RSA NETWITNESS® PLATFORM

Guide de mise en route

pour la plate-forme RSA NetWitness® 11.3

Informations de contact

RSA Link à l'adresse https://community.rsa.com contient une base de connaissances qui répond aux questions courantes et fournit des solutions aux problèmes connus, une documentation produit, des discussions communautaires et la gestion de dossiers.

Marques commerciales

Pour obtenir la liste des marques commerciales de RSA, rendez-vous à l'adresse suivante : france.emc.com/legal/emc-corporation-trademarks.htm#rsa.

Contrat de licence

Licences tierces

Ce produit peut inclure des logiciels développés par d'autres entreprises que RSA. Le texte des contrats de licence applicables aux logiciels tiers présents dans ce produit peut être consulté sur la page de la documentation produit du site RSA Link. En faisant usage de ce produit, l'utilisateur convient qu'il est pleinement lié par les conditions des contrats de licence.

Remarque sur les technologies de chiffrement

Ce produit peut intégrer une technologie de chiffrement. Étant donné que de nombreux pays interdisent ou limitent l'utilisation, l'importation ou l'exportation des technologies de chiffrement, il convient de respecter les réglementations en vigueur lors de l'utilisation, de l'importation ou de l'exportation de ce produit.

Distribution

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

June 2019

Sommaire

Mise en route avec NetWitness Platform 6
Présentation 6
Architecture 6
Composants de base et en aval 9
Connexion à la plateforme NetWitness 10
Changement de votre mot de passe 13
Identifier votre rôle 15
Navigation de base de la plate-forme NetWitness 16
Accès aux vues principales 17
Menus secondaires 17
Options supplémentaires 17
Vues principales 18
SURVEILLER 18
RÉPONDRE 21
ENQUÊTER 23
CONFIGURER 28
ADMIN 31
Configuration de votre vue par défaut par le rôle du SOC 33
Définition de votre vue par défaut 35
Conseils de dépannage de base pour la configuration des utilisateurs 37
Configuration des préférences utilisateur 38
Préférences (la plupart des vues à l'exception des vues Répondre et de certaines vues Enquêter) 38
Afficher vos préférences 39
Définir la langue et le fuseau horaire 39
Activer ou désactiver les notifications système de votre compte utilisateur 40
Activer ou désactiver les menus contextuels de votre compte utilisateur 40
Préférences utilisateur (vue Répondre et certaines vues Enquêter) 40
Afficher vos préférences utilisateur 40
Définissez la langue, le fuseau horaire, ainsi que le format de la date et de l'heure 41
Sélectionner l'emplacement de démarrage de NetWitness Platform par défaut 42
Sélectionner la vue Enquêter par défaut 42
Choisir l'apparence de NetWitness Platform 43
Gestion des tableaux de bord 45
Notions de base relatives aux tableaux de bord 45
Titre du tableau de bord 45

Liste de sélection des tableaux de bord ... 45
Barre d'outils du tableau de bord ... 46
Tableau de bord par défaut ... 47
Sélection d'un tableau de bord préconfiguré ... 47
Activation ou désactivation des tableaux de bord ... 48
Activation d'un tableau de bord ... 49
Désactivation d'un tableau de bord ... 51
Définition d'un tableau de bord en tant que favori ... 51
Création de tableaux de bord personnalisés ... 52
Utilisation des dashlets ... 53
Ajouter un dashlet ... 55
Modifier les propriétés du dashlet ... 56
Réorganiser un dashlet ... 58
Agrandir un dashlet unique ... 59
Supprimer un dashlet ... 60
Importation et exportation de tableaux de bord ... 60
Importer le tableau de bord ... 60
Exporter un tableau de bord ... 61
Copie d'un tableau de bord ... 61
Partage d'un tableau de bord ... 62
Gestion des tâches ... 63
Afficher la barre d'état Tâches ... 63
Voir Toutes vos tâches ... 64
Interrompre et reprendre l'exécution planifiée d'une tâche récurrente ... 64
Annuler une tâche ... 64
Supprimer une tâche ... 65
Télécharger une tâche ... 65
Affichage et suppression des notifications ... 66
Afficher les notifications récentes ... 66
Afficher toutes vos notifications ... 67
Supprimer tous les enregistrements de notification ... 67
Affichage de l'aide dans l'application ... 68
Afficher l'aide incorporée ... 68
Afficher les info-bulles ... 68
Afficher l'aide en ligne ... 68
Recherche de documents dans RSA Link ... 69
Localiser la documentation NetWitness Platform ... 69
Localiser le contenu RSA ... 69
Localiser les sources d'événements prises en charge par RSA ... 69
Localiser les Guides de configuration du matériel ... 70

Rechercher des documents à l'aide du navigateur NetWitness 70
Suivre les mises à jour de contenu 70
Envoyez vos commentaires à RSA 71
Références de démarrage de la plateforme NetWitness 72
Préférences utilisateur 73
Panneau Notifications et barre d'état Notifications 79
Panneau Tâches et barre d'état Tâches 82

Mise en route avec NetWitness Platform

Présentation

RSA NetWitness® Platform est une puissante suite de détection des menaces qui permet aux centres d'opérations de sécurité (SOC) de localiser, de hiérarchiser et de trier rapidement les menaces. NetWitness Platform vous aide à isoler et à corriger les menaces connues, ainsi que celles qui étaient auparavant inconnues. Il fournit un aperçu approfondi des paquets, des logs et des points de terminaison qui vous offrent une vue inégalée sur votre entreprise ou votre activité.

NetWitness Platform est puissant, mais il est plus facile à utiliser pour les analystes de niveau 1 car il automatise le processus d'identification et de hiérarchisation des menaces suspectes. Les analystes de niveau 2 et de niveau 3 peuvent rechercher et localiser les menaces en recherchant et en filtrant les événements, puis en examinant les événements à l'aide des outils de reconstruction et d'analyse.

Architecture

RSA NetWitness Platform est un système distribué et modulaire qui permet des architectures de déploiement hautement flexibles s'adaptant aux besoins de l'organisation. NetWitness Platform permet aux administrateurs de collecter trois types de données à partir de l'infrastructure réseau, des données par paquets, des données de logs et des données de points de terminaison. Les aspects clés de l'architecture sont les suivants :

- **Collecte de données distribuées**. Le service **Decoder** permet d'acquérir les données de paquets, alors que le service **Log Decoder** permet d'acquérir les données des fichiers log. Le services Decoder analysent et reconstruisent tout le trafic réseau collecté depuis les niveaux 2 à 7, ou les données de fichiers log et d'événements issues de centaines de périphériques et de sources d'événements, y compris les données de NetWitness Endpoint (si installé et configuré). Le **Concentrator** indexe les métadonnées extraites d'un réseau ou les données des fichiers log afin d'autoriser l'interrogation et l'analytique en temps réel à l'échelle de l'entreprise tout en facilitant le reporting et la génération d'alertes. Le **Broker** agrège les données capturées par d'autres appareils et sources d'événements. Les Brokers agrègent les données provenant des Concentrators configurés ; les Concentrators agrègent les données provenant des Decoders. Ainsi, un Broker fait le lien entre les multiples datastores en temps réel, conservés dans les différentes paires Decoder/Concentrator à travers l'infrastructure.
- **Alerte en temps réel**. Le service NetWitness Platform **Event Stream Analysis (ESA)** fournit une analytique de flux avancée, comme la corrélation et le traitement d'événements complexes avec des débits élevés et une faible latence. Il peut traiter de gros volumes de données d'événements disparates provenant des services Concentrator. ESA utilise un langage EPL (Event Processing Language) avancé qui permet aux analystes de réaliser le filtrage, l'agrégation, les jointures, la reconnaissance des modèles et la corrélation entre plusieurs flux d'événements disparates. Event Stream Analysis offre une puissante détection des incidents et la génération d'alertes.
- **Analytique en temps réel** (Analyse automatique des événements) La fonctionnalité Détection automatisée des menaces de RSA comprend des modules ESA Analytics préconfigurés pour détecter le trafic de commandes et de contrôles.

- **Serveur NetWitness**. Serveur NetWitness est impliqué dans les modules Reporting, Investigation, Administration et d'autres aspects de l'interface utilisateur.
- **Capacité**. NetWitness Platform possède une architecture à capacité modulaire compatible avec des unités DAC (direct-attached capacity) ou des réseaux de stockage SAN, qui s'adapte aux besoins de l'organisation en matière d'investigation à court terme, et d'analytique et de conservation de données à plus long terme.

NetWitness Platform offre une grande souplesse de déploiement. Vous pouvez composer son architecture de plusieurs dizaines d'hôtes physiques ou d'un seul hôte physique selon les caractéristiques spécifiques du client et les besoins en matière de sécurité. D'autre part, l'ensemble du système NetWitness Platform a été optimisé pour s'exécuter sur une infrastructure virtuelle.

L'architecture du système comprend les composants principaux suivants : services Decoder, Broker, Concentrator, Archiver, ESA et Warehouse Connector. Les composants NetWitness Platform peuvent être utilisés parallèlement en tant que système, ou peuvent être utilisés individuellement.

- Lors de l'implémentation d'un système de gestion des événements et des informations de sécurité (SIEM), la configuration de base inclut les composants suivants : Log Decoder, Concentrator, Broker, Event Stream Analysis (ESA) etServeur NetWitness.
- Lors de l'implémentation approfondie, la configuration de base inclut les composants suivants : Decoder, Concentrator, Broker, ESA, Analyse de logiciel malveillant et Endpoint Log Hybrid. Le service Serveur de réponse est également nécessaire et permet de hiérarchiser les alertes.

Ce tableau présente brièvement les principaux composants :

Composant système	Description
Decoder / Log Decoder	• NetWitness Platform collecte les données de paquets, logs et points de terminaison. • Les données de paquets (c'est-à-dire les paquets réseau) sont collectées par l'intermédiaire du Decoder via la prise robinet du réseau ou le port SPAN, généralement défini comme un point de sortie sur le réseau d'une organisation. • Un Log Decoder peut collecter quatre types de log différents, à savoir Syslog, ODBC, événements Windows et fichiers plats. • Les événements Windows font référence à la méthode de collecte de Windows 2008 tandis que les fichiers plats sont obtenus via SFTP. • Les deux types de services Decoder reçoivent des données transactionnelles brutes qui sont enrichies, clôturées et agrégées à d'autres composants de NetWitness Platform. • Le processus d'acquisition et d'analyse des données transactionnelles repose sur un framework dynamique et ouvert.

Composant système	Description
Endpoint Log Hybrid	• Collecte et gère les données de terminaux (hôte) à partir d'hôtes Windows, Mac ou Linux. • Enregistre les données relatives à chaque action critique, telles que les processus, les fichiers, les modifications du registre, les connexions réseau et les interactions entre les consoles utilisateur. • Collecte les logs à partir des hôtes Windows si la collecte est configurée. • Génère des métadonnées pour corréler les données de terminal avec des sessions provenant d'autres sources d'événements, comme les logs et le réseau. • Effectue l'analyse de la mémoire dynamique, l'analyse du trafic réseau et la détection du comportement suspect de l'utilisateur.
Concentrator	• Fournit une fonctionnalité d'indexation et de requête aux collectes NetWitness. • Peut éventuellement transférer des données au service ESA.
Broker	• Distribue l'accès à la collecte NetWitness à travers de nombreux services Concentrator ou Archiver, faisant de l'activité NetWitness Platform une collecte unique.
Archiver	• Le service Archiver permet d'archiver les logs à long terme en indexant et en compressant les données des fichiers log, puis en les envoyant dans un espace de stockage d'archives. • Cet espace de stockage d'archives est optimisé pour assurer une conservation des données à long terme et générer des rapports de conformité. • Archiver stocke des logs bruts et des métadonnées de logs issus des Log Decoders en vue de leur conservation à long terme et utilise des DAC (Direct-Attached Capacity) dans le cadre du stockage. **Remarque :** Les paquets bruts et les métadonnées de paquets ne sont pas stockés dans Archiver.

Composant système	Description
Event Stream Analysis (ESA)	• Le service Event Stream Analysis (ESA) fournit une analytique de flux d'événements, telle que la corrélation et le traitement complexe d'événements, avec un haut débit et une faible latence. Il est capable de traiter de gros volumes de données d'événements disparates provenant des services Concentrator. • ESA utilise un langage avancé de traitement des événements (Event Processing Language) permettant aux utilisateurs de réaliser le filtrage, l'agrégation, l'association, la reconnaissance de schémas et la corrélation entre des flux d'événements multiples et disparates. • ESA contribue à une puissante fonction de détection des incidents et de génération d'alertes. • La fonctionnalité Détection automatisée des menaces de RSA comprend des modules ESA Analytics préconfigurés pour détecter le trafic de commandes et de contrôles.

Composants de base et en aval

Dans NetWitness Platform, les services Core intègrent et analysent les données, génèrent les métadonnées et agrègent les métadonnées générées aux données brutes. Les services Core comprennent les services Decoder, Log Decoder, Concentrator et Broker. Les systèmes en aval utilisent les données stockées sur les services Core à des fins d'analytique. Par conséquent, les opérations des services en aval dépendent des services Core. Les systèmes en aval incluent Archiver, ESA, Malware Analysis, Investigation et Reporting.

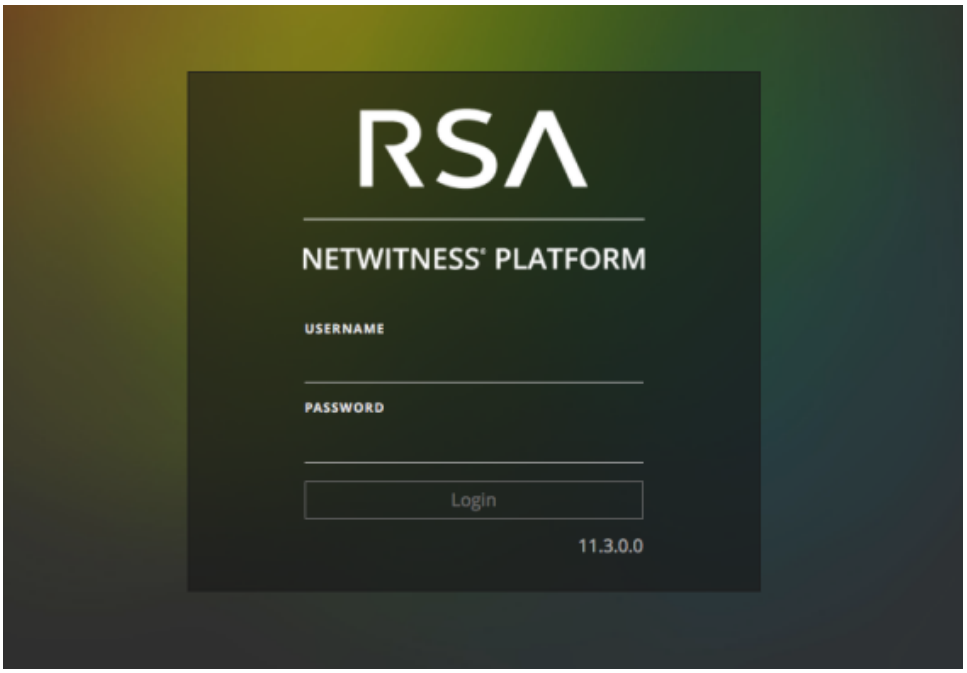
Bien que les services Core puissent fonctionner et fournir une bonne solution analytique sans les systèmes en aval, les composants en aval fournissent une analytique supplémentaire. ESA offre une corrélation en temps réel à travers les sessions et événements, ainsi qu'entre différents types d'événements, tels que les données de log, de paquets et de points de terminaison. La vue Enquêter permet d'explorer les données, d'examiner les événements et les fichiers, mais également de reconstituer des événements dans un environnement sécurisé. Le service Malware Analysis assure l'inspection automatisée en temps réel des activités malveillantes dans les sessions réseau et les fichiers associés.

Connexion à la plateforme NetWitness

La connexion à RSA NetWitness® Platform varie en fonction de votre environnement. Vous pouvez avoir un compte utilisateur interne ou un compte utilisateur externe. Les comptes utilisateur internes sont locaux à NetWitness Platform et les utilisateurs internes peuvent se connecter à NetWitness Platform et recevoir des autorisations basées sur les rôles. Les comptes utilisateur externes sont authentifiés en dehors de NetWitness Platform et sont mappés sur les rôles NetWitness Platform. Si vous êtes un utilisateur externe et que vous ne pouvez pas accéder à NetWitness Platform ni afficher les informations dont vous avez besoin, contactez votre administrateur système. Votre administrateur peut attribuer les rôles appropriés à votre compte.

Remarque : NetWitness Platform prend en charge les versions modernes (ou actuelles) de Google Chrome, Mozilla Firefox et Apple Safari. Il est possible d'utiliser un autre navigateur, mais certaines fonctionnalités peuvent ne pas fonctionner comme prévu.

1. Utilisez une icône fournie par votre administrateur, ou saisissez ce qui suit dans votre navigateur Web :
   `https://<hostname or IP address>/login`
   `<hostname or IP address>` correspondant au nom d'hôte ou à l'adresse IP de votre serveur NetWitness.
   L'écran de connexion s'affiche.



2. Saisissez votre nom d'utilisateur et votre mot de passe, puis cliquez sur **Se connecter**.
   Si votre connexion est réussie, vous serez connecté(e) à la page de destination spécifiée dans vos préférences utilisateur.

Si vous êtes bloqué(e) :

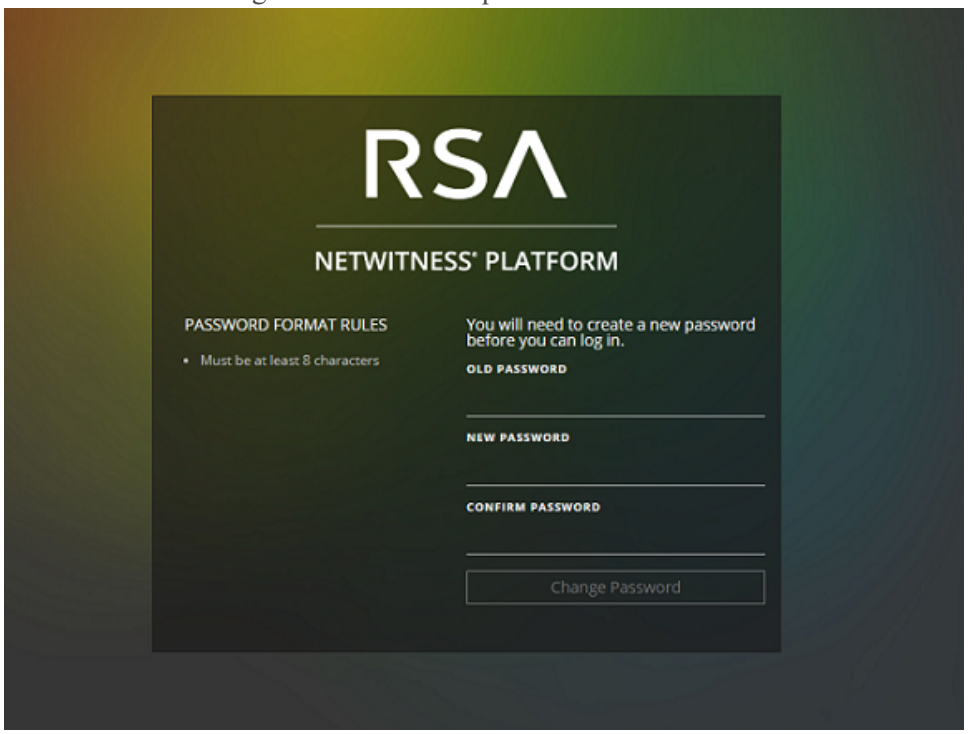
Remarque : Ces informations s'appliquent uniquement aux comptes internes. Elle ne s'applique pas aux comptes Active Directory ou PAM.

Si vous tentez de vous connecter à plusieurs reprises avec un nom d'utilisateur ou un mot de passe incorrect, votre compte sera verrouillé. Contactez votre administrateur pour déverrouiller votre compte.

Si vous disposez d'un nouveau compte ou si votre compte a expiré :

Remarque : Cette procédure s'applique uniquement aux comptes internes. Elle ne s'applique pas aux comptes Active Directory ou PAM.

1. Dans la boîte de dialogue permettant de créer un nouveau mot de passe, entrez votre ancien mot de passe, tapez un nouveau mot de passe et confirmez-le. Les règles de format de mot de passe (définies par votre administrateur système) sont fournies à gauche et votre nouveau mot de passe doit être conforme aux règles de format indiquées.



2. Cliquez sur **Changer le mot de passe**.

Si vous ne disposez pas de l'accès approprié à NetWitness Platform :

Si vous pouvez vous connecter correctement, mais que vous ne pouvez pas afficher les informations dont vous avez besoin, il est possible que vous ayez besoin d'un rôle d'utilisateur attribué à votre compte utilisateur. Contactez votre administrateur pour obtenir de l'aide.

Déconnexion de la plate-forme NetWitness

Pour fermer la session à partir de la vue Répondre et de certaines vues Enquêter :

1. Dans la barre Menu principal, sélectionnez  .
2. Dans les préférences utilisateur, cliquez sur **Déconnexion**.

Pour se déconnecter des autres vues :

Dans la barre Menu principal, sélectionnez  **> Déconnexion**.

Changement de votre mot de passe

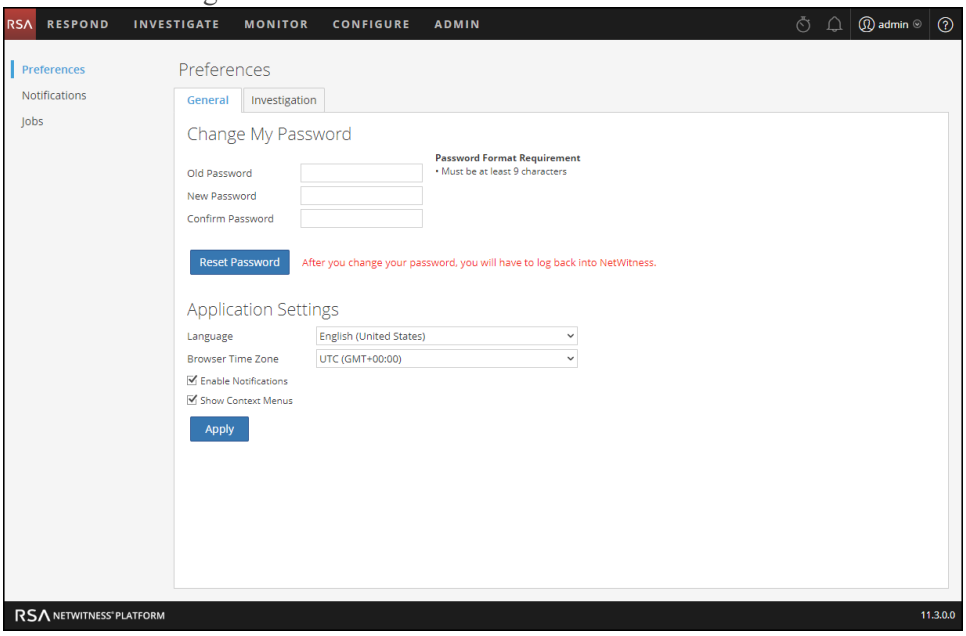
Vous pouvez modifier le mot de passe que vous utilisez pour l'authentification RSA NetWitness® Platform à tout moment dans vos préférences utilisateur. Votre administrateur définit les exigences de force de mot de passe appropriées pour votre mot de passe NetWitness Platform, telles que la longueur minimale de mot de passe et le nombre minimum de caractères majuscules, minuscules, décimaux, alphabétiques non latins et spéciaux. Ces exigences sont ensuite affichées lors de la modification de votre mot de passe.

Remarque : Cette procédure s'applique uniquement aux comptes internes. Elle ne s'applique pas aux comptes Active Directory ou PAM.

Pour changer votre mot de passe :

1. Exécutez l'une des opérations suivantes :
   - Pour la plupart des vues, telles que, Surveiller, Configurer, Administrateur ou Enquêter sélectionnez > **Profil**.
   - Dans la vue Répondre et dans certaines vues Enquêter (Analyse d'événements, Hôtes, Fichiers et Utilisateurs), sélectionnez dans la boîte de dialogue Préférences utilisateur, cliquez sur **Modifier mon mot de passe**.

   La boîte de dialogue Préférences s'affiche.



2. Dans la section **Modifier mon mot de passe**, entrez le mot de passe que vous avez utilisé pour vous authentifier auprès de NetWitness Platform dans le champ **Ancien mot de passe**.
3. Dans le champ **Nouveau mot de passe**, saisissez le mot de passe à utiliser à la prochaine connexion.
4. Dans le champ **Confirmer le mot de passe**, saisissez une seconde fois le nouveau mot de passe.

5. Cliquez sur **Réinitialiser le mot de passe**.
   Vous serez déconnecté(e) de NetWitness Platform pour que les modifications prennent effet. Le nouveau mot de passe prend effet dès la connexion suivante à NetWitness Platform.

Identifier votre rôle

Les rôles répertoriés ici sont les rôles ou les fonctions typiques d'un centre d'opérations de sécurité (SOC). Déterminez le ou les rôles que vous effectuez dans le SOC. Vous pouvez utiliser ces fonctions comme guide pour décider comment configurer et naviguer dans RSA NetWitness® Platform afin de pouvoir effectuer efficacement vos tâches.

