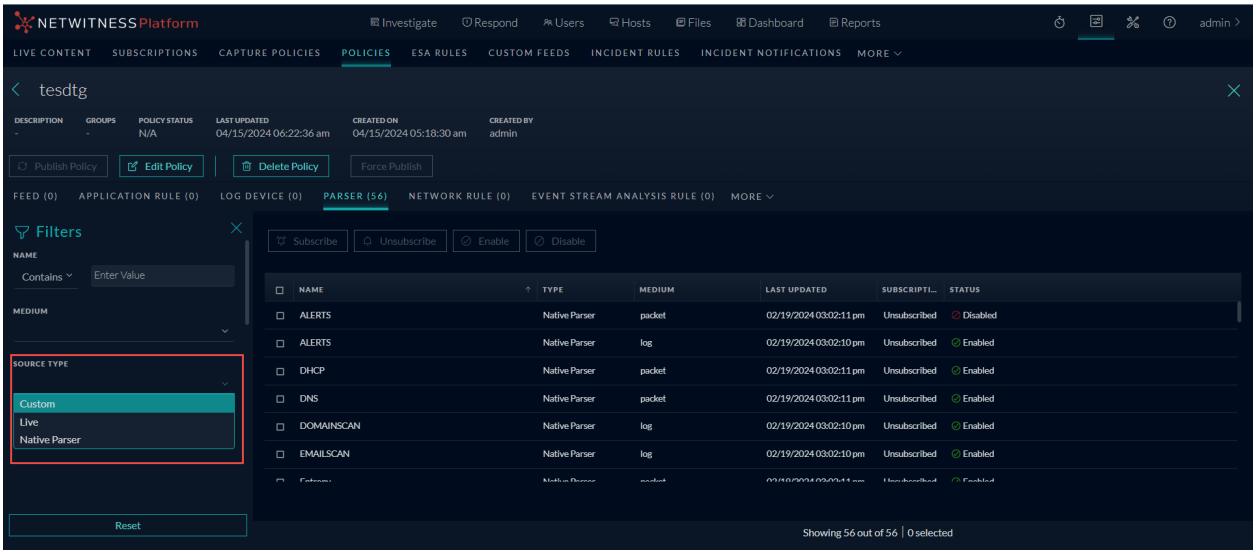
Un identifiant distinctif est créé pour le parser natif dans la page **Créer une stratégie** ou **Modifier la stratégie** afin de vous aider à faire la distinction entre un parser natif et un parser LUA lors de la création d'une stratégie.



Pour en savoir plus, consultez la rubrique **Créer et publier des stratégies** du *Guide de gestion centralisée du contenu basée sur des stratégies*.

Filtrer les parsers natifs

Vous pouvez filtrer les parsers natifs sur les pages **Créer une stratégie**, **Modifier la stratégie** et **Détails de la stratégie**, ce qui vous permet de sélectionner ou d'afficher facilement les parsers natifs requis pour la stratégie. Cela rationalisera le processus et vous permettra d'ajouter ou de supprimer facilement des analyseurs natifs lors de la création ou de la modification d'une stratégie.



Pour en savoir plus, consultez la rubrique **Créer et publier des stratégies** du *Guide de gestion centralisée du contenu basée sur des stratégies*.

Services Concentrator, Decoder, Log Collector et Archiver

Les améliorations suivantes sont apportées aux services Concentrator, Decoder, Log Collector et Archiver dans la version 12.5.0.0 :

Présentation de l'empreinte digitale JA4 TLS

JA4 identifie les modèles de trafic spécifiques à l'application en analysant les négociations d'établissement d'une liaison TLS (Client Hello), ce qui renforce les capacités de détection des menaces dans UEBA.

Pour plus d'informations, consultez la rubrique **Prise en charge de l'entité JA4 pour UEBA** dans le *Guide de configuration de Decoder*.

Sources d'événements Logstash

Introduction de la prise en charge du plug-in NetWitness JDBC Logstash Input pour collecter les fichiers journaux des bases de données MSSQL, IBMDB2 et Oracle.

Pour en savoir plus, consultez la rubrique **Configurer les sources de l'événement Logstash dans la rubrique NetWitness** du *Guide de Log Collection*.

