RSA NETWITNESS® SUITE

Guide de gestion de la confidentialité des données

pour la version 11.0

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, de la documentation produit, des discussions communautaires et la gestion de dossiers.

Marques commerciales

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

Contrat de licence

Ce logiciel et la documentation qui l'accompagne sont la propriété d'EMC et considérés comme confidentiels. Délivrés sous licence, ils ne peuvent être utilisés et copiés que conformément aux modalités de ladite licence et moyennant l'inclusion de la note de copyright ci-dessous. Ce logiciel et sa documentation, y compris toute copie éventuelle, ne peuvent pas être remis ou mis de quelque façon que ce soit à la disposition d'un tiers.

Aucun droit ou titre de propriété sur le logiciel ou sa documentation ni aucun droit de propriété intellectuelle ne vous est cédé par la présente. Toute utilisation ou reproduction non autorisée de ce logiciel et de sa documentation peut faire l'objet de poursuites civiles et/ou pénales.

Ce logiciel est modifiable sans préavis et ne doit nullement être interprété comme un engagement de la part d'EMC.

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

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

février 2018

Sommaire

Présentation de la protection des données

Cette rubrique présente aux responsables de la confidentialité des données et aux administrateurs qui gèrent l'exposition des données confidentielles dans RSA NetWitness® Suite , le concept et les considérations liées à l'implémentation de la confidentialité. En outre, elle comprend des informations et des cas d'utilisation recommandés.

Remarque : Un plan de confidentialité des données touche la plupart des composants de NetWitness Suite. La personne qui configure la confidentialité des données doit comprendre les composants réseau de NetWitness Suite, la configuration des hôtes et services NetWitness Suite présentée dans le *Guide de mise en route de l'hôte et des services*, et les types d'informations qui requièrent une protection.

Dans certaines zones comme l'Union européenne, la réglementation impose que les systèmes d'information disposent de moyens de protection des données confidentielles. Toutes les données pouvant décrire directement ou indirectement « Qui a fait quoi, et quand ? » peuvent être considérées comme des données confidentielles. Les noms d'utilisateur, adresses e-mail et noms d'hôte en sont des exemples. NetWitness Suite fournit une gamme de contrôles dont les clients peuvent tirer le meilleur parti pour protéger les données sensibles et confidentielles. Ces contrôles peuvent être associés de différentes façons pour protéger les données confidentielles sans réduire de manière significative la fonction analytique.

Le rôle d'utilisateur intitulé Responsable de la confidentialité des données (DPO, Data Privacy Officer) a été ajouté à NetWitness Suite 10.5 pour prendre en charge la gestion des données confidentielles. Il peut configurer NetWitness Suite pour limiter l'exposition des métadonnées et du contenu brut (paquets et logs) en associant différentes techniques. Les méthodes disponibles pour protéger les données dans NetWitness Suite comprennent les éléments suivants :

- Obfuscation des données
- Application de la rétention des données
- Consignation des audits

Obfuscation des données

NetWitness Suite propose des options configurables pour l'obfuscation des données. Les Responsables de la confidentialité des données peuvent signaler les clés méta considérées comme confidentielles dans leur environnement, et limiter les emplacements où ces métavaleurs et données brutes s'affichent sur le réseau NetWitness Suite. À la place des valeurs d'origine, NetWitness Suite fournit des représentations obfusquées afin de permettre les procédures d'enquête et l'analytique. En outre, les Responsables de la confidentialité des données et les administrateurs sont en mesure d'empêcher la persistance des métavaleurs confidentielles et des paquets ou logs bruts.

Trois méthodes collaborent pour implémenter l'obfuscation des données :

- Obfuscation des métavaleurs pour les clés méta confidentielles avec valeur salt en option. Les clés méta dont la protection est configurée sont représentées par des valeurs obfusquées au moment de la création sur Decoder ou Log Decoder. Les valeurs obfusquées sont hachées et considérées comme impossibles à lire. Pour l'implémentation, vous devez configurer l'algorithme de hachage et la valeur salt de Decoder et Log Decoder, et configurer les clés de langue confidentielles comme étant protégées dans tous les services Core.
- L'accès basé sur les rôles (RBAC) aux paquets et logs bruts et aux métavaleurs confidentielles. Le Responsable de la confidentialité des données peut utiliser des rôles avec des fonctions d'autorisation granulaire pour restreindre les données affichées par les analystes au cours de la configuration, de l'analyse et des procédures d'enquête. Le *Guide de la sécurité du système et de la gestion des utilisateurs* couvre de manière détaillée l'implémentation RBAC dans NetWitness Suite. Pour l'implémentation, vous devez configurer la visibilité du contenu et des méta par rôle sur les différents modules Broker, Concentrator, Decoder, Log Decoder et Archiver.
- Prévention de la persistance des métavaleurs confidentielles et des paquets et logs bruts. Pour l'implémentation, vous devez configurer les clés méta sur les parsers comme étant transitoires pour les différents Decoders et Log Decoders.

Application de la rétention des données

NetWitness Suite peut s'assurer que les données sont conservées aussi longtemps que nécessaire ou le temps indiqué. Un administrateur peut configurer la rétention de données à l'aide de seuils d'âge et de temps ou bien par service. Les planificateurs fonctionnant sur chaque service suppriment automatiquement les données qui atteignent ces seuils. Une fois que les données sont supprimées, elles ne sont plus disponibles via les interfaces utilisateur, les requêtes ou les appels API (Application Programming Interface). Certains composants NetWitness Suite prennent également en charge la purge de données par le biais de leur remplacement.

Un administrateur peut gérer la rétention de données de différentes façons :

- Configurer la durée de persistance des données dans le stockage sur le système.
- Pour les services Core, supprimer de manière stratégique les données confidentielles qui pourraient s'y trouver en configurant la suppression automatique des données d'un âge spécifique.
- Configurer NetWitness Suite de façon à ce que les données d'origine ne soient pas envoyées ou enregistrées vers les autres composants. Si des données confidentielles se retrouvent dans

une autre base de données des serveurs Reporting Engine, Malware Analysis et Serveur NetWitness, la rétention de données peut aussi s'appliquer à ces emplacements. Pour Event Stream Analysis, cette configuration est gérée dans la vue Explorer les services.

Remarque : Si le Responsable de la confidentialité des données décide que des données déjà collectées sont confidentielles après la disponibilité du système, l'administrateur peut remplacer manuellement les données dans les bases de données ou fichiers où les données sont enregistrées.

Consignation des audits

Les administrateurs peuvent tirer parti des logs d'audit créés par NetWitness Suite à l'aide de la fonction de Consignation globale des audits. La fonction de consignation des audits génère des entrées de log d'audit sur de nombreuses activités, et voici des exemples d'entrées de log liées à la confidentialité des données :

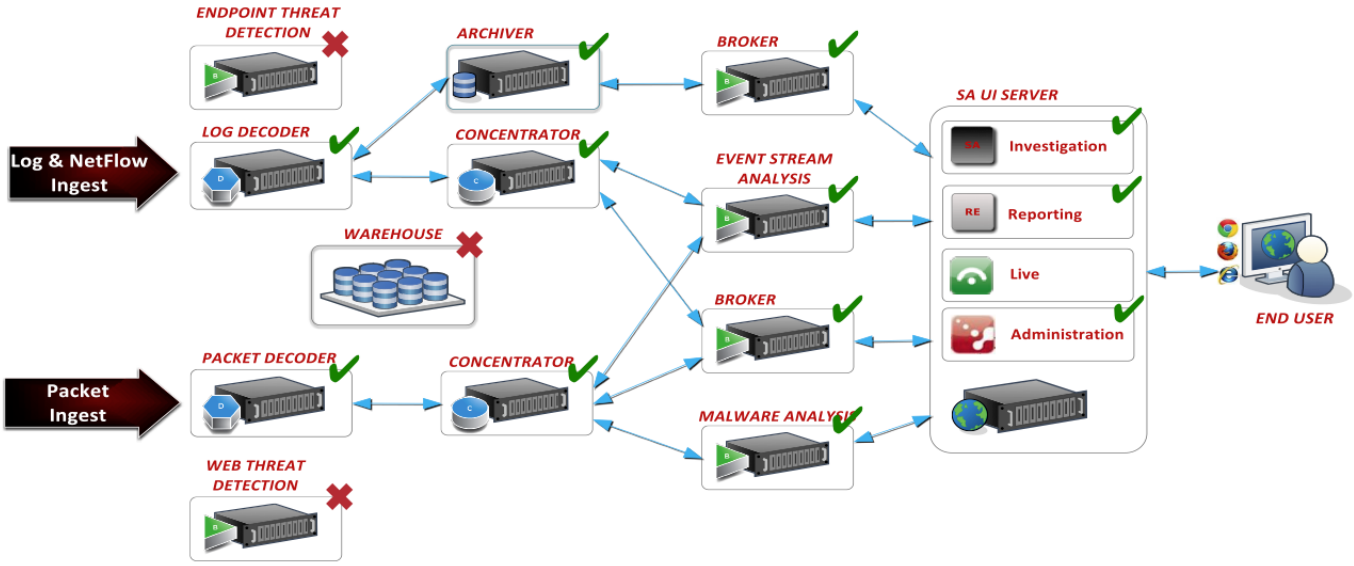
- Modifications des autorisations et utilisateurs attribués à des rôles
- Tentatives réussies et échecs de connexion à NetWitness Suite, et déconnexions
- Suppression de données
- Exportations et téléchargements de données
- Navigation des utilisateurs vers les interfaces utilisateurs et requêtes réalisées par les utilisateurs
- Tentatives (réussies ou non) d'afficher ou de modifier des données confidentielles, y compris l'identification de leur auteur.

Toutes les entrées de log font partie d'une piste d'audit standard pour NetWitness Suite. Les administrateurs peuvent configurer NetWitness Suite pour transférer les logs d'audit vers une destination précise, y compris des systèmes tiers, afin de proposer des fonctions supplémentaires de filtrage et de reporting. Pour plus d'informations sur la consignation globale des audits, reportez-vous à la section **Configurer la consignation globale des audits** dans le *Guide de configuration système*.

Composants couverts par la fonction de confidentialité des données

La figure ci-dessous identifie les composants NetWitness Suite couverts par la fonction de confidentialité des données de la version 10.5 ou ultérieure à l'aide d'une coche verte. Les composants marqués d'une X ne sont pas pris en charge par la fonction de confidentialité des données. Le *Guide de mise en route NetWitness Suite* propose une description fonctionnelle des composants de NetWitness Suite.

Remarque : Les fonctions de confidentialité des données NetWitness Suite ne sont pas prises en charge pour Warehouse et les métadonnées protégées peuvent parvenir à Warehouse via Warehouse Connector, à moins que le filtrage ne soit explicitement configuré grâce aux métafiltres de Warehouse Connector. Si des métadonnées protégées parviennent à Warehouse, les utilisateurs ayant un accès direct à Warehouse peuvent envoyer des requêtes sur ces données. Les Responsables de la confidentialité des données doivent empêcher cela par le biais de contrôles administratifs, techniques et procéduraux en dehors de NetWitness Suite.



Implémentation de la fonction de confidentialité des données par composant

Le tableau suivant identifie les fonctions de confidentialité des données pour chaque composant NetWitness Suite. Pour chaque composant, une coche indique si le composant prend en charge l'obfuscation de données, l'application de la rétention de données, le remplacement des données et la consignation des audits.

Composant	Obfuscation des données	Application de la rétention des données	Remplacement des données	Consignation des audits
Ingestion				
Decoder	√	√	√	√
Log Decoder	√	√	√	√
Agrégation des métadonnées				
Concentrator	√	√	√	√
Broker	s.o.	√ (stockage dans le cache DPO uniquement)[1]		√
Analyse en temps réel				
Investigation	√	√ (stockage dans le cache DPO uniquement)[2]		√
Event Stream Analysis	√			√
Malware Analysis	√	√		√
Respond	√	√		√
Reporting				

Composant	Obfuscation des données	Application de la rétention des données	Remplacement des données	Consignation des audits
Reporting Engine	√	√		√
Analyse à long terme				
Archiver	√	√	√ (sans compression)[3]	√
Warehouse				

Remarques :
1 - Les Brokers peuvent mettre les données en cache mais celui-ci doit être vidé en configurant un transfert indépendant et d'autres suppressions de cache si nécessaire. L'administrateur peut configurer le transfert de cache pour un Broker à l'aide du planificateur dans l'onglet Fichiers de la vue Configuration des services.
2 - La procédure d'enquête et le serveur Serveur NetWitness placent des données dans le cache, qui sont effacées automatiquement toutes les 24 heures.
3 - La procédure de remplacement décrite dans la rubrique Configurer la rétention de données s'applique aux données non compressées.

Instructions de configuration spécifiques aux composants

Les composants et modules NetWitness Suite ayant accès aux métadonnées confidentielles et leurs correspondances obfusquées sont Investigation, Event Stream Analysis (ESA), Malware Analysis, Respond et Reports. Elles obtiennent l'accès aux données en fonction des autorisations définies pour le rôle auquel appartient l'utilisateur. L'administrateur ou le Responsable de la confidentialité des données configure chaque Decoder ou Log Decoder pour identifier les métaclés signalées pour l'obfuscation.

Ces composants disposent d'instructions supplémentaires pour s'assurer qu'elles fonctionnent comme prévu avec un plan de confidentialité des données :

- **Event Stream Analysis**. Lorsqu'ESA reçoit des données confidentielles de NetWitness Suite Core, ESA ne transmet que la version obfusquée des données. ESA ne stocke pas ou n'affiche pas les données protégées. Il existe des instructions supplémentaires pour la configuration de

règles EPL avancées et les sources d'enrichissement (décrites dans la section **Données sensibles** du guide *Alertes basées sur ESA*). Accédez à la Table des matières principale pour la version 11.0 trouver des documents NetWitness Suite 11.0.