SOC Team

SOC Manager
(SOC Management and Reporting)

- Gérer la préparation du SOC
- Répondre aux incidents
- Répondre aux violations de données

Data Privacy Officer

- Surveiller et protéger les informations confidentielles

Incident Reponder
(T1 Analyst)

- Répondre aux incidents
- Corriger les incidents

Threat Hunter
(T2/T3 Analyst)

- Rechercher activement des menaces
- Réaliser une analyse approfondie
- Recommander des problèmes à corriger
- Corriger des problèmes

Content Expert
(Threat Intelligence)

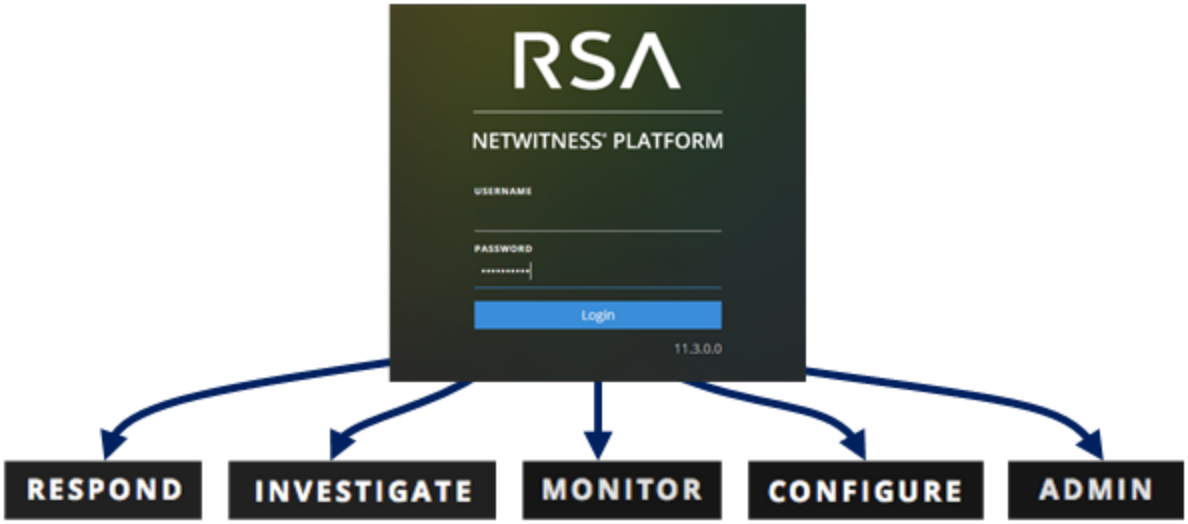
- Examiner de nouveaux renseignements sur des menaces
- Évaluer et créer de nouveaux flux
- Créer de nouvelles règles de corrélation pour signaler des indicateurs de compromission

System Administrator

- Installer et configurer des équipements et des logiciels
- Gérer l'accès utilisateur
- Surveiller et optimiser les performances
- Sauvegarder et restaurer des données
- Gérer le stockage et l'archivage
- Mettre à jour le logiciel
- Créer des rapports de conformité réglementaire

Navigation de base de la plate-forme NetWitness

L'application RSA NetWitness® Platform est divisée en cinq zones fonctionnelles principales, appelées vues, basées sur des rôles SOC (Security Operation Center) standard.



- **RÉPONDRE** : Cette vue est destinée aux Responsables de la réponse aux incidents, qui peuvent afficher la liste des incidents prioritaires à des fins de triage. Ces incidents proviennent de sources telles que les règles ESA, NetWitness Endpoint, ou des modules ESA Analytics pour la détection automatisée des menaces. Vous pouvez également afficher toutes les alertes reçues par NetWitness Platform ici.
  Dans la version 10.6, cette vue correspondait à la vue Gestion des incidents. La liste Alertes de la vue Répondre remplace les alertes ESA 10.6 > vue Résumé.
- **ENQUÊTER** : Cette vue est principalement destinée aux responsables de la recherche des menaces avancées, qui préfèrent rechercher les menaces manuellement en utilisant les métadonnées, les données d'événement brutes, ainsi que la reconstruction et l'analyse d'événements NetWitness Platform. Les responsables de la réponse aux incidents utilisent également cette vue pour obtenir des détails sur les événements associés à un incident faisant l'objet d'une enquête. Dans cette vue, les responsables de la recherche des menaces et les responsables de la réponse aux incidents peuvent utiliser les fonctions de reconstruction d'événements en analyse approfondie, ainsi que les fonctions d'analyse d'événements.
- **SURVEILLER** : Cette vue est destinée à tous les utilisateurs. Vous pouvez afficher des tableaux de bord et des rapports sur différentes zones d'intérêt en fonction de vos autorisations utilisateur. NetWitness Platform s'ouvre par défaut sur cette vue.
  Dans la version 10.6, cette vue correspond à la vue Tableau de bord.
- **CONFIGURER** : Cette vue est destinée au Personnel chargé des renseignements sur les menaces (experts de contenu), qui configure des sources de données et les intègre à NetWitness Platform. Les experts en contenu utilisent cette zone pour télécharger et gérer le contenu Live. Il peut également créer et gérer des incidents, ainsi que des règles ESA.

Dans la version 10.6, cette vue correspondait à Live, Incidents > Configurer et Alertes > Configurer depuis la version précédente.

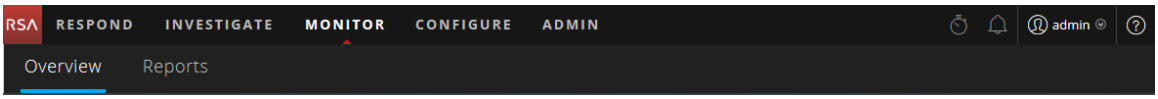
- **ADMIN** : Cette vue est destinée aux Administrateurs système, qui configurent et gèrent l'application globale.
  Dans la version 10.6, il s'agit de la vue Administration sans les sections de la vue Configurer.

Accès aux vues principales

Les options qui ouvrent chacune des vues principales sont répertoriées en haut de la fenêtre du navigateur. Si vous disposez des autorisations appropriées, à tout moment, vous pouvez accéder à n'importe quelle vue figurant en haut de chaque fenêtre du navigateur.

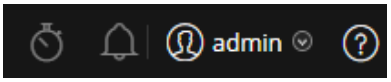
Menus secondaires

Certaines vues sont dotées de menus secondaires avec des vues supplémentaires que vous pouvez sélectionner, qui varient en fonction des tâches que vous pouvez effectuer. L'exemple suivant illustre le menu SURVEILLER.



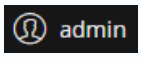
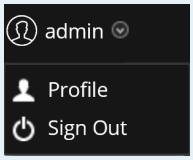
Options supplémentaires

Outre les vues principales, il existe des options supplémentaires en haut de la fenêtre du navigateur qui sont communes à l'ensemble de l'application.



Le tableau suivant décrit ces options communes :

Option commune	Nom	Description
	Tâches	Dans les vues ENQUÊTER, SURVEILLER, CONFIGURER et ADMIN, cliquez sur cette icône pour afficher et gérer vos tâches dans la barre d'état Tâches. Les tâches sont des tâches à la demande ou planifiées qui prennent un certain temps à s'exécuter dans l'application NetWitness Platform.

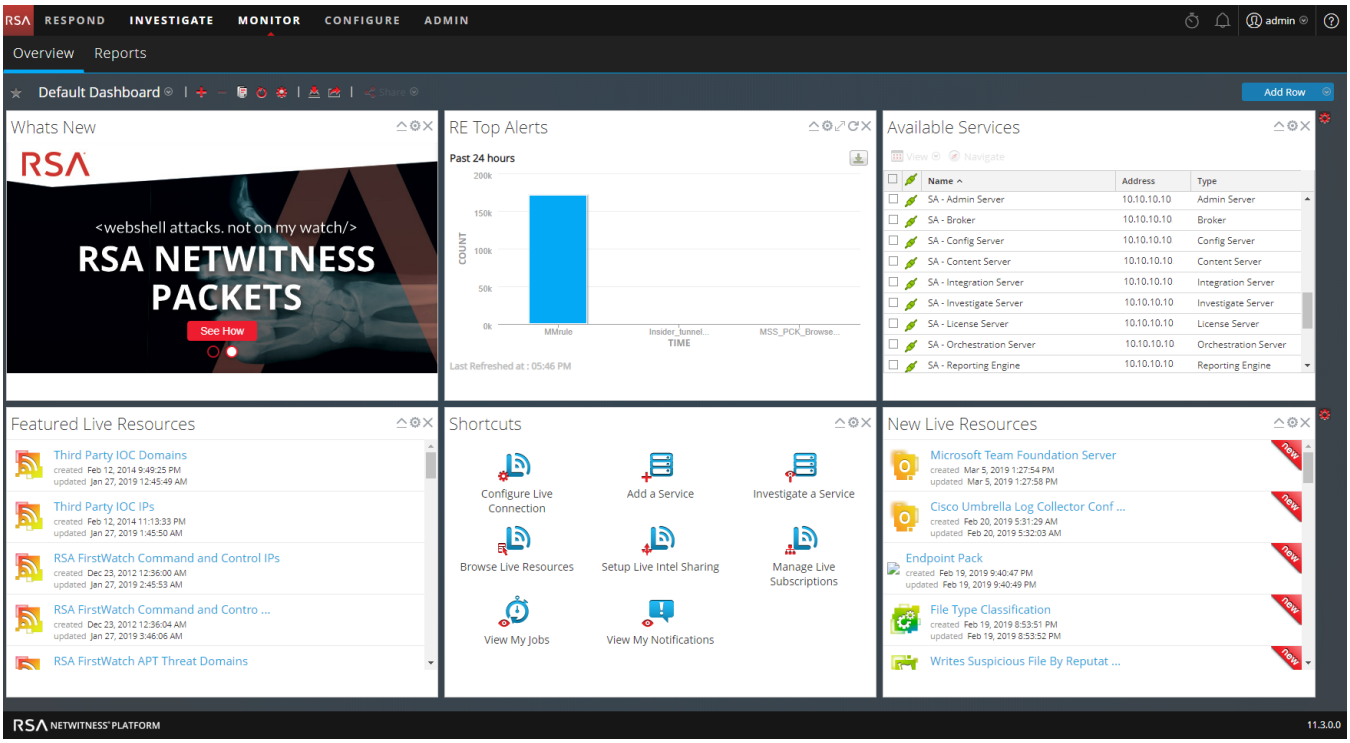
Option commune	Nom	Description
	Notifications	Cliquez sur cette icône pour afficher les notifications issues de l'application.
	Préférences utilisateur	Cliquez sur cette icône pour afficher vos options de préférences utilisateur disponibles. Vous pouvez gérer vos préférences utilisateur et vous déconnecter de NetWitness Platform.
	Profil utilisateur	Cliquez sur votre profil utilisateur pour afficher les options disponibles. Vous pouvez gérer vos préférences utilisateur, changer votre mot de passe et vous déconnecter de NetWitness Platform.
	Aide	Cliquez sur cette icône pour afficher les sections d'aide NetWitness Platform.

Vues principales

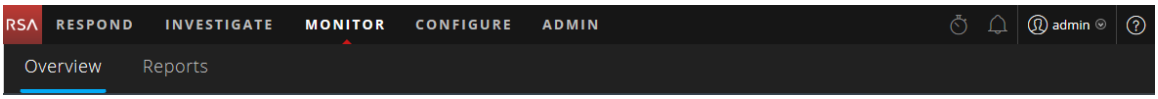
Les sections suivantes décrivent les vues principales.

SURVEILLER

La vue SURVEILLER contient le tableau de bord NetWitness Platform. La vue Surveiller fournit des tableaux de bord et des rapports préconfigurés que vous pouvez utiliser. Vous pouvez également créer les vôtres.



Menu SURVEILLER



Le menu SURVEILLER comprend les options suivantes :

- **Présentation** : La vue Présentation vous permet d'afficher et de gérer vos tableaux de bord. Vous pouvez sélectionner les tableaux de bord préconfigurés suivants :
  - Par défaut
  - Identité
  - Investigation
  - Opérations - Analyse de fichiers
  - Opérations - Logs
  - Opérations - Réseau
  - Opérations - Analyse de protocole
  - Présentation
  - RSA SecurID
  - Menaces - Traque active

- Menaces - Intrusion
- Menaces - Indicateurs de programme malveillant

Dans la version 10.6, cette vue correspondait à la vue Tableau de bord.

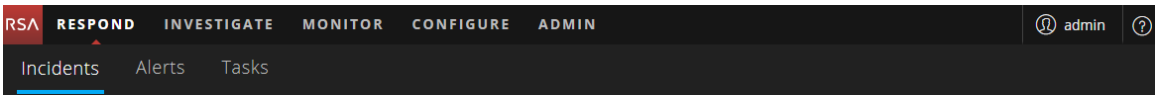
- **Rapports** : La vue Rapports vous permet d'afficher et de gérer des rapports pertinents pour votre rôle SOC en fonction de vos autorisations attribuées.

Que puis-je faire ici ?	Chemin	Me montrer comment
Sélectionner un tableau de bord	SURVEILLER > Présentation	Voir Gestion des tableaux de bord.
Créer un tableau de bord	SURVEILLER > Présentation	Voir Gestion des tableaux de bord.
Gérer les tableaux de bord	SURVEILLER > Présentation	Voir Gestion des tableaux de bord.
Afficher un rapport	SURVEILLER > Rapports > Vue	Reportez-vous au *Guide de création de rapports de l'utilisateur*.
Gérer les rapports	SURVEILLER > Rapports > Gérer	Reportez-vous au *Guide de création de rapports de l'utilisateur*.

RÉPONDRE

La vue Répondre présente les analystes avec une file d'attente d'incidents dans l'ordre de gravité. Lorsque vous intégrez un incident à la file d'attente, vous recevez des données de support pertinentes pour vous aider à enquêter sur l'incident. À partir de là, vous pouvez déterminer la portée de l'incident et le faire remonter ou bien le corriger, le cas échéant.

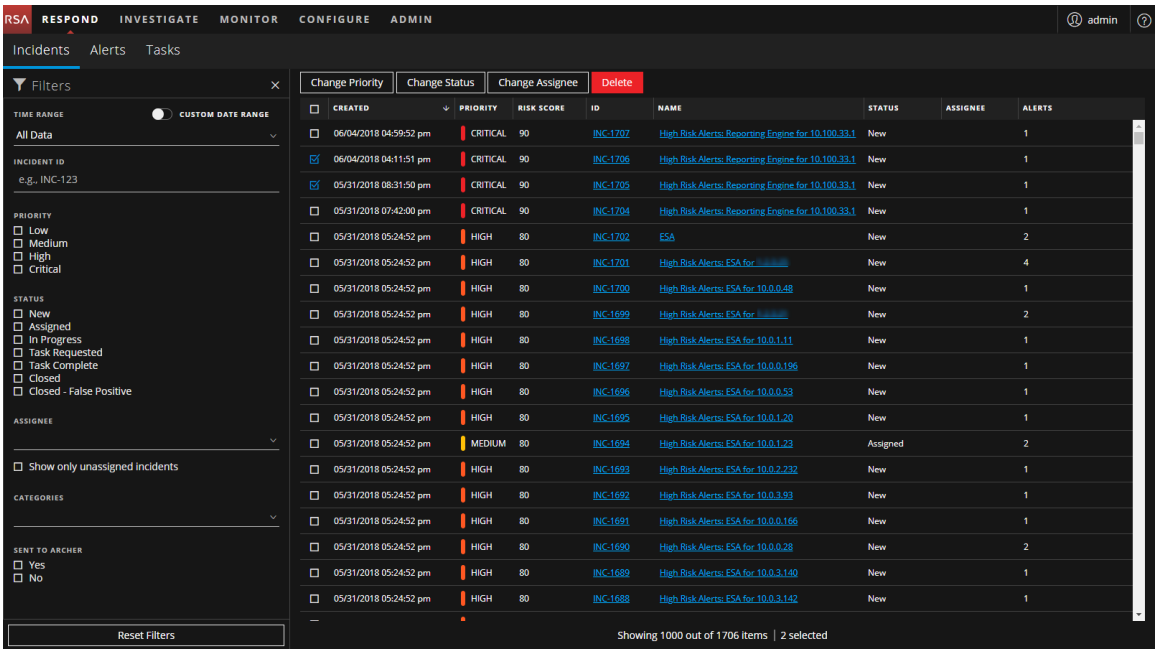
Menu RÉPONDRE



Le menu RÉPONDRE comprend les options suivantes :

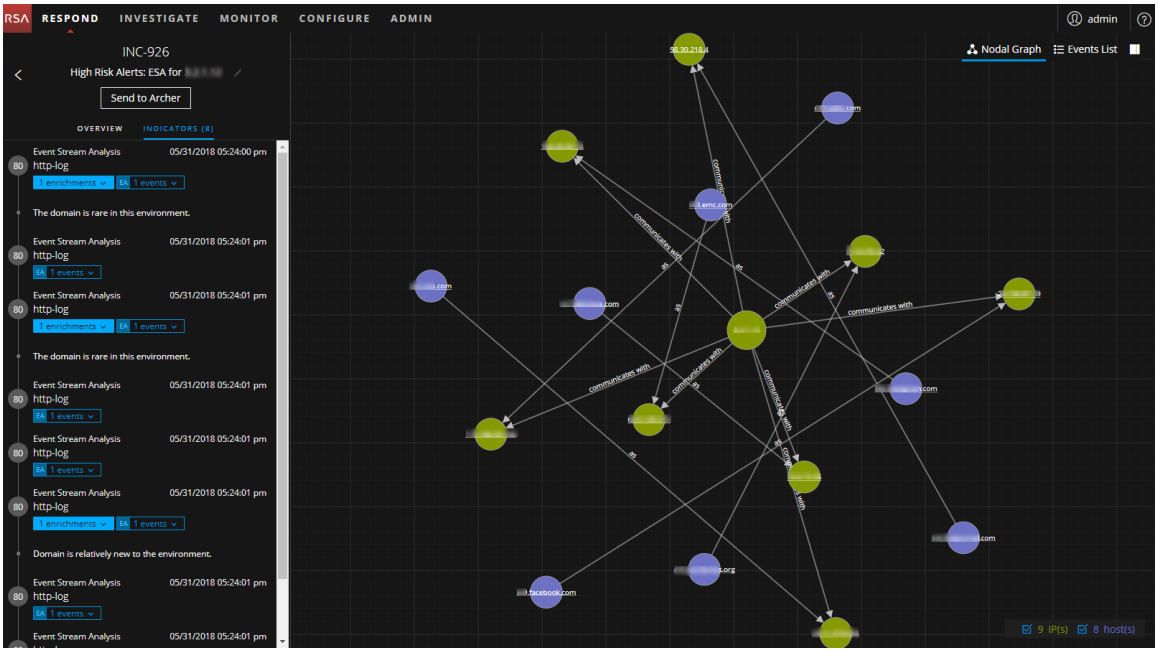
- **Incidents** : La liste des incidents regroupe tous les incidents avec des informations de base. La vue Détails de l'incident fournit des informations détaillées sur l'incident.
- **Alertes** : Les vues Liste des alertes et Détails relatifs aux alertes fournissent des informations sur toutes les alertes de menace et les indicateurs reçus parNetWitness Platform à un même emplacement.
- **Tâches** : La vue Liste des tâches vous permet de créer des tâches et de les suivre jusqu'à la fin de leur exécution.

La figure suivante présente la vue Répondre - Vue Liste d'incidents, qui affiche la liste des incidents priorisés.

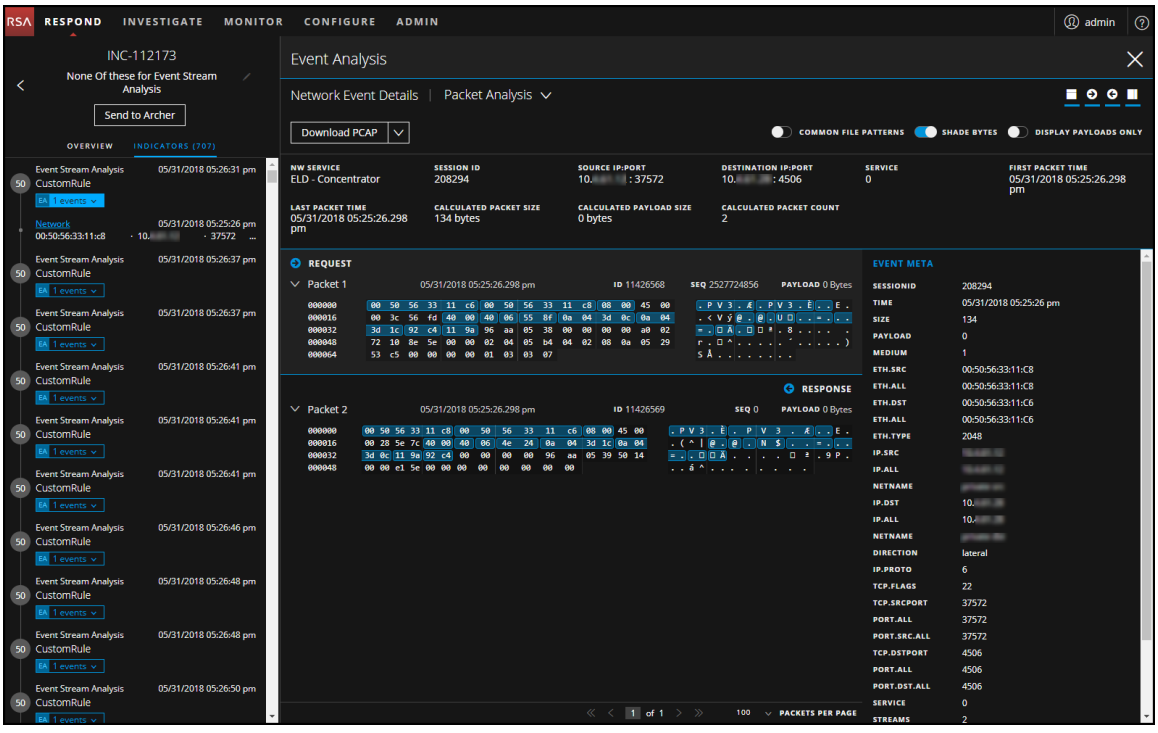


Lorsque vous utilisez NetWitness Platform en tant qu'outil de gestion des cas, vous pouvez également gérer les incidents à partir de cette vue. Les nouveaux incidents apparaissent en haut de la file d'attente des incidents.

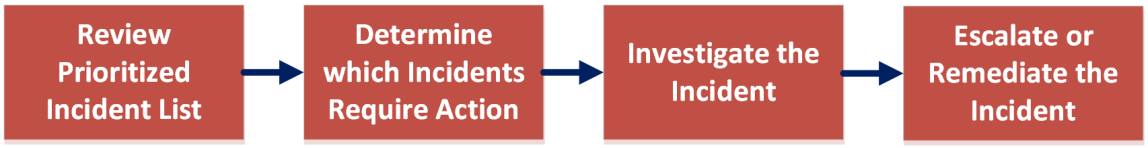
La figure suivante présente un exemple de la vue Répondre - vue Détails relatifs à l'incident sélectionné.



La vue Répondre est conçue pour aider à évaluer des incidents, contextualiser ces données, collaborer avec d'autres analystes et pivoter vers une procédure d'enquête approfondie en fonction des besoins. La figure suivante est un exemple d'analyse d'événements de la vue Détails de l'incident.



La figure suivante illustre le workflow général de la vue Répondre.



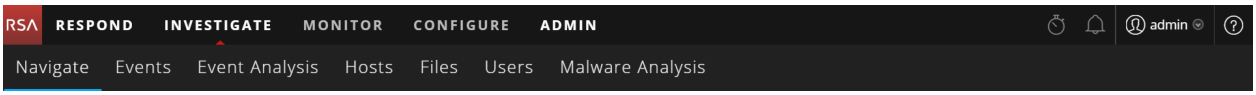
Dans la vue Répondre, les analystes examinent la liste des incidents classés par ordre de priorité et déterminent les incidents nécessitant une action. Ils cliquent sur un incident pour obtenir une image claire de l'incident avec les détails à l'appui afin d'approfondir leur enquête. Les analystes peuvent ensuite déterminer comment répondre à la menace, en faisant remonter l'incident ou en le corrigeant.

Que puis-je faire ici ?	Chemin	Me montrer comment
Afficher les listes d'incidents prioritaires	RÉPONDRE > Incidents (vue Liste des incidents)	Consultez le *Guide d'utilisation de NetWitness Respond*.
Déterminer les incidents exigeant une action (Triage d'un incident)	RÉPONDRE > Incidents (vue Détails relatifs aux incidents)	Consultez le *Guide d'utilisation de NetWitness Respond*.
Enquêter sur l'incident	RÉPONDRE > Incidents (vue Détails relatifs aux incidents)	Consultez le *Guide d'utilisation de NetWitness Respond*. (Vous pouvez également faire pivoter la vue Enquêter.)
Faire remonter ou corriger l'incident	RÉPONDRE > Incidents (vue Détails relatifs aux incidents) et RÉPONDRE > Tâches (vue Liste des tâches)	Consultez le *Guide d'utilisation de NetWitness Respond*.
Vérifier les alertes	RÉPONDRE > Alertes (vues Liste des alertes et Détails relatifs aux alertes)	Consultez le *Guide d'utilisation de NetWitness Respond*.

ENQUÊTER

La vue Enquêter présente sept vues différentes dans un ensemble de données, permettant aux analystes de voir les métadonnées et les données brutes des points de terminaison, les logs, les événements et les indicateurs potentiels de compromis. En plus de rechercher des données sur un service spécifique, vous pouvez pivoter à partir de la vue Répondre, la vue Moniteur, une entrée d'un rapport généré par Reporting Engine, ou une application tierce correctement configurée. Vous pouvez commencer votre procédure d'enquête dans l'une des sept vues Enquêter, puis poursuivre l'enquête dans une autre vue Enquêter. La manière dont vous procédez est déterminée par la question à laquelle il faut répondre. Si vous trouvez un événement nécessitant une réponse, vous pouvez créer un incident dans la vue Répondre où un Responsable de la réponse aux incidents prendra d'autres mesures. Le *Guide d'utilisation de NetWitness Investigate* fournit des informations détaillées.

