RSA NETWITNESS® SUITE

Guide de configuration d'Endpoint Insights

pour la version 11,1

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

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.

juillet 2018

Sommaire

Présentation de NetWitness Endpoint Insights

Remarque : Les informations de ce guide s'appliquent à la version 11.1 ou ultérieure.

RSA NetWitness Endpoint collecte les données des points de terminaison à partir des hôtes Windows, Mac Linux. Ces données peuvent être utilisées pour des procédures d'enquêtes du reporting, des alertes