- **Malware Analysis**. Malware Analysis référence certaines clés méta pendant la notation, y compris `alias.host`, `client` et bien d'autres. Pour éviter toute perte de fonctionnalité analytique, Malware Analysis doit être configuré comme un client de confiance, c'est-à-dire configuré pour se connecter à l'infrastructure NetWitness Suite Core avec un compte équivalent à celui d'un utilisateur de rôle Responsable de la confidentialité des données. Sinon, si les clés méta référencées par Malware Analysis sont balisées pour l'obfuscation et ne sont pas accessibles par Malware Analysis, certains indicateurs de compromission (IOC) peuvent être rendus inefficaces.
- **Service du serveur Respond.** Service du serveur Respond utilise un fichier de mappage de confidentialité des données pour afficher les données obfusquées dans les alertes (consultez la section **Obfusquer les données privées** dans le *Guide de l'utilisateur Respond* et il dispose d'une période de rétention de données configurable pour les alertes (consultez la section **Définir une période de rétention pour les alertes et les incidents** dans le *Guide de l'utilisateur Respond*). Accédez à la Table des matières principale pour la version 11.0 trouver des documents NetWitness Suite 11.0.
- **Rapports.** Dans Reporting Engine, chaque service Core est ajouté comme deux sources de données séparées, avec deux comptes de services séparés : une source de données dispose d'un compte de service représentant le rôle de Responsable de la confidentialité des données, et l'autre source de données dispose d'un compte de service représentant un rôle autre que celui du Responsable de la confidentialité des données. La section **Configurer la confidentialité des données pour le Reporting Engine** dans le *Guide de configuration de Reporting Engine* comporte les procédures de configuration de la confidentialité des données pour Reporting Engine. Accédez à la Table des matières principale pour la version 11.0 trouver des documents NetWitness Suite 11.0.

Configurations recommandées

Cette rubrique décrit la mise en œuvre recommandée pour la confidentialité des données pour NetWitness Suite. En outre, elle présente plusieurs exemples d'utilisation supplémentaires pour gérer l'exposition des données sensibles/confidentielles dans NetWitness Suite. Les administrateurs peuvent configurer les hôtes et services NetWitness Suite en réponse aux exigences de confidentialité des données de leur environnement. RSA dispose de configurations recommandées pour la confidentialité des données et la rétention de données.

Configuration recommandée pour la confidentialité des données

La configuration recommandée pour obtenir la meilleure valeur analytique avec obfuscation des données consiste à définir les métadonnées sensibles/confidentielles, puis à conserver les valeurs d'origine et obfusquées (hachage) des données sensibles/confidentielles sur disque pour les composants Decoder, Log Decoder, Concentrator et Broker.

Il est supposé qu'une petite partie des métadonnées (environ 10 clés méta) est classée comme protégée, et qu'un algorithme de hachage compatible FIPS 140 est utilisé avec une valeur salt pour compliquer l'ingénierie inverse de la valeur d'origine. La solution préconisée consiste à utiliser un algorithme de hachage SHA256 avec une valeur salt dont la longueur est comprise entre 16 et 60 caractères.

Remarque : Par défaut, les valeurs de hachage sont stockées au format binaire pour réduire les temps de réponse. En outre, ce format nécessite moins d'espace de stockage dans la base de données que l'enregistrement au format chaîne. Le format texte/chaîne correspond à la méthode de stockage recommandée.

Broker et Investigation peuvent comporter des données d'origine obfusquées dans le cache, si des responsables de la confidentialité des données se servent d'Investigation pour confirmer la valeur d'origine à laquelle est mappée la valeur obfusquée pendant les procédures d'enquête. Des services en aval peuvent également limiter l'utilisation des valeurs sensibles d'origine au traitement en mémoire afin que les données ne soient pas conservées sur disque sur les systèmes en aval. Cela est vérifié pour ESA et Malware Analysis.

La solution recommandée pour supprimer les données nécessaires repose sur l'application automatique et intégrée de la rétention de données, car elle entraîne la suppression des données à un certain seuil. Vous pouvez utiliser cette méthode pour les composants suivants dans NetWitness Suite 10.5 : Decoder, Log Decoder, Log Collector, Archiver, Malware Analysis, Incident Management et Reporting Engine. Vous pouvez configurer manuellement Event Stream Analysis afin qu'il prenne en charge de manière similaire l'application automatique de la rétention de données.

Pour gérer le stockage du cache, le serveur Serveur NetWitness efface le cache relatif aux procédures d'enquête des événements, toutes les 24 heures. Vous pouvez également configurer le composant Broker pour exécuter une suppression périodique du cache stocké localement.

Options relatives aux configurations de rétention de données

NetWitness Suite fournit des contrôles alternatifs qui permettent à l'administrateur d'appliquer des restrictions plus strictes au stockage des données sensibles/confidentielles lorsque l'obscurcissement des données est activé.

Stockage des données avec options de rétention de données en vigueur

Le tableau suivant résume l'emplacement de stockage des données dans la configuration par défaut en l'absence de confidentialité des données, et pour chaque solution alternative de rétention de données. Une coche indique que les données sensibles/confidentielles sont enregistrées dans le composant. Une croix (X) indique qu'aucune donnée sensible/confidentielle n'est stockée dans le composant.

Composant	Configuration par défaut	Options de stockage des données		
	Stockage des données d'origine	Stockage des données d'origine et du hachage (recommandé)	Stockage du hachage uniquement	Aucun stockage des données (toutes les métadonnées sont transitoires)
Réception				
Décoder	√	√	X	X
Log Decoder	√	√	X	X
Agrégation des métadonnées				
Concentrator	√	√	X	X

Composant	Configuration par défaut	Options de stockage des données		
	Stockage des données d'origine	Stockage des données d'origine et du hachage (recommandé)	Stockage du hachage uniquement	Aucun stockage des données (toutes les métadonnées sont transitoires)
Broker	√ (Cache uniquement)	√ (Cache uniquement)	X	X
Analyse en temps réel				
Procédure d'enquête	√	√ (Cache uniquement)	X	X
Event Stream Analysis	√	X	X	X
Malware Analysis	√	X	X	X
Service du serveur Respond	√	X	X	X
Reporting				
Reporting Engine	√	√ (Facultatif)	X	X
Analyse à long terme				

Composant	Configuration par défaut	Options de stockage des données		
	Stockage des données d'origine	Stockage des données d'origine et du hachage (recommandé)	Stockage du hachage uniquement	Aucun stockage des données (toutes les métadonnées sont transitoires)
Archiver	√ (Facultatif)	√ (Facultatif)	X	X
Warehouse	√ (Facultatif)	√ (Facultatif)	X	X
Contenu				
Live	s.o.	s.o.	s.o.	s.o.
Analyse des fraudes				
RSA Fraud and Risk Intelligence Suite	s.o.	s.o.	s.o.	s.o.
End Point Protection				
NetWitness Endpoint	s.o.	s.o.	s.o.	s.o.

Composant	Configuration par défaut	Options de stockage des données		
	Stockage des données d'origine	Stockage des données d'origine et du hachage (recommandé)	Stockage du hachage uniquement	Aucun stockage des données (toutes les métadonnées sont transitoires)

Remarques :

La mention « Cache uniquement » signifie que les données sensibles se trouvent dans le cache du serveur Broker ou Serveur NetWitness. La rubrique Configurer la rétention de données fournit des informations détaillées sur le nettoyage automatisé et manuel du cache.

La mention « Facultatif » signifie qu'il existe effectivement un stockage des données sensibles, mais qu'il peut être limité par des configurations facultatives. Par exemple, pour limiter l'emplacement de stockage des données sensibles, n'activez pas l'accès DPO pour Reporting, et n'agrégez pas les données protégées d'origine dans Archiver.

Option 1 : aucun enregistrement des données d'origine sur disque, stockage du hachage uniquement

Les administrateurs peuvent éliminer la persistance des données sensibles sur disque, et stocker uniquement une valeur obfusquée si le risque d'exposition est trop important. Dans ce scénario, les métadonnées générées durant l'analyse dans les composants Decoder et Log Decoder sont utilisées uniquement en mémoire. Elles ne sont pas écrites sur disque. Les administrateurs peuvent configurer chaque clé méta sur un Decoder ou Log Decoder transitoire pour s'assurer que les métadonnées sensibles ne sont pas écrites sur le disque. Les services en aval ne voient pas les valeurs d'origine. Ils doivent utiliser les valeurs obfusquées pour mener les procédures d'enquête et effectuer l'analytique.

Pour configurer ce modèle de confidentialité des données, l'obfuscation des données doit être activée avec des valeurs de hachage configurées. Vous pouvez configurer chaque clé méta sur un Decoder ou Log Decoder transitoire pour vous assurer que les valeurs d'origine ne sont pas écrites sur disque.

- Les valeurs d'origine identifiées comme sensibles sont extraites des données brutes lors de l'analyse dans le Decoder et Log Decoder et sont accessibles sur le système lors de l'analyse (parsers, règles, feeds).
- Le Decoder n'enregistre pas les valeurs d'origine des clés méta identifiées comme sensibles. Il stocke uniquement le hachage des valeurs d'origine avec d'autres métadonnées non sensibles relatives à l'événement.

Ces options ont un effet secondaire, elles entraînent une dégradation de la capacité analytique. Toutefois, vous pouvez les configurer pour répondre aux besoins de votre environnement.

- En configurant toutes données sensibles en mode Transitoire, ces valeurs sensibles ne sont pas conservées en permanence sur le disque, et les fonctionnalités d'analyse utilisant la valeur d'origine ne sont disponibles qu'au moment de l'analyse (parsers, règles, feeds).
- Les systèmes Event Stream Analysis (ESA) et Malware Analysis doivent s'appuyer sur les métavaleurs obfusquées lors de leurs opérations respectives de mise en corrélation et d'attribution de score.
- Reporting Engine se limite à l'extraction de rapports à l'aide des valeurs non sensibles et non obfusquées.
- Le responsable de la confidentialité des données ne peut pas visualiser la valeur d'origine. Toutefois, il peut utiliser la valeur de hachage et la valeur salt configurées pour déterminer si une valeur obfusquée représente une valeur d'origine spécifique connue.

Option 2 : aucun stockage des valeurs d'origine ou des valeurs obfusquées (non recommandé)

Les administrateurs peuvent éliminer complètement la persistance de la valeur d'origine sur disque si le risque d'exposition est trop important. Comme pour l'option 1, dans ce scénario, les métadonnées générées durant l'analyse dans les composants Decoder et Log Decoder sont utilisées uniquement en mémoire. Elles ne sont pas écrites sur disque. Les administrateurs peuvent configurer chaque clé méta sur un Decoder ou Log Decoder transitoire pour s'assurer que les métadonnées sensibles ne sont pas écrites sur le disque. Les services en aval ne voient pas les valeurs d'origine, et ne disposent pas de valeurs obfusquées pour mener les procédures d'enquête et effectuer l'analytique.

Pour configurer ce modèle de confidentialité des données, configurez chaque clé méta sur un Decoder ou Log Decoder transitoire afin de vous assurer que les valeurs d'origine ne sont pas écrites sur disque.

- Les valeurs d'origine identifiées comme sensibles sont extraites des données brutes lors de l'analyse dans le Decoder et Log Decoder et sont accessibles sur le système lors de l'analyse

(parsers, règles, feeds).

- Le Decoder n'enregistre pas les valeurs d'origine des clés méta identifiées comme sensibles. Il stocke uniquement les métadonnées non sensibles relatives à l'événement.

Ces options ont un effet secondaire, elles entraînent une dégradation très importante de la capacité analytique. Toutefois, vous pouvez les configurer pour répondre aux besoins de votre environnement.

- En configurant toutes données sensibles en mode Transitoire, ces valeurs sensibles ne sont pas conservées en permanence sur le disque, et les fonctionnalités d'analyse utilisant la valeur d'origine ne sont disponibles qu'au moment de l'analyse (parsers, règles, feeds). Consultez Configurer la rétention de données.
- Aucun des composants en aval n'a de visibilité des valeurs d'origine, obfusquées ou non.
- Le responsable de la confidentialité des données n'a aucune visibilité des valeurs d'origine, obfusquées ou non.

Options de remplacement des données facultatives

Plusieurs options de remplacement des données sont disponibles, et vous devez comprendre entièrement chacune d'elles avant la mise en œuvre du remplacement des données.

Option 1 : Limiter l'espace disque pour le remplacement continu des anciennes données

Si vous connaissez la période souhaitée de rétention de données pour le stockage des données, et par conséquent l'espace de stockage requis pour ces données, vous pouvez utiliser cette information pour limiter la taille du matériel sous-jacent ou de la partition correspondante. En réduisant l'espace de stockage du disque dur ou la taille de la partition, vous limitez également la quantité d'espace disponible à remplir avant qu'il ne soit remplacé par de nouvelles données. Les nouvelles données reçues remplacent en permanence les données plus anciennes. Chaque solution doit être mise en place au moment du déploiement pour être efficace.

Les effets secondaires de cette option sont les suivants :

- La suppression de certains disques limite le nombre de ressources disponibles pour la distribution des E/S, ce qui entraîne une dégradation des performances.
- La réduction de la taille de la partition peut entraîner une dégradation des performances. Toutefois, cela atténue en partie l'impact sur les performances que représente la suppression des disques.

Option 2 : utiliser le stockage hiérarchisé pour remplacer les données de manière planifiée

S'il s'avère nécessaire de remplacer les données de manière automatique et planifiée, configurez les composants Decoder et Concentrator pour utiliser le stockage hiérarchisé. La configuration du stockage hiérarchisé fournit un mécanisme qui appelle un script après la suppression d'un fichier de base de données de l'application, mais avant sa suppression du système de fichiers. Si nécessaire, au lieu de déplacer le fichier vers le deuxième niveau, ou stockage à froid (données peu actives), qui est la fonction prévue dans l'exemple d'utilisation d'un stockage hiérarchisé, le script peut faire appel à un utilitaire de destruction tel que `shred` de CentOS pour remplacer le fichier. Cet outil est moins efficace lorsque la base de données est stockée sur un système de fichiers de consignation comme XFS, où réside la base de données Core, et sur un disque logique RAID similaire à ceux auxquels se connectent les hôtes Core.

La plupart des autres composants NetWitness Suite ne disposent pas de cette option. Leurs données sont stockées dans une base de données qui ne prend pas en charge le mécanisme de stockage hiérarchisé. Le seul autre composant qui peut utiliser cette méthode de remplacement est Reporting Engine, car il enregistre les rapports et les alertes sous forme de fichiers individuels. Toutefois, comme les graphiques Reporting Engine sont stockés dans une base de données, ils ne sont pas impactés par cette technique.

Option 3 : purger les données via l'option de rédaction de chaînes et de modèles

La purge des données fournit un mécanisme qui remplace de manière stratégique un sous-ensemble spécifique de données du système en cas de persistance des données sensibles, volontairement ou par accident. L'utilitaire NetWitness Suite `wipe` permet d'écrire des modèles uniques sur les données des bases de données des métadonnées et des paquets pour les services Core, qui peuvent contenir des paquets ou des logs RAW de sessions actives, en fonction d'un identifiant de session. Tous les composants Core sont capables de remplacer un sousensemble de données trouvé via l'exécution d'une chaîne de requête, notamment les modèles regex. Les identifiants de session résultant de la requête sont fournis à l'utilitaire NetWitness Suite wipe.