Menu ENQUÊTER



Le menu ENQUÊTER comprend les options suivantes :

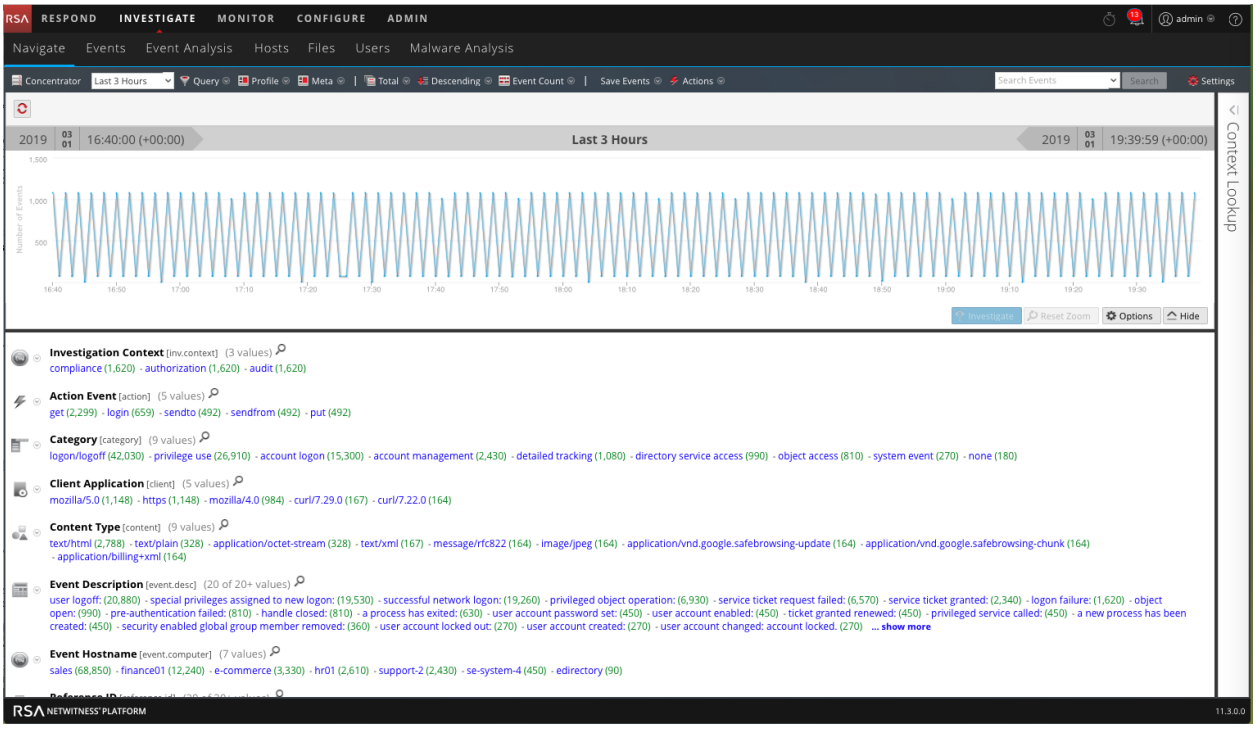
- **Parcourir** : La vue Naviguer fournit la liste des clés méta et des valeurs méta avec un accent particulier sur les métadonnées. Vous pouvez explorer les données, ouvrir un événement sélectionné dans la vue Événements ou la vue Analyse d'événements, afficher la reconstruction d'un événement, rechercher des événements, rechercher un contexte supplémentaire à partir du service Context Hub et configurer les préférences de la vue Naviguer.
- **Événements** : La vue Événements fournit une liste d'événements avec un accent particulier sur les données brutes. Vous pouvez parcourir une liste simple d'événements, une liste détaillée et une liste de logs. Vous pouvez rechercher des événements, ouvrir un événement sélectionné dans la vue Analyse d'événements, afficher la reconstruction d'un événement, rechercher un contexte supplémentaire à partir du service Context Hub et configurer les préférences de la vue Événements.
- **Analyse d'événements** : la vue Analyse d'événements fournit une liste d'événements avec le focus mis sur les métadonnées et données brutes. Vous pouvez afficher une reconstruction qui offre des indices utiles pour identifier les points d'intérêt dans une reconstruction, pivoter vers un point de terminaison autonome, rechercher un contexte supplémentaire dans le service Context Hub (versions 11.2 et versions ultérieures), rechercher des données dans Live et réaliser des recherches externes.
- **Vue Hôtes** : (Version 11.1 ou supérieure) La vue Hôtes répertorie tous les hôtes avec un agent NetWitness Endpoint en cours d'exécution. Pour chaque hôte, vous pouvez afficher les détails de l'analyse, le suivi des événements relatifs aux alertes, les anomalies, les détails du processus et les informations relatives aux utilisateurs connectés. Dans la vue Hôtes, vous pouvez accéder aux vues Naviguer, Analyse d'événements et Utilisateurs.
- **Vue Fichiers** : (Version 11.1 et versions ultérieures) La vue Fichiers fournit une vue globale de tous les fichiers de votre déploiement. Vous pouvez appliquer différents filtres, trier et classer les fichiers en fonction de leur état pour réduire le nombre de fichiers à analyser et identifier les fichiers suspects ou malveillants. Dans la vue Fichiers, vous pouvez accéder aux vues Naviguer et Analyse d'événements.
- **Vue Utilisateurs** : (Version 11.2 et ultérieures) La vue Utilisateurs fournit une visibilité sur les comportements des utilisateurs à risque dans votre entreprise avec RSA NetWitness UEBA. Vous pouvez afficher une liste d'utilisateurs à haut risque et un récapitulatif des alertes principales concernant les comportements risqués dans votre environnement, puis sélectionner un utilisateur ou une alerte et afficher des détails sur le comportement risqué et une chronologie pendant laquelle les comportements se sont produits.

  Remarque : La vue Utilisateurs n'est disponible que si le rôle Administrateur ou Analyste UEBA vous est assigné.

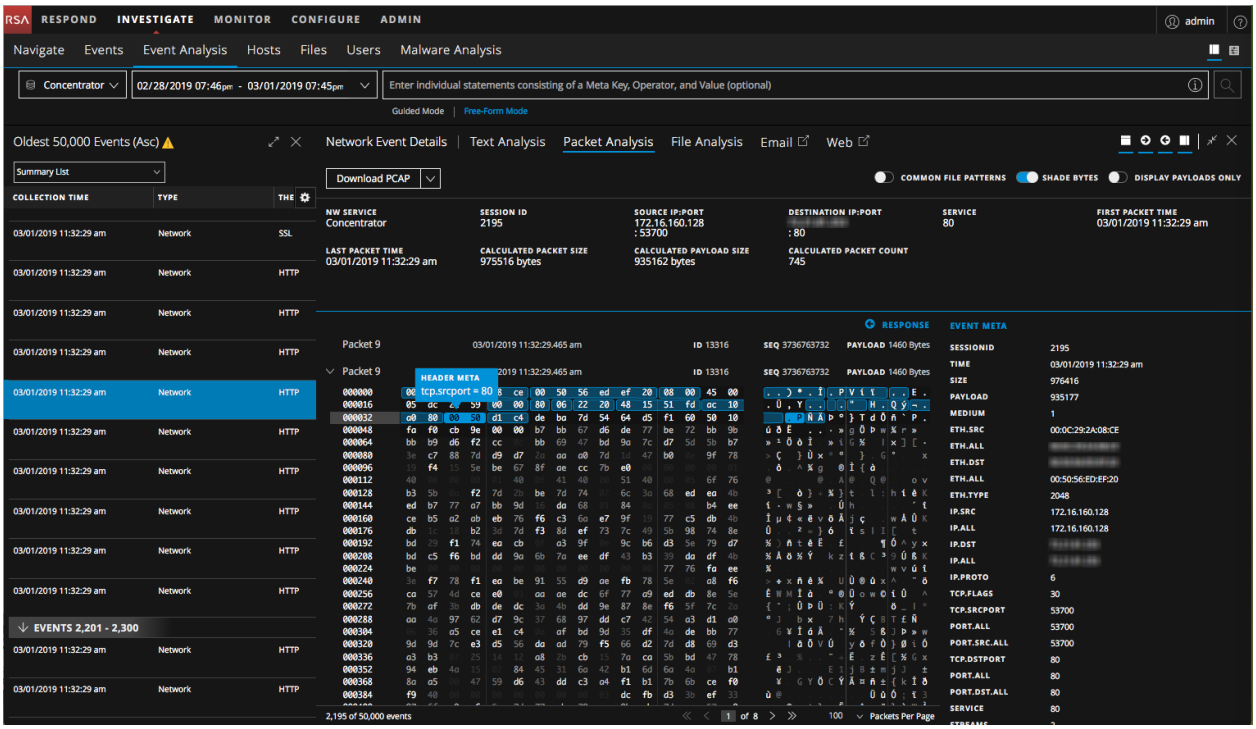
- **Analyse de logiciel malveillant** : Malware Analysis est un processeur automatisé d'analyse de malware, conçu pour analyser certains types d'objets fichiers (par exemple, Windows PE, PDF et MS Office) afin d'évaluer la probabilité de leur malveillance. À l'aide de Malware Analysis, vous

pouvez classer par ordre de priorité le grand nombre de fichiers capturés afin de concentrer les efforts d'analyse sur les fichiers qui sont les plus susceptibles d'être malveillants.

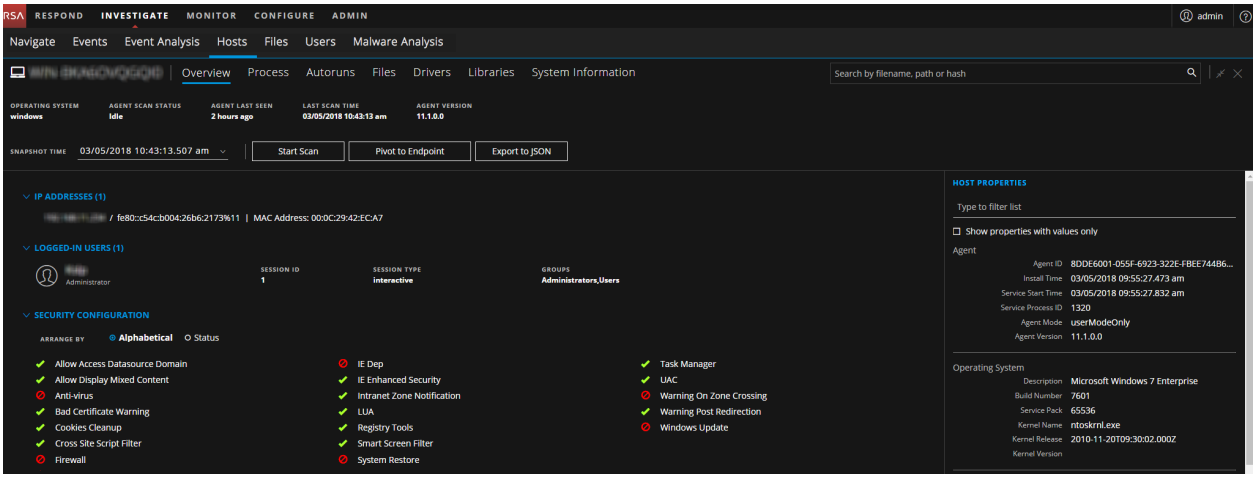
La figure ci-dessous présente la vue Naviguer.



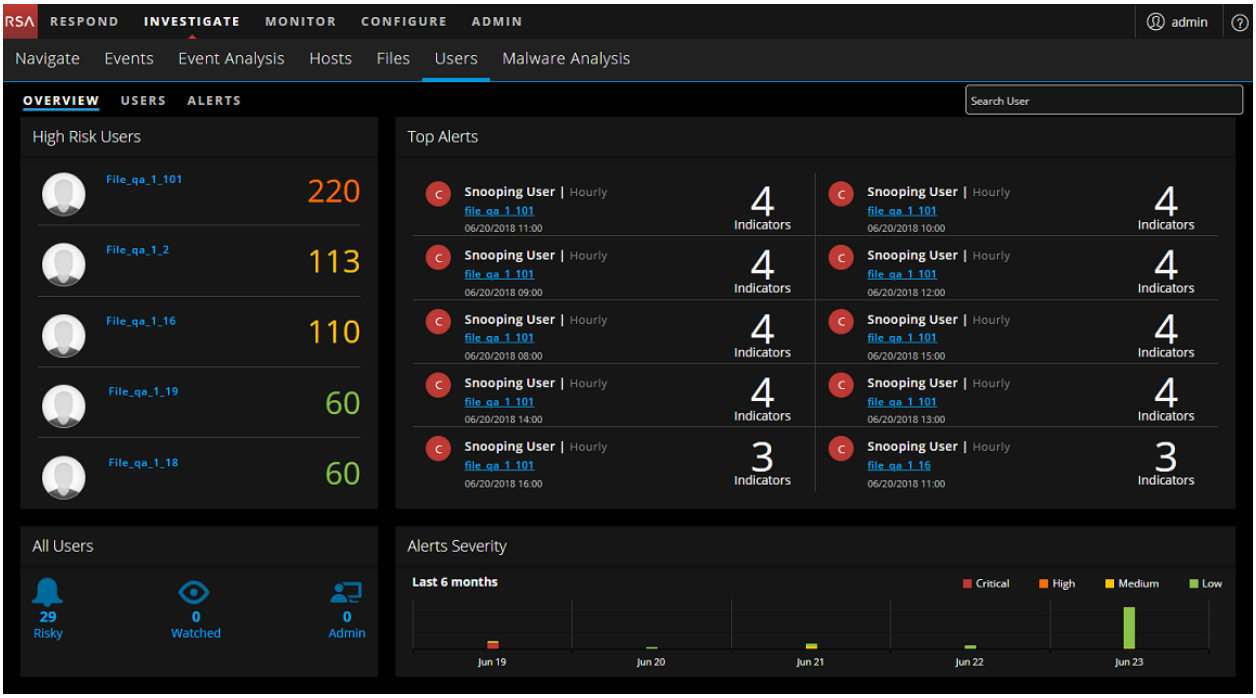
La figure suivante montre la vue Analyse d'événements.



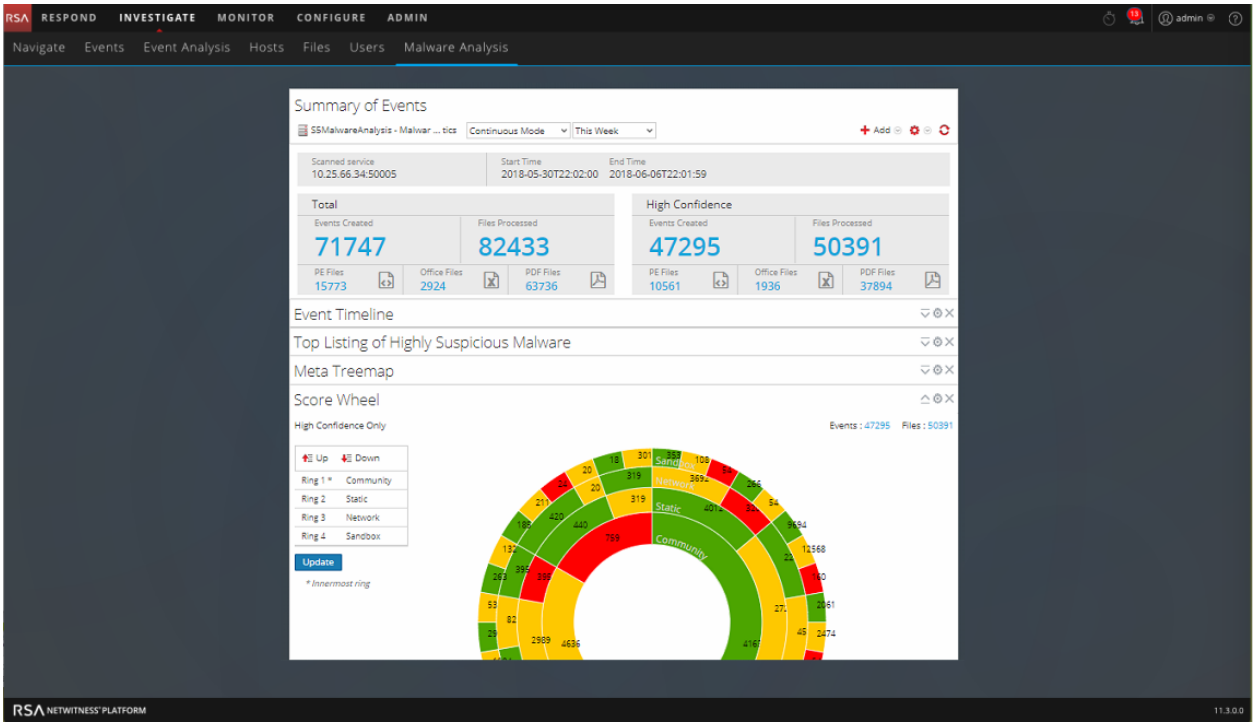
La figure suivante montre la vue Hôtes - vue Détails de l'hôte.



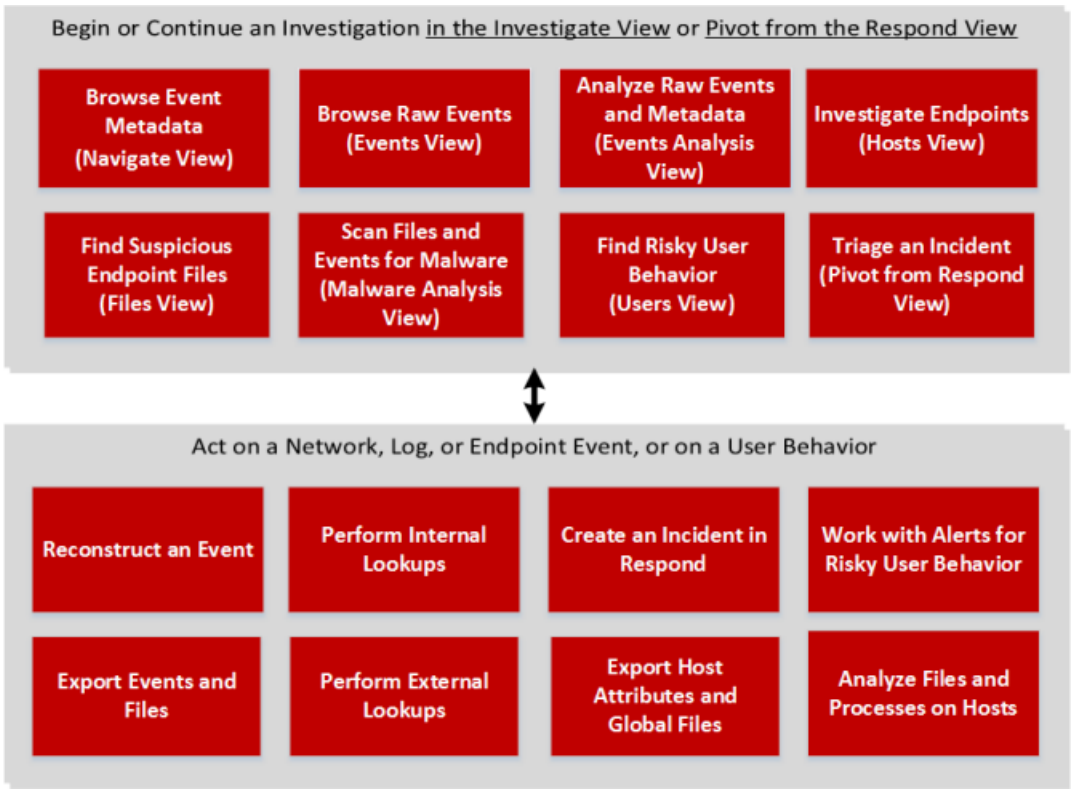
La figure ci-dessous montre la vue Utilisateurs.



La figure suivante montre le récapitulatif des événements de Malware Analysis.



La figure suivante illustre le type d'investigation pour chaque vue du bloc supérieur. Le bloc inférieur affiche les tâches que vous pouvez effectuer dans le cadre d'une procédure d'enquête.

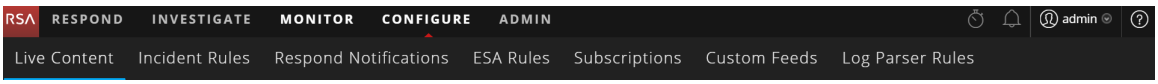


Que puis-je faire ici ?	Chemin	Me montrer comment
Configurer les vues et préférences d'une procédure d'enquête	Vue ENQUÊTER	Voir « Configurer les vues et préférences d'une procédure d'enquête » dans le *Guide d'utilisation de NetWitness Investigate*.
Parcourir les métadonnées d'événement	Vue Naviguer	Voir « Procédure d'enquête relative aux métadonnées dans la vue Naviguer » dans le *Guide d'utilisation de NetWitness Investigate*.
Parcourir les événements bruts	Vue Événements	Voir « Examen des événements bruts dans la vue Événements » dans le *Guide d'utilisation de NetWitness Investigate*.
Analyser les métadonnées et les événements bruts	Vue Analyse d'événements	Voir « Analyser des métadonnées et des événements bruts » dans le *Guide d'utilisation de NetWitness Investigate*.
Examiner les points de terminaison	Vue Hôtes	Consultez le *guide d'utilisation de NetWitness Endpoint*.
Rechercher des fichiers de point de terminaison suspects	Vue Fichiers	Consultez le *guide d'utilisation de NetWitness Endpoint*.
Analyser les fichiers et les événements des programmes malveillants	Vue Analyse de logiciel malveillant	Consultez le *Guide d'utilisation de l'analyse de logiciel malveillant*.
Détecter un comportement utilisateur risqué	Vue Utilisateurs	Consultez le *Guide d'utilisation NetWitness UEBA*.
Effectuer le tri de l'incident	Pivoter à partir de la vue Répondre	Consultez le *Guide d'utilisation de NetWitness Respond*.

CONFIGURER

La vue Configurer permet au Personnel chargé des renseignements sur les menaces (experts de contenu) de configurer des sources de données et de les intégrer à NetWitness Platform à un emplacement approprié.

Menu CONFIGURER



Le menu CONFIGURER comprend les options suivantes :

- **Contenu Live** : (Services Live) La vue Contenu Live vous permet de rechercher et de s'abonner aux ressources Services Live. Services Live est le composant de NetWitness Platform qui gère la communication et la synchronisation entre les services NetWitness Platform et une bibliothèque de

contenu Live disponibles pour les clients RSA NetWitness Platform. Vous pouvez afficher, rechercher, déployer et vous abonner au contenu à partir du RSA Live Content Management System (CMS) pour les services et les logiciels NetWitness Platform. Lorsque vous vous abonnez à une ressource, vous acceptez de recevoir régulièrement des mises à jour de la part de RSA Services Live. Dans la version 10.6, cela correspondait à Live > Rechercher.

- **Règles de l'incident** : La vue Règles de l'incident vous permet de créer des règles d'incidents avec plusieurs critères pour créer automatiquement des incidents. Vous pouvez afficher les incidents prioritaires dans la vue Répondre.
  Dans la version 10.6, cela correspondait à Incidents > Configurer. Dans la version 11.1 ou supérieure, les règles d'agrégation sont appelées Règles de l'incident.
- **Notifications de réponse** La vue Notifications de réponse vous permet d'envoyer automatiquement des notifications par e-mail aux responsables du SOC et aux analystes affectés aux incidents lors de la création ou de la mise à jour des incidents.
- **Règles ESA** : La vue Règles ESA vous permet de gérer les règles Event Stream Analysis qui spécifient des critères de comportement problématique ou d'événements menaçants sur votre réseau. Lorsque le service ESA détecte une menace correspondant aux critères des règles, il génère une alerte.
  Vous pouvez créer vos propres règles ESA ou les télécharger depuis Services Live. La bibliothèque de règles affiche toutes les règles ESA créées ou téléchargées. Pour activer les règles, vous devez les ajouter à un déploiement. Les déploiements mappent les règles de votre bibliothèque de règles aux services ESA appropriés.
  Dans la version 10.6, cela correspondait à Alertes > Configurer.
- **Abonnements** : (Services Live) La vue Abonnements vous permet de gérer le contenu Live auquel vous êtes abonné dans la vue Contenu Live. Pour configurer Services Live sur NetWitness Platform, configurez la connexion et la synchronisation entre le serveur CMS et NetWitness Platform.
  Dans la version 10.6, cela correspondait à Live > Configurer.
- **Feeds personnalisés** : (Services Live) La vue Feeds personnalisés rationalise la tâche de création et de gestion des feeds personnalisés, ainsi que le renseignement des feeds pour les Decoders et Log Decoders sélectionnés. Vous pouvez configurer et gérer des sources d'identité personnalisées. NetWitness Platform utilise des feeds pour créer des métadonnées en fonction des valeurs de métadonnées définies en externe. Un feed est une liste de données qui sont comparées à des sessions au fur et à mesure de leur capture ou de leur traitement. Pour chaque correspondance, des métadonnées supplémentaires sont créées.
  Vous pouvez créer des feeds personnalisés pour fournir l'extraction des métadonnées supplémentaires, par exemple, pour prendre en charge des applications personnalisées de réseau.
  Dans la version 10.6, cela correspondait à Live > Feeds.
- **Règles des analyseurs de logs** : l'onglet Règles des analyseurs de logs affiche des informations sur les analyseurs de logs individuels, ainsi que sur l'analyseur par défaut « Analyser tout » qui permet d'analyser les journaux qui ne sont pas associés à un analyseur de journal particulier. Cet onglet contient les informations suivantes :

- Vous pouvez afficher les règles pour un type de source d'événement particulier, y compris l'analyseur par défaut.
- Vous pouvez afficher les noms, les valeurs littérales et les méta pour chaque analyseur de log configuré.
- Vous pouvez ajouter des analyseurs de logs.
- Vous pouvez ajouter, modifier et supprimer des règles personnalisées pour les analyseurs de logs.

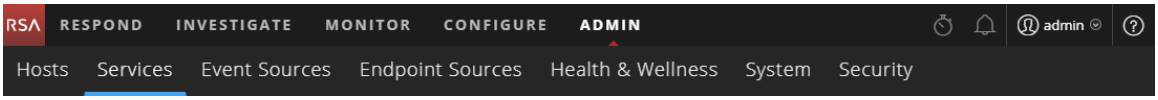
Remarque : L'onglet Règles des analyseurs de logs est disponible dans le menu Configurer, dans les versions 11.2 et ultérieures. Dans les versions antérieures, il se trouve dans Admin > Sources d'événements.

Que puis-je faire ici ?	Chemin	Me montrer comment
Créer un compte Services Live.	Portail d'inscription RSA Live : https://cms.netwitness.com/registration/	Reportez-vous au *Guide de gestion des services Live*.
Trouver et déployer des ressources Services Live	CONFIGURER > Contenu Live	Reportez-vous au *Guide de gestion des services Live*.
Créer automatiquement des incidents.	CONFIGURER > Règles de l'incident	Voir le *Guide de configuration de NetWitness Respond*
Configurer les notifications de réponse.	CONFIGURER > Notifications de réponse	Voir le *Guide de configuration de NetWitness Respond*.
Configurer des alertes.	CONFIGURER > Règles ESA	Voir le *Guide d'utilisation des règles d'alertes de corrélation ESA*.
Configurer les services Services Live dans NetWitness Platform	CONFIGURER > Abonnement	Reportez-vous au *Guide de gestion des services Live*.
Configurer et gérer les feeds d'identité et les feeds personnalisés.	CONFIGURER > Feeds personnalisés	Reportez-vous au *Guide de gestion des services Live*.
Afficher et modifier les analyseurs de logs et les règles d'analyseur de journal.	CONFIGURER > Règles des analyseurs de logs	Consultez le *Guide de personnalisation de l'analyseur de journal*.

ADMIN

Dans la vue Admin, les administrateurs peuvent gérer les hôtes et les services réseau, surveiller l'intégrité de NetWitness Platform, ainsi que gérer la sécurité au niveau du système. Ils peuvent également configurer les ressources du système global et gérer les sources d'événements.