Métadonnées étendues

Une configuration facultative pour augmenter la longueur des valeurs qui peuvent être stockées dans la base de métadonnées afin de fournir une plus grande précision dans certains cas d'utilisation nécessitant des correspondances de longues chaînes.

Métadonnées étendues fournit un moyen de configurer de manière sélective certaines clés méta pour prendre en charge des valeurs supérieures à 256 octets. Grâce à cette fonctionnalité, les métavaleurs auparavant tronquées par la limite de 256 octets peuvent désormais être étendues jusqu'à 4 096 octets de longueur.

Pour en savoir plus, consultez les directives relatives aux métadonnées étendues qui figurent dans le *Guide de l'utilisateur de métadonnées étendues NetWitness pour la version 12.5*.

Suivi des règles d'application

Compte la fréquence à laquelle une règle d'application est mise en correspondance ainsi que la possibilité de réinitialiser le compteur à des fins de dépannage.

Pour plus d'informations, consultez le *Guide de l'API pour la version 12.5*.

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.

- Amazon AWS CloudWatch
- Okta Workforce Identity Cloud

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

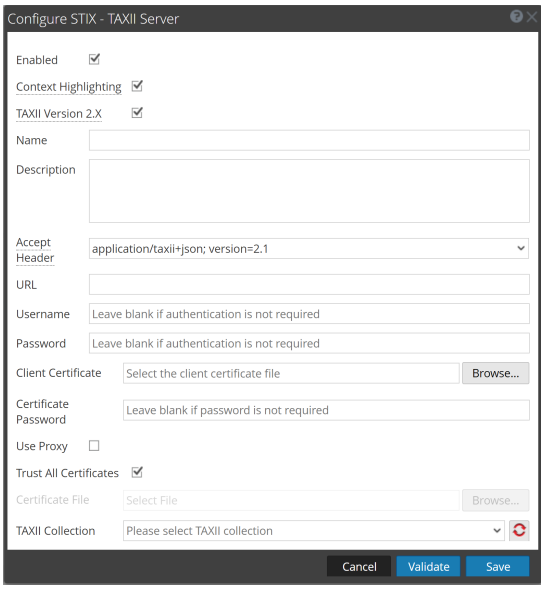
Context Hub

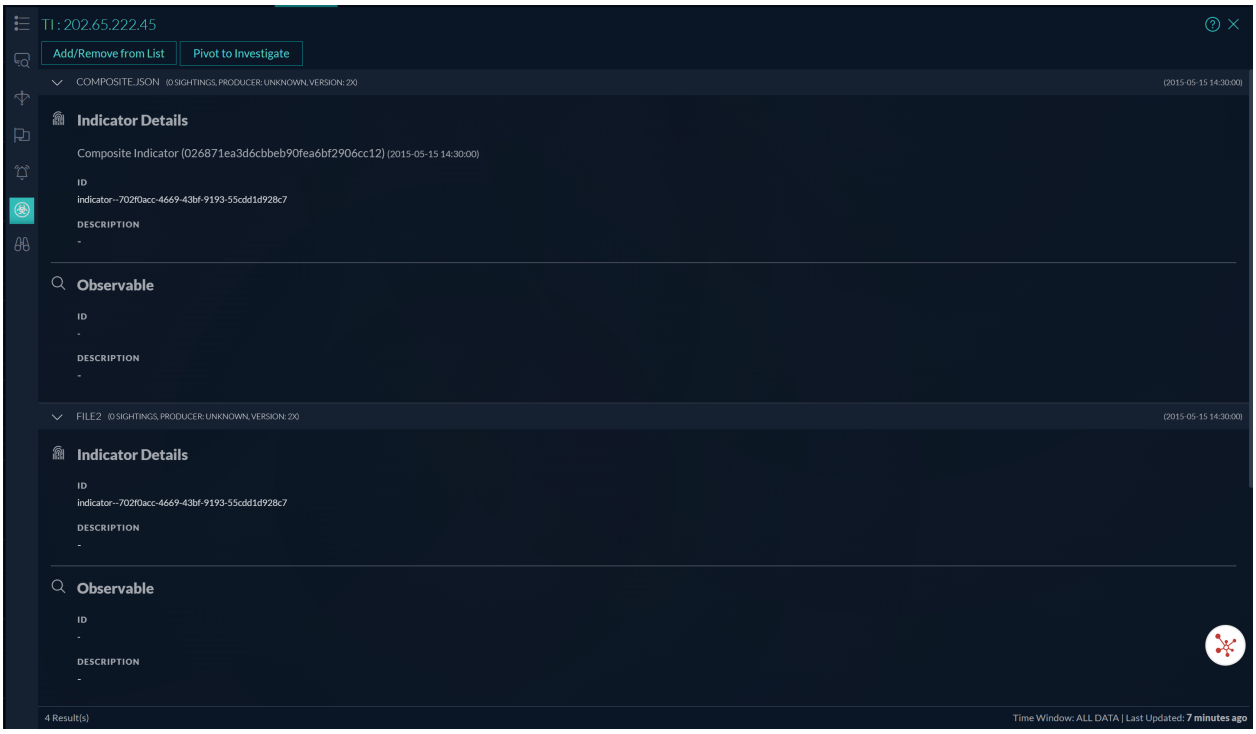
La section suivante décrit les nouvelles améliorations apportées au composant Context Hub :