Remarque : Cette option n'est pas disponible si les données de la base de données Core ont été compressées (ce qui est habituellement le cas dans les déploiements Archiver).

Dans la plupart des composants NetWitness Suite, la base de données utilisée ne fournit pas de mécanisme intégré de rédaction ou de suppression sécurisée. Le composant Malware Analysis peut remplacer l'objet de données dans la base de données par la valeur `private` au lieu de le supprimer durant le processus de gestion de la rétention de données. Toutefois, cela ne constitue pas un mécanisme de suppression sécurisée.

Attention : L'utilisation de cette méthode sur un grand nombre de sessions a deux inconvénients : elle peut prendre beaucoup de temps et impacter les performances.

Limites du remplacement des données

Il existe des limites aux techniques de remplacement décrites dans le cadre des options 2 et 3. Pour permettre le remplacement des données des secteurs du disque, les options ci-dessus et l'outil en ligne de commande (`shred`, une fonction de CentOS), présentée comme une solution alternative, doivent reposer sur des hypothèses concernant la structure du disque. Les hôtes NetWitness Suite utilisent des disques SSD et des configurations RAID dans le but d'améliorer les performances et la fiabilité, et ceux-ci inhibent le fonctionnement des techniques de remplacement. Si les techniques de remplacement modifient les disques SSD et les configurations RAID dans le but d'améliorer la sécurité, il en résulte inévitablement un prix à payer au niveau des performances, notamment en matière de taux de réception, de vitesse des requêtes et éventuellement dans d'autres domaines. Les outils en ligne de commande permettant d'effectuer des remplacements sont recommandés uniquement pour des exemples d'utilisation particuliers, où il est nécessaire de masquer des données spécifiques. Les outils ne sont pas destinés à une méthode d'utilisation continue en temps réel, en raison de son impact potentiel sur les performances.

Procédures de démarrage rapide

Cette section fournit des instructions de bout en bout pour préparer la configuration des fonctions de confidentialité des données, puis terminer la configuration de la solution recommandée en la matière.

- Préparer la configuration de la protection des données
- Configurer la solution de protection des données recommandée

Préparer la configuration de la protection des données

Cette rubrique fournit des instructions générales pour planifier et configurer des règles de confidentialité des données sur le réseau NetWitness Suite. Avant de commencer la configuration, vous devez comprendre quelles données doivent être protégées sur votre réseau et développer un plan. Vous devrez :

1. Identifier les clés méta qui contiennent des données sensibles et doivent être protégées. Cette décision s'appuie sur les exigences spécifiques à votre site.
2. Décider de quels utilisateurs ont besoin d'accéder aux données méta sensibles et au contenu brut. La première décision consiste à déterminer s'il faut déparer les rôles de responsable de la confidentialité et d'administrateur pour votre site en configurant un rôle système d'administrateur personnalisé sur Decoder et Log Decoder et en supprimant l'autorisation `dpo.manage`. Par défaut, les administrateurs possèdent toutes les autorisations, comprenant la capacité à configurer la transformation de hachage salé utilisée pour obfusquer des données ; certains sites peuvent vouloir réserver cet accès aux responsables de la confidentialité. La section **Rôles et autorisations de l'utilisateur** dans le *Guide de mise en route des hôtes et des services* contient plus de détails sur les autorisations exactes que possède chaque rôle et l'objectif des autorisations.
3. Planifez les modifications de configuration que vous avez besoin d'apporter dans votre déploiement NetWitness Suite pour la prise en charge d'une confidentialité des données adéquate.
4. Évaluez la façon dont votre configuration peut impacter le contenu prêt à l'emploi et personnalisé. Par exemple, par défaut, le contenu disponible via Live for Reporting Engine n'est pas centré sur les valeurs méta obfusquées.

Dans un déploiement unique, certaines configurations sur la confidentialité des données dans les services Core doivent être identiques. Le tableau ci-dessous répertorie ces paramètres et utilise une coche pour identifier les services pour lesquels la configuration doit être identique.

	Configurez les mêmes éléments pour :				
Paramètre de confidentialité des données	**Decoder**	**Log Decoder**	**Archiver**	**Concentrator**	**Broker**
Algorithme de hachage et salé pour les données sensibles	√	√			
Attributs de confidentialité de données clés de langage dans le fichier d'index personnalisé (comprend la configuration des clés telles que protégées)	√	√	√	√	√
Clés méta transitoires (non persistantes sur le disque) par service et analyseur	√	√			

	Configurez les mêmes éléments pour :				
Paramètre de confidentialité des données	**Decoder**	**Log Decoder**	**Archiver**	**Concentrator**	**Broker**
Visibilité des données méta et du contenu brut par groupe d'utilisateurs du système. (Les clés méta doivent exister dans le fichier d'index personnalisé.)	√	√	√	√	√
L'utilisateur auquel est attribué le rôle d'utilisateur de service `Aggregation` est ajouté.*	√	√	√		

* Lors de la tentative d'accès aux données sur un service agrégé, le Log Collector ou le Broker demande l'authentification. Lorsque vous êtes invité à saisir le nom d'utilisateur et le mot de passe, vous devez vous authentifier en tant qu'utilisateur auquel est attribué le rôle de service `Aggregation`. La section **Rôle d'agrégation** dans le *Guide de mise en route des hôtes et des services* fournit des informations détaillées relatives à ce rôle. Suivez les instructions de la section **Ajouter, répliquer ou supprimer un utilisateur du service** dans le *Guide de mise en route des hôtes et des services* pour créer un utilisateur et attribuer le nouvel utilisateur du rôle d'utilisateur du service d'agrégation.

Configurer la solution de protection des données recommandée

Cette rubrique indique aux administrateurs et aux agents de protection des données comment configurer la solution de protection des données recommandée sur un réseau NetWitness Suite. Voici les étapes de base à suivre afin de configurer le système NetWitness Suite pour identifier les données sensibles et déterminer quelles sont les personnes autorisées à les visualiser. La configuration recommandée génère des valeurs obfusquées de certaines clés méta d'origine. Elle permet la persistance des données d'origine et des données obfusquées afin qu'elles soient à la disposition des utilisateurs auxquels un rôle d'accès privilégié a été attribué.

Cette configuration comporte plusieurs parties :

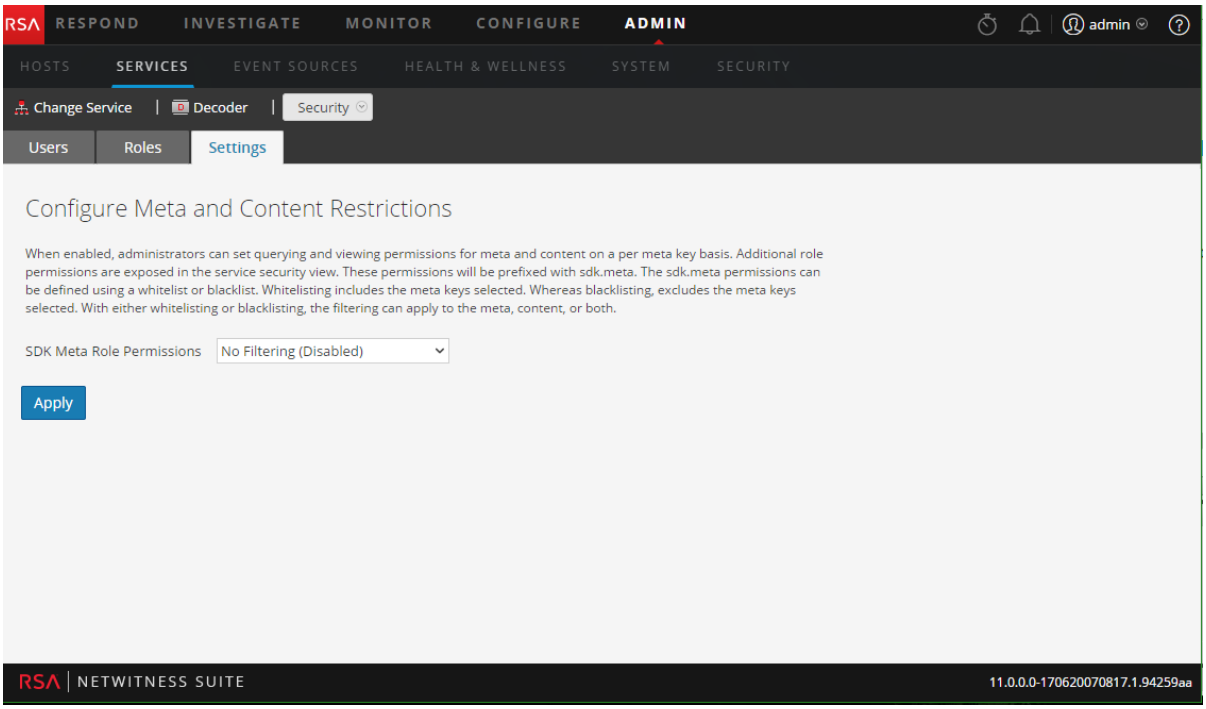
1. Créez deux utilisateurs avec des niveaux d'autorisation distincts. Un utilisateur (le responsable de la confidentialité des données) peut visualiser toutes les métadonnées, alors qu'un autre utilisateur (l'analyste) n'a pas l'autorisation d'afficher certaines métadonnées et certains contenus associés à des métadonnées.
2. Configurez deux transformations à l'aide d'une valeur salt et d'un hachage pour créer une version obfusquée des clés méta d'origine `username` et `ip.src`.
3. Configurer la rétention de données sur les services Decoder et Concentrator.

Remarque : Pour que vous puissiez effectuer cette procédure, les conditions suivantes doivent être remplies :
Concentrator et Decoder doivent être ajoutés au serveur Serveur NetWitness à l'aide de connexions approuvées.
La version Serveur NW doit être la version 10.5 ou supérieure.
La version des services Core doit être la version 10.5 ou une version supérieure.
L'agrégation doit utiliser des comptes d'agrégation sur tous les services Core.

Configurer les métadonnées et les restrictions de contenu sur les Brokers, Concentrators et Decoders

Pour limiter les métadonnées et le contenu brut visibles par les utilisateurs, activez les rôles système SDK afin d'effectuer des contrôles plus granulaires. Pour ce faire, configurez les restrictions relatives aux métadonnées et au contenu sur chaque service dans la vue Sécurité des services.

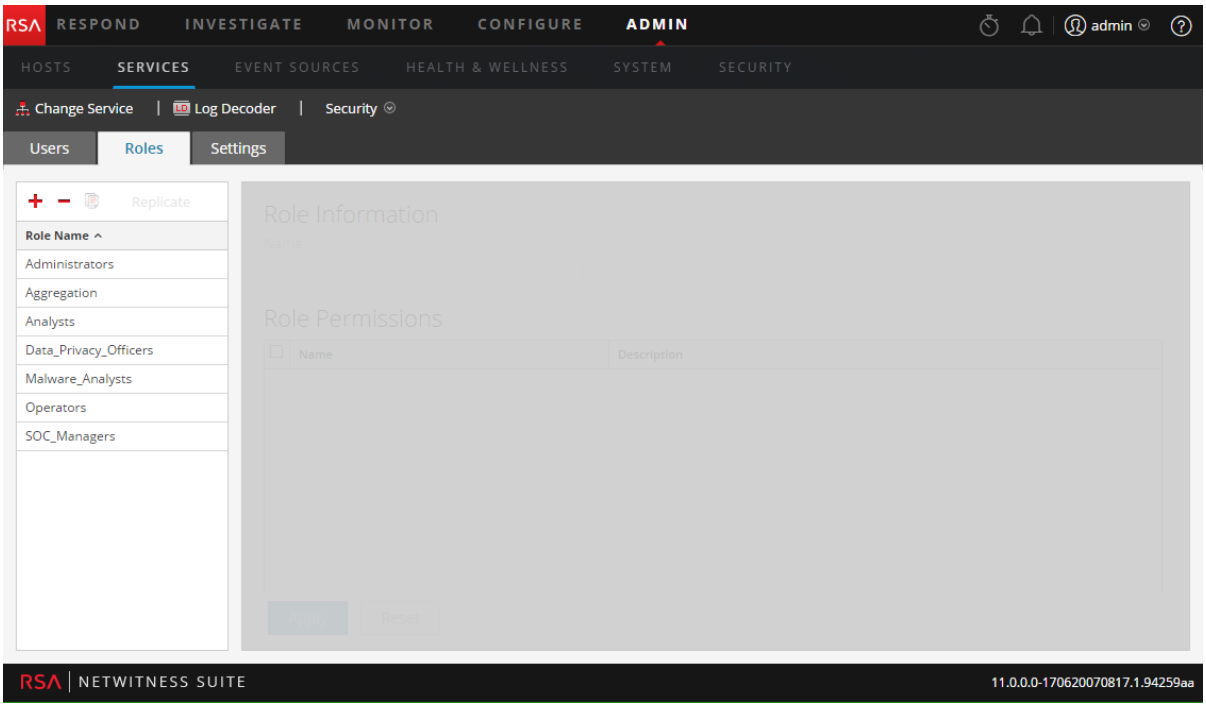
1. Dans la vue **Services d'administration**, sélectionnez un service, puis cliquez sur  > **Vue > Sécurité**.
2. Cliquez sur l'onglet **Paramètres**.



3. Dans le champ **Autorisations de rôle méta SDK**, sélectionnez **Liste noire méta et contenu**. Cliquez sur **Appliquer**.

   Cela permet à l'administrateur de mettre sur liste noire des clés méta individuelles afin que seul le responsable de la confidentialité des données puisse voir les clés méta et le contenu. Les nouveaux rôles de chaque clé méta sont ajoutés à l'onglet Rôles.

4. Cliquez sur l'onglet **Rôles**.



5. Sous l'onglet Rôles,

   a. Sélectionnez les clés méta que les analystes ne doivent pas voir. Par exemple, sélectionnez `sdk.meta.username` et `sdk.meta.ip.src`.

      Cela empêche l'analyste de voir les clés méta sensibles au niveau de la confidentialité, à savoir `username` et `ip.src`, ainsi que tous les contenus de sessions comprenant des métadonnées.

   b. Désélectionnez `sdk.packet`. Cela empêche l'analyste d'exporter en bloc les paquets et logs bruts.

   c. Cliquez sur **Appliquer**.