Menu ADMIN



Le menu ADMIN comprend les options suivantes :

- **Hôtes** : La vue Hôtes est l'emplacement où vous installez et gérez les hôtes. L'hôte est la machine sur laquelle les services s'exécutent. Il peut s'agir d'une machine physique ou virtuelle.
- **Services** : La vue Services permet de gérer les services, les rôles et les utilisateurs des services. Elle permet également de mettre à jour les fichiers de configuration des services, d'explorer et de modifier les propriétés des services. Un service exécute une fonction unique, comme un service Decoder, qui capture les données réseau sous forme de paquets.
- **Sources d'événements** : La vue Sources d'événements vous permet de gérer les sources d'événements et de configurer leurs stratégies d'alerte. Les organisations surveillent généralement les sources d'événements dans des groupes en fonction de la criticité des sources d'événements. Vous pouvez créer des règles de surveillance pour chaque groupe de sources d'événements et les classer en fonction de leur priorité.
- **Sources de terminal** : la vue Sources de terminal vous permet de gérer et de mettre à jour les configurations d'agent Endpoint par le biais de groupes et de gérer le comportement des agents à l'aide de règles. Vous pouvez utiliser les règles par défaut ou les personnaliser.
- **Intégrité** : La vue Intégrité vous permet de surveiller l'état de santé des hôtes et des services NetWitness Platform au sein de votre environnement réseau.
- **Système** : La vue Système vous permet de définir des configurations NetWitness Platform globales. Vous pouvez configurer les paramètres de la consignation globale des audits, de la messagerie électronique, de la consignation système, des tâches, de RSA Services Live, de l'intégration d'URL, des services Investigation, Event Stream Analysis (ESA), ESA Analytics et des performances avancées. En outre, vous pouvez gérer les versions NetWitness Platform et configurer le serveur d'attribution de licence local.
- **Sécurité** : La vue Administration - Sécurité permet de gérer les comptes utilisateur et les rôles d'utilisateur, de mapper les groupes externes aux rôles NetWitness Platform et de modifier les autres paramètres du système liés à la sécurité. Ces paramètres s'appliquent au système NetWitness Platform et sont utilisés parallèlement aux paramètres de sécurité des différents services.

Remarque : Pour les versions 11.2 et ultérieures, l'onglet Sources d'événements > Règles des analyseurs de logs se trouve dans la vue Configurer.

Que puis-je faire ici ?	Chemin	Me montrer comment
Gérer les hôtes.	ADMIN > Hôtes	Consultez le *Guide de mise en route des hôtes et des services*.
Gérer les services, notamment gérer l'accès et la sécurité des utilisateurs de services.	ADMIN > Services	Consultez le *Guide de mise en route des hôtes et des services*.
Gérer les sources d'événements et configurer leurs règles d'alerte.	ADMIN > Sources d'événements	Voir *Gestion de la source d'événements*.
Gérer les sources de points de terminaison et configurer leurs règles d'alerte.	ADMIN > Sources de terminal	Voir *Gestion de la source d'événements*.
Configurer et contrôler les alarmes pour les hôtes et services dans votre domaine NetWitness Platform.	ADMIN > Intégrité > Alarme	Consultez le *Guide de maintenance du système*.
Analyser les statistiques relatives aux hôtes et services NetWitness Platform s'exécutant sur les hôtes.	ADMIN > Intégrité > Surveillance	Consultez le *Guide de maintenance du système*.
Cette section vous indique comment créer et appliquer des stratégies dans vos hôtes et services afin de vous aider à gérer l'intégrité de votre domaine NetWitness Platform.	ADMIN > Intégrité > Règles	Consultez le *Guide de maintenance du système*.
Définir des configurations globales pour NetWitness Platform.	ADMIN > Système	Consultez le *Guide de configuration système*.
Configurer la consignation globale des audits.	ADMIN > Système > Audit global	Consultez le *Guide de configuration système*.
Configurer la sécurité du système.	ADMIN > Sécurité	Consultez le *Guide de la sécurité du système et de la gestion des utilisateurs*.
Gérer les utilisateurs à l'aide de rôles et d'autorisations.	ADMIN > Sécurité	Consultez le *Guide de la sécurité du système et de la gestion des utilisateurs*.
Configurer l'authentification PKI (Public Key Infrastructure) PKI est disponible dans NetWitness Platform 11.3 et versions supérieures.	ADMIN > Sécurité	Consultez le *Guide de la sécurité du système et de la gestion des utilisateurs*.

Configuration de votre vue par défaut par le rôle du SOC

Une fois connecté à RSA NetWitness® Platform, vous pouvez faciliter la navigation dans l'application en configurant votre vue par défaut en fonction de votre rôle Opérations de sécurité (SOC). Définissez votre vue par défaut, également connue sous le nom de page de lancement, dans vos préférences utilisateur.

La figure suivante montre les vues NetWitness Platform principales.

- **Répondre** : Cette vue est destinée aux Responsables de la réponse aux incidents, qui peuvent afficher la liste des incidents à des fins de triage et de gestion des alertes. Dans la version 10.6, cette vue correspondait à la vue Gestion des incidents. Désormais, la vue Répondre > Alertes remplace la vue Alertes ESA 10.6 > Vue récapitulative.
  La vue Répondre est la vue d'ouverture par défaut. Si vous n'êtes pas autorisé(e) à consulter la vue Répondre, la vue Surveiller sera votre vue par défaut.
- **Enquêter** : Cette vue est destinée aux Responsables de la recherche des menaces, chargés d'enquêter et de traquer activement les menaces avancées. D'autres analystes, tels que les responsables de la réponse aux incidents, peuvent pivoter dans cette vue pour procéder à une analyse plus approfondie d'un incident.
- **Surveiller** : Cette vue est destinée à tous les utilisateurs ; il s'agit de la vue classique dans les précédentes versions de l'application. Vous pouvez afficher des tableaux de bord et des rapports sur différentes zones d'intérêt en fonction de vos autorisations utilisateur. Vous avez la possibilité de sélectionner un tableau de bord préconfiguré, d'importer un tableau de bord ou de créer votre propre tableau de bord personnalisé.
- **Configurer** : Cette vue est destinée au Personnel chargé des renseignements sur les menaces (experts de contenu), qui configure des sources de données et les intègre à NetWitness Platform. Les experts en contenu utilisent cette zone pour télécharger et gérer le contenu Live. Il peut également créer et gérer des incidents, ainsi que des règles ESA.
  Dans la version 10.6, cette vue correspondait à Live, Incidents > Configurer et Alertes > Configurer.
- **Admin** : Cette vue est destinée aux Administrateurs système, qui configurent et gèrent l'application globale.

Vous pouvez sélectionner une des vues NetWitness Platform principales en tant que vue par défaut. Outre les vues principales, NetWitness Platform a prédéfini des tableaux de bord que vous pouvez sélectionner dans la vue Surveiller en fonction des tâches que vous effectuez :

- Tableau de bord Par défaut
- Tableau de bord Identité
- Tableau de bord Opérations - Logs

- Tableau de bord Opérations - Réseau
- Tableau de bord Présentation
- Tableau de bord Menace - Indicateurs
- Tableau de bord Menace - Intrusion

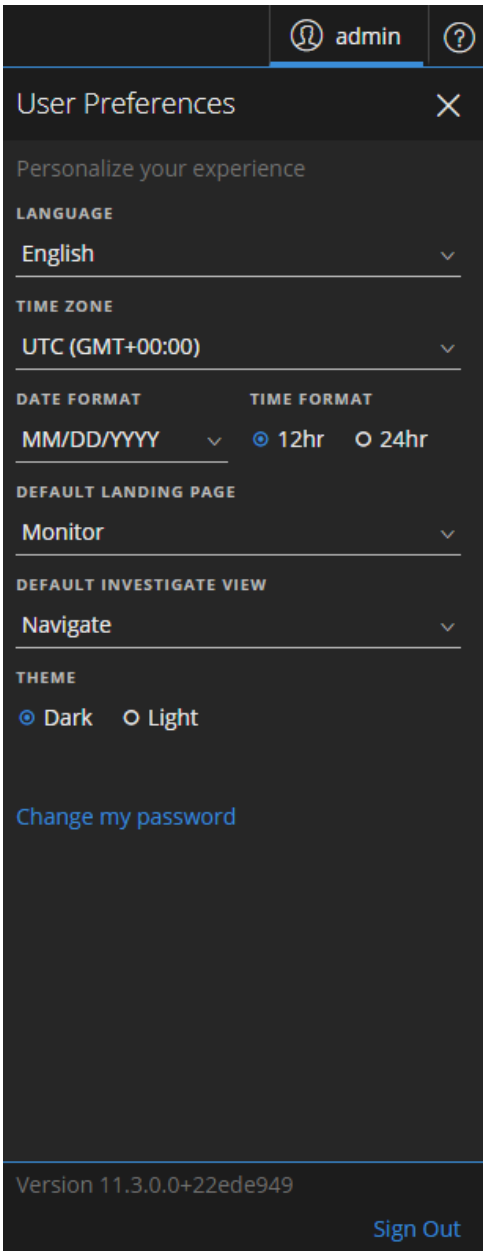
Le tableau suivant présente les rôles SOC classiques et les vues disponibles que vous pouvez sélectionner en tant que page de lancement dans vos préférences utilisateur en fonction de votre rôle SOC. Si vous disposez de plusieurs rôles, sélectionnez la vue qui vous convient le mieux lorsque vous vous connectez à NetWitness Platform.

Rôles SOC	Description du rôle	Considérer comme page de lancement par défaut
Responsable de la réponse aux incidents (Analyste Niveau 1)	Traite les incidents et les alertes mis en file d'attente en vue de les examiner et atténuer	**RÉPONDRE**
Responsable de la recherche des menaces (Analyste Niveau 2/Niveau 3)	Enquête et traque activement les menaces avancées	Pour plus d'informations sur la sélection de la vue Investigate par défaut, consultez le Guide de l'utilisateur NetWitness Investigate.
Responsable du SOC (Gestion et création de rapports SOC)	Gère la préparation du SOC et répond aux incidents et violations de données.	**SURVEILLER** (Le tableau de bord est en mode SURVEILLER.) Lorsque vous êtes connecté(e), sélectionnez le tableau de bord prédéfini approprié à votre rôle SOC. Vous pouvez également importer un tableau de bord ou créer votre propre tableau de bord.
Expert du contenu (Renseignements sur les menaces)	Configure des sources de données et les intègre à NetWitness Platform.	**SURVEILLER** ou **CONFIGURER** (Le tableau de bord est en mode SURVEILLER. Lorsque vous êtes connecté(e), sélectionnez le tableau de bord prédéfini approprié à votre rôle SOC. Vous pouvez également importer un tableau de bord ou créer votre propre tableau de bord. Si vous choisissez SURVEILLER en tant que vue par défaut, vous pouvez accéder à la vue CONFIGURER à partir du menu principal.)
Responsable de la confidentialité des données (DPO)	Similaire à un administrateur, mais un DPO surveille et protège les données sensibles.	**SURVEILLER** (Le tableau de bord est en mode SURVEILLER. Lorsque vous êtes connecté(e), sélectionnez le tableau de bord prédéfini approprié à votre rôle SOC. Vous pouvez également importer un tableau de bord ou créer votre propre tableau de bord.)

Rôles SOC	Description du rôle	Considérer comme page de lancement par défaut
Administrateur système	Se concentre sur la configuration et la stabilité de l'application globale. Gére l'accès utilisateur.	**ADMIN**

Définition de votre vue par défaut

1. (Vue Répondre et certaines vues Enquêter) Dans la barre de menu principal, sélectionnez  .
   La boîte de dialogue Préférences utilisateur affiche vos préférences actuelles.



2. Dans le champ **Page de lancement par défaut**, sélectionnez la vue par défaut que vous aimeriez voir lorsque vous vous connectez à NetWitness Platform. Utilisez le tableau ci-dessus pour effectuer votre sélection en fonction de votre rôle SOC. Par exemple, si vous êtes Responsable de la réponse aux incidents, vous pouvez sélectionner **Répondre** et si vous êtes Responsable de la recherche des menaces, vous pouvez sélectionner **Enquêter**.

   Vos préférences prennent effet immédiatement. Vous pouvez modifier votre page de lancement par défaut à tout moment. Pour plus d'informations sur les autres préférences, reportez-vous à la section Configuration des préférences utilisateur.

3. Pour vérifier que vous pouvez voir la bonne vue par défaut, cliquez sur **Déconnexion** pour vous déconnecter, puis vous reconnecter à NetWitness Platform.

Conseils de dépannage de base pour la configuration des utilisateurs

Le tableau suivant fournit des conseils de dépannage de base qui peuvent être utiles en vue de la configuration des utilisateurs dans NetWitness Platform.

Problème	Conseils de résolution des problèmes
Lorsque je me connecte à NetWitness Platform, je vois la mauvaise vue par défaut.	Vérifiez que la vue par défaut est définie dans le champ Page de lancement par défaut dans vos préférences utilisateur. Si vous choisissez la vue SURVEILLER, vous pouvez sélectionner le tableau de bord prédéfini qui convient le mieux à votre rôle SOC. Vous pouvez également importer ou créer votre propre tableau de bord.
Je vois la bonne vue, mais les métadonnées ne se chargent pas.	Assurez-vous que vous utilisez la dernière version du navigateur. Si cela ne fonctionne pas, essayez d'utiliser un autre navigateur. Par exemple, si vous utilisez Safari, tentez d'utiliser Firefox ou Chrome.
J'utilise Internet Explorer 10 et j'obtiens le message d'erreur suivant : `The page can't be displayed.`	NetWitness Platform prend en charge les versions actuelles de Firefox, Chrome et Safari. Si vous utilisez Internet Explorer, les fonctionnalités ne fonctionnent pas toutes comme prévu. Essayez d'utiliser l'un des navigateurs pris en charge :
Lorsque j'ouvre une session, je ne vois rien.	Consultez votre administrateur. Vous devrez peut-être attribuer un rôle d'utilisateur à votre compte ou effectuer une autre procédure de dépannage.
Je ne vois pas où changer ma page de lancement par défaut.	Accédez aux Préférences utilisateur dans la vue Répondre, ou contactez votre administrateur.

Configuration des préférences utilisateur

Vous pouvez afficher et gérer vos préférences d'application globales RSA NetWitness® Platform à partir de votre profil utilisateur. Il existe deux boîtes de dialogue de préférences utilisateur globales qui, comportent différentes options. Boîte de dialogue Préférences utilisateur accessible depuis les vues Répondre et Enquêter suivantes : Analyse d'événements, Hôtes, Fichiers et Utilisateurs. La boîte de dialogue Préférences est accessible à partir de la plupart des autres vues. La boîte de dialogue que vous voyez dépend de l'endroit où vous accédez aux préférences de l'utilisateur.

Vous pouvez :

- Modifier la langue de l'application
- Définir le fuseau horaire de l'application
- Définir le format de date et d'heure de l'application*
- Sélectionner l'emplacement de démarrage NetWitness Platform par défaut*
- Sélectionner la vue Enquêter par défaut*
- Choisir un thème foncé ou clair pour l'application*
- Modifier votre mot de passe (toutes les vues à l'exception de la vue Répondre) - Voir la section Changement de votre mot de passe pour plus d'informations.
- Activer ou désactiver les notifications*
- Activer ou désactiver les menus contextuels**

* Vous pouvez effectuer cette modification à partir de la boîte de dialogue **Préférences utilisateur** accessible depuis les vues Répondre et certaines vues Enquêter : Analyse d'événements, Hôtes, Fichiers et Utilisateurs.

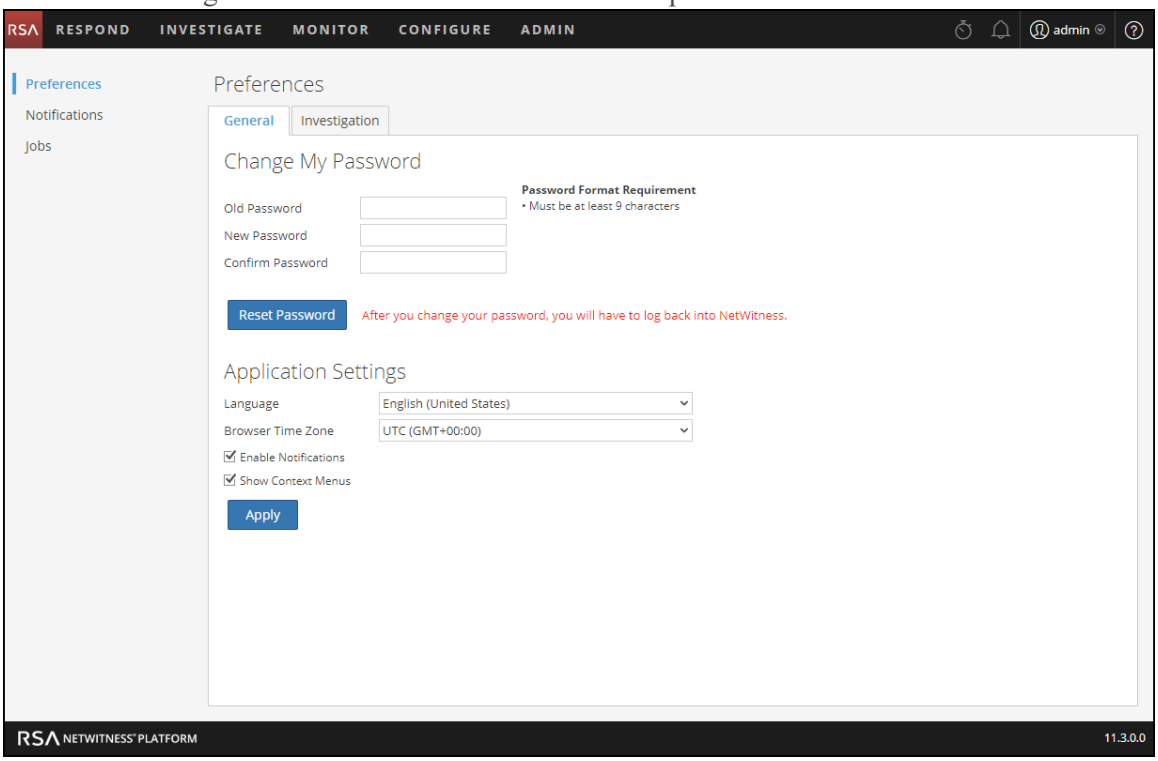
** Vous pouvez effectuer cette modification à partir de la boîte de dialogue **Préférences** accessible à partir de la plupart des vues (à l'exception des vues Répondre et de certaines vues Enquêter : Analyse d'événement, Hôtes, Fichiers et Utilisateurs).

Préférences (la plupart des vues à l'exception des vues Répondre et de certaines vues Enquêter)

Cette section donne des instructions concernant les différentes tâches qui peuvent être exécutées dans la boîte de dialogue Préférences, laquelle est accessible dans la plupart des vues à l'exception de Répondre et de certaines vues Enquête.

Afficher vos préférences

Dans le coin supérieur droit de la fenêtre du navigateur NetWitness Platform, sélectionnez > **Profil**. La boîte de dialogue Préférences utilisateur affiche vos préférences actuelles.



Définir la langue et le fuseau horaire

Remarque : L'option Préférence de langue s'applique à NetWitness Platform, version 11.2 et versions ultérieures.

Vous pouvez modifier la langue de votre choix pour toute la plate-forme NetWitness. La langue par défaut est l'anglais (États-Unis).

1. Dans la boîte de dialogue Préférences utilisateur, sélectionnez vos préférences de localisation :
   a. **Langue** : Sélectionnez votre langue préférée pour NetWitness Platform.
   b. **Fuseau horaire** : Définir le fuseau horaire à utiliser dans NetWitness Platform.
2. Cliquez sur **Apply**.
   Vos préférences prennent effet immédiatement.

Remarque : Lorsque l'heure d'été (DST) commence ou se termine, si le fuseau horaire sélectionné pour l'utilisateur actuellement connecté indique DST, l'interface utilisateur se met à jour automatiquement pour refléter l'heure correcte.

Activer ou désactiver les notifications système de votre compte utilisateur

Par défaut, les notifications du système NetWitness Platform sont activées lors de la création d'un nouveau compte. Vous pouvez désactiver et activer ces notifications à tout moment.

1. Dans la boîte de dialogue Préférences :
   - Pour activer les notifications de votre compte utilisateur, cochez la case **Activer les notifications**.
   - Pour désactiver les notifications, décochez la case **Activer les notifications**.
2. Cliquez sur **Appliquer**.
   Votre préférence prend effet immédiatement.

Activer ou désactiver les menus contextuels de votre compte utilisateur

Par défaut, les menus contextuels sont activés lors de la création d'un nouveau compte utilisateur. Les menus contextuels fournissent des fonctions supplémentaires pour des vues spécifiques lorsque vous cliquez avec le bouton droit de la souris dans une vue.

1. Dans la boîte de dialogue Préférences :
   - Pour activer les menus contextuels de votre compte utilisateur, cochez la case **Activer les menus contextuels**.
   - Pour désactiver les menus contextuels, décochez la case **Activer les menus contextuels**.
2. Cliquez sur **Appliquer**.
   Votre préférence prend effet immédiatement.

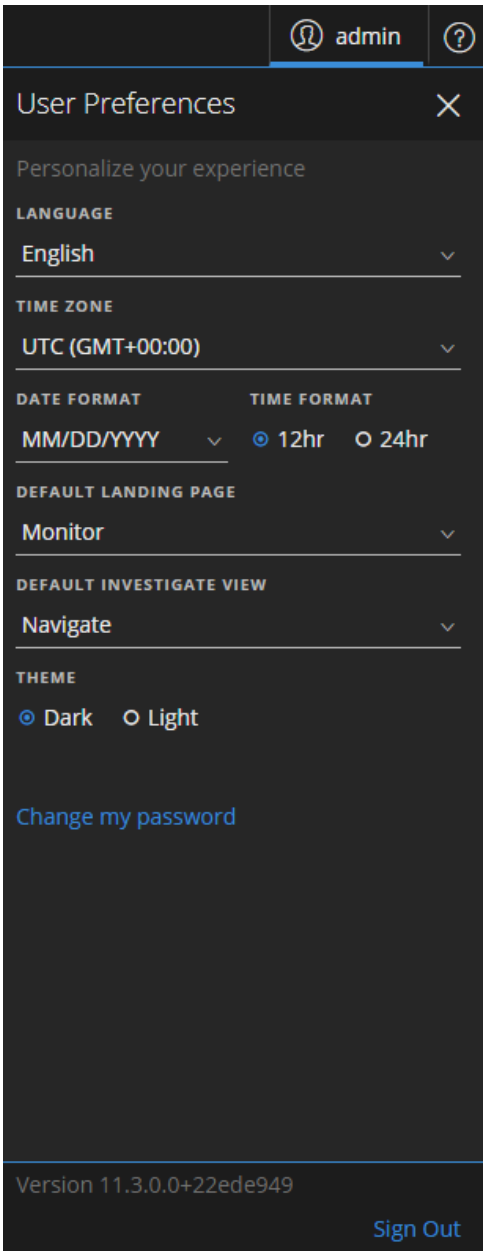
Remarque : Les paramètres disponibles dans l'onglet Enquêter de la boîte de dialogue Préférences sont documentés dans le *Guide d'utilisation de NetWitness Investigate*.

Préférences utilisateur (vue Répondre et certaines vues Enquêter)

Cette section donne des instructions concernant les différentes tâches qui peuvent être exécutées dans la boîte de dialogue Préférences utilisateur, laquelle est accessible dans les vues Répondre et certaines vues Investigate.

Afficher vos préférences utilisateur

Dans le coin supérieur droit de la fenêtre du navigateur NetWitness Platform, sélectionnez  .
La boîte de dialogue Préférences utilisateur affiche vos préférences actuelles lors de l'accès via la vue Répondre et les vues Enquêter suivantes : Analyse d'événements, Hôtes, Fichiers et Utilisateurs.



Toutes les sélections que vous effectuez prennent effet immédiatement.

Définissez la langue, le fuseau horaire, ainsi que le format de la date et de l'heure

Remarque : L'option Préférence de langue s'applique à NetWitness Platform, version 11.2 et versions ultérieures.

Vous pouvez modifier la langue de votre choix pour toute la plate-forme NetWitness. La langue par défaut est l'anglais (États-Unis). Vous pouvez modifier le fuseau horaire, ainsi que le format de la date et de l'heure de votre emplacement.

1. Ouvre la boîte de dialogue Préférences utilisateur.
2. Dans la boîte de dialogue Préférences utilisateur, sélectionnez vos préférences de localisation :
   a. **Langue** : Sélectionnez votre langue préférée pour NetWitness Platform.
   b. **Fuseau horaire** : Définir le fuseau horaire à utiliser dans NetWitness Platform.
   c. **Format de date :**: Définit le format de l'ordre de l'affichage mois (MM), jour (JJ) et année (AAAA). Par exemple, le format MM/JJ/AAAA affiche la date sous la forme de 05/11/2017.
   d. **Format de l'heure** : Définit l'heure au format 12 ou 24 heures. Par exemple, 2 h 00 au format 12 heures est 14 h 00 au format 24 heures.

   Les modifications effectuées dans les vues Répondre et Procédure d'enquête prennent effet immédiatement.

Remarque : Lorsque l'heure d'été (DST) commence ou se termine, si le fuseau horaire sélectionné pour l'utilisateur actuellement connecté indique DST, l'interface utilisateur se met à jour automatiquement pour refléter l'heure correcte.

Sélectionner l'emplacement de démarrage de NetWitness Platform par défaut

1. Ouvre la boîte de dialogue Préférences utilisateur.
2. Dans le champ **Page de lancement par défaut**, sélectionnez la vue d'ouverture que vous aimeriez voir lorsque vous vous connectez à NetWitness Platform. Vous pouvez choisir Répondre, Enquêter, Surveiller, Configurer et Admin en fonction de votre rôle d'utilisateur. Par exemple, vous pouvez choisir Répondre pour accéder directement à la section pertinente de l'application destinée aux responsables de la réponse aux incidents. Reportez-vous à la section Configuration de votre vue par défaut par le rôle du SOC pour vous aider à sélectionner la vue par défaut appropriée.
   Cette sélection définit la vue par défaut pour l'ensemble de l'application. Les modifications prennent effet immédiatement.

Sélectionner la vue Enquêter par défaut

1. Ouvre la boîte de dialogue Préférences utilisateur.
2. Dans le champ **Vue Enquêter par défaut**, sélectionnez la page de lancement par défaut lorsque vous vous connectez à NetWitness Platform, puis accédez à la vue Enquêter. Vous pouvez choisir les vues Naviguer, Événements, Analyse d'événements, Hôtes, Fichiers, Utilisateurs ou Analyse de malware en tant que vue Enquêter par défaut. Par exemple, vous pouvez choisir la vue Événements en tant que vue Enquêter par défaut pour accéder directement à la page Événements afin d'afficher les événements générés pour un service. Voir Configuration de votre vue par défaut par le rôle du SOC pour vous aider à sélectionner la vue par défaut appropriée. Pour plus d'informations, consultez le *Guide d'utilisation de NetWitness Investigate*.

Remarque : Une fois que vous avez appliqué la modification dans le menu déroulant, il faut parfois quelques secondes pour que les modifications soient effectives.