Intelligence sur les menaces améliorée avec l'intégration de STIX 2.x

NetWitness a amélioré ses capacités de détection des menaces et de surveillance de la sécurité en intégrant la prise en charge des flux STIX 2.x, y compris les versions 2.0 et 2.1. Les administrateurs peuvent désormais utiliser STIX 2.x (format JSON) pour configurer Fichier, REST et Serveur TAXII en tant qu'indicateurs de source de données pour Context Hub. Cette amélioration vous permet de créer des flux personnalisés à l'aide de sources de données STIX 2.x. La plateforme NetWitness analyse les données en arrière-plan afin de tirer des informations stratégiques sur les menaces et d'identifier les modèles malveillants, en fournissant un contexte enrichi grâce à la fonction Recherche contextuelle sur les pages **Investigate** et **Respond** et en aidant les analystes à mener des enquêtes plus efficacement.

Cette amélioration simplifie l'utilisation de l'intelligence sur les menaces structurée en éliminant de nombreuses contraintes antérieures, permettant ainsi d'élaborer des rapports plus détaillés et plus efficace des observations. Cette intégration implique la conversion de l'intelligence sur les menaces structurée, depuis un format STIX vers un format que le système SIEM peut facilement comprendre et utiliser, afin de renforcer l'efficacité en matière de protection contre les menaces.





Pour en savoir plus, consultez la rubrique **Configurer STIX en tant que source de données** dans le Guide de configuration de Context Hub.