6. Sous l'onglet Rôles, vérifiez qu'aucune valeur sdk.meta n'est sélectionnée pour le rôle `Data_Privacy_Officers`. Cliquez sur **Appliquer**.

   Un responsable de la confidentialité des données peut afficher la totalité des métadonnées et des sessions.

   Dans l'onglet Rôles, vérifiez que le rôle `Aggregation` dispose des autorisations suivantes : sélectionnez `aggregate`,`sdk.content`, `sdk.meta` et `sdk.packets`..

Ajouter un compte d'analyste et d'agent de protection des données à Serveur NetWitness

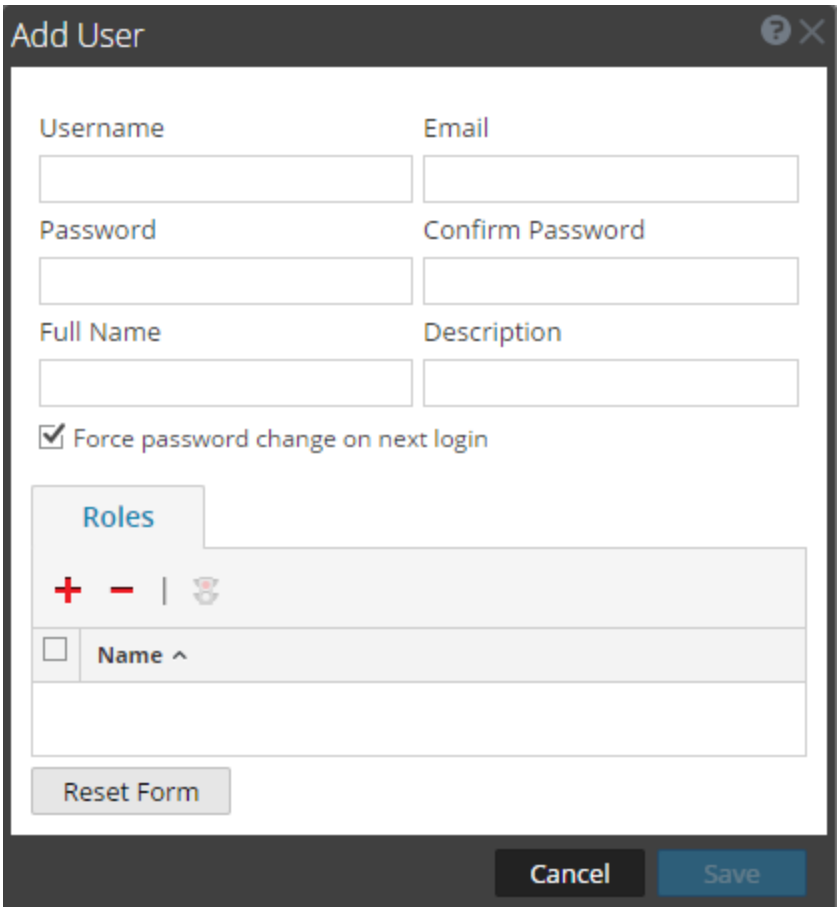
Vous devez ajouter deux nouveaux comptes utilisateur à NetWitness Suite au niveau système pour représenter un responsable de la confidentialité des données disposant de privilèges et un analyste classique. Si l'environnement est configuré à l'aide de connexions approuvées par défaut, vous n'avez pas besoin de créer les nouveaux comptes utilisateur sur les services Core (Brokers, Concentrators et Decoders). Lorsqu'un utilisateur est créé dans Serveur NetWitness, ce dernier peut se connecter aux services.

Remarque : Le nom du rôle est obligatoire pour le serveur et les services, il doit être identique pour les deux. Si vous créez un nouveau rôle personnalisé dans Serveur NetWitness, veillez à l'ajouter également à tous les services Core.

1. Créez un nouveau compte d'utilisateur pour l'agent de protection des données :

   a. Dans la vue **Sécurité des services**, sélectionnez l'onglet **Utilisateurs**. Dans la barre d'outils de l'onglet **Utilisateurs**, cliquez sur  .

      La boîte de dialogue Ajouter un utilisateur s'affiche.



b. Créez le nouveau compte avec les informations d'identification suivantes :

Username = <nouveau nom d'utilisateur pour la connexion, par exemple, DPOadmin>
Email = <nouvelle adresse e-mail de l'utilisateur, par exemple DPOadmin@rsa.com>
Password = <nouveau mot de passe de l'utilisateur pour la connexion, par exemple, RSAprivacy1!@>
Full Name = <nouveau nom complet de l'utilisateur, par exemple DPO Administrator>

c. Cliquez sur l'onglet Rôles, +, puis sélectionnez le rôle `Data_Privacy_Officers` du nouvel utilisateur.

d. Sélectionnez **Enregistrer**.

2. Créez un nouveau compte d'utilisateur pour l'analyste avec des privilèges limités :

a. Dans la vue **Sécurité des services**, sélectionnez l'onglet **Utilisateurs**. Dans la barre d'outils de l'onglet **Utilisateurs**, cliquez sur +.

La boîte de dialogue Ajouter un utilisateur s'affiche.

b. Créez le nouveau compte avec les informations d'identification suivantes :

Username = <nouveau nom d'utilisateur pour la connexion, par exemple, NonprivAnalyst>
Email = <nouvelle adresse e-mail de l'utilisateur, par exemple NonprivAnalyst@rsa.com>
Password = <nouveau mot de passe de l'utilisateur pour la connexion, par exemple, RSAprivacy2!@>
Full Name = <nouveau nom complet de l'utilisateur, par exemple Nonprivileged Analyst>

c. Cliquez sur l'onglet Rôles, +, puis sélectionnez le rôle `Analysts` du nouvel utilisateur.

d. Sélectionnez **Enregistrer**.

Configurer des données obfusquées pour les Decoders et les Concentrators

Cette procédure crée les valeurs obfusquées présentées aux utilisateurs qui n'ont pas accès aux valeurs d'origine.

1. Configurez une valeur salt pour rendre la valeur obfusquée unique. Des analystes travaillant pour des entreprises distinctes peuvent avoir le même prénom et éventuellement le même nom d'utilisateur de connexion. L'utilisation d'une valeur salt restreint la possibilité pour une personne externe à votre organisation de déterminer votre mécanisme d'obfuscation. Dans cet exemple, vous utilisez une valeur salt simple et un algorithme SHA-256. Toutefois, vous pouvez configurer la valeur salt et modifier l'algorithme de hachage. Pour plus d'informations, consultez la rubrique Configurer l'obfuscation des données.

   a. Pour définir l'algorithme salt et de hachage, sélectionnez la vue **ADMIN > Services**.

   b. Sélectionnez un **Decoder** dans la vue **Services d'administration** et cliquez sur  > **Vue > Config**.

   c. Cliquez sur l'onglet **Confidentialité des données**, puis sélectionnez l'algorithme de hachage (SHA-256). Dans le champ Sel, saisissez un hachage, par exemple **rsasecurity**, puis cliquez sur **Appliquer**.

2. Définissez les transformations, notamment le format de hachage, entre la clé méta d'origine et la clé méta obfusquée dans Decoder. Le format de hachage par défaut est binaire, mais la configuration recommandée nécessite l'utilisation du format texte/chaîne.

   a. Cliquez sur l'onglet **Fichiers**, puis dans le menu déroulant, sélectionnez **index-decoder-custom.xml**. (Vous pouvez appliquer la même configuration à Log Decoder dans le fichier index-logdecoder-custom.xml.)

   b. Saisissez les lignes suivantes dans la zone de saisie disponible :

```
<?xml version="1.0" encoding="utf-8"?>
<language level="IndexNone" defaultAction="Auto">
<key name="username" description="Username" format="Text"
protected="true"><transform
destination="username.hash"/></key>
<key name="username.hash" description="Username Hash"
format="Text"/>
<key name="ip.src" description="Source IP Address"
format="IPv4" protected="true"><transform
destination="ip.src.hash"/></key>
<key name="ip.src.hash" description="Source IP Address
Hash" format="Text"/>
</language>
```

c. Pour redémarrer le service Decoder, dans la barre d'outils, sélectionnez **Système** dans le menu déroulant **Vue** (portant actuellement le nom Config). Dans la vue Système de services, sélectionnez **Arrêter le service**. Le service doit redémarrer automatiquement.

3. Définissez les clés méta de Concentrator dans le fichier index-concentrator-custom.xml :

a. Cliquez sur l'onglet **Fichiers**, puis dans le menu déroulant, sélectionnez **index-concentratorcustom.xml**

b. Saisissez les lignes suivantes dans la zone de saisie disponible :

```
<?xml version="1.0" encoding="utf-8"?>
<language level="IndexValues" defaultAction="Auto">
<key name="username" description="Username" format="Text"
level="IndexValues" protected="true"/>
<key name="username.hash" description="Username Hash"
format="Text" level="IndexValues" token="true"/>
<key name="ip.src" description="Source IP Address"
format="IPv4" level="IndexValues" protected="true"/>
<key name="ip.src.hash" description="Source IP Address
Hash" format="Text" level="IndexValues" token="true"/>
</language>
```

c. Pour redémarrer le service Concentrator, dans la barre d'outils, sélectionnez **Système** dans le menu déroulant **Vue** (portant actuellement le nom Config). Dans la vue Système de services, sélectionnez **Arrêter le service**. Le service doit redémarrer automatiquement.

Configurer la rétention de données dans les Concentrators et les Decoders

La configuration de la rétention des données garantit que les données résidant dans les composants Core de NetWitness Suite sont supprimés après un certain temps. La configuration de la rétention de données sur les Concentrators et les Decoders n'est pas requise pour tous les environnements, mais il peut être nécessaire d'être en conformité avec les lois et réglementations applicables. Il importe d'évaluer une période de rétention appropriée pour votre environnement. Les paramètres Planificateur de rétention des données que vous définissez s'appliquent à TOUTES les données présentes sur un Concentrator ou un Decoder.

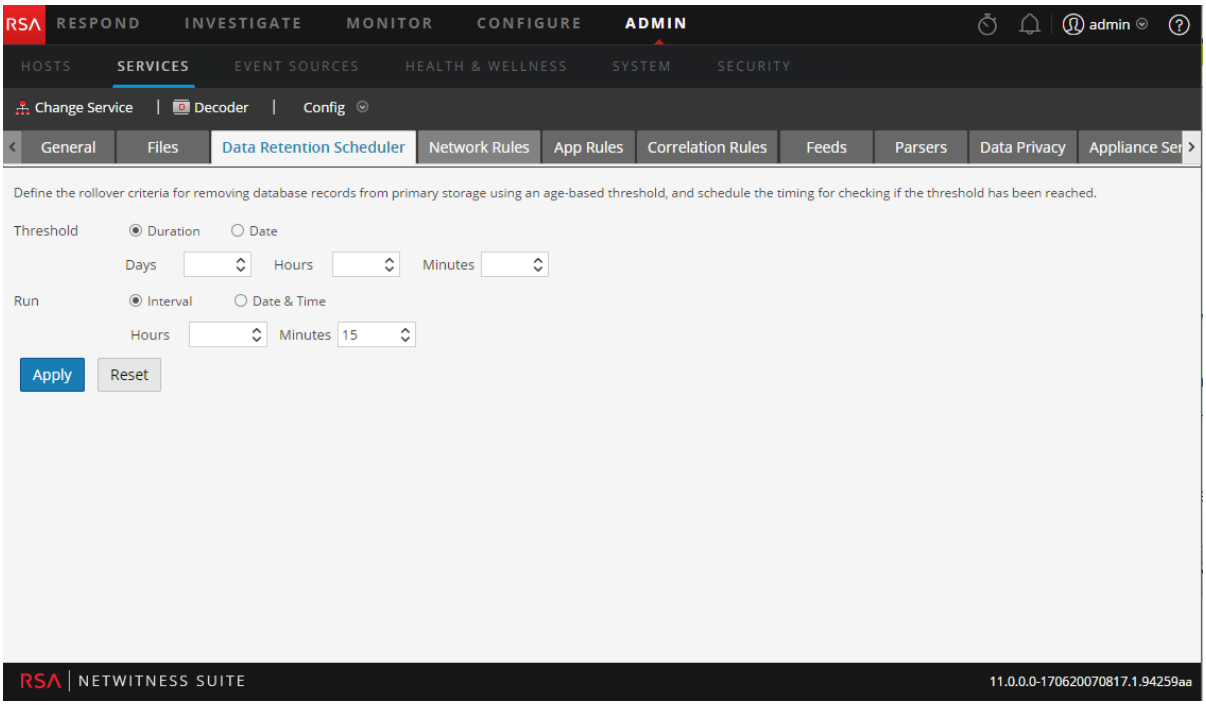
Dans l'exemple suivant, NetWitness Suite est configuré pour vérifier toutes les 15 minutes si le seuil de durée est atteint. Si le seuil est atteint, NetWitness Suite supprime les données antérieures à 90 jours dans les bases de données applicables.

Attention : La période de rétention de 90 jours n'est qu'un exemple. Ajustez vos critères de transfert selon l'emplacement des données et les lois applicables. Dans un environnement de confidentialité des données strictes comme en Europe où les lois exigent que les informations PII (Personally Identifiable Information) ne soient pas enregistrées ou supprimées fréquemment, vous devrez peut-être ajuster la période.

Cette procédure est facultative. Si vous ne définissez aucune limite de période de rétention, le système supprime automatiquement les données les plus anciennes lorsque l'espace de disque dur est saturé.

(Facultatif) Pour chaque Decoder et Concentrator :

1. Accédez à la vue **Configuration des Services > onglet Planificateur de rétention des données**.



2. Définissez la période de rétention des données. Par exemple, définissez le **Seuil** sur **Durée**, puis dans le champ **Jours**, sélectionnez **90**.
3. Définissez la fréquence de vérification du planificateur pour voir si le seuil a été atteint. Par exemple, définissez l'exécution sur **Intervalle**, puis dans le champ **Minutes**, sélectionnez **15**.
4. Pour enregistrer la configuration, cliquez sur **Appliquer**.