Choisir l'apparence de NetWitness Platform

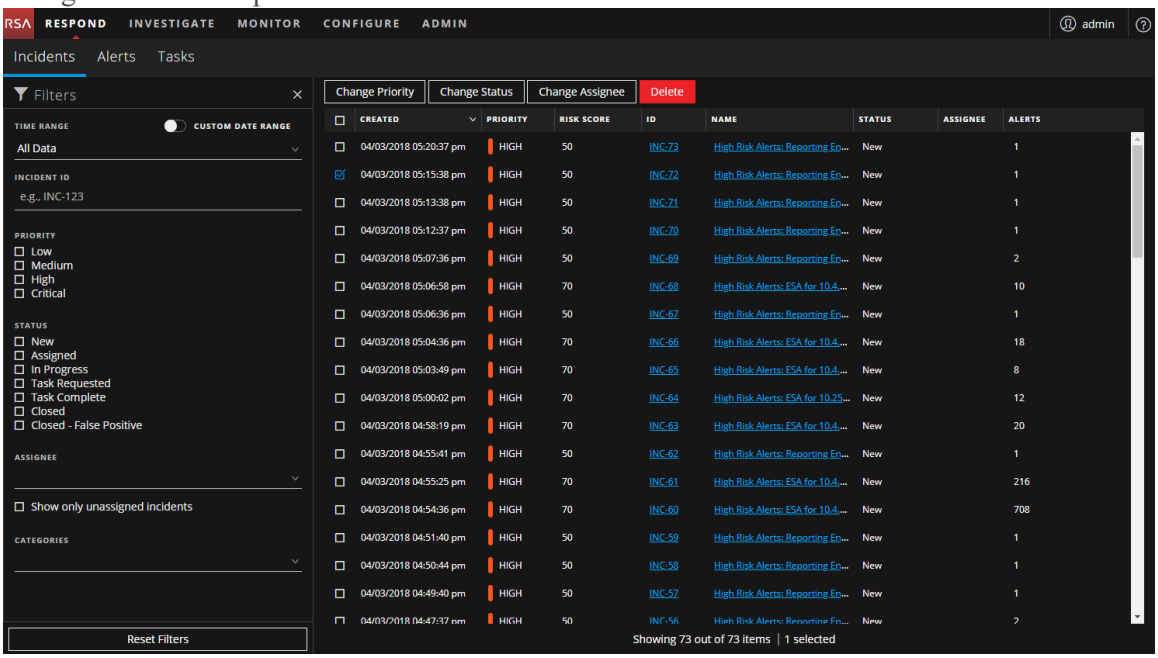
Remarque : Cette option est disponible dans NetWitness Platform versions 11.1 ou supérieures.

Vous pouvez choisir un thème foncé ou un thème clair pour votre application, en fonction de vos préférences personnelles. Lorsque vous modifiez le thème, la vue Répondre et certaines vues Enquêter adoptent le thème clair ou foncé. Votre sélection modifie uniquement la façon dont NetWitness Platform s'affiche pour vous, pas pour les autres utilisateurs.

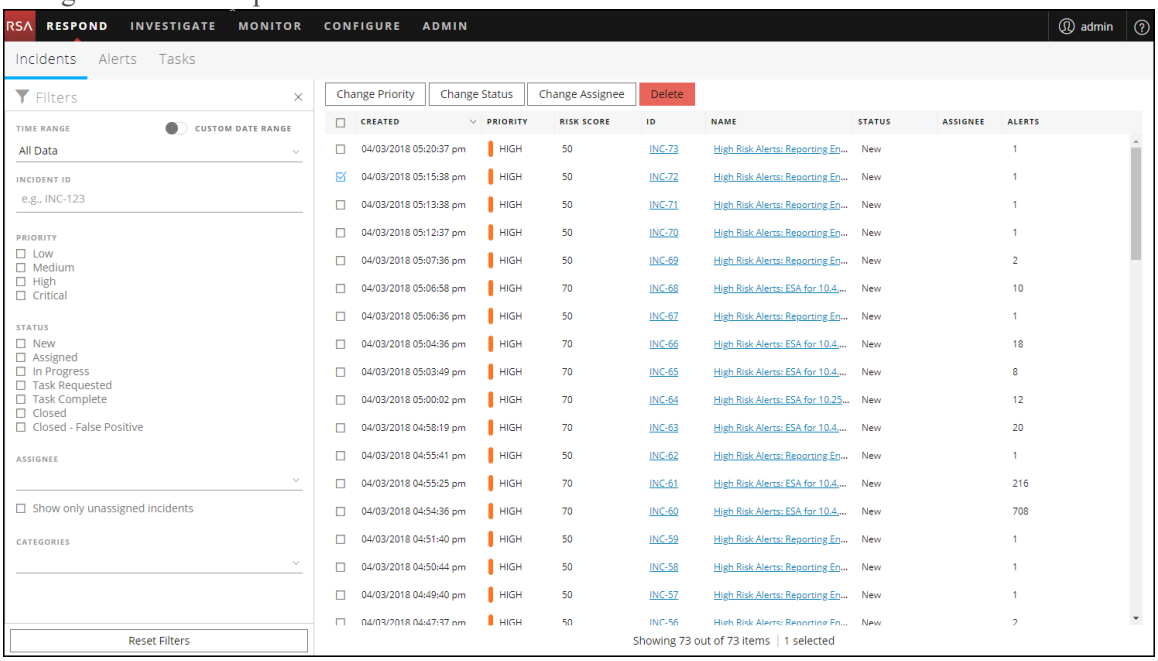
1. Ouvre la boîte de dialogue Préférences utilisateur.
2. Sous **THEME**, sélectionnez l'une des options suivantes :
   - **Foncé** : Le thème foncé est idéal pour les environnements plus foncés ou lorsque vous n'avez pas besoin d'autant de contraste.
   - **Clair** : Le thème clair est préférable pour les environnements plus clairs, lorsque vous avez besoin de plus de contraste, ou lorsque vous procédez à une projection de l'application pour que d'autres personnes la voient. Dans la mesure où certaines vues ne sont pas concernées par les modifications de thème, vous pouvez choisir le thème clair pour une expérience de visualisation plus cohérente.

Les modifications prennent effet immédiatement.

La figure ci-dessous présente le thème foncé.



La figure ci-dessous présente le thème clair.



Gestion des tableaux de bord

Un tableau de bord est un groupe de dashlets qui vous permet de visualiser dans un même espace les principaux snapshots des différents composants que vous considérez importants. Dans RSA NetWitness® Platform, vous pouvez composer des tableaux de bord pour obtenir les informations et les mesures de haut niveau qui dépeignent l'image globale d'un déploiement de NetWitness Platform. Vous pouvez aussi afficher uniquement les informations qui sont les plus pertinentes pour les opérations quotidiennes.

Par défaut, le tableau de bord NetWitness Platform par défaut s'affiche lorsque vous vous connectez à NetWitness Platform. Il contient quelques dashlets très utiles pour vous initier à réaliser vos propres personnalisations. Les tableaux de bord de tous les composants NetWitness Platform peuvent être ajoutés au tableau de bord NetWitness Platform par défaut ou à un tableau de bord NetWitness Platform personnalisé.

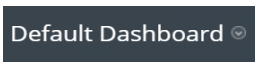
Vous pouvez afficher des tableaux de bord et des rapports sur différentes zones d'intérêt en fonction de vos autorisations utilisateur. Vous avez la possibilité de sélectionner un tableau de bord préconfiguré, d'importer un tableau de bord ou de créer votre propre tableau de bord personnalisé. Les tableaux de bord vous aident à visualiser rapidement et facilement les rapports. Vous pouvez configurer vos tableaux de bord pour afficher les informations qui prennent en charge votre workflow. Cette rubrique décrit les tâches de haut niveau qui peuvent être effectuées lorsque vous configurez un tableau de bord.

Notions de base relatives aux tableaux de bord

Si la vue Surveiller est votre page de lancement par défaut après la connexion à NetWitness Platform, vous verrez toujours le tableau de bord par défaut ou le tableau de bord actuellement configuré immédiatement après avoir terminé le processus de connexion. Pour revenir au tableau de bord à partir d'un autre composant NetWitness Platform, accédez à **SURVEILLER** > **Présentation**.

Titre du tableau de bord

Le titre du tableau de bord fait référence au tableau de bord actuellement actif, par exemple, le tableau de bord par défaut.



Liste de sélection des tableaux de bord

Vous pouvez accéder à des tableaux préconfigurés et personnalisés dans la liste de sélection des tableaux de bord. Lorsque vous sélectionnez un tableau de bord, son titre s'affiche sous la barre d'outils NetWitness Platform.

Un tableau de bord contient :

- Une barre d'outils
- Le titre et la liste de sélection des tableaux de bord

Barre d'outils du tableau de bord

La barre d'outils du tableau de bord est disponible en regard du titre du tableau de bord sélectionné. Elle permet d'effectuer une variété d'opérations sur les tableaux de bord et les dashlets.

Remarque : Les options Copier, Supprimer, Importer, Exporter, Partager et Ajouter une ligne sont désactivées pour les tableaux de bord préconfigurés.

Option	Description
★	Définit le tableau de bord sélectionné en tant que favori.
Default Dashboard	Affiche la liste des tableaux de bord disponibles à partir de laquelle vous pouvez effectuer une sélection.

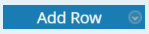
Option	Description
	Affiche la boîte de dialogue Créer un tableau de bord, qui vous permet de définir ou d'ajouter un tableau de bord personnalisé.
	Supprime un tableau de bord personnalisé. Le tableau de bord par défaut ne peut pas être supprimé.
	Vous permet de copier un tableau de bord.
	Affiche la boîte de dialogue Gérer un dashlet.
	Exporte un tableau de bord au format de fichier .zip.
	Importe un tableau de bord au format de fichier .zip ou .cfg.
	Vous permet de partager un tableau de bord avec un autre utilisateur.
	Permet à l'utilisateur d'ajouter des lignes et des colonnes au tableau de bord en fonction de ses besoins. Cliquez sur l'icône  au sein d'une ligne pour ajouter un dashlet.

Tableau de bord par défaut

Le tableau de bord par défaut est configuré pour afficher des dashlets spécifiques dans des positions spécifiques. Le tableau de bord par défaut fait office de modèle de composition de tableau de bord et de point de départ pour une personnalisation.

- Vous pouvez personnaliser les informations du tableau de bord par défaut en modifiant, ajoutant, déplaçant, agrandissant et supprimant les dashlets.
- Après avoir modifié le tableau de bord par défaut, il est toujours possible de rétablir sa mise en page d'origine ().
- Le tableau de bord par défaut ne peut pas être supprimé ni partagé.

Sélection d'un tableau de bord préconfiguré

Lors de l'installation de la Suite NetWitness Platform, les tableaux de bord préconfigurés suivants sont automatiquement activés et deviennent disponibles :

- Par défaut
- Identité
- Investigation

- Opérations - Analyse de fichiers
- Opérations - Logs
- Opérations - Réseau
- Opérations - Analyse de protocole
- Présentation
- RSA SecurID
- Menaces - Traque active
- Menaces - Intrusion
- Menaces - Indicateurs de programme malveillant

Vous ne pouvez pas effectuer les actions suivantes sur un tableau de bord préconfiguré :

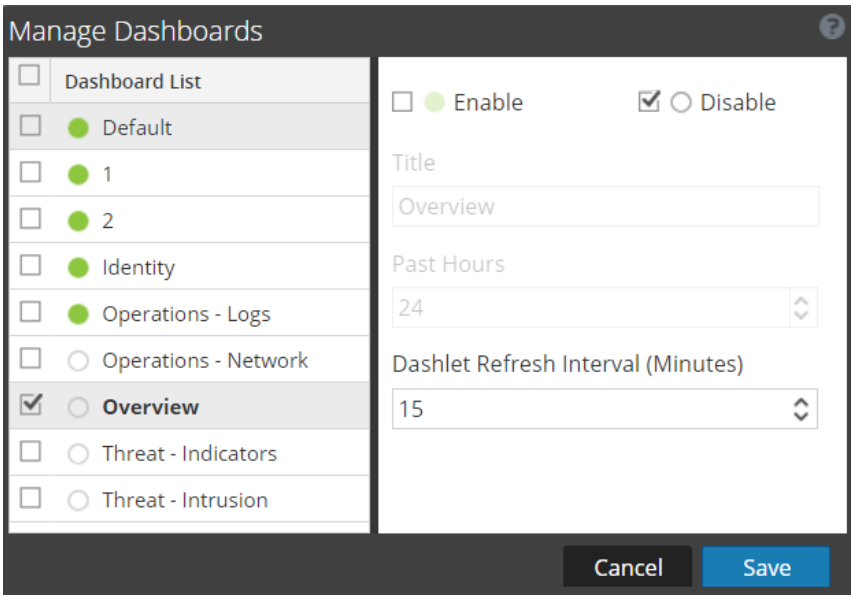
- Modifier un tableau de bord
- Exporter un tableau de bord
- Partager un tableau de bord
- Supprimer un tableau de bord

Pour plus d'informations sur chaque tableau de bord préconfiguré, reportez-vous au Catalogue des tableaux de bord dans l'espace Contenu RSA sur RSA Link.

Activation ou désactivation des tableaux de bord

Lorsque vous activez ou désactivez un tableau de bord, tous les dashlets du tableau de bord sont activés ou désactivés, ainsi que les graphiques associés, sauf s'ils sont utilisés dans un autre tableau de bord.

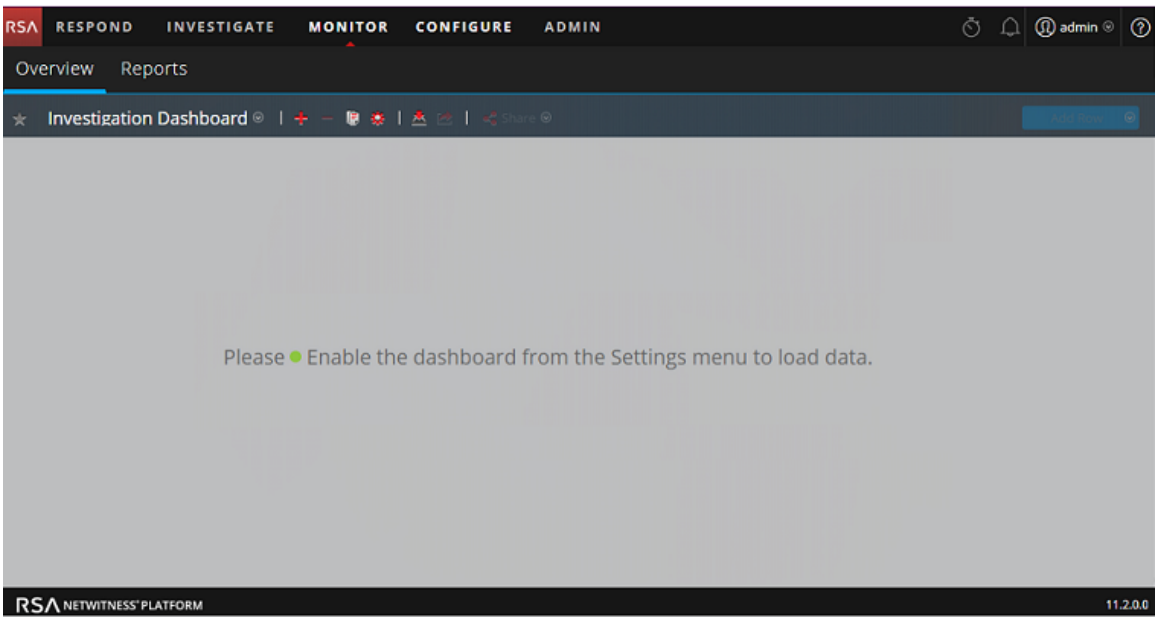
Les modules NetWitness Platform ne peuvent afficher que les dashlets présentés dans la boîte de dialogue Gérer un dashlet. Le tableau de bord principal propose tous les dashlets NetWitness Platform. Exemple des dashlets actuellement disponibles.



Nom	Description
Liste des tableaux de bord	Affiche la liste des tableaux de bord par défaut, préconfigurés et personnalisés.
Enable	S'affiche si le dashlet sélectionné est activé.
Disable	S'affiche si le dashlet sélectionné est désactivé.
Titre	Affiche le titre du dashlet sélectionné et permet également de renommer le tableau de bord.
Heures passées	Affiche la durée de collecte des données.
Intervalles d'actualisation du dashlet (en minutes)	Affiche l'intervalle d'actualisation d'un dashlet.

Activation d'un tableau de bord

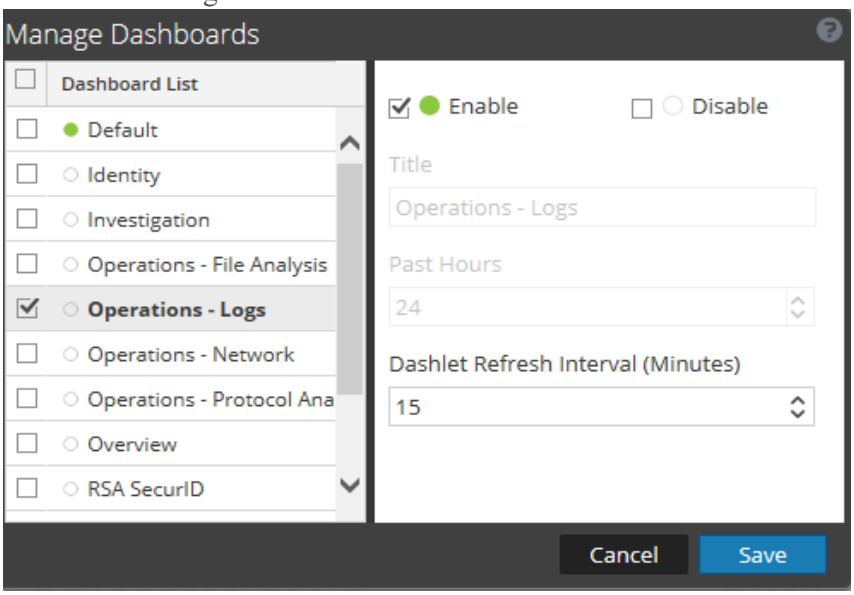
Si vous sélectionnez un tableau de bord qui n'est pas activé, un écran masqué s'affiche.



Pour activer un ou plusieurs tableaux de bord :

1. Accédez au tableau de bord à activer.

2. Dans la barre d'état du tableau de bord, cliquez sur  (Gérer les tableaux de bord).
   La boîte de dialogue Gérer les tableaux de bord s'affiche.



3. Dans la liste Tableaux de bord, sélectionnez les tableaux de bord à activer.

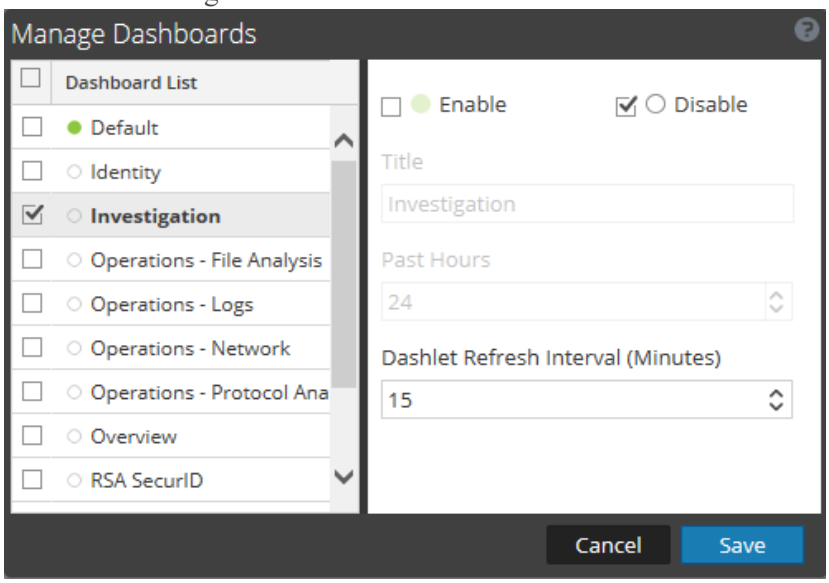
4. Cochez la case **Activer**.

5. C**liquez sur** Enregistrer
   .

Désactivation d'un tableau de bord

Pour désactiver un ou plusieurs tableaux de bord :

1. Accédez au tableau de bord à désactiver.
2. Dans la barre d'outils du tableau de bord, cliquez sur (Gérer les tableaux de bord).
   La boîte de dialogue Gérer les tableaux de bord s'affiche.



3. Dans la liste Tableaux de bord, sélectionnez les tableaux de bord à désactiver.
4. Sélectionnez la case **Désactivé**.
5. Cliquez sur **Enregistrer**.

Définition d'un tableau de bord en tant que favori

Pour personnaliser les vues de NetWitness Platform, vous pouvez définir un tableau de bord préconfiguré ou personnalisé en tant que favori. Le tableau de bord NetWitness Platform propose tous les dashlets NetWitness Platform. La boîte de dialogue Favoris définit un tableau de bord spécifique comme votre tableau de bord favori et sera répertorié comme favori chaque fois que vous vous connecterez à NetWitness Platform.

1. Accédez à un tableau de bord.
2. Dans la barre d'outils du tableau de bord, cliquez sur

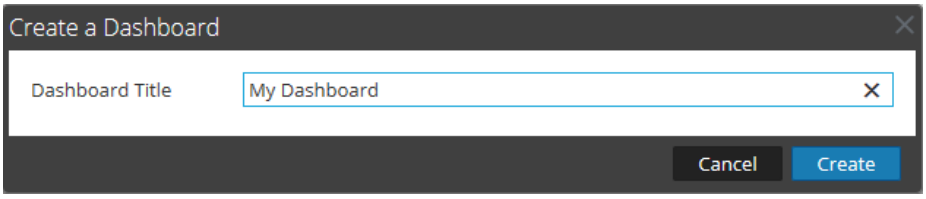
   Si l'icône Favoris est rouge, cela signifie que le tableau de bord sélectionné est défini en tant que favori et apparaît en haut de la ligne.

Création de tableaux de bord personnalisés

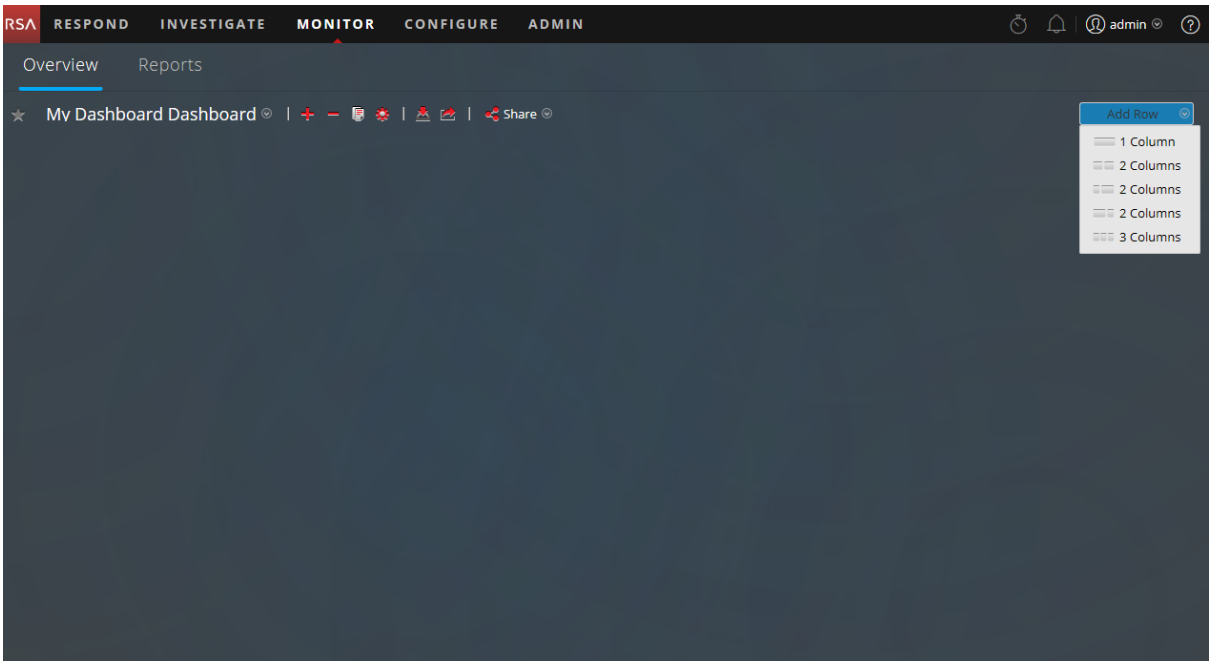
Vous pouvez créer des tableaux de bord personnalisés à des fins particulières, par exemple, pour représenter une zone géographique ou fonctionnelle spécifique du réseau. Chaque tableau de bord personnalisé est ajouté à la liste Sélection de tableaux de bord.

Pour créer un tableau de bord personnalisé :

1. Dans la barre d'outils du tableau de bord, cliquez sur  .
   La boîte de dialogue Créer un tableau de bord s'affiche.



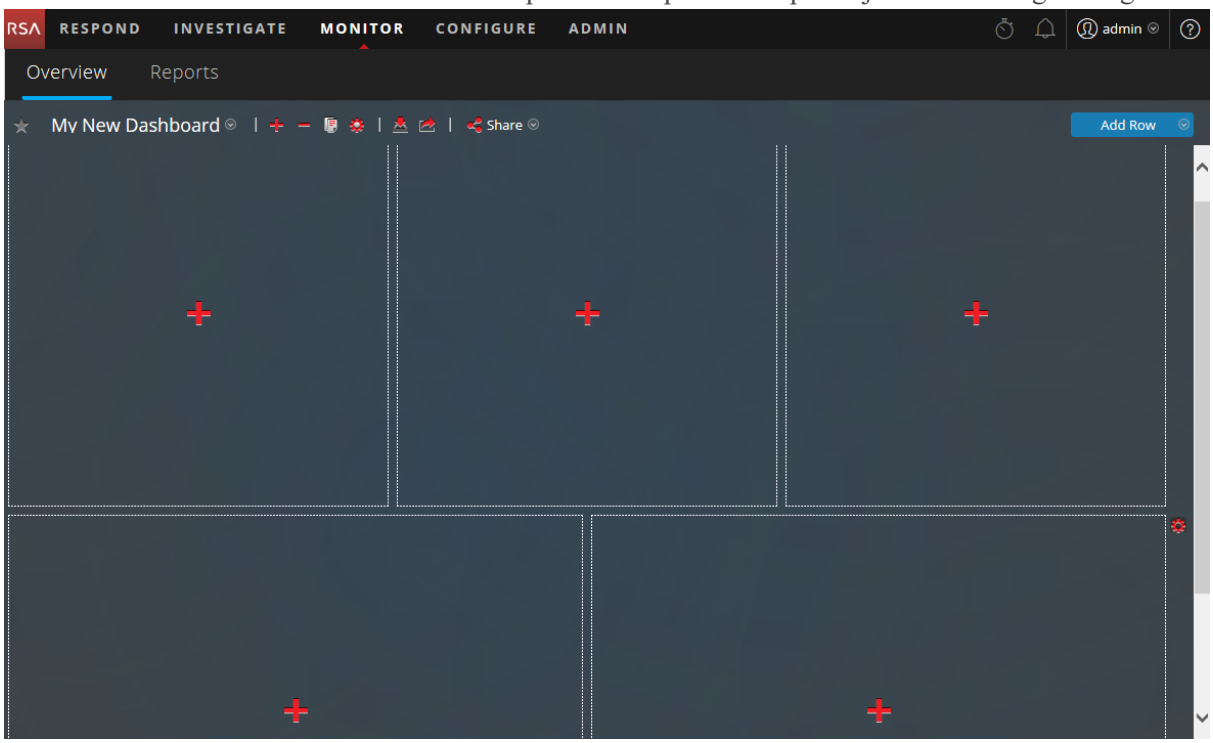
2. Saisissez un titre pour le nouveau tableau de bord, puis cliquez sur **Créer**.
   Le nouveau tableau de bord s'affiche sous la forme d'un écran vide.