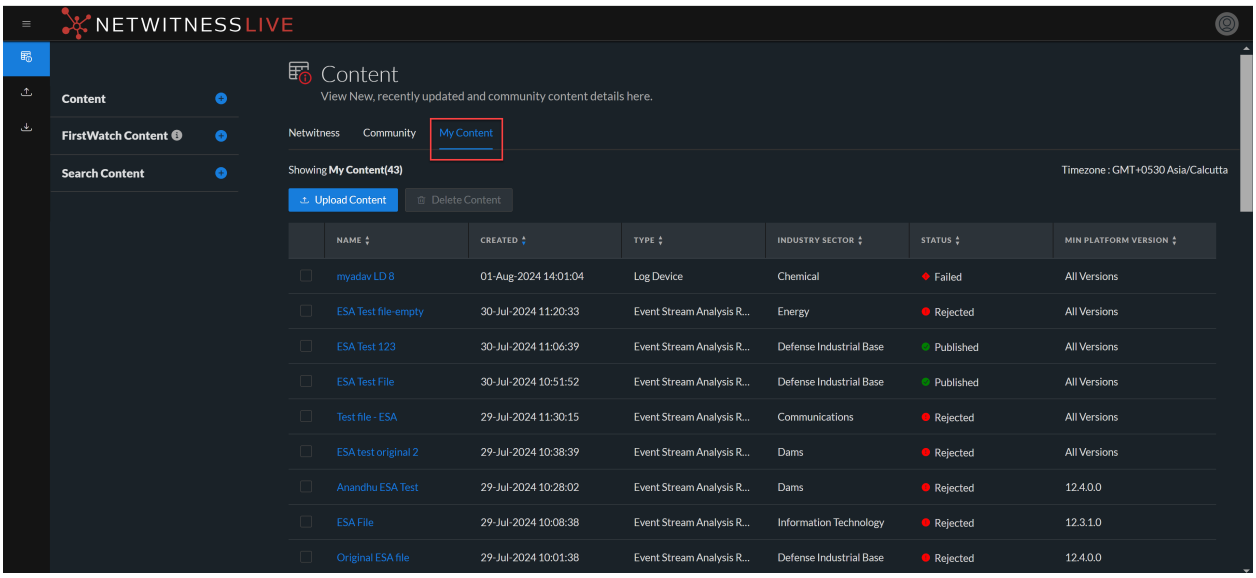
Service Live Cloud

La section suivante décrit les nouvelles améliorations apportées au composant Live Cloud Service :

Gérer le contenu personnalisé de la communauté sur NetWitness Live

NetWitness présente la nouvelle fonctionnalité Mon contenu, qui permet aux utilisateurs de gérer de manière transparente le contenu personnalisé directement depuis l'interface utilisateur NetWitness Live. Cela comprend le chargement, la suppression et le téléchargement de contenu créé par l'utilisateur, comme les dispositifs de journalisation, les règles Event Stream Analysis, les parsers, les flux, etc. Cette fonctionnalité offre aux utilisateurs un moyen plus efficace de partager du contenu personnalisé utile et pertinent entre les utilisateurs, ce qui réduit ainsi le temps et les efforts nécessaires pour publier du contenu par l'intermédiaire d'équipes de publication de contenu. Les utilisateurs peuvent choisir parmi une gamme d'options de contenu adaptées à leurs besoins et à leurs cas d'utilisation.

Remarque : La fonctionnalité Mon contenu de NetWitness Live prend uniquement en charge les contenus Log Device et ESA dans cette version.



Pour en savoir plus, consultez la rubrique **Gérer le contenu personnalisé** du Guide de gestion des services NetWitness Live.

Mises à jour de sécurité

Corrige les dernières vulnérabilités de sécurité signalées dans diverses bibliothèques utilisées par NetWitness Platform, dont une vulnérabilité critique (CVE-2016-1000027), 35 vulnérabilités majeures, 103 modérées et 16 vulnérabilités mineures.

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 12.5.0.0

- NetWitness 12.4.2.0 vers 12.5.0.0
- NetWitness 12.4.1.0 vers 12.5.0.0
- NetWitness 12.4.0.0 vers 12.5.0.0
- NetWitness 12.3.1.0 vers 12.5.0.0
- NetWitness 12.3.0.0 vers 12.5.0.0
- NetWitness 12.2.0.1 vers 12.5.0.0
- NetWitness 12.2.0.0 vers 12.5.0.0

Pour plus d'informations sur la mise à niveau vers 12.5.0.0, consultez le Guide de mise à niveau pour NetWitness 12.5.0.0

IMPORTANT : NetWitness conseille aux utilisateurs de vérifier leurs versions logicielles, en notant que les versions jusqu'à 12.2 ont atteint leur fin de vie (EOL) le 31 mars 2024. Pour en savoir plus, consultez https://community.netwitness.com/t5/product-life-cycle/product-version-life-cycle-for-rsa-netwitness-platform/ta-p/569875. Pour tirer parti des dernières fonctionnalités et mises à jour de sécurité, NetWitness vous recommande de passer à la version 12.5.

IMPORTANT : Si vous souhaitez mettre à niveau les versions 11.7.x ou 11.7.x.x vers la version 12.5.0.0, 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 12.5.