Valider la protection de la confidentialité des données

À ce stade, les utilisateurs ont été ajoutés avec des rôles disposant d'autorisations sur certains types de métadonnées. L'étape suivante consiste à vérifier que l'utilisateur restreint (l'analyste) ne peut pas visualiser ce qu'un utilisateur non restreint (le responsable de la confidentialité des données) peut afficher. En outre, vous devez vous assurer que la configuration de la rétention de données limite la durée de conservation de ces dernières sur les systèmes.

1. Visualiser l'obfuscation basée sur les rôles en action :
   a. Connectez-vous en tant qu'utilisateur non restreint (DPOadmin), puis assurez-vous que cet utilisateur peut voir toutes les données, notamment les données sensibles protégées `username` et `ip.src`, quelle que soit la session contenant ces métadonnées.
   b. Déconnectez-vous, puis reconnectez-vous en tant qu'utilisateur responsable de la confidentialité des données.

c. Pour chaque Decoder et Log Decoder, importez un fichier PCAP ou log dans la vue Système de services. Utilisez l'option **Télécharger le fichier de paquet** pour télécharger un fichier PCAP contenant les métadonnées `username` et `ip.src`.

d. Une fois l'importation terminée, consultez les métadonnées dans la vue **Procédure d'enquête > Naviguer**, en choisissant le Concentrator connecté au Decoder dans lequel les données viennent d'être importées.

e. Faites défiler la fenêtre vers le bas pour vous assurer que les clés méta `username` et `ip.src`, ainsi que leurs valeurs correspondantes, sont visibles.

f. Cliquez sur l'un des numéros verts en regard d'une valeur `username` ou `ip.src`, puis vérifiez que la session se charge dans la vue Événements.

g. Notez l'identifiant SID à vérifier lorsque vous vous connecterez en tant qu'utilisateur restreint.

h. Déconnectez-vous, puis connectez-vous en tant qu'utilisateur restreint (NonprivAnalyst).

i. Répétez les étapes c à f pour vérifier que l'utilisateur ne peut pas voir les métadonnées `username` ou `ip.src`, ni les sessions qui les contiennent, à l'instar de celle évoquée précédemment.

j. Pour atteindre une session spécifique, accédez à la vue **Procédure d'enquête > Naviguer**. Dans le menu **Actions**, sélectionnez **Accéder à l'événement**, puis saisissez l'identifiant SID.

2. Vérifiez que les données conservées dans la base de données correspondent à la durée de conservation configurée dans le planificateur de rétention des données.

a. Déconnectez-vous, puis connectez-vous en tant qu'utilisateur non restreint (DPOadmin).

b. Dans Concentrator, accédez à la vue **Services > Explorer**.

c. Dans l'arborescence de nœuds, sélectionnez le nœud **base de données**, puis **statistiques**.

d. Examinez la valeur `meta.oldest.file.time`, et vérifiez que son ancienneté ne dépasse pas le seuil défini dans le planificateur de rétention des données.

e. Passez au service Decoder et répétez les étapes b à d, vérifiez `stats meta.oldest.file.time` et `packet.oldest.file.time`.

Procédures détaillées

Cette rubrique regroupe des procédures utilisées par un responsable de la confidentialité des données pour implémenter un plan de confidentialité des données pour le réseau NetWitness Suite. Ces procédures font partie intégrante d'une configuration globale et interviennent si nécessaire pour implémenter le plan de confidentialité des données et gérer le flux d'informations sur le réseau.

- Configurer l'obfuscation des données
- Configurer la rétention de données
- Configurer les comptes d'utilisateur dans le cadre de la protection des données

Configurer l'obfuscation des données

Cette rubrique fournit les procédures de configuration nécessaires pour l'obfuscation des données dans NetWitness Suite. Dans un déploiement unique, toutes les configurations de service Core d'une solution de confidentialité des données doivent être identiques. Veillez à utiliser le même hachage et la même valeur salt dans l'ensemble des modules Decoder et Log Decoder.

Remarque : Pour permettre l'obfuscation des données, les comptes utilisateur doivent être configurés comme décrit dans la section Configurer les comptes d'utilisateur dans le cadre de la protection des données.

Configurer l'algorithme de hachage et la valeur salt Decoder

Le hachage de valeur obtenu dans le cadre de la solution de confidentialité des données a lieu au moment de la création des clés méta sur Decoder et Log Decoder. Ces deux services ont des paramètres par défaut pour une utilisation avec toutes les clés méta dont les valeurs sont transformées en l'absence d'un type d'algorithme de hachage spécifié ou de la valeur salt. Les valeurs NetWitness Suite initiales des paramètres par défaut sont : algorithme de hachage (SHA-256) et valeur salt (aucune).

Remarque : NetWitness Suite 10.4 et les versions antérieures prennent en charge l'utilisation de l'algorithme de hachage SHA-1 pour la compatibilité en amont. RSA déconseille l'utilisation de l'algorithme SHA-1. Celuiei n'est pas disponible dans NetWitness Suite 10.5 et les versions supérieures.

Si vous souhaitez changer les paramètres par défaut, modifiezles dans la vue Configuration des services NetWitness Suite onglet Confidentialité des données, ou dans les nœuds suivants de la vue Explorer des services Security Analytics :

- `/decoder/parsers/transforms/default.type`

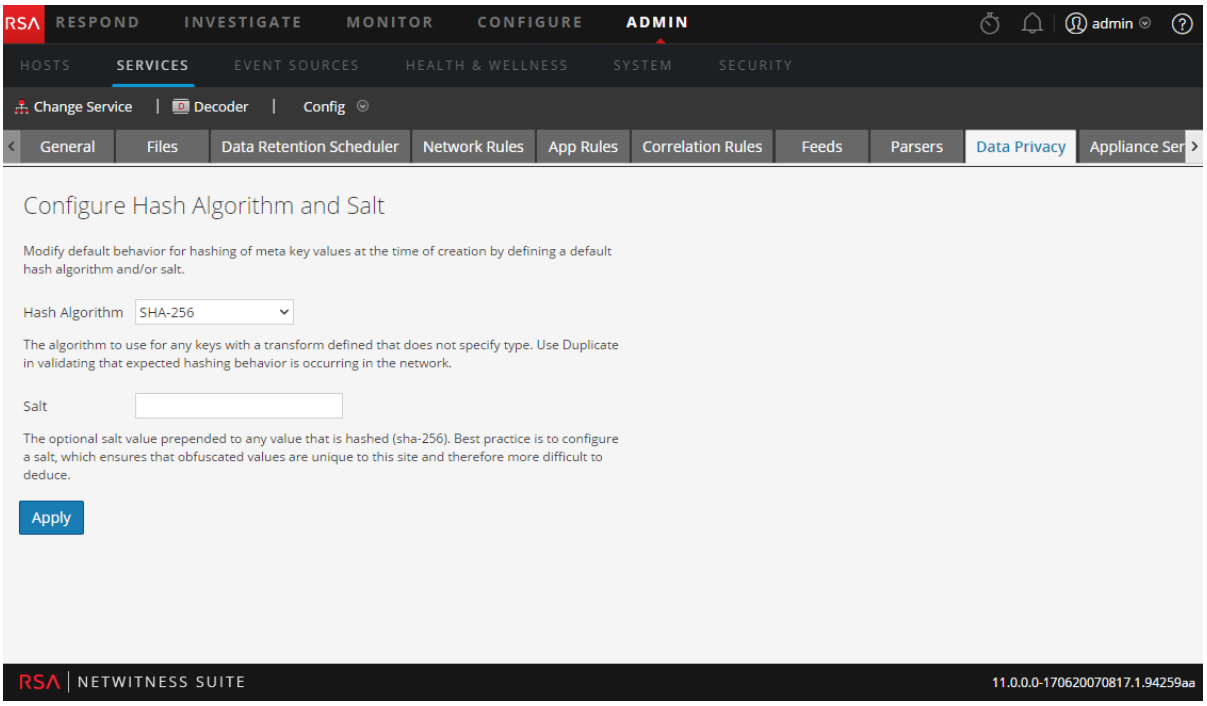
  Algorithme à utiliser pour toutes les clés avec une transformation définie qui ne précise pas le `type`. Les algorithmes pris en charge sont les suivants : `duplicate` et `sha-256`.

- `/decoder/parsers/transforms/default.salt`

  La valeur salt ajoutée à toute valeur hachée (`sha-256`). Cette valeur est facultative, une valeur salt vide est valide et produit un hachage sans valeur salt. La valeur salt n'est pas définie par défaut afin que vous puissiez créer une valeur salt unique pour votre environnement. En général, plus la valeur salt est longue et complexe, plus la sécurité est accrue. Vous pouvez utiliser une valeur salt comprenant jusqu'à 60 caractères sans que cela ait un impact majeur. Il est recommandé d'utiliser une valeur salt d'au moins 16 caractères.

Pour modifier l'algorithme de hachage et la valeur salt par défaut :

1. Dans la section **Admin**, sélectionnez la vue **Services**.
2. Dans la grille **Services**, sélectionnez un service Decoder ou Log Decoder, puis cliquez sur  Vue **Config**. Cliquez sur l'onglet **Confidentialité des données**.



3. Dans la section **Configurer l'algorithme de hachage et le sel**, sélectionnez un **Algorithme de hachage** à utiliser pour les clés méta avec une transformation définie qui ne précise pas de type. `sha-256`. (Un second algorithme, `duplicate`, peut être utilisé par les administrateurs pour valider que le comportement de ce hachage doit bien se produire sur le réseau.)
4. (Facultatif) Dans le champ **Sel**, saisissez une valeur salt à placer juste avant la valeur hachée. Cette valeur est facultative, une valeur salt vide est valide et produit un hachage sans valeur salt. La valeur salt n'est pas définie par défaut afin que vous puissiez créer une valeur salt unique pour votre environnement. En général, plus la valeur salt est longue et complexe, plus la sécurité est accrue. Les bonnes pratiques de sécurité recommandent une valeur salt de 100 bits minimum ou 16 caractères de long. Si une valeur salt unique est requise pour chaque clé méta, vous devez la configurer dans le fichier d'index, comme indiqué dans l'exemple 3 ci-dessous.
5. Cliquez sur **Appliquer**.

   Les nouveaux paramètres prennent effet immédiatement.

Configurer des clés de langue

Dans NetWitness Suite 10.5, le langage de NetWitness Suite Core possédait plusieurs attributs de clés de langue supplémentaires pour faciliter la mise en œuvre de la confidentialité des données. Vous pouvez modifier ces attributs dans le fichier d'index personnalisé de chaque service Decoder ou Log Decoder. Le fichier d'index personnalisé (par exemple index-decoder-custom.xml) est modifiable dans la vue Configuration des services > onglet Fichiers. Après avoir apporté des modifications aux fichiers d'index, comme celles indiquées dans les exemples ci-dessous, vous devez redémarrer le service selon une séquence spécifique.

Selon les exigences de confidentialité des données définies pour votre site, configurez des clés méta individuelles à protéger à l'aide des attributs suivants de `key` :

- `protected`

  Cet attribut indique que NetWitness Suite doit considérer les valeurs comme étant protégées et contrôler étroitement toute version de la valeur. Lors de la propagation de l'attribut protected, NetWitness Suite vérifie que les systèmes fiables en aval traitent les valeurs en conséquence. Ajoutez cet attribut à tous les services qui créent les valeurs protégées (c'est-à-dire Decoder ou Log Decoder), et tous les services qui fournissent un accès fiable (requête/valeurs de SDK, agrégation) en dehors des services Core. Seule exception à cette règle : un Broker sans fichier d'index spécifié n'a pas besoin de l'ajout de l'attribut.

- `token`

  Cet attribut spécifie que les valeurs de cette clé remplacent d'autres valeurs et peuvent être visuellement intéressantes. L'attribut `token` est un attribut d'information. Il sert principalement aux éléments d'interface utilisateur qui affichent la valeur dans un format plus utile ou visuellement plus agréable.

- `transform`

  Cet élément enfant de `key` indique que les valeurs d'une métaclé donnée doivent être transformées et que la valeur de résultat est conservée dans une autre métaclé. L'élément `transform` est requis uniquement dans les services Decoder et Log Decoder. Il s'agit d'un élément d'information, s'il est spécifié dans d'autres services Core. L'élément `transform` possède les attributs et enfants suivants :

Nom	Type	Description	Facultatif ou requis
`destination`	Propriété	Spécifie le nom de clé où la valeur transformée doit persister.	obligatoire

Nom	Type	Description	Facultatif ou requis
type	Propriété	Algorithme de transformation à appliquer. S'il n'est pas spécifié, la valeur /decoder/parsers/transforms/default.type est utilisée.	facultatif
param	élément enfant	Paire nom/valeur, où chaque élément param possède un attribut name, et où le texte de l'élément enfant représente la valeur. Le seul élément param pris en charge sert à indiquer une valeur salt spécifique d'une clé. S'il n'est pas spécifié, la valeur /decoder/parsers/transforms/default.salt est utilisée.	facultatif

Exemple 1

Dans Decoder ou Log Decoder, marquez username comme étant protégé, et hachez toutes les valeurs en username.hash avec l'algorithme et la valeur salt par défaut :

```
<key name="username" description="Username" format="Text"
protected="true"><transform destination="username.hash"/></key>
```

Exemple 2

Dans Concentrator, marquez username comme étant protégé, et username.hash comme étant un jeton :

```
<?xml version="1.0" encoding="utf-8"?>
<language level="IndexNone" defaultAction="Auto">
<key description="Username" format="Text" level="IndexValues"
name="username" protected="true"/>
<key description="Username Hash" format="Binary" level="IndexValues"
name="username.hash" token="true"/>
</language>
```

Exemple 3

Dans Decoder ou Log Decoder, marquez `username` comme étant protégé, et hachez toutes les valeurs en `username.bin` avec l'algorithme et la valeur salt par défaut :

```
<key name="username" description="Username" format="Text"
protected="true">
<transform destination="username.bin" type="sha-256">
<param name="salt">0000</param>
</transform></key>
```

Configurer la visibilité des métadonnées et du contenu en fonction du rôle d'utilisateur dans les services Core

Sur chaque service Broker, Concentrator, Decoder, Log Decoder et Archiver affichés dans la vue Sécurité des services, les administrateurs peuvent configurer la visibilité des métadonnées et du contenu en fonction du groupe d'utilisateurs ou du rôle attribué à un utilisateur. Il s'agit de la capacité de rôles méta SDK, et il est activé par défaut.