3. Ajoutez des lignes au tableau de bord, qui peut contenir une ou plusieurs colonnes, à l'aide de l'option **Ajouter une ligne** (

) situé sur le côté droit de l'écran. Cliquez sur la configuration de colonne souhaitée dans la liste déroulante pour ajouter une ligne au tableau de bord

avec le nombre de colonnes sélectionné. Répétez cette procédure pour ajouter davantage de lignes.



4. Vous pouvez ajouter les dashlets souhaités au tableau de bord en cliquant sur  dans l'espace réservé vide d'une ligne. Pour en savoir plus sur l'ajout et la gestion des dashlets, reportez-vous à la section Utilisation des dashlets.

Une fois que vous avez créé des tableaux de bord personnalisés, vous pouvez effectuer les opérations suivantes :

- Basculer entre les tableaux de bord en sélectionnant une option dans la liste Sélection de tableaux de bord
- Supprimer un tableau de bord personnalisé
- Importer ou exporter un tableau de bord

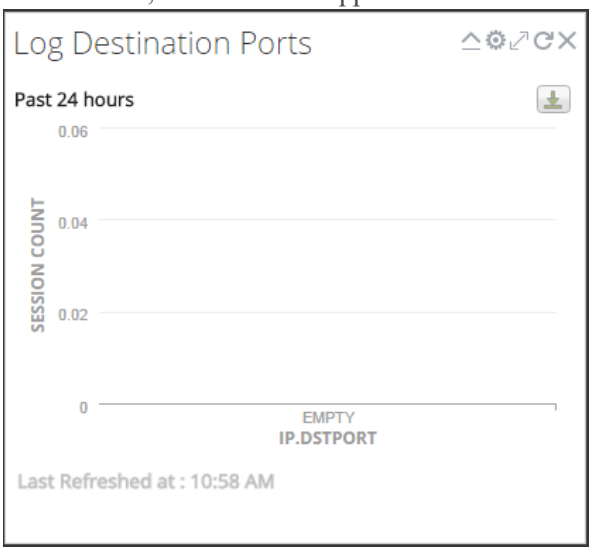
Chaque tableau de bord contient :

- Une barre d'outils
- Le titre et la liste de sélection des tableaux de bord
- Aucun ou plusieurs dashlets

Utilisation des dashlets

NetWitness Platform utilise les dashlets pour afficher les sous-ensembles ciblés des informations système, des services, des tâches, des ressources, des inscriptions, des règles et bien d'autres informations.

Les contrôles d'un dashlet sont disponibles dans la barre de titre. Tous les dashlets utilisent un ensemble de contrôles, et seuls ceux applicables au dashlet spécifié apparaissent dans la barre de titre du dashlet.



Le tableau suivant affiche la description de chaque icône sur le dashlet.

Icône	Nom	Description
	Réduire à la verticale	Réduit le dashlet à la verticale pour ne faire apparaître que le titre.
	Développer à la verticale	Développe le dashlet à sa taille d'origine.
	Recharger	Recharge le dashlet.
	Paramètres	Affiche les paramètres configurables du dashlet.
	Agrandir	Affiche un graphique ou un dashlet en mode plein écran dans les dashlets dont le contenu ne tient pas à l'horizontale dans la largeur du dashlet.
	Supprimer	Supprime le dashlet du tableau de bord.
Dernière actualisation à		Affiche l'heure à laquelle les données sont interrogées dans le graphique associé.
Afficher plus		Lorsque vous cliquez dessus, accède au tableau de bord correspondant qui est lié au dashlet principal et affiche plus de détails. Si vous n'avez pas lié le tableau de bord à un dashlet existant, ce lien ne sera pas disponible sur le dashlet. Pour configurer cette option, cliquez sur et, dans le champ Lien du tableau de bord, sélectionnez un tableau de bord associé pour afficher plus de détails sur un dashlet spécifique.

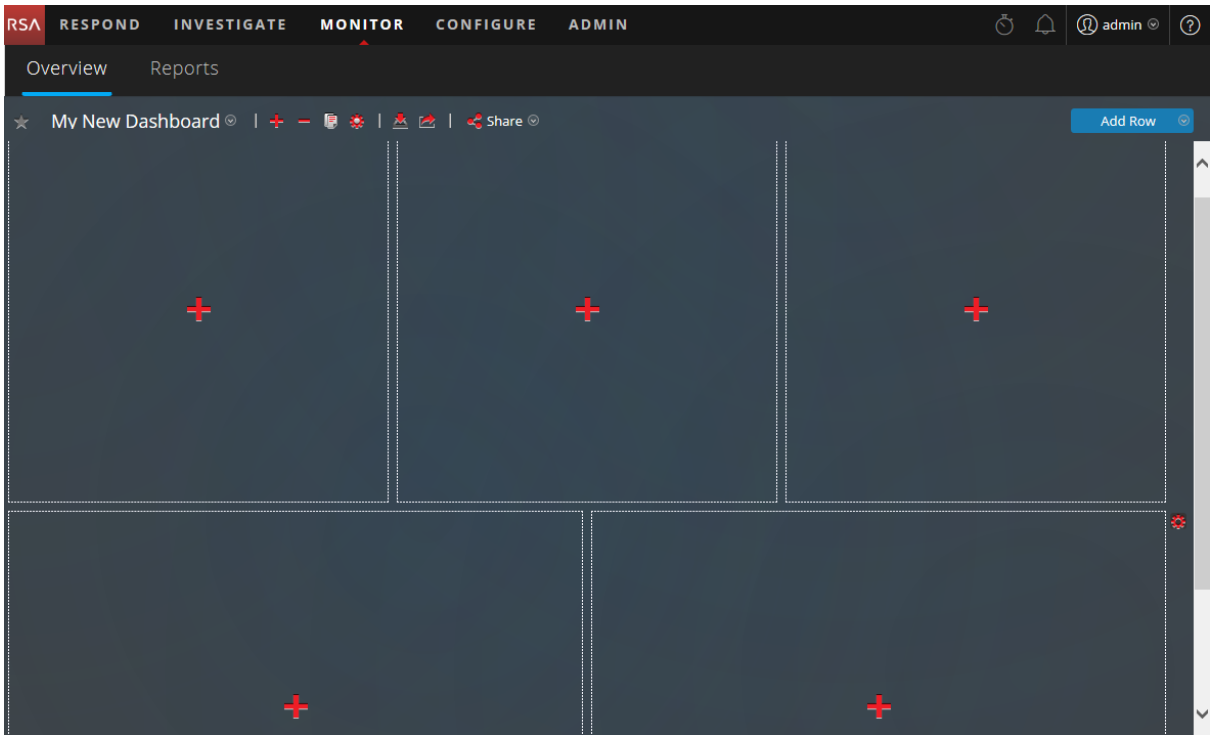
Vous pouvez ajouter des dashlets au tableau de bord par défaut ou créer un tableau de bord personnalisé avec votre propre ensemble utile de dashlets pour améliorer l'efficacité de votre workflow.

Ajouter un dashlet

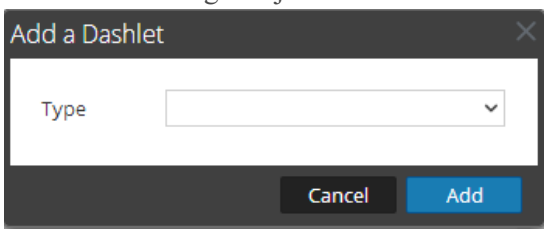
Pour personnaliser les vues dans NetWitness Platform, vous pouvez ajouter des dashlets à un tableau de bord par défaut ou créer des tableaux de bord personnalisés. Toutefois, vous ne pouvez pas ajouter de dashlets aux tableaux de bord préconfigurés.

Pour ajouter un dashlet :

1. Accédez à un tableau de bord ou créez un tableau de bord.

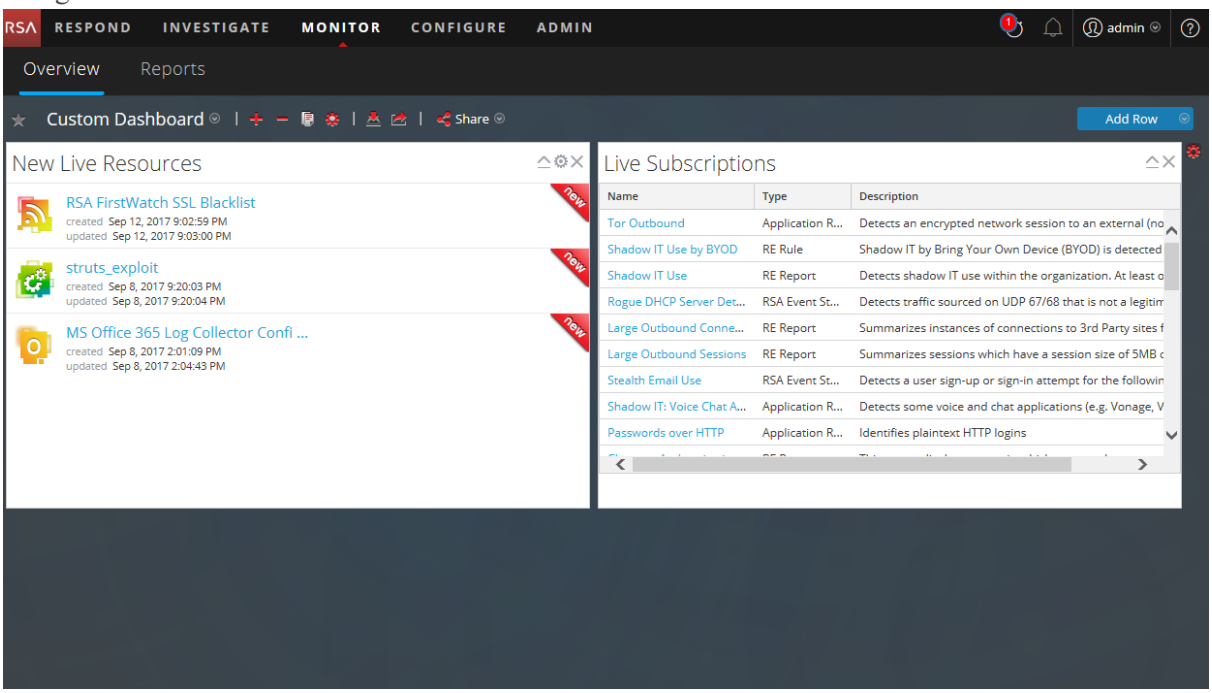


2. Cliquez sur + dans l'espace réservé dans lequel vous souhaitez ajouter le dashlet.
La boîte de dialogue Ajouter un dashlet s'affiche.



3. Cliquez sur la liste de sélection **Types** pour afficher les dashlets disponibles, puis sélectionnez le type de dashlet que vous souhaitez ajouter. Selon le type de dashlet que vous ajoutez, certains champs configurables s'afficheront dans la boîte de dialogue **Ajouter un dashlet**.
4. Saisissez le titre du dashlet. Le titre peut contenir des lettres, des chiffres, des caractères spéciaux et des espaces.
5. Si d'autres champs configurables sont disponibles pour ce dashlet, définissez les valeurs appropriées.
6. Lorsque tous les champs obligatoires sont configurés, cliquez sur **Ajouter**.
Le dashlet est ajouté au tableau de bord dans l'espace réservé sélectionné et est automatiquement

enregistré.



Modifier les propriétés du dashlet

Tous les dashlets préconfigurés sont en lecture seule et leurs propriétés ne peuvent pas être modifiées. D'autres dashlets sont modifiables pour permettre aux utilisateurs de personnaliser l'apparence des données qu'ils affichent. Un dashlet possédant des propriétés modifiables dispose d'une option Paramètres (⚙) permettant d'afficher toutes les options configurables.

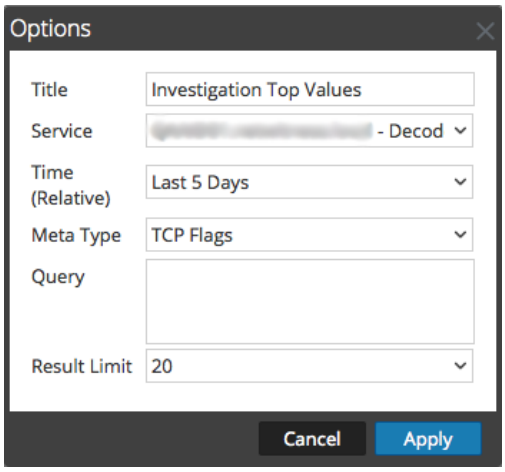
Après avoir ajouté les dashlets, vous pouvez les faire glisser-déplacer ou les permuter entre eux.

Les dashlets ne possédant pas de propriétés configurables, comme le dashlet Abonnements Live, n'affichent pas l'option Paramètres dans leur barre de titre. Beaucoup de dashlets ont un titre modifiable dans lequel vous pouvez modifier les propriétés suivantes :

- Titre d'affichage du dashlet.
- Types de services à surveiller. Par exemple, vous pouvez uniquement surveiller les Decoders, ou bien les Decoders et les Concentrators.

Les autres dashlets ont des paramètres que vous définissez pour spécifier le type et la quantité des informations à afficher dans le dashlet. Par exemple, un dashlet Graphique en temps réel dispose de l'option Paramètres.

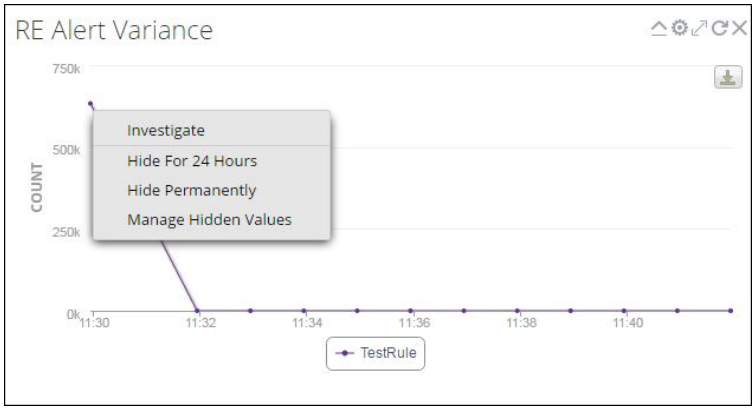
1. Pour afficher et modifier les options d'un dashlet, cliquez sur l'icône Paramètres (⚙) dans la barre de titre.
   La boîte de dialogue Options s'affiche.



2. Modifiez les propriétés affichées. Par exemple, dans un dashlet Valeurs principales Investigation, vous pouvez remplacer la limite de résultats 20 par 40.
3. Cliquez sur **Appliquer**.

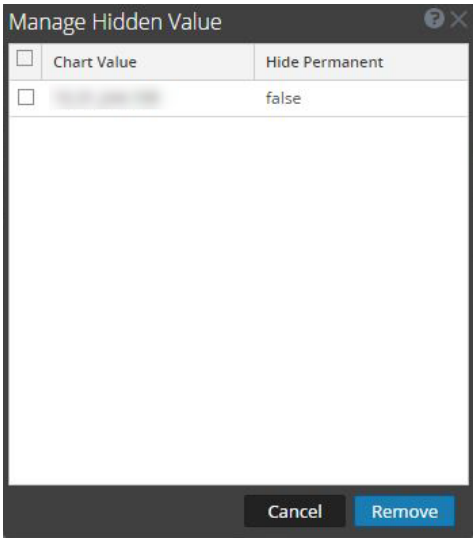
Certains dashlets ont des options de configuration pour personnaliser l'apparence ou le contenu du dashlet. Les options suivantes sont disponibles pour les dashlets Alertes principales RE, Variance d'alertes RE et Graphiques en temps réel RE à l'aide du clic gauche de la souris :

- **Masquer pendant 24 heures**: Cette option vous permet de masquer la valeur sélectionnée pour les prochaines 24 heures. Après 24 heures, les données seront automatiquement affichées dans le dashlet, si la valeur est configurée et répertoriée en haut.
- **Masquer définitivement**: Cette option vous permet de masquer la valeur sélectionnée de façon définitive jusqu'à ce que vous l'ajoutiez à l'aide de l'option Gérer les valeurs masquées.



- **Gérer les valeurs masquées** : Cette option affiche la liste de toutes les valeurs masquées. Cochez la case correspondant à une valeur, puis cliquez sur **Supprimer** pour afficher les données dans le

graphique.



Les options Masquer pendant 24 heures, Masquer définitivement et Gérer les valeurs masquées ne sont pas disponibles pour les graphiques Geomap.

Remarque : Lorsque vous modifiez une valeur dans un tableau de bord préconfiguré, il s'agit d'une modification propre à l'utilisateur. Les modifications apportées à un tableau de bord préconfiguré s'appliquent uniquement à votre tableau de bord et ne peuvent pas être affichées par d'autres utilisateurs qui utilisent le même tableau de bord préconfiguré. Par exemple, si vous masquez une valeur dans un tableau de bord Présentation, les modifications seront applicables uniquement à votre tableau de bord. Si un autre utilisateur affiche le même tableau de bord de présentation, la valeur sera toujours affichée. Il en va de même pour un tableau de bord personnalisé. Lorsque vous masquez une valeur dans le tableau de bord personnalisé et partagez le même tableau de bord avec un autre utilisateur, les valeurs s'affichent toujours même si le tableau de bord est partagé.

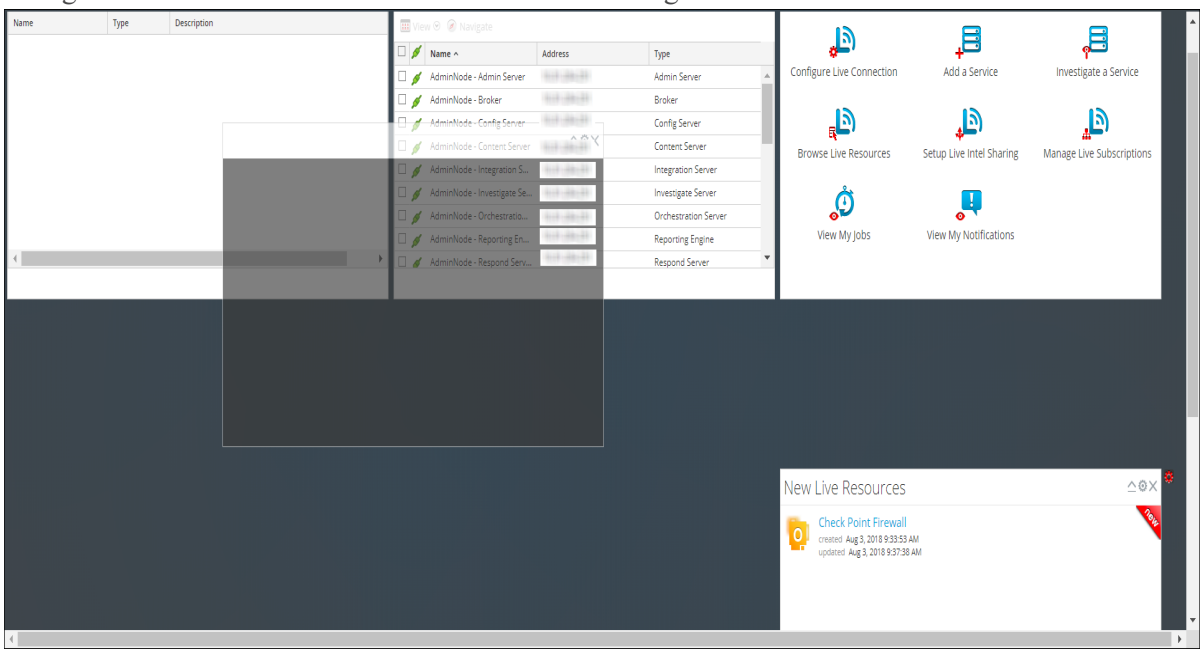
Pour plus d'informations sur les dashlets disponibles, reportez-vous au Catalogue des tableaux de bord dans l'espace Contenu RSA sur RSA Link.

Réorganiser un dashlet

Vous pouvez disposer les dashlets selon vos préférences en les faisant glisser dans un ordre différent sur le tableau de bord.

1. Pour déplacer un dashlet, placez le pointeur de la souris sur le titre du dashlet à déplacer.
   Le curseur directionnel ✥ apparaît sur le dashlet. Cliquez sur le titre du dashlet à déplacer tout en maintenant la touche de la souris enfoncée.
2. Continuez à appuyer sur le bouton gauche de la souris et faites glisser la fenêtre vers le nouvel emplacement.

La figure ci-dessous illustre un dashlet en cours de réorganisation.



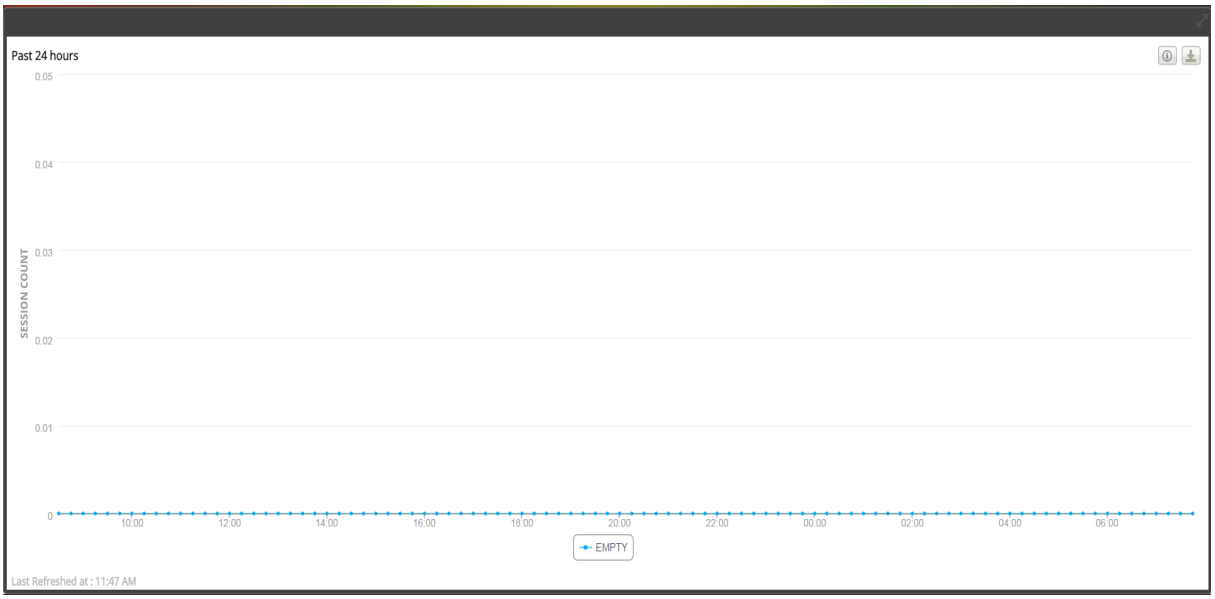
3. Relâchez le bouton de la souris une fois le dashlet à la position souhaitée.
   Le dashlet occupant actuellement cette position se déplace vers le bas.

Agrandir un dashlet unique

Cette section explique comment ouvrir un dashlet sur tout l'espace du tableau de bord NetWitness Platform principal avec le même titre de dashlet. Les dashlets disposant d'un grand nombre de colonnes ou de graphiques, par exemple des dashlets de Création de rapports, sont plus faciles à afficher lorsqu'ils sont agrandis, afin que l'intégralité du contenu soit visible sans défilement.

Pour agrandir un dashlet, cliquez sur l'icône d'agrandissement dans la barre de titre du dashlet : ⤢. Le dashlet s'affiche en plein écran.

Pour réduire un dashlet, cliquez sur la même icône de contrôle dans la barre de titre du dashlet : ⤢. Le dashlet est restauré à la taille précédente.



Supprimer un dashlet

1. Cliquez sur ✕ dans la barre de titre :
   Une fenêtre de confirmation s'affiche pour confirmer si vous souhaitez supprimer le dashlet.
2. Si vous souhaitez le supprimer, cliquez sur **Oui**. Le dashlet est supprimé du tableau de bord.
   Cliquez sur **Non**, si vous ne souhaitez pas le supprimer.

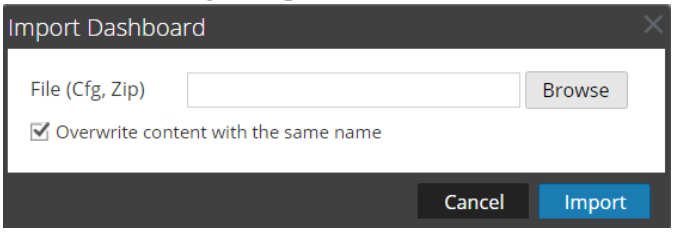
Remarque : Après avoir supprimé le dashlet, l'espace vide est remplacé par un espace réservé où vous pouvez ajouter un autre dashlet à l'aide d'une procédure d'ajout de dashlet figurant ci-dessus.

Importation et exportation de tableaux de bord

La possibilité de personnaliser les tableaux de bord en fonction de l'évolution des circonstances et des conditions peut engendrer un grand nombre de tableaux de bord inutiles au quotidien. Plutôt que de repartir à zéro chaque fois que vous voulez recréer un tableau de bord personnalisé particulier, vous pouvez exporter vos tableaux de bord qui ne sont pas en cours d'utilisation. Lorsque vous êtes prêt à utiliser un tableau de bord précédemment exporté, importez-le dans NetWitness Platform.

Importer le tableau de bord

1. Dans la barre d'outils du tableau de bord, cliquez sur (Importer le tableau de bord).
   La boîte de dialogue Importer le tableau de bord s'affiche.



2. Accédez au fichier du tableau de bord dans la boîte de dialogue **Importer le tableau de bord**. Vous pouvez importer des fichiers .cfg et .zip.
3. Cliquez sur **Importer**.
   Le tableau de bord s'affiche dans NetWitness Platform.

Remarque : Si vous importez un tableau de bord à partir de Security Analytics 10.6. x vers NetWitness Platform11.x, le tableau de bord, ainsi que les règles et graphiques associés doivent être importés séparément. En revanche, lorsque vous importez un tableau de bord de NetWitness Platform11.x vers NetWitness Platform, le tableau de bord, toutes les règles et les graphiques associés, sont importés au format .zip.