IMPORTANT : Le connecteur Warehouse utilise un coffre-fort pour stocker en toute sécurité les informations d'identification des sources et destinations d'intégration de données. Toutefois, les utilisateurs qui effectuent la mise à niveau depuis une version antérieure vers la version 12.5 ne peuvent pas démarrer les flux configurés sans migrer leurs informations d'identification existantes dans le nouveau coffre-fort. Par conséquent, les utilisateurs doivent créer manuellement une nouvelle clé de coffre-fort et actualiser le mot de passe de leurs sources et destinations configurées dans Warehouse Connector, le cas échéant. Pour obtenir des instructions détaillées sur la création de la nouvelle clé de coffre-fort, consultez la section **Warehouse Connector** sous **Tâches post-mise à niveau** du Guide de mise à niveau pour NetWitness 12.5.0.0.

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

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

Pour plus d'informations, voir https://community.netwitness.com/t5/netwitness-platform-online/what-s-new-in-previous-releases-12-x/ta-p/695650.

Problèmes corrigés dans la version 12.5.0.0

Cette section répertorie les problèmes résolus dans la version 12.5.0.0.

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 dans Endpoint

Numéro de suivi	Description
SACE-21629	Le mécanisme d'interrogation sur le serveur Endpoint n'expirait pas comme prévu lors de la vérification de la file d'attente de messages du serveur relais, en raison d'une limite du délai d'expiration trop importante.

Corrections de la page d'accueil

Numéro de suivi	Description
ASOC-148336	Les utilisateurs peuvent désormais sélectionner « Page d'accueil » comme page de destination par défaut dans l'option de configuration des préférences utilisateur sans rencontrer d'écran vide.

Correctifs relatifs aux plates-formes

Numéro de suivi	Description
ASOC-146908	Lors de la mise à niveau, l'hôte ne parvient pas à démarrer dans le noyau el8 une fois la migration du système d'exploitation terminée.

Corrections du décodeur

Numéro de suivi	Description
ASOC-147188	Lors de l'exécution de la commande optionnelle Prune dans le cadre de la migration DPDK, des messages d'échec continus relatifs à certaines interfaces sont affichés dans les fichiers journaux.
ASOC-144467	Lors du rechargement du plug-in hébergé, l'instance du plug-in est supprimée au lieu d'être rechargée à partir du service Decoder ou de l'arborescence hébergée.
ASOC-154781	La mise à niveau du décodeur vers 12.4.x finit par remplir la partition /var/netwitness/decoder avec les données parsestatdb.

Problèmes connus dans la version 12.5.0.0

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 12.5.0.0

Le tableau suivant répertorie les numéros de build des différents composants de NetWitness 12.5.0.0

Composant	Numéro de version
Serveur admin NetWitness	rsa-nw-admin-server-12.5.0.0-240117024246.5.165a1f70.el8.alma.noarch.rpm
NetWitness Contenu d'analyse avancée	rsa-nw-advanced-analytics-content-12.5.0.0-231212110357.5.9b3b362.el8.alma.noarch.rpm
NetWitness Serveur d'analyse avancée	rsa-nw-advanced-analytics-server-12.5.0.0-231212110325.5.9b3b362.el8.alma.noarch.rpm
NetWitness Appareil	rsa-nw-appliance-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Archiver	rsa-nw-archiver-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Plugin d'audit	rsa-audit-plugins-12.5.0.0-4892.5.9d0750b41.el8.noarch.rpm
NetWitness Audit RT	rsa-audit-rt-12.5.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitness Démarrage	rsa-nw-bootstrap-12.5.0.0-2401240926.5.a3d68ef.el8.noarch.rpm
NetWitness Broker	rsa-nw-broker-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Carlos RT	rsa-carlos-rt-12.5.0.0-2787.5.721a8daa7.el7.x86_64.rpm
NetWitness Cloud	rsa-nw-cloud-12.5.0.0-12867.5.957818c84.el8.x86_64.rpm
NetWitness Serveur Cloud Connector	rsa-nw-cloud-connector-server-12.5.0.0-240116135943.5.4220688.el8.alma.noarch.rpm
NetWitness Serveur de lien Cloud	rsa-nw-cloud-link-server-12.5.0.0-240117032857.5.d4a8422.el8.alma.noarch.rpm
NetWitness Collectd	rsa-collectd-12.5.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitness Collectd SMS	rsa-collectd-sms-12.5.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitness Description du composant	rsa-nw-component-descriptor-12.5.0.0-2402280945.5.4c3391a.el8.noarch.rpm
NetWitness Concentrateur	rsa-nw-concentrator-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Gestion de la configuration	rsa-nw-config-management-12.5.0.0-2402050947.5.b7e9f64.el8.noarch.rpm
NetWitness Serveur de configuration	rsa-nw-config-server-12.5.0.0-240109020724.5.dc657b7.el8.alma.noarch.rpm
NetWitness Console	rsa-nw-console-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm

NetWitness Serveur de contenu	rsa-nw-content-server-12.5.0.0-240109040529.5.314fc043.el8.alma.noarch.rpm
NetWitness Serveur ContextHub	rsa-nw-contexthub-server-12.5.0.0-240122010054.5.d98d0ac61.el8.alma.noarch.rpm
NetWitness Serveur de corrélation (ESA)	rsa-nw-correlation-server-12.5.0.0-240117103632.5.61d080a9.el8.alma.noarch.rpm
NetWitness Contenu du tableau de bord	rsa-nw-dashboard-content-20231220155210-5.noarch.rpm
NetWitness Decoder	rsa-nw-decoder-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Contenu analytique Decoder	rsa-nw-decoder-analytics-content-20231220155210-5.noarch.rpm
NetWitness Contenu Decoder	rsa-nw-decodercontent-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Déploiement de mise à niveau	rsa-nw-deployment-upgrade-12.5.0.0-2402150604.5.dbd95e3.el8.noarch.rpm
Agents NetWitness Endpoint	rsa-nw-endpoint-agents-12.5.0.0-2402061657.5.db93b9a.el8.x86_64.rpm
NetWitness Serveur Endpoint Broker	rsa-nw-endpoint-broker-server-12.5.0.0-240103053136.5.8430874.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-12.5.0.0-240125030031.5.12c246114.el8.alma.noarch.rpm
NetWitness Esper Enterprise	rsa-nw-esper-enterprise-12.5.0.0-2311071130.5.04c15de.el8.alma.noarch.rpm
NetWitness Serveur d’intégration	rsa-nw-integration-server-12.5.0.0-240117101347.5.0ed5cc33.el8.alma.noarch.rpm
Serveur NetWitness Investigate	rsa-nw-investigate-server-12.5.0.0-240109023320.5.2a0d2764.el8.alma.noarch.rpm
Serveur Web existant NetWitness	rsa-nw-legacy-web-server-12.5.0.0-240122162503.5.40628dd.el8.almalinux.noarch.rpm
NetWitness Serveur de licences	rsa-nw-license-server-12.5.0.0-240111044400.5.a6108af.el8.alma.noarch.rpm
NetWitness Log Collector	rsa-nw-logcollector-12.5.0.0-15127.5.527ec7727.el8.x86_64.rpm
NetWitness Contenu Log Collector	rsa-nw-logcollectorcontent-20240105141144-5.x86_64.rpm
NetWitness Log Collector Perl	rsa-nw-logcollector-perl-12.5.0.0-15127.5.527ec7727.el8.x86_64.rpm