Remarque : Les administrateurs souhaitant configurer la visibilité des métadonnées et du contenu par l'utilisateur ne doivent pas désactiver l'autorisation `sdk.content` (dans l'onglet Rôles). Si l'autorisation `sdk.content` a été désactivée dans l'onglet Rôles, les paquets et logs bruts ne sont pas visibles sur le nœud `system.roles`. Le nœud `system.roles` gère le filtrage à l'aide de la méthode de configuration sous l'onglet Paramètres.

Avec la fonction `sdk.content` activée, l'étape suivante consiste à sélectionner la méthode de filtrage des métadonnées et le contenu sous l'onglet Paramètres. La sélection d'une option de liste noire ou de liste blanche permet d'attribuer des autorisations supplémentaires pour des clés méta spécifiques disponibles dans l'onglet Rôles. Le résultat est que les administrateurs peuvent choisir un rôle d'utilisateur (analystes, par exemple) sous l'onglet Rôles et sélectionner les clés méta spécifiques (et le contenu) pour figurer sur la liste noire ou blanche de ce groupe d'utilisateurs. Les autorisations s'appliquent à tous les utilisateurs du groupe d'utilisateurs.

Le tableau suivant répertorie les options de filtrage dans l'onglet Paramètres et les valeurs numériques utilisées à des fins de désactivation (0), ainsi que les types de filtrages (1 à 6). Il n'est pas nécessaire de connaître la valeur numérique à moins de configurer la visibilité manuelle du contenu et des métadonnées dans le nœud `system.roles`.

Valeur du nœud system.roles	Option de l'onglet Paramètres	Métadonnées de l'événement	Événement d'origine.

Valeur du nœud system.roles	Option de l'onglet Paramètres	Métadonnées de l'événement	Événement d'origine.
0	**Aucun filtrage.** Les rôles système qui définissent les autorisations sur la base d'une clé méta sont désactivés.	Visible	Visible
1	**Métadonnées et contenu de la liste blanche.** Par défaut, aucune métadonnée ni aucun paquet ne sont visibles. Si vous sélectionnez des rôles méta SDK individuels en fonction du groupe d'utilisateurs, les utilisateurs sont autorisés à voir les métadonnées et les paquets correspondant au rôle méta SDK choisi.	Invisible Sélectionner pour afficher	Invisible Sélectionner pour afficher
2	**Métadonnées de la liste blanche uniquement.** Par défaut, les paquets sont affichés, mais aucune métadonnée n'est visible. Si vous sélectionnez des rôles méta SDK individuels en fonction du groupe d'utilisateurs, les utilisateurs sont autorisés à voir les métadonnées correspondant au rôle choisi.	Invisible Sélectionner pour afficher	Visible

Valeur du nœud system.roles	Option de l'onglet Paramètres	Métadonnées de l'événement	Événement d'origine.
3	**Contenu de la liste blanche uniquement.** Par défaut, les métadonnées sont visibles, mais aucun paquet n'est visible. Si vous sélectionnez des rôles méta SDK individuels en fonction du groupe d'utilisateurs, les utilisateurs sont autorisés à voir les paquets correspondant au rôle choisi.	Visible	Invisible Sélectionner pour afficher
4	**Métadonnées et contenu de la liste noire.** Par défaut, toutes les métadonnées et tous les paquets sont visibles. Si vous sélectionnez des rôles méta SDK individuels en fonction du groupe d'utilisateurs, les utilisateurs ne sont pas autorisés à voir les métadonnées et les paquets correspondant au rôle choisi.	Visible Sélectionner pour masquer	Visible Sélectionner pour masquer
5	**Métadonnées de la liste noire uniquement.** Par défaut, toutes les métadonnées et tous les paquets sont visibles. Si vous sélectionnez des rôles méta SDK individuels en fonction du groupe d'utilisateurs, les utilisateurs ne sont pas autorisés à voir les métadonnées correspondant au rôle choisi.	Visible Sélectionner pour masquer	Visible

Valeur du nœud system.roles	Option de l'onglet Paramètres	Métadonnées de l'événement	Événement d'origine.
6	**Contenu de la liste noire uniquement.** Par défaut, toutes les métadonnées et tous les paquets sont visibles. Si vous sélectionnez des rôles méta SDK individuels en fonction du groupe d'utilisateurs, les utilisateurs ne sont pas autorisés à voir les paquets correspondant au rôle choisi.	Visible	Visible Sélectionner pour masquer

Trois facteurs déterminent ce qu'un utilisateur peut voir :

- Paramètre de rôle méta SDK (liste noire ou blanche).
- Les clés méta restreintes configurées pour le groupe auquel appartient l'utilisateur.
- Les clés méta de la session en cours d'analyse.

Attention : Sachez qu'avec la mise sur liste noire, l'approbation implicite est accordée à tous sauf aux métadonnées configurées. Pour qu'un Decoder ait un RBAC activé et utilise une fiabilité implicite, il doit uniquement utiliser la configuration système sur liste noire ; la configuration système sur liste blanche entraînerait des problèmes avec les clés méta qui ne sont pas explicitement activées et donc invisibles. Il est impossible d'accorder une confiance implicite avec les règles de la liste blanche, car l'univers des clés méta ne peut pas être connu. Si vous souhaitez utiliser la configuration sur liste blanche, une solution de contournement consiste à désactiver le paramètre RBAC pour le Decoder et à empêcher les comptes utilisateur de se connecter directement au Decoder et activer RBAC.

Voici un exemple de maillage de la configuration du rôle méta SDK avec un groupe disposant de clés méta restreintes.

Configuration :

- Le paramètre de rôle méta SDK est **Liste noire méta et contenu**. Si cette option est implémentée, la totalité des métadonnées et du contenu (paquets et logs) est visible par défaut.
- L'administrateur a restreint les clés méta configurées pour le groupe Analystes afin d'empêcher l'affichage des données sensibles (par exemple `username`).

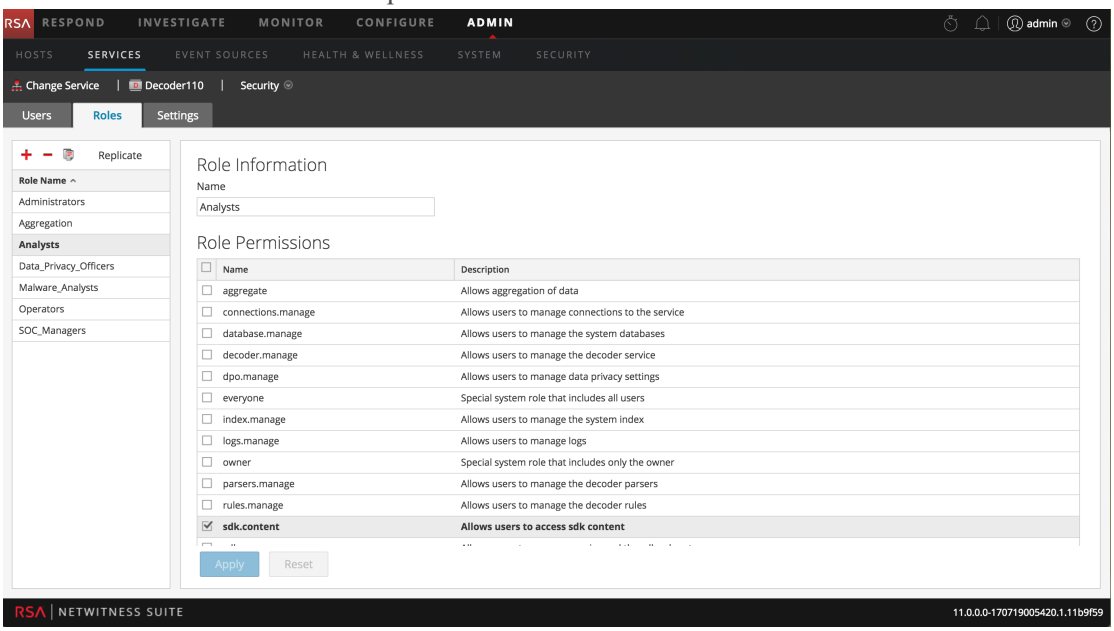
- Les paquets et les logs d'une session qui comprend la clé méta `username` ne sont pas visibles par un analyste.

Résultat : un utilisateur membre du groupe Analystes enquête sur une session. En fonction du contenu de la session, les résultats sont différents :

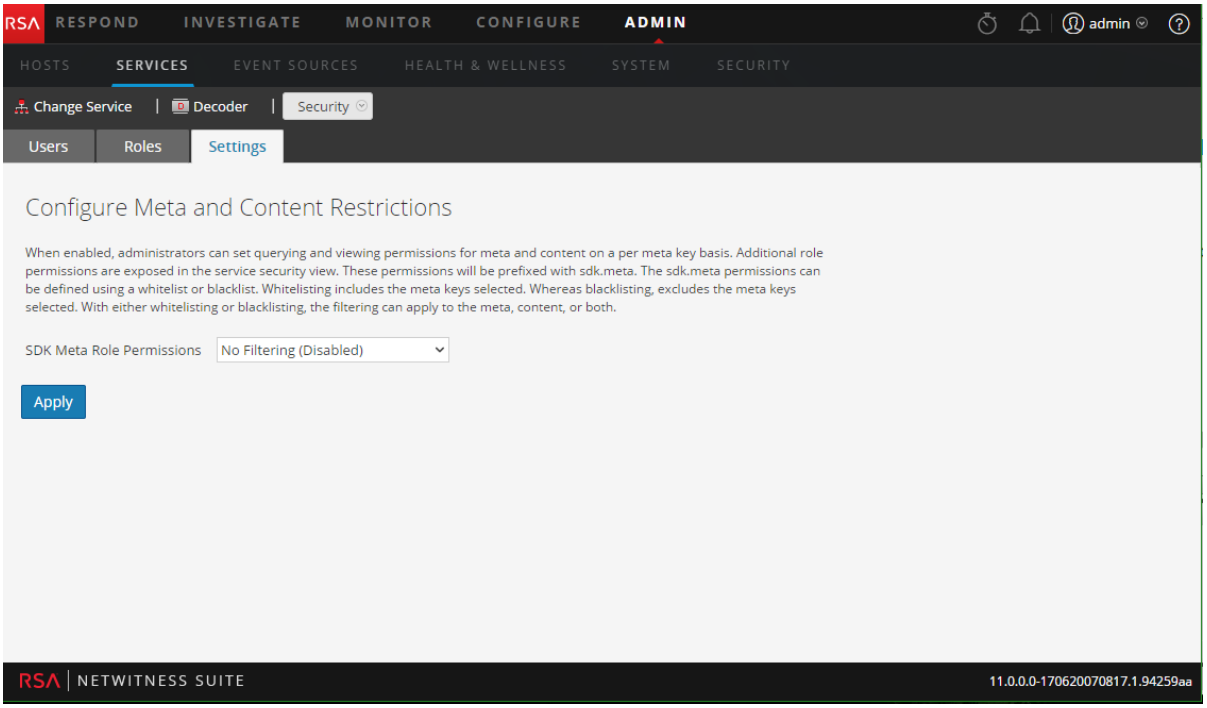
- La session 1 comprend les clés méta suivantes : `ip`, `eth`, `host` et `file`. La session ne comporte pas `username`. Par conséquent, tous les paquets et logs de la session sont affichés.
- La session 2 comprend les clés méta suivantes : `ip`, `time`, `size`, `file`, `username`. Dans la mesure où la session comporte `username`, aucun paquet ou log de la session n'est visible par l'analyste.

Pour configurer les restrictions relatives aux métadonnées et au contenu pour Decoder ou Log Decoder :

1. Dans la vue **Admin**, sélectionnez **Services**.
2. Dans la grille **Services**, sélectionnez un service Broker, Concentrator, Decoder, Log Decoder ou Archiver, cliquez sur  **> Vue > Sécurité**. Cliquez sur l'onglet **Rôles**, sélectionnez un rôle et vérifiez que le`sdk.content` rôle est activé.

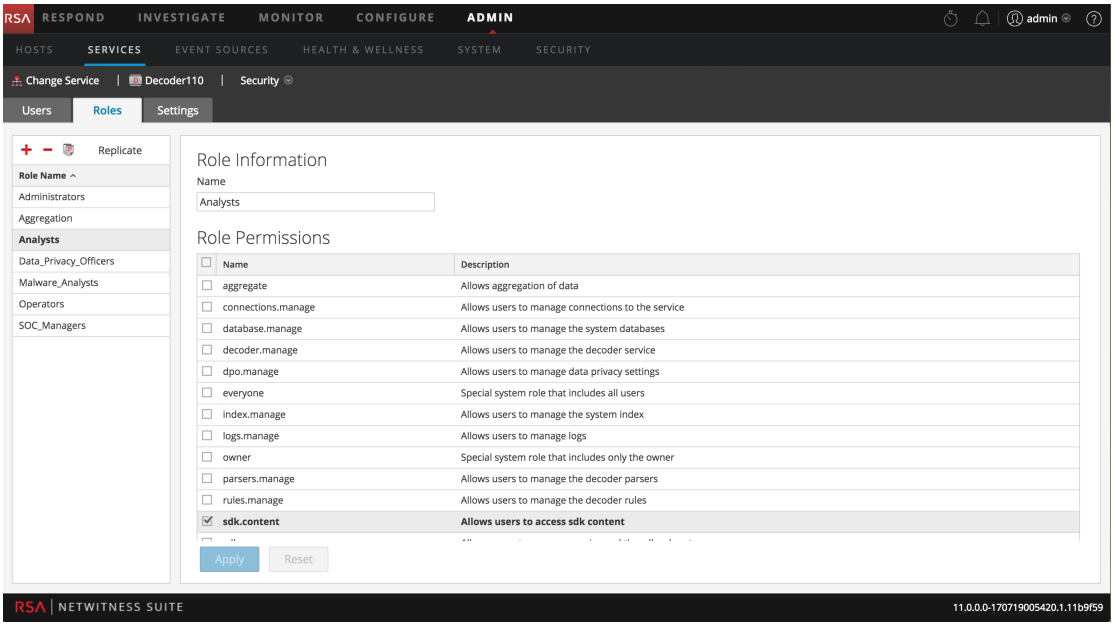


3. Cliquez sur l'onglet **Paramètres**.



4. Sélectionnez l'une des méthodes de filtrage (liste noire ou liste blanche), les types de contenus (métadonnées et contenu, métadonnées uniquement ou contenu uniquement), puis cliquez sur **Appliquer**.
5. Cliquez sur l'onglet **Rôles**, puis sur un rôle pour lequel vous souhaitez autoriser l'accès au contenu (liste blanche) ou bloquer l'accès au contenu (liste noire), tel que cela est spécifié dans le paramètre Autorisations de rôle méta SDK.