Exporter un tableau de bord

Remarque : Lorsque vous exportez un tableau de bord Reporter Realtime, le contenu Reporting Engine correspondant est également exporté

Les tableaux de bord exportés sont conçus pour fonctionner au sein de la même instance NetWitness Platform. Il est également possible de partager vos tableaux de bord personnalisés avec d'autres utilisateurs de votre entreprise, à condition qu'ils disposent des autorisations équivalentes.

Pour exporter un tableau de bord, il doit être ouvert pour accéder à l'option Exporter le tableau de bord sous le menu déroulant Modifier dans la barre d'outils du tableau de bord.

1. Accédez au tableau de bord que vous voulez exporter. Tous les tableaux de bord existants apparaissent dans le menu déroulant **Dashboard Selection List** du tableau de bord en cours d'affichage.
2. Dans la barre d'outils du tableau de bord, cliquez sur  (Exporter le tableau de bord).
   Le fichier exporté est enregistré au format .zip.

Remarque : La fonction d'exportation n'est pas applicable aux tableaux de bord préconfigurés.

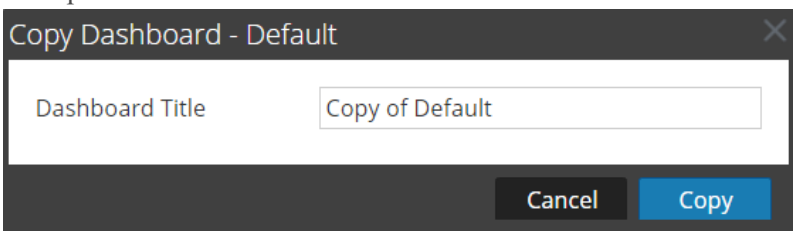
Copie d'un tableau de bord

Pour personnaliser les vues dans NetWitness Platform, vous pouvez ajouter des dashlets au tableau de bord NetWitness ou à un tableau de bord personnalisé. Le tableau de bord NetWitness Platform, comme son nom l'indique, réunit tous les dashlets NetWitness Platform. La boîte de dialogue Copier le tableau de bord crée un tableau de bord en double, qui peut être personnalisé. Lorsque vous copiez un tableau de bord, le nom par défaut comporte un préfixe `Copy of`. Par exemple, si le nom du tableau de bord d'origine est `XYZ`, le titre par défaut du tableau de bord copié sera `Copy of XYZ`.

Pour copier un tableau de bord :

1. Accédez à un tableau de bord.
2. Dans la barre d'outils du tableau de bord, cliquez sur  .
   La boîte de dialogue Copier le tableau de bord s'affiche. La capture d'écran suivante est un exemple

de copie d'un tableau de bord.



3. Saisissez le titre du tableau de bord.
4. Cliquez sur **Copy**.

Partage d'un tableau de bord

Dans NetWitness Platform, en tant qu'administrateur, vous pouvez partager des tableaux de bord à des fins de visualisation avec d'autres rôles tels que des administrateurs, des analystes, des opérateurs, etc. Lorsque vous partagez un dashlet, les utilisateurs peuvent uniquement afficher le tableau de bord, créer un tableau de bord en tant que favori, copier le tableau de bord et exporter le tableau de bord. Dans le cas d'autres rôles tels que les analystes, les opérateurs etc., vous pouvez partager le tableau de bord uniquement avec des rôles similaires. Par exemple, un analyste sera en mesure de partager un tableau de bord avec d'autres analystes uniquement.

1. Accédez à un tableau de bord.
2. Dans la barre d'outils du tableau de bord, cliquez sur 

, puis sélectionnez la case à cocher du rôle avec lequel vous souhaitez partager le tableau de bord.

Remarque : Si vous ne souhaitez pas partager le tableau de bord, désactivez la case à cocher du rôle.

Gestion des tâches

Inévitablement, il existe des tâches à la demande ou planifiées, dans RSA NetWitness® Platform qui demandent quelques minutes. Le système de tâches NetWitness Platform vous permet de lancer une tâche de longue durée et de continuer à utiliser d'autres parties de NetWitness Platform pendant son exécution. Vous pouvez non seulement surveiller la progression de la tâche, mais aussi recevoir des notifications lorsqu'elle se termine indiquant si elle a été réalisée avec succès ou si elle a échoué.

Lorsque vous utilisez NetWitness Platform, vous pouvez ouvrir une vue rapide de vos tâches dans la barre d'outils. Vous pouvez effectuer des recherches à tout moment, mais lorsque l'état de la tâche change, l'icône Tâches ( ) est balisée avec le nombre de tâches en cours d'exécution. Lorsque toutes les tâches sont terminées, ce nombre disparaît.

Vous pouvez également visualiser les tâches dans ces deux vues.

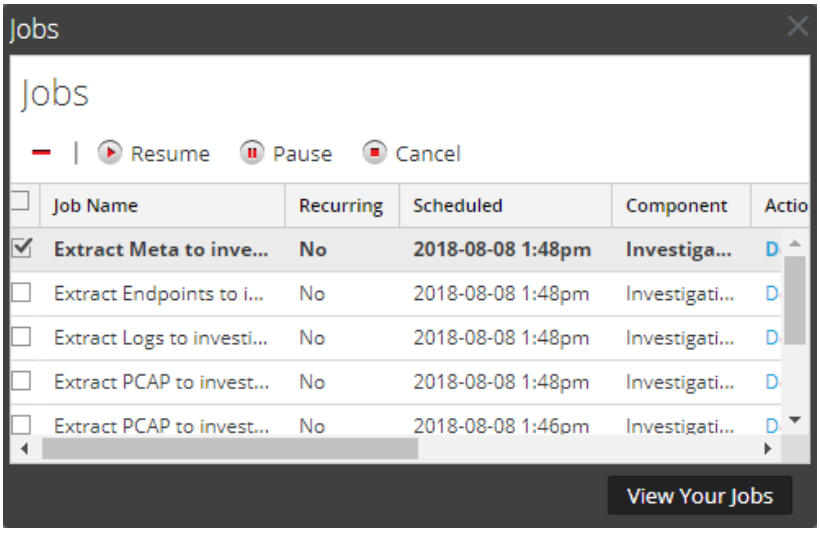
- Dans le panneau Tâches du profil, vous pouvez voir les mêmes tâches dans un panneau entier. Il n'y a que vos tâches.
- Dans la vue Système, les utilisateurs dotés des privilèges administratifs peuvent visualiser et gérer toutes les tâches pour tous les utilisateurs depuis un seul panneau de tâches.

La structure du panneau des tâches est la même dans toutes les vues.

Afficher la barre d'état Tâches

Dans la barre d'outils NetWitness Platform , cliquez sur l'icône Tâches ( ).

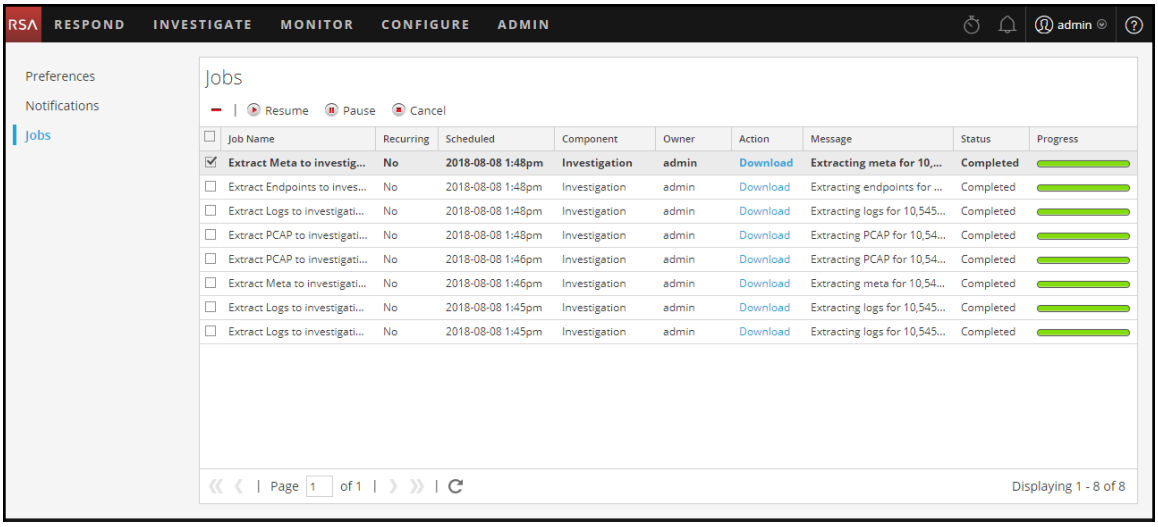
La barre d'état Tâches s'affiche.



La barre d'état Tâches répertorie toutes les tâches récurrentes ou non dont vous êtes le propriétaire, à l'aide d'un sous-ensemble de colonnes disponibles dans le panneau Tâches. Sinon, la barre d'état Tâches et la vue Profil d'utilisateur panneau - Tâches sont identiques. Dans la vue Système d'administration, le panneau Tâches répertorie des informations sur toutes les tâches NetWitness Platform pour tous les utilisateurs.

Voir Toutes vos tâches

Pour afficher une vue complète de vos tâches, dans la barre de tâches, cliquez sur **Consultez vos tâches**.
Le panneau Tâches s'affiche :



Interrompre et reprendre l'exécution planifiée d'une tâche récurrente

Les options Interrompre et Reprendre s'appliquent uniquement aux tâches récurrentes. Lorsque vous suspendez une tâche récurrente, cela n'a aucun effet sur cette exécution. L'exécution suivante (en supposant que la tâche est toujours suspendue) est ignorée.

1. Pour arrêter la prochaine exécution d'une tâche récurrente, dans un **panneau Tâches**, sélectionnez la tâche, puis cliquez sur **Suspendre**.
   L'exécution suivante de la tâche est ignorée, et la planification est interrompue jusqu'à ce que vous cliquiez sur Reprendre.
2. Pour redémarrer l'exécution des tâches récurrentes interrompues, sélectionnez la tâche, puis cliquez sur **Reprendre**.
   L'exécution suivante de la tâche se produit comme prévu, et la planification de la tâche reprend.

Annuler une tâche

Pour annuler des tâches qui sont exécutées ou en attente d'exécution :

1. Dans la barre d'état **Tâches** ou dans le panneau **Tâches**, sélectionnez une ou plusieurs tâches.
2. Cliquez sur **Annuler**.
   Une boîte de dialogue de confirmation s'affiche.
3. Cliquez sur **Yes**.
   Les tâches sont annulées mais les entrées restent affichées dans la liste à l'état **Annulé**.

Si vous annulez une tâche récurrente, cela annule cette exécution de la tâche. Lors de l'occurrence planifiée suivante de la tâche, elle s'exécute normalement.

Supprimer une tâche

Attention : Lorsque vous supprimez une tâche, elle est instantanément supprimée de la liste. Aucune boîte de dialogue de confirmation n'est proposée. Si vous supprimez une tâche récurrente, toutes les exécutions futures sont également supprimées.

Les utilisateurs peuvent supprimer leurs propres tâches avant, pendant et après l'exécution. Les administrateurs peuvent supprimer n'importe quelle tâche. Pour supprimer des tâches :

1. Sélectionnez une ou plusieurs tâches.
2. Cliquez sur .
   Les tâches sont supprimées de la liste.

Télécharger une tâche

Si une tâche affiche l'état du téléchargement dans la colonne Action, c'est que vous pouvez télécharger le résultat de la tâche. Si vous utilisez la vue Enquêter et extrayez les données de paquets pour une session sous la forme d'un fichier PCAP, ou que vous extrayez les fichiers de charge utile (par exemple, des documents et des images Word) à partir d'une session, un fichier est créé. Pour télécharger le fichier vers votre système local, cliquez sur **Télécharger**.

Affichage et suppression des notifications

Dans RSA NetWitness® Platform, vous pouvez afficher les notifications système récentes sans quitter le domaine dans lequel vous travaillez. Vous pouvez ouvrir une vue rapide des notifications à partir de la barre d'outils NetWitness Platform. Vous pouvez les consulter à n'importe quel moment, mais lorsqu'une nouvelle notification est reçue, l'icône Notifications est signalée ( ).

Voici des exemples de notifications :

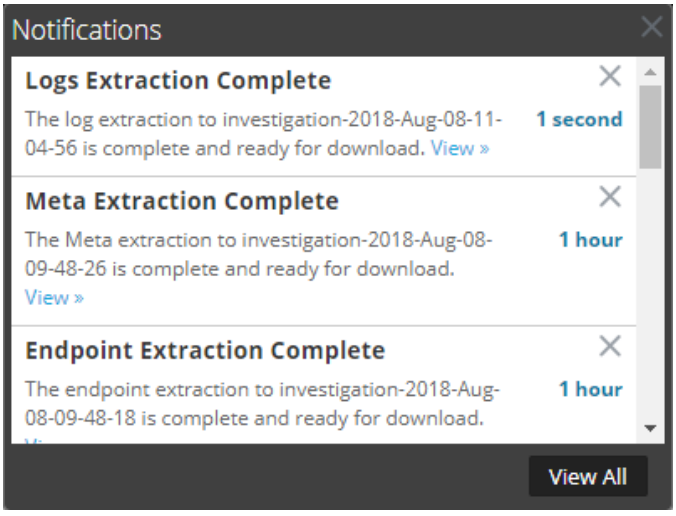
- Mise à niveau de l'hôte terminée.
- Fin du push du parser aux décodeurs.
- Nouvelle version logicielle disponible.

Vous pouvez voir les notifications dans ces deux vues :

- Dans la barre Notifications, vous pouvez voir vos notifications récentes.
- Dans le panneau Notifications du profil, vous pouvez afficher toutes vos notifications.

Afficher les notifications récentes

Pour afficher les notifications récentes, cliquez sur l'icône Notifications ( ).
La barre Notifications s'affiche.

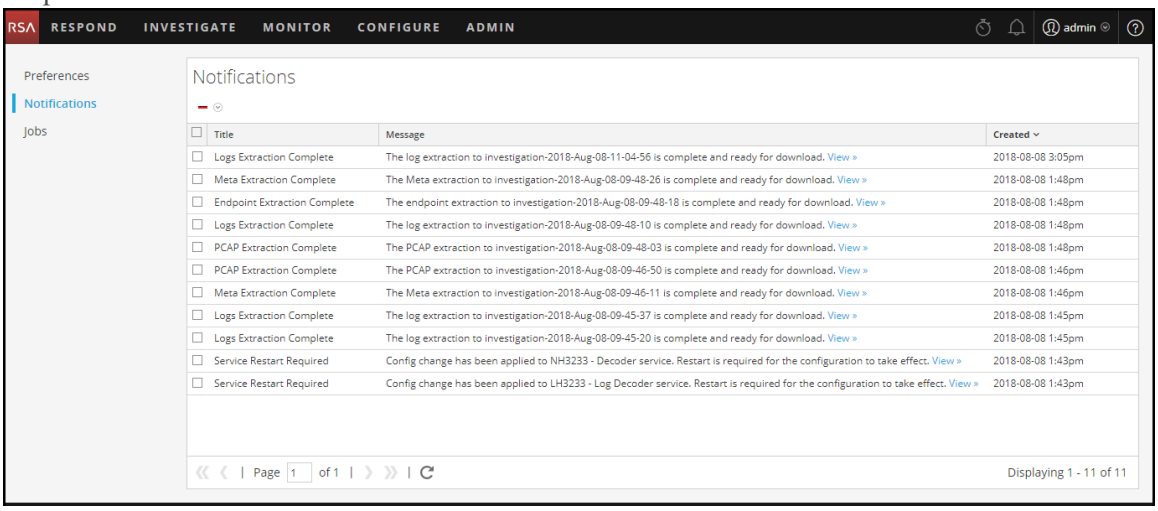


Afficher toutes vos notifications

Pour afficher toutes vos notifications, procédez de l'une des façons suivantes :

- Cliquez sur pour ouvrir la barre d'état Notifications, puis cliquez sur **Afficher** tout dans cette même barre d'état.
- Dans le coin supérieur droit de la fenêtre du navigateur NetWitness Platform, sélectionnez > **Profil**, puis dans le panneau Options de la boîte de dialogue Préférences, sélectionnez **Notifications**.

Le panneau Notifications affiche toutes vos notifications.



Supprimer tous les enregistrements de notification

Pour supprimer les enregistrements de notification :

1. Dans la liste **Notifications du profil**, sélectionnez les notifications que vous souhaitez supprimer.
2. Cliquez sur .

   Les notifications sélectionnées sont supprimées de cette liste et de la barre d'état Notifications.

Affichage de l'aide dans l'application

Il existe différentes façons d'obtenir de l'aide lors de l'utilisation de RSA NetWitness® Platform. Vous pouvez utiliser l'aide incorporée, info-bulles et liens d'aide en ligne.

Afficher l'aide incorporée

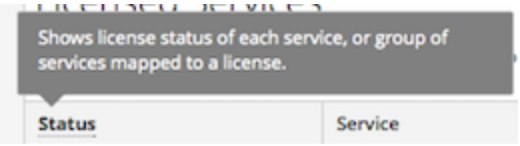
L'aide incorporée fournit des informations supplémentaires sur la procédure à suivre dans les sections ou les champs que vous visualisez dans l'interface utilisateur NetWitness Platform. Pour afficher l'aide en ligne, placez le pointeur sur  . L'aide en ligne affiche une brève description de l'élément.

Exemple d'aide en ligne :

Afficher les info-bulles

Les info-bulles vous permettent de voir rapidement une description du texte ou des informations supplémentaires concernant une action, un champ ou un paramètre. Les info-bulles apparaissent sous forme de texte souligné. Pour afficher l'info-bulle et voir une brève description du terme, passez votre souris au-dessus du texte souligné.

Exemple d'info-bulle :

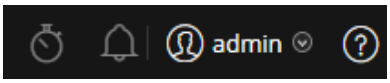


Afficher l'aide en ligne

Les liens de l'aide en ligne vous mènent hors de NetWitness Platform pour vous diriger vers la documentation en ligne de RSA Link. Ce site dispose d'un ensemble de documentation complète pour NetWitness Platform. Les liens dirigent l'utilisateur directement vers la section qui décrit la partie de l'interface utilisateur en cours d'affichage.

Pour afficher la section d'aide en ligne pour l'emplacement actuel, cliquez sur  dans la barre d'outils NetWitness Platform ou dans une boîte de dialogue. La section d'aide correspondante s'affiche dans une fenêtre de navigation séparée. Cette section décrit les fonctionnalités et fonctions de la vue actuelle ou de la boîte de dialogue. Vous pouvez naviguer rapidement vers les procédures connexes à partir de cette section.

La figure suivante est un exemple d'icône d'aide en ligne dans la barre d'outils NetWitness Platform.



Recherche de documents dans RSA Link

La documentation RSA NetWitness® Platform se trouve sur RSA Link, la communauté et le portail de support RSA. RSA Link réunit toutes vos ressources RSA en un seul endroit. Il comprend des avis, de la documentation sur les produits, des articles de la base de connaissances, des téléchargements et de la formation. Pour visionner une *visite guidée de RSA Link*, visitez la page https://community.rsa.com/videos/21554.

Localiser la documentation NetWitness Platform

La documentation relative aux paquets et réseaux NetWitness Platform est accessible via le lien suivant : https://community.rsa.com/docs/DOC-40370

Pour accéder à la documentation relative aux paquets et logs NetWitness Platform :

1. Sur la page d'accueil de RSA Link (https://community.rsa.com), cliquez sur **RSA NETWITNESS PLATFORM**.
2. Sur la page RSA NetWitness Platform, cliquez sur **DOCUMENTATION**, puis sélectionnez **RSA NETWITNESS LOGS AND NETWORK**.

Pour accéder à la documentation NetWitness Endpoint 4.x :

1. Sur la page d'accueil de RSA Link (https://community.rsa.com), cliquez sur **RSA NETWITNESS PLATFORM**.
2. Sur la page RSA NetWitness Platform, cliquez sur **DOCUMENTATION**, puis sélectionnez **RSA NETWITNESS ENDPOINT**.

Localiser le contenu RSA

Le contenu RSA est le lien suivant : https://community.rsa.com/community/products/netwitness/rsa-content

Pour accéder au contenu RSA :

1. Sur la page d'accueil de RSA Link (https://community.rsa.com), cliquez sur **RSA NETWITNESS PLATFORM**.
2. Sur la page de RSA NetWitness Platform, cliquez sur **DOCUMENTATION**, puis sélectionnez **ADDITIONAL RESOURCES** > **RSA LIVE CONTENT**.

Localiser les sources d'événements prises en charge par RSA

Les sources d'événements prises en charge par RSA sont accessibles via le lien suivant : https://community.rsa.com/community/products/netwitness/parser-network/event-sources

Pour accéder aux sources d'événements prises en charge par RSA :

1. Sur la page d'accueil de RSA Link (https://community.rsa.com), cliquez sur **RSA NETWITNESS PLATFORM**.
2. Sur la page de RSA NetWitness Platform, cliquez sur **DOCUMENTATION**, puis sélectionnez **ADDITIONAL RESOURCES** > **EVENT SOURCE CONFIGURATION**.

Localiser les Guides de configuration du matériel

Les Guides de configuration du matériel sont accessibles via le lien suivant : https://community.rsa.com/community/products/netwitness/hardware-setup-guides

1. Sur la page d'accueil de RSA Link (https://community.rsa.com), cliquez sur **RSA NETWITNESS PLATFORM**.
2. Sur la page de RSA NetWitness Platform, cliquez sur **DOCUMENTATION** and select **ADDITIONAL RESOURCES** > **HARDWARE SETUP GUIDES**.

Rechercher des documents à l'aide du navigateur NetWitness

Vous pouvez rechercher la documentation RSA NetWitness Platform souhaitée dans RSA Link à l'aide de l'outil NetWitness Navigator.

1. Sur la page d'accueil de RSA Link (https://community.rsa.com), cliquez sur **RSA NETWITNESS PLATFORM**.
2. Sous PRODUCT RESOURCES (à droite de la page), cliquez sur **RSA NetWitness Navigator**.
3. Sélectionnez les critères de recherche de votre choix parmi les options disponibles. Lors de la recherche de documentation, vous devez sélectionner **User Documentation** comme type de contenu. En outre, l'option Cost est ignorée pour la documentation utilisateur.
4. Cliquez sur **VIEW RESULTS** pour afficher la liste des documents correspondants.
5. Cliquez sur **RESET OPTIONS** pour effacer vos options de recherche précédentes.

Suivre les mises à jour de contenu

Vous pouvez suivre des pages ou des documents pour être informé(e) des changements.

1. Connectez-vous à RSA Link.
2. Accédez à une page ou un document et dans le coin supérieur droit, sélectionnez soit **Follow**, soit **Actions** > **Follow**.

Envoyez vos commentaires à RSA

Votre avis est très important pour nous et nous aident à fournir une meilleure expérience pour nos clients. Veuillez envoyer vos suggestions à sahelpfeedback@rsa.com.

Références de démarrage de la plateforme NetWitness

La section suivante contient des informations de référence sur l'interface utilisateur liées à la mise en route de l'application NetWitness Platform.

- Préférences utilisateur
- Panneau Notifications et barre d'état Notifications
- Panneau Tâches et barre d'état Tâches

Préférences utilisateur

Pour ajuster RSA NetWitness® Platform afin de l'adapter à votre environnement et à vos pratiques de travail, vous pouvez définir vos propres préférences globales de l'application. Vous pouvez :

- Modifier la langue de l'application
- Définir le fuseau horaire de l'application
- Définir les formats de date et d'heure
- Sélectionner l'emplacement de démarrage NetWitness Platform par défaut*
- Sélectionner la Vue par défaut Enquêter
- Choisir un thème foncé ou clair pour l'application
- Modifier votre mot de passe
- Activer les notifications
- Activer des menus contextuels
- Modifier les préférences d'Investigate décrites dans le *Guide d'utilisation de NetWitness Investigate*.

Vos options de préférences globales varient selon que vous y accédez à partir de la vue Répondre ou d'autres vues, telles qu'Enquêter, Surveiller, Configurer et Administrateur. Deux boîtes de dialogue de préférences utilisateur globales sont accessibles depuis la barre de menus principale :

- Boîte de dialogue **Préférences utilisateur** : Accessible à partir de Respond et les vues Enquêter suivantes : Analyse d'événements, Hôtes, Fichiers et Utilisateurs.
- Boîte de dialogue **Préférences** : Accessible à partir de la plupart des autres vues.

Que voulez-vous faire ?

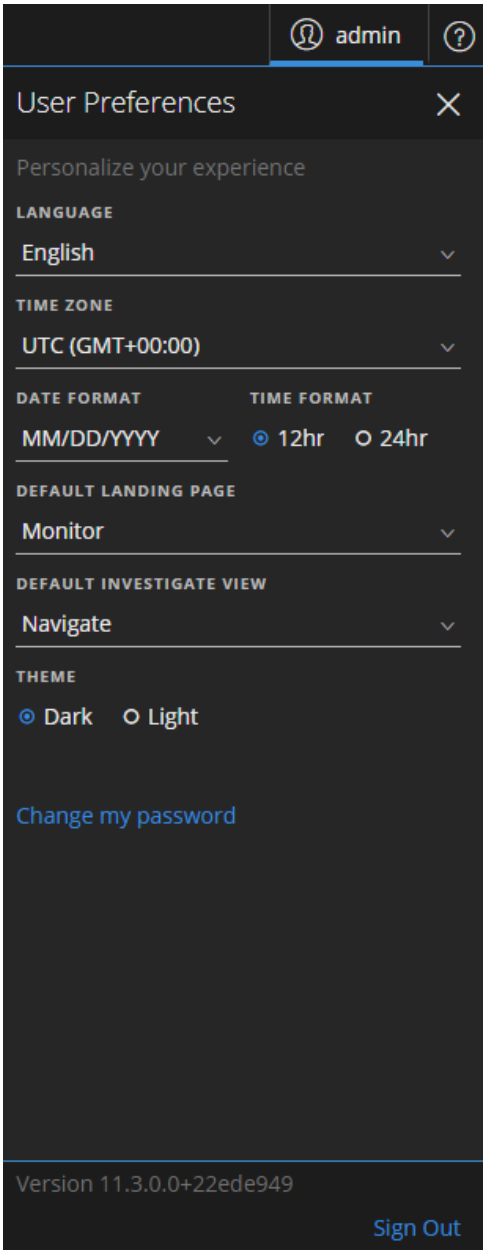
Rôle	Je souhaite...	Me montrer comment
Tout	Modifier mon mot de passe	Modifier mon mot de passe
Tout	Choisir ma page de lancement par défaut	Configuration de votre vue par défaut par le rôle du SOC
Tout	Définir mes préférences utilisateur	Configuration des préférences utilisateur

Rubriques connexes

- Navigation de base de la plate-forme NetWitness

Préférences utilisateur (vue Répondre et certaines vues Enquêter)

Pour accéder à vos préférences utilisateur, cliquez sur .
La boîte de dialogue Préférences utilisateur affiche vos préférences actuelles et la version de NetWitness Platform.