NetWitness Outils Log Collector	rsa-nw-logcollector-tools-12.5.0.0-15127.5.527ec7727.el8.x86_64.rpm
NetWitness Log Decoder	rsa-nw-logdecoder-12.5.0.0-12866.5.1aefe557c.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-12.5.0.0-12866.5.1aefe557c.el8.x86_64.rpm
NetWitness Serveur Malware Analytics	rsa-nw-malware-analytics-server-12.5.0.0-240207115909.5.1511622.el8.almalinux.x86_64.rpm
NetWitness Utilitaire de méta-exportation	rsa-nw-metaexport-utility-12.5.0.0-110124.5.el8.x86_64.rpm
NetWitness Serveur de metrics	rsa-nw-metrics-server-12.5.0.0-240109050254.5.c078db1.el8.alma.noarch.rpm
NetWitness Serveur infrarouge de nœud	rsa-nw-node-infra-server-12.5.0.0-240116091133.5.70861f6.el8.alma.noarch.rpm
NetWitness Interface de ligne de commande Orchestration	rsa-nw-orchestration-cli-12.5.0.0-2401091103.5.7317baa.el8.noarch.rpm
Serveur NetWitness Orchestration	rsa-nw-orchestration-server-12.5.0.0-240119064852.5.a87bb81f.el8.alma.noarch.rpm
NetWitness Espace réservé	rsa-nw-placeholder-12.5.0.0-2310040926.5.cebd204.el8.noarch.rpm
NetWitness Presidio Airflow	rsa-nw-presidio-airflow-12.5.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Serveur de configuration Presidio	rsa-nw-presidio-configserver-12.5.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Presidio Core	rsa-nw-presidio-core-12.5.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Initialisation de la recherche Presidio Elastic	rsa-nw-presidio-elasticsearch-init-12.5.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Presidio Ext NetWitness	rsa-nw-presidio-ext-netwitness-12.5.0.0-2401151152.5.18bd06b.el8.noarch.rpm
NetWitness Presidio Manager	rsa-nw-presidio-manager-12.5.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Sortie Presidio	rsa-nw-presidio-output-12.5.0.0-2401310542.5.2446840.el8.noarch.rpm
NetWitness Interface utilisateur Presidio	rsa-nw-presidio-ui-12.5.0.0-2402270745.5.0844250.el8.noarch.rpm

NetWitness Protobufs	rsa-protobufs-rt-12.5.0.0-928.5.6254aabd8.el8.x86_64.rpm
NetWitness Outils de récupération	rsa-nw-recovery-tool-12.5.0.0-2401230435.5.f34a9fd.el8.noarch.rpm
NetWitness Serveur relais	rsa-nw-relay-server-12.5.0.0-240112083607.5.6d41796.el8.alma.noarch.rpm
NetWitness Serveur Reporting Engine	rsa-nw-re-server-12.5.0.0-5996.5.b76234be4.el8.x86_64.rpm
Serveur NetWitness Respond	rsa-nw-respond-server-12.5.0.0-240110052505.5.1eda6132f.el8.alma.noarch.rpm
NetWitness Serveur d'actions de réponse	rsa-nw-response-actions-server-12.5.0.0-240116034125.5.0af5d71.el8.alma.noarch.rpm
NetWitness Mise à jour de l'autorité de certification racine	rsa-nw-root-ca-update-12.5.0.0-2401221231.5.96cd15b.el8.noarch.rpm
NetWitness Outils SA	rsa-sa-tools-12.5.0.0-2401251338.5.89600eb.el8.noarch.rpm
NetWitness Interface de ligne de commande de sécurité	rsa-nw-security-cli-12.5.0.0-2401091103.5.18ab320.el8.noarch.rpm
NetWitness Serveur de sécurité	rsa-nw-security-server-12.5.0.0-240123034132.5.11d93f41.el8.alma.noarch.rpm
NetWitness Shell	rsa-nw-shell-12.5.0.0-240108140410.5.0b0d73f5.el8.alma.noarch.rpm
NetWitness Plugins de rapport SOS	rsa-nw-sosreport-plugins-12.5.0.0-2401162235.5.af21a76.el8.noarch.rpm
NetWitness SMS Runtime RT	rsa-sms-runtime-rt-12.5.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitness Serveur SMS	rsa-sms-server-12.5.0.0-4892.5.9d0750b41.el8.x86_64.rpm
NetWitness Serveur source	rsa-nw-source-server-12.5.0.0-240207074107.5.4b84868b1.el8.alma.noarch.rpm
NetWitness Contenu du serveur source	rsa-nw-sourceserver-content-20240105141144-5.x86_64.rpm
Interface utilisateur NetWitness	rsa-nw-ui-12.5.0.0-240131063757.5.d1b137ecbc.el8.alma.noarch.rpm
NetWitness Workbench	rsa-nw-workbench-12.4.5.0-12866.5.1aefe557c.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 12.5.0.0	https://community.netwitness.com/t5/netwitness-platform-online/tkb-p/netwitness-online-documentation
Guide de mise à niveau de NetWitness Platform 12.5.0.0	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.