Les autorisations relatives au rôle sélectionné s'affichent, ainsi que les autorisations de rôle méta SDK disponibles pour la sélection, par exemple `sdk.meta.action`. Si vous avez sélectionné l'une des options de liste blanche dans le paramètre Autorisations de rôle méta SDK, vous devez attribuer chaque rôle méta SDK pour rendre le contenu sélectionné visible par les utilisateurs possédant ce rôle méta SDK. Si vous avez sélectionné l'une des options de liste noire dans le paramètre Autorisations de rôle méta SDK, le contenu sélectionné n'est pas visible par les utilisateurs possédant ce rôle méta SDK.



6. Sélectionnez les autorisations de rôle méta SDK pour les utilisateurs possédant ce rôle. Cliquez sur **Appliquer**.

   Les paramètres entrent en vigueur immédiatement et s'appliquent aux nouveaux paquets et logs traités par Decoder ou Log Decoder.

Configurer les clés méta non écrites sur disque pour chaque parser sur un Decoder

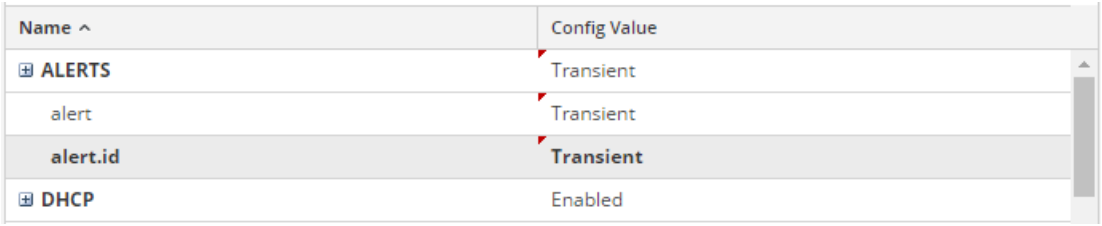
Sur un Decoder et Log Decoder, un responsable de la confidentialité des données peut configurer les clés méta individuelles qui ne sont pas écrites sur disque. Pour ce faire, le responsable de la confidentialité des données spécifie les clés méta comme étant transitoires dans l'index et la configuration du parser.

Remarque : La même fonctionnalité était disponible auparavant sur Log Decoder. Vous pouviez la configurer durant l'installation des analyseurs en modifiant le fichier table-map.xml. Désormais, elle est intégrée dans la vue Configuration des services.

Pour configurer les clés méta sélectionnées pour des parsers individuels, sans les écrire sur disque :

1. Dans la section **Admin**, sélectionnez la vue **Services**.
2. Dans la grille **Services**, sélectionnez un service Decoder ou Log Decoder, puis cliquez sur  **> Vue > Config**.
3. Dans la section **Configuration des analyseurs** de l'onglet **Général**, sélectionnez un analyseur, puis sélectionnez **Transitoire** dans la liste déroulante **Valeur de configuration**. Accédez à la liste en cliquant sur la valeur de configuration (Activé, Désactivé ou Transitoire).

   La modification de configuration est indiquée par un triangle rouge.

4. Cliquez sur **Appliquer**.

   La modification prend effet immédiatement. L'analyseur configuré avec l'état Transitoire ne stocke plus de clés méta sur disque.

Configurer la rétention de données

Un utilisateur NetWitness Suite avec le rôle d'administrateur peut configurer NetWitness Suite pour garantir que les données sensibles sont bien supprimées après une période de rétention spécifique, quel que soit la fréquence de réception du système. Par exemple, la politique peut être de conserver les paquets (données et métadonnées brutes) pour 24 heures uniquement, et de conserver les logs (données et métadonnées brutes) pour un maximum de sept jours. Si des données sensibles se retrouvent dans une autre base de données des serveurs Reporting Engine, Malware Analysis, Event Stream Analysis et Serveur NetWitness, la rétention de données peut aussi s'appliquer à ces emplacements. L'administrateur doit configurer chaque service individuellement pour tous les composants NetWitness Suite (sauf Event Stream Analysis) en fonction de la politique et de la réglementation sur la confidentialité des données.

Les données sensibles peuvent également se trouver dans la mémoire cache.

- Les Brokers peuvent mettre les données en cache mais celui-ci doit être vidé en configurant un transfert indépendant et d'autres suppressions de cache si nécessaire. L'administrateur peut configurer le transfert de cache pour un Broker en modifiant le fichier du planificateur dans la vue Configuration des services - onglet Fichiers.
- La procédure d'enquête et le serveur Serveur NetWitness placent des données dans le cache, qui sont effacées automatiquement toutes les 24 heures.
- Si le responsable de la confidentialité des données exporte des données, cette opération est identique à l'enregistrement des données sur le serveur Serveur NetWitness dans la file d'attente des tâches. Pour effacer ces données, l'administrateur ou le responsable de la confidentialité des données doit régulièrement nettoyer la file d'attente des tâches.

Rétention de données

Vous pouvez planifier une tâche récurrente pour les services Decoder, Log Decoder et Concentrator dans NetWitness Suite pour vérifier si les données sont prêtes à être supprimées. Le planificateur de rétention des données permet de configurer la planification de base, et les paramètres avancés du planificateur sont toujours disponibles en modifiant le fichier du planificateur dans la vue Configuration des services sous l'onglet Fichier ou le nœud de la vue Explorer.

Le service Archiver fournit des options flexibles de stockage et de rétention des données. Vous pouvez placer différents types de données de log dans des collections individuelles et les gérer séparément. Ces collections vous permettent de spécifier la quantité d'espace de stockage total à utiliser et le nombre de jours de stockage des logs dans la collection. Vous pouvez également déterminer si vous souhaitez supprimer les données du log ou les déplacer vers un stockage hors ligne à froid après avoir atteint l'espace de stockage maximal spécifié pour la collection.

Ainsi, vous pouvez placer des informations sensibles dans une collection et configurer une limitation de la durée de conservation à 30 jours, par exemple. Pour supprimer les données après 30 jours, inutile d'activer le stockage à chaud ou à froid pour cette collection.

Comparaison entre la suppression et la rétention de données de log

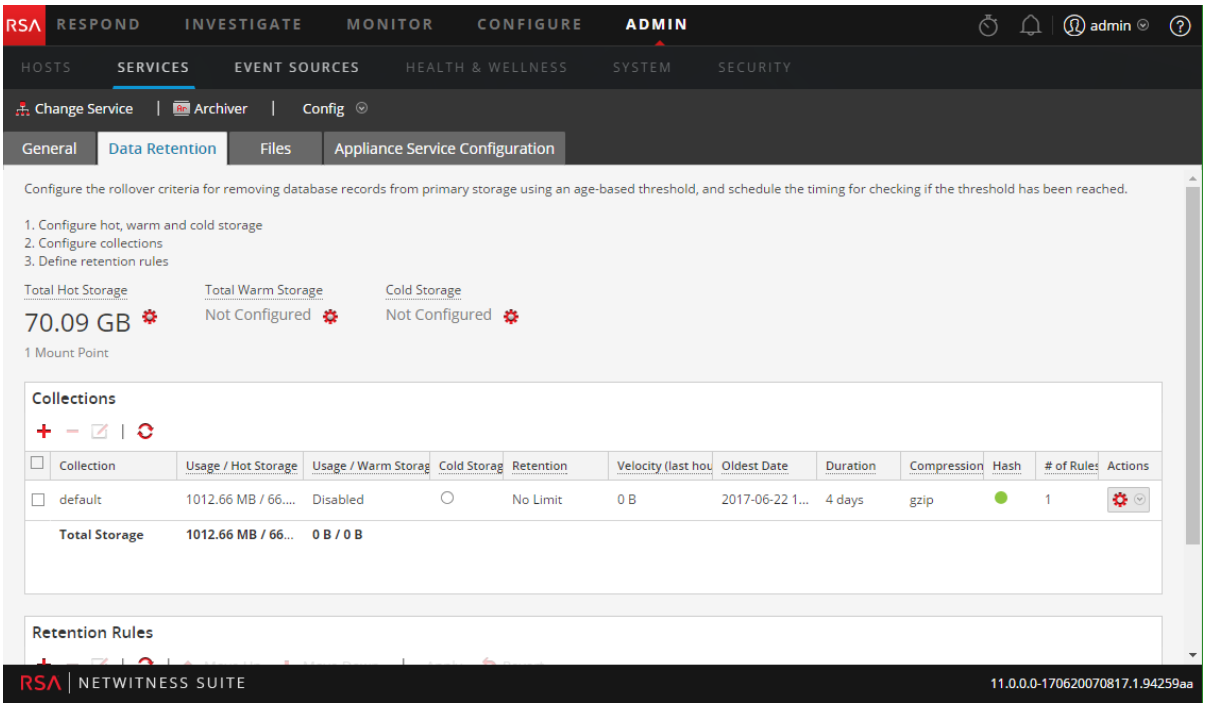
Les administrateurs peuvent configurer un stockage hiérarchisé (niveau intensif, niveau à chaud et niveau à froid) sur un service Archiver. Le stockage à froid contient les données les plus anciennes qui sont, soit requises pour le fonctionnement de l'activité, soit mandatées par des exigences réglementaires. Lorsqu'une collection atteint ses limites de rétention pour le stockage intensif et à chaud, NetWitness Suite supprime les données du log de stockage intensif ou à chaud. Si le stockage à froid est configuré, une copie est placée dans le stockage à froid avant que les logs ne soient supprimés du stockage intensif ou du stockage à chaud. Vous pouvez choisir d'activer le stockage à froid pour chaque collection de stockage des logs. NetWitness Suite ne gère pas le stockage à froid.

Activer ou désactiver le stockage à froid dans une collection de stockage de logs

Lorsque les données de log d'une collection atteignent les limites de rétention pour le stockage intensif et à chaud, vous pouvez les supprimer ou les déplacer vers un stockage hors ligne (à froid).

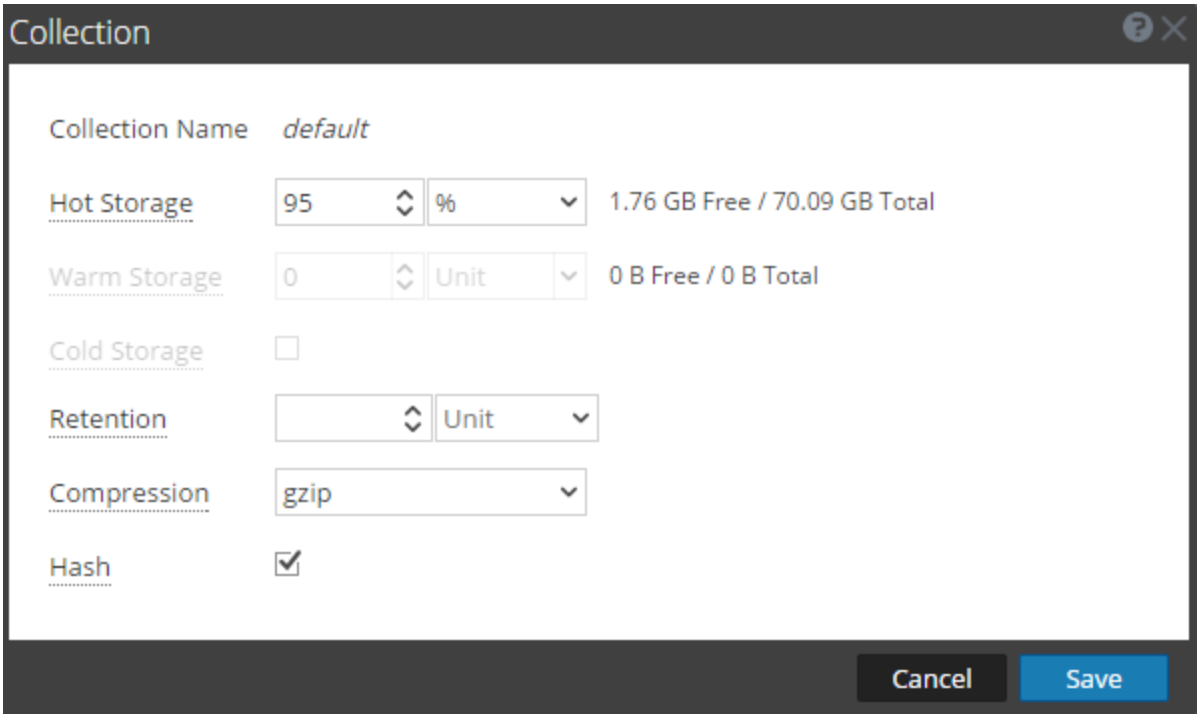
Pour activer ou désactiver le stockage à froid dans une collection de stockage de rétention des logs sur un service Archiver :

1. Dans la section **Admin**, sélectionnez la vue **Services**.
2. Sélectionnez le service Archiver, puis  **> Vue > Config**.
3. Cliquez sur l'onglet **Rétention de données**.



4. Dans la section **Collections** de l'onglet Rétention de données, sélectionnez une collection, puis cliquez sur .

   La boîte de dialogue Collection s'affiche.



Remarque : Si la taille de stockage maximale de la collection ne permet pas la rétention de données complètes pour la période de rétention spécifiée, NetWitness Suite supprime les données ou les déplace vers le stockage à chaud ou le stockage à froid, si spécifié dans la collection.

5. Activer ou désactiver le stockage à froid :
   - Pour supprimer les données des logs lorsque la collection atteint ses limites de rétention spécifiées, désactivez la case à cocher **Stockage à froid**.
   - Pour déplacer les données de log vers le stockage hors ligne lorsque la collection atteint ses limites de rétention spécifiées, activez la case à cocher **Stockage à froid**.
6. Cliquez sur **Enregistrer**.

Configurer la rétention et le stockage des logs sur un service Archiver

Pour configurer la rétention et le stockage des logs sur un service Archiver, reportez-vous à la section **Configurer le stockage et la rétention des logs Archiver** dans le *Guide de configuration d'Archiver*.