Le tableau suivant décrit les options de préférence globales de l'application auxquelles vous pouvez accéder depuis la boîte de dialogue Préférences utilisateur.

Option	Description
Langue	(Cette option s'applique à NetWitness Platform, versions 11.2 et ultérieures.) Définit la langue préférée pour toute la plate-forme NetWitness. La langue par défaut est l'anglais (États-Unis).
Fuseau horaire	Définit le fuseau horaire à utiliser dans NetWitness Platform.
Format de date	Définit le format de l'ordre de l'affichage mois (MM), jour (JJ) et année (AAAA). Par exemple, le format MM/JJ/AAAA affiche la date sous la forme de 05/11/2017.
Format de l'heure	Définit l'heure au format 12 ou 24 heures. Par exemple, 2 h 00 au format 12 heures est 14 h 00 au format 24 heures.
Page de lancement par défaut	Vous permet de sélectionner la vue par défaut lorsque vous vous connectez à NetWitness Platform. Vous pouvez choisir Répondre, Enquêter, Surveiller, Configurer et Administrateur en fonction de votre rôle d'utilisateur. Par exemple, vous pouvez choisir Répondre pour accéder directement à la section pertinente de l'application destinée aux responsables de la réponse aux incidents. Cette sélection définit la vue par défaut pour l'ensemble de l'application.
Vue par défaut Enquêter	(Cette option s'applique à NetWitness Platform 11.1 ou supérieure.) Sélectionnez la valeur par défaut de la page de lancement de la vue Enquêter. Vous pouvez choisir les vues Naviguer, Événements, Analyse d'événements, Hôtes, Fichiers, Utilisateurs ou Analyse de malware en tant que vue par défaut Enquêter. Par exemple, vous pouvez choisir la vue Événements en tant que vue Enquêter par défaut pour accéder directement à la page Événements afin d'afficher les événements générés pour un service.
Thème	(Cette option s'applique à NetWitness Platform 11.1 et versions ultérieures.) Modifie l'apparence de la vue Répondre et certaines vues Enquêter que vous voyez dans l'application. Vous pouvez choisir un thème clair ou foncé. • **Foncé** : Le thème foncé est idéal pour les environnements plus foncés ou lorsque vous n'avez pas besoin d'autant de contraste. • **Clair** : Le thème clair est préférable pour les environnements plus clairs, lorsque vous avez besoin de plus de contraste, ou lorsque vous procédez à une projection de l'application pour que d'autres personnes la voient. Dans la mesure où certaines vues ne sont pas concernées par les modifications de thème, vous pouvez choisir le thème clair pour une expérience de visualisation plus cohérente. Votre sélection modifie uniquement la façon dont NetWitness Platform s'affiche pour vous, pas pour les autres utilisateurs.

Option	Description
Modifier mon mot de passe	Ouvre la boîte de dialogue Préférences dans laquelle vous pouvez modifier votre mot de passe.
Version	Affiche la version de NetWitness Platform.
Déconnexion	Permet de vous déconnecter de NetWitness Platform.

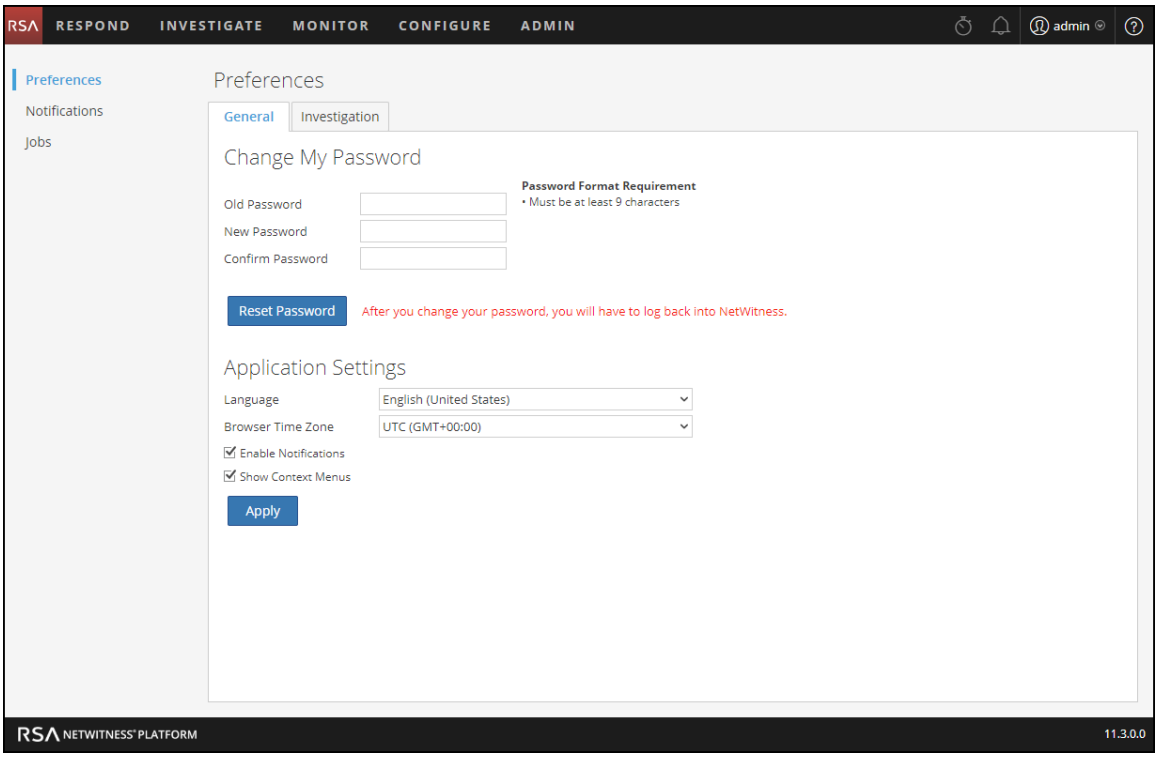
Toutes les sélections que vous effectuez prennent effet immédiatement.

Préférences

Pour accéder à d'autres préférences utilisateur, effectuez l'une des opérations suivantes :

- Pour la plupart des vues, telles qu'Enquêter, Surveiller, Configurer ou Administrateur, accédez à > **Profil**.
- Dans la vue Répondre et dans certaines vues Enquêter (Analyse d'événements, Hôtes, Fichiers et Utilisateurs), sélectionnez dans la boîte de dialogue Préférences utilisateur, cliquez sur **Modifier mon mot de passe**.

La boîte de dialogue Préférences utilisateur affiche vos préférences actuelles.



Les tableaux suivants décrivent les options globales de préférences de l'application accessibles à partir de la boîte de dialogue Préférences.

Modifier mon mot de passe

Cette section vous permet de modifier votre mot de passe. Votre administrateur définit les exigences de force de mot de passe appropriées pour votre mot de passe NetWitness Platform, telles que la longueur minimale de mot de passe et le nombre minimum de caractères majuscules, minuscules, décimaux, alphabétiques non latins et spéciaux. Ces exigences sont ensuite affichées lors de la modification de votre mot de passe.

Le tableau suivant décrit les options de la section Modifier mon mot de passe.

Option	Description
Ancien mot de passe	Saisissez le mot de passe que vous avez utilisé pour vous connecter à NetWitness Platform.
Nouveau mot de passe	Saisissez le mot de passe que vous souhaitez utiliser pour la connexion suivante.
Confirmer le mot de passe	Saisissez de nouveau le nouveau mot de passe.
Réinitialiser le mot de passe	Met à jour votre profil utilisateur avec le nouveau mot de passe. Vous serez déconnecté de NetWitness Platform pour que les modifications prennent effet. Le nouveau mot de passe prend effet dès la connexion suivante à NetWitness Platform. La modification du mot de passe est appliquée à votre connexion au système et à tous les services NetWitness Platform sur lesquels votre compte a été ajouté.

Si vous avez modifié votre mot de passe, vous serez déconnecté de NetWitness Platform pour que les modifications prennent effet. Le nouveau mot de passe prend effet dès la connexion suivante à NetWitness Platform.

Paramètres d'application

Le tableau suivant décrit les options de la section Paramètres d'application.

Option	Description
Langue	(Cette option s'applique à NetWitness Platform, versions 11.2 et ultérieures.) Définit la langue préférée pour toute la plate-forme NetWitness. La langue par défaut est l'anglais (États-Unis).
Fuseau horaire du navigateur	Définit le fuseau horaire à utiliser dans NetWitness Platform. Votre préférence de fuseau horaire s'affiche dans la barre d'outils.
Activer les notifications	Cette case à cocher active et désactive les notifications pour votre compte utilisateur. Par défaut, les notifications du système NetWitness Platform sont activées lors de la création d'un nouveau compte.
Activer des menus contextuels	Cette case à cocher active et désactive les menus contextuels pour votre compte utilisateur. Par défaut, les menus contextuels sont activés lors de la création d'un nouveau compte utilisateur. Les menus contextuels fournissent des fonctions supplémentaires pour des vues spécifiques lorsque vous cliquez avec le bouton droit de la souris dans une vue.

Option	Description
Appliquer	Met à jour vos préférences et applique les modifications immédiatement.

Panneau Notifications et barre d'état Notifications

RSA NetWitness® Platform fournit les notifications système permettant de conseiller les utilisateurs sur certaines actions ou conditions.

- Mise à niveau de l'hôte terminée.
- Fin du push de l'analyseur aux décodeurs.
- Panne d'un service (log critique d'un certain type).
- Visualisation terminée.
- Rapport terminé.
- Nouvelle version logicielle disponible.

Dans NetWitness Platform, vous pouvez afficher les notifications système récentes sans quitter la section dans laquelle vous travaillez. Vous pouvez ouvrir une vue rapide des notifications à partir de la barre d'outils NetWitness Platform. Vous pouvez les consulter à n'importe quel moment, mais lorsqu'une nouvelle notification est reçue, l'icône Notifications est signalée ().

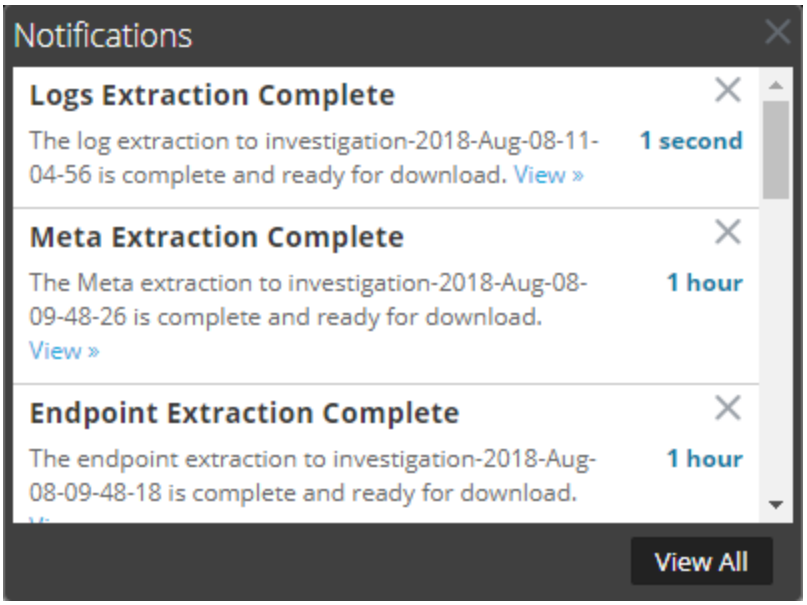
Lorsque vous consultez les notifications dans la barre d'état Notifications, seules les notifications récentes sont affichées. Vous pouvez accéder à toutes vos notifications à partir de votre profil utilisateur et à partir du plateau Notifications en sélectionnant l'option Afficher tout. Les procédures de visualisation des notifications sont fournies dans Affichage et suppression des notifications.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Tout	Afficher toutes les notifications	Affichage et suppression des notifications
Tout	Supprimer des notifications	Affichage et suppression des notifications

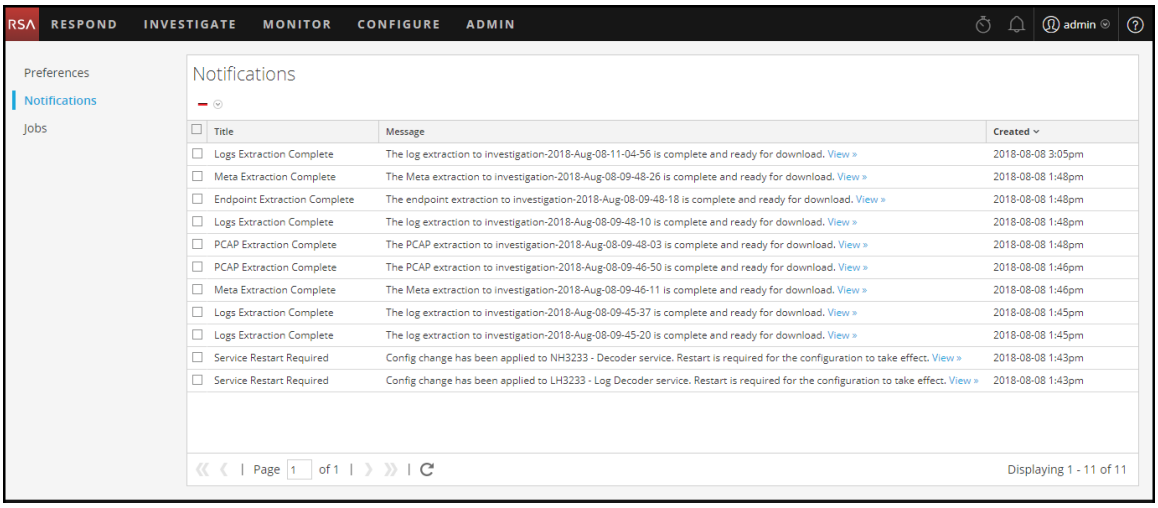
Pour accéder au panneau Notifications, procédez de l'une des façons suivantes :

- Cliquez sur pour ouvrir la barre d'état Notifications, puis cliquez sur **Afficher tout** dans cette même barre d'état.



- Dans le coin supérieur droit de la fenêtre du navigateur NetWitness Platform, sélectionnez > **Profil**, puis dans le panneau Options de la boîte de dialogue Préférences, sélectionnez **Notifications**.

  Le panneau Notifications s'affiche.



Le plateau Notifications affiche vos notifications récentes. Il contient un sous-ensemble des informations dans le panneau Notifications. Le panneau Notifications affiche toutes vos notifications. Le tableau ci-dessous décrit le panneau Notifications et les fonctions de la barre d'état Notifications.

Fonctionnalité	Description
	(Panneau Notifications uniquement) Affiche un menu déroulant qui vous permet de supprimer la notification sélectionnée ou toutes les notifications dans le panneau Notifications et dans la barre d'état Notifications.
Titre	Le titre de la notification, par exemple, **Extraction de logs terminée**.
Message	Message entier, par exemple, **L'extraction de fichier journal vers la procédure d'enquête est terminée et prête pour le téléchargement**.
Afficher	Certains messages comprennent un lien **Afficher**, affichant l'endroit où vous pouvez agir. Par exemple, s'il y a un fichier à télécharger, le fait de cliquer sur ce lien permet d'ouvrir le panneau Tâches, puis la vue à partir de laquelle vous pouvez télécharger le fichier.
Créé	Date et heure de création de la notification. Dans la barre d'état Notifications, cela correspond au nombre d'heures ou de jours depuis la création de la notification.
Afficher tout	(Plateau de notification uniquement) Ouvre le panneau Notifications, qui répertorie toutes vos notifications.

Panneau Tâches et barre d'état Tâches

Les travaux sont démarrés par divers composants RSA NetWitness® Platform ; par exemple, le téléchargement de ressources CMS (Content Management System) de Services Live et l'extraction de fichiers journaux, méta et PCAP à partir de NetWitness Investigate.

Dans la vue ADMIN > Système, les administrateurs peuvent gérer toutes les tâches NetWitness Platform dans le panneau Tâches. D'autres utilisateurs non administratifs peuvent afficher leurs propres tâches dans le panneau Tâches du profil.

De plus, lorsque vous utilisez NetWitness Platform, vous pouvez ouvrir une vue rapide de vos tâches dans la barre d'outils NetWitness Platform. Lorsque l'état d'une tâche change, l'icône Tâches () est balisée avec le nombre de tâches en cours d'exécution. Lorsque toutes les tâches sont terminées, ce nombre disparaît.

Dans le panneau Tâches, vous pouvez :

- Afficher et trier les tâches
- Interrompre ou reprendre une tâche
- Annuler une tâche
- Supprimer une tâche
- Télécharger une tâche

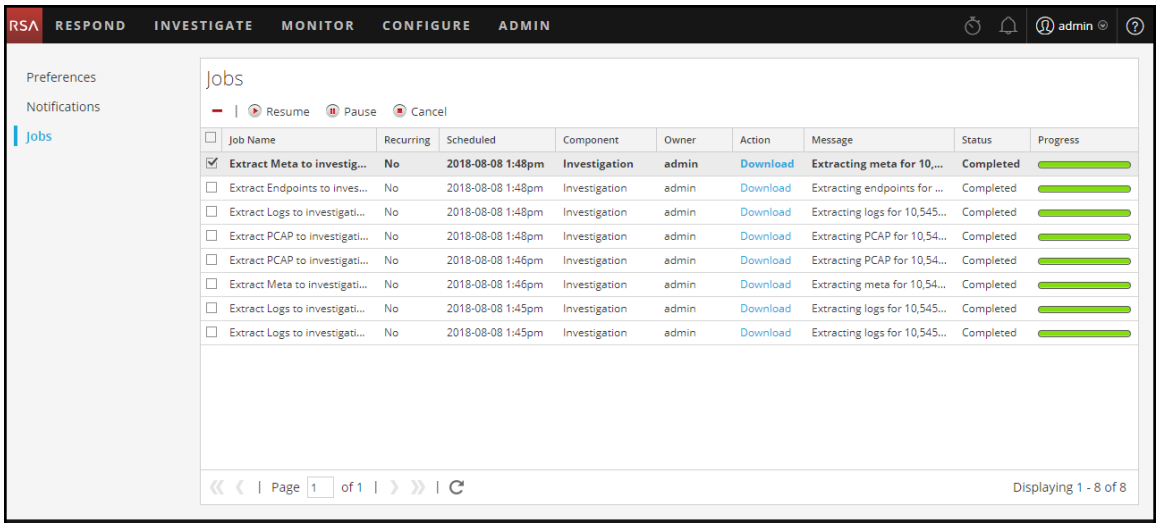
La structure du panneau des tâches est la même dans toutes les vues.

Que voulez-vous faire ?

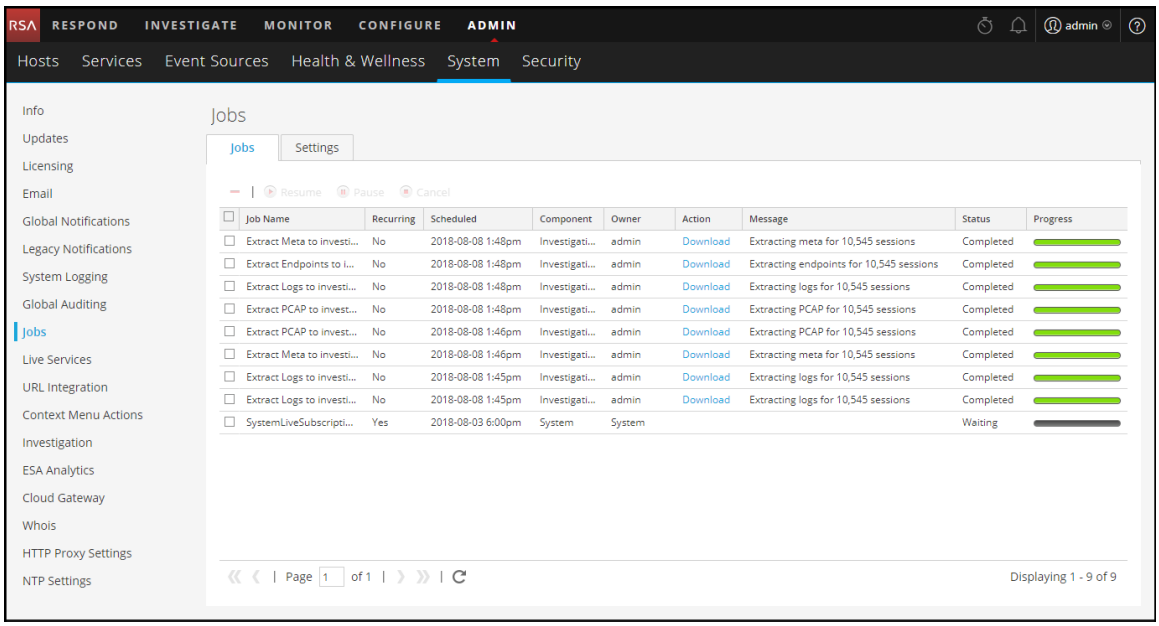
Rôle	Je souhaite...	Me montrer comment
Tout	Suspendre et reprendre une tâche planifiée	Gestion des tâches
Tout	Annuler ou supprimer une tâche	Gestion des tâches
	Télécharger une tâche	Gestion des tâches

Pour accéder aux panneau Tâches, procédez de l'une des façons suivantes :

- Dans le coin supérieur droit de la fenêtre du navigateur NetWitness Platform, sélectionnez  > **Profil**, puis dans le panneau Options de la boîte de dialogue Préférences, sélectionnez **Tâches**. Le panneau Tâches s'affiche : Il montre les tâches d'un utilisateur particulier.

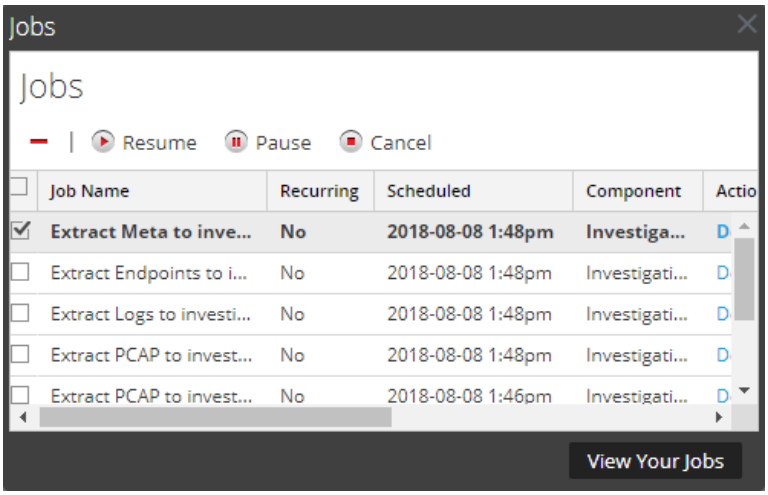


- Accédez à **ADMIN > Système**, puis sélectionnez **Tâches** dans le panneau des options.Le panneau Tâches dans la vue Système d'administration s'affiche. Il montre les tâches pour tous les utilisateurs.



Le panneau Tâches organise les informations relatives aux tâches sous la forme d'une liste. Les colonnes contiennent une barre de progression de la tâche, le nom de la tâche, indiquent si la tâche est récurrente ou non, le composant NetWitness Platform qui contrôle la tâche, le propriétaire de la tâche, l'état, tout message associé, ainsi qu'un bouton pour télécharger les fichiers de capture de paquets d'une tâche ou les fichiers de charge utile.

Pour afficher la barre d'état Tâches, cliquez sur l'icône **Tâches**.



La barre d'état Tâches répertorie toutes les tâches dont vous êtes propriétaire, récurrentes ou non, à l'aide d'un sous-ensemble de colonnes disponibles dans le panneau **Tâches**. Sinon, la barre d'état Tâches et le panneau Tâches du profil sont identiques. Dans la vue Système d'administration, le panneau Tâches répertorie des informations sur toutes les tâches NetWitness Platform pour tous les utilisateurs.

Le tableau suivant décrit les options disponibles du panneau Tâches.

Option	Description
Resume	L'option Reprendre s'applique uniquement aux tâches récurrentes qui ont été suspendues. Lorsque vous reprenez une tâche suspendue, l'exécution suivante de la tâche se déroule comme planifié.
Pause	L'option Suspendre ne s'applique qu'aux tâches récurrentes. Lorsque vous suspendez une tâche récurrente, cela n'a aucun effet sur cette exécution. L'exécution suivante (en supposant que la tâche est toujours suspendue) est ignorée.
Cancel	Annule une tâche récurrente ou non récurrente. Vous pouvez annuler une tâche en cours d'exécution. Si vous annulez une tâche récurrente, cela annule cette exécution de la tâche. Lors de l'occurrence planifiée suivante de la tâche, elle s'exécute normalement.
—	Supprime une tâche récurrente ou non récurrente du panneau Tâches. Lorsque vous supprimez une tâche, elle est instantanément supprimée du panneau Tâches. Aucune boîte de dialogue de confirmation n'est proposée. Si vous supprimez une tâche récurrente, toutes les exécutions futures sont également supprimées.

Le tableau suivant décrit les fonctions de la barre d'état Tâches et de la colonne du panneau Tâches.

Fonctionnalité	Description
Boîte de sélection	Permet de sélectionner une ou plusieurs tâches.
Nom de la tâche	Affiche le nom de la tâche, par exemple, **Extraire des fichiers** ou **Service de mise à niveau**.
Recurring	Indique si la tâche est récurrente ou non récurrente. **Oui** = récurrent, **Non** = non récurrent.
Planifiée	Indique la date et l'heure auxquelles la tâche a été planifiée pour démarrer.
Composant	Désigne le composant d'origine de la tâche, par exemple, **Procédure d'enquête** ou **Administration**.
Propriétaire	Indique le propriétaire de la tâche. Le propriétaire de la tâche n'est pas inclus dans la **barre d'état Tâches**, car seules les tâches de l'utilisateur actuel s'affichent ici. La colonne peut être ajoutée.
Action	Affiche la tâche dans une autre vue ou télécharge les fichiers de la tâche dans le répertoire **Téléchargements** sur le système local. Seules les tâches complètement terminées disposent d'un lien **Vue** dans la colonne **Action**. Seules les tâches qui créent un fichier disposent d'un lien **Télécharger** dans la colonne **Action**.
Message	Affiche des informations complémentaires concernant la tâche, par exemple, **Extraire des fichiers** ou **Sessions introuvables**.
État	Indique l'état de la tâche. Les valeurs d'état communes sont **Interrompu**, **Exécuté**, **Annulé**, **En échec**, **Terminé**, mais d'autres valeurs sont également disponibles.
Progress	Affiche le pourcentage d'exécution d'une tâche.
Consultez vos tâches	(Plateau de tâches uniquement) Affiche vos tâches dans le panneau **Tâches.**