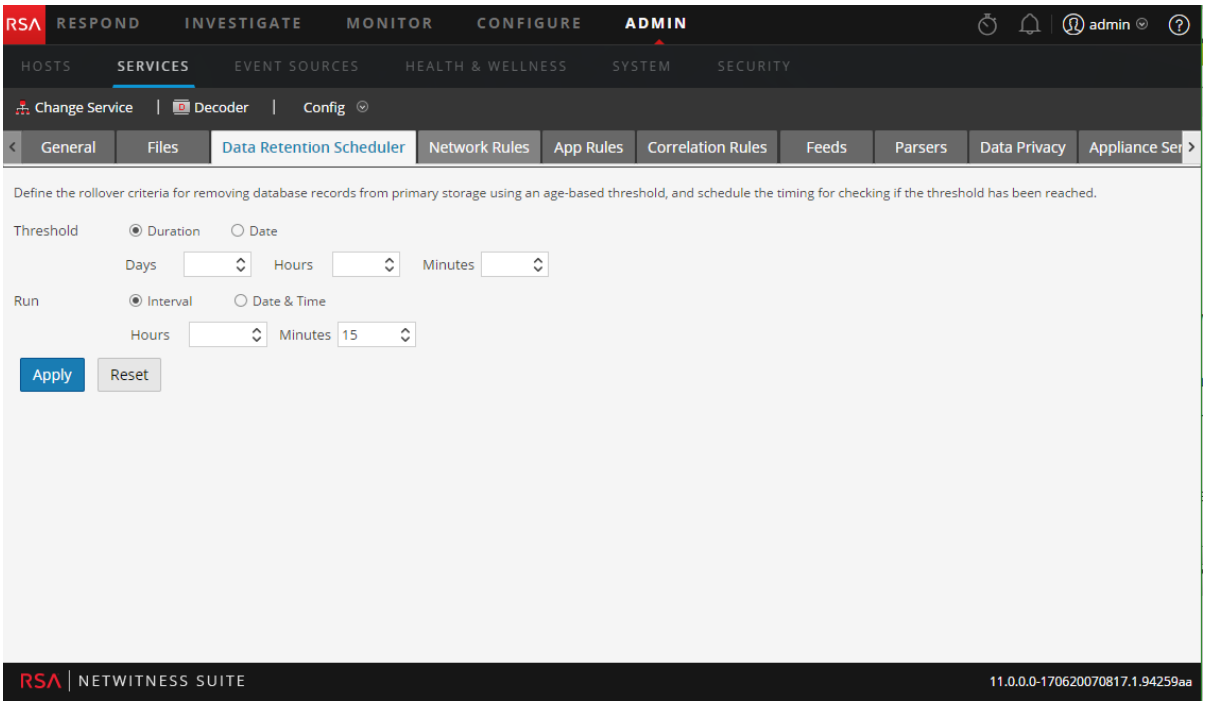
Planifier une tâche récurrente pour vérifier les seuils de rétention des données

La configuration du planificateur de rétention des données garantit que les données résidant dans les composants Decoder, Log Decoder et Concentrator sont supprimées après un certain temps. Par exemple, la rétention de données sur un service Decoder peut être configuré pour vérifier toutes les 15 minutes si le seuil de durée spécifié est atteint. Si le seuil est atteint, NetWitness Suite supprime les données antérieures à 4 heures dans les bases de données applicables.

Attention : Le planning remplace le planning précédent et prend effet immédiatement. Si la période de rétention est réduite, les données dépassant cette période de rétention sont supprimées.

Pour un Decoder, Log Decoder ou Concentrator :

1. Dans la section **Admin**, sélectionnez la vue **Services**.
2. Dans la grille **Services**, sélectionnez un service Decoder, Log Decoder ou Concentrator, puis cliquez sur  **> Vue > Config**.
3. Cliquez sur l'onglet **Planificateur de rétention des données**.



4. Définissez le seuil basé sur la période de stockage des données ou la date à laquelle les données ont été stockées. Exécutez l'une des opérations suivantes :

   a. Pour définir la durée pendant laquelle les données peuvent être stockées avant leur suppression, sélectionnez le paramètre **Durée**, puis spécifiez le nombre de jours (365 au maximum), d'heures (24 au maximum) et de minutes (60 au maximum) qui se sont écoulés depuis l'horodatage des données.

   b. Pour définir la suppression des données basée sur la date de l'horodatage, sélectionnez le paramètre **Date**, puis spécifiez la date et l'heure du mois dans les champs Calendrier et Heure.

5. Effectuez l'une des opérations suivantes pour configurer le **planning de vérification des critères de déploiement** :

   a. Si vous souhaitez définir un intervalle régulier au cours duquel la vérification de la base de données planifiée se produit, sélectionnez le paramètre **Intervalle** et précisez les **heures** et les **minutes** entre les contrôles réguliers.

   b. Si vous souhaitez définir une date et une heure régulières auxquelles la vérification de la base de données planifiée se produit, sélectionnez le paramètre **Date et heure** et spécifiez l'heure de l'horloge système au format `hh:mm:ss` pour le transfert.

      - Pour spécifier le jour, sélectionnez **Tous les jours**, **Jours de la semaine** ou **Week-end**. Par défaut, le planificateur définit le paramètre **Tous les jours**.
      - Pour spécifier une autre série de jours de la semaine, sélectionnez **Personnalisé** et cliquez sur chaque jour où le contrôle de la base de données se produit.

> **Attention :** Le planning remplace le planning précédent et prend effet immédiatement. Si la période de rétention est réduite, les données dépassant cette période de rétention sont supprimées.

6. Cliquez sur **Appliquer** pour terminer la configuration.

Configurer les comptes d'utilisateur dans le cadre de la protection des données

Cette rubrique présente les procédures qui permettent de configurer des comptes d'utilisateur qui fonctionnent avec l'obfuscation des données dans NetWitness Suite. Pour que l'obfuscation des données fonctionne, les comptes et les autorisations de plusieurs types d'utilisateurs doivent être configurés.

- Personnalisez le rôle système `Administrators` par défaut dans NetWitness Suite pour supprimer les autorisations qui ne doivent être disponibles que pour le spécialiste de la confidentialité des données.
- Ajoutez deux comptes d'utilisateur au niveau du système pour représenter un spécialiste de la confidentialité des données et un analyste type.
- Ajoutez un compte d'utilisateur au niveau du service avec le rôle d'agrégation afin que les services Decoder et Log Decoder puissent agréger les données vers un Concentrator ou un Broker.
- Sur le Reporting Engine, configurez deux comptes de service distincts. Un compte de service pour le reporting général ne contenant pas de données sensibles et un autre compte pour les utilisateurs privilégiés avec un accès à toutes les données y compris les données sensibles. Cette procédure est décrite dans le *Guide de configuration de Reporting Engine* sous **Configurer les autorisations d'accès aux sources de données**.

Personnaliser le rôle d'utilisateur Administrateurs par défaut au niveau du service

Pour séparer les fonctions de spécialiste de la confidentialité des données et d'administrateur sur chaque Decoder et Log Decoder, vous devez supprimer l'autorisation `dpo.manage` d'un clone du rôle Administrateurs.

1. Dans la vue **Services d'administration**, sélectionnez un service Decoder ou Log Decoder.

   Cliquez sur  **> Vue > Sécurité**.

2. Dans la vue **Sécurité des services**, cliquez sur l'onglet **Rôles**, sélectionnez **Administrateurs** et cliquez sur  .

   Dans la boîte de dialogue **Saisir le nom du rôle**, saisissez un nouveau nom de rôle comme Non_DPO_Administrators et cliquez sur **Enregistrer**.

3. Sélectionnez le nouveau rôle.

Les informations du rôle s'affichent pour modification.

4. Cliquez sur la case en regard de **dpo.manage** afin de la désactiver, puis cliquez sur **Appliquer**.

   L'autorisation permettant de gérer la configuration de la confidentialité des données est supprimée pour le nouveau rôle.

5. Sous l'onglet **Utilisateurs**, sélectionnez chaque utilisateur ayant le rôle **Administrateurs** et modifiez son rôle par le rôle cloné.

6. Vérifiez que les utilisateurs ayant le rôle Administrateurs modifié peuvent se connecter à l'aide des privilèges d'administrateur.

7. Vérifiez que les utilisateurs ayant le rôle Administrateurs modifié ne peuvent pas configurer les restrictions relatives aux métadonnées et au contenu sous l'onglet Paramètres.

Ajouter un compte d'utilisateur avec le rôle d'utilisateur d'agrégation au niveau du service

Pour vous assurer que les services Decoder et Log Decoder peuvent agréger les données vers un Concentrator ou un Broker :

1. Dans la vue **Services d'administration**, sélectionnez un service Decoder ou Log Decoder.

   Cliquez sur  **> Vue > Sécurité**.

2. Sous l'onglet **Utilisateurs**, ajoutez un utilisateur avec le rôle `Aggregation`, puis cliquez sur **Appliquer**.

   Remarque : La rubrique **Rôle d'agrégation** dans le *Guide de mise en route des hôtes et des services* fournit des détails sur l'application de ce rôle d'utilisateur.

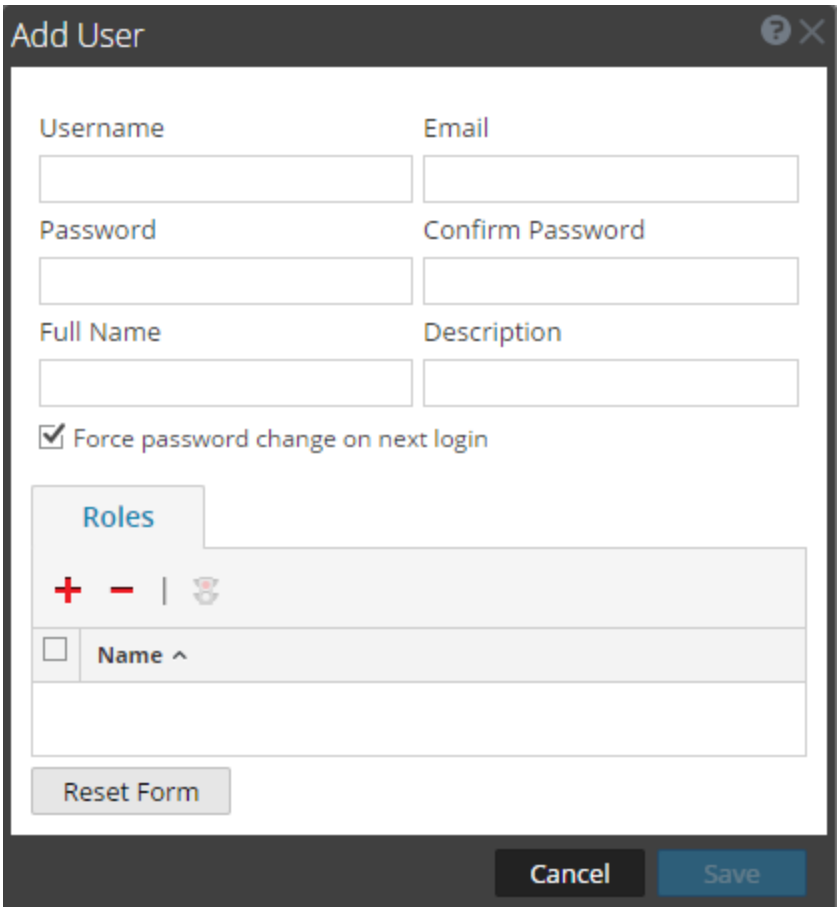
Ajouter un compte d'analyste et d'agent de protection des données sur Serveur NetWitness

Vous devez ajouter deux nouveaux comptes utilisateur dans NetWitness Suite au niveau du système pour représenter un spécialiste de la confidentialité des données et un analyste type. Si l'environnement est configuré à l'aide de connexions approuvées par défaut, vous n'avez pas besoin de créer les nouveaux comptes utilisateur sur les services Core (Brokers, Concentrators et Decoders). Lorsqu'un utilisateur est créé sur Serveur NetWitness, ce dernier peut se connecter aux services.

Remarque : Le nom du rôle est obligatoire pour le serveur et les services, il doit être identique pour les deux. Si vous créez un nouveau rôle personnalisé sur Serveur NetWitness, veillez à lui ajouter également tous les services Core.

1. Créez un nouveau compte d'utilisateur pour l'agent de protection des données :
   a. Dans la vue **Sécurité**, sélectionnez l'onglet **Utilisateurs** et cliquez sur +.

      La boîte de dialogue Ajouter un utilisateur s'affiche.



   b. Créez le nouveau compte avec les informations d'identification suivantes :

      Username = <nouveau nom d'utilisateur pour la connexion, par exemple, DPOadmin>
      Email = <nouvelle adresse e-mail de l'utilisateur, par exemple, DPOadmin@rsa.com>
      Password = <nouveau mot de passe de l'utilisateur pour la connexion, par exemple, RSAprivacy!@>
      Full Name = <nouveau nom complet de l'utilisateur, par exemple DPO Administrator>

   c. Dans la section **Rôles et attributs**, cliquez sur l'onglet **Rôles**, +, puis sélectionnez le rôle `Data_Privacy_Officers` pour le nouvel utilisateur.

   d. Sélectionnez **Enregistrer.**

2. Créez un nouveau compte d'utilisateur pour l'analyste avec des privilèges limités :
   a. Dans la vue **Admin > Sécurité**, cliquez sur l'onglet **Utilisateurs**. Dans la barre d'outils de l'onglet **Utilisateurs**, cliquez sur +.

La boîte de dialogue Ajouter un utilisateur s'affiche.

b. Créez le nouveau compte avec les informations d'identification suivantes :

Username = <nouveau nom d'utilisateur pour la connexion, par exemple, NonprivAnalyst>
Email = <nouvelle adresse e-mail de l'utilisateur, par exemple, NonprivAnalyst@rsa.com>
Password = <nouveau mot de passe de l'utilisateur pour la connexion, par exemple, RSAprivacy!@>
Full Name = <nouveau nom complet de l'utilisateur, par exemple Nonprivileged Analyst>

c. Dans la section **Rôles et attributs**, cliquez sur l'onglet **Rôles**,  , puis sélectionnez le rôle `Analysts` pour le nouvel utilisateur.

d. Sélectionnez **Enregistrer.**

Références de la confidentialité des données

Les documents de référence suivants sont disponibles pour gérer la confidentialité des données et la rétention de données. Accédez à la Table des matières principale pour la version 11.0 trouver des documents NetWitness Suite 11.0.

- Reportez-vous à la section **Onglet Confidentialité des données** dans le *Guide de configuration de Decoder et Log Decoder*.
- Reportez-vous à la section **Onglet Rétention de données - Archiver** dans le *Guide de configuration d'Archiver*.
- Reportez-vous à la section **Onglet Planificateur de rétention des données** dans le *Guide de mise en route des hôtes et des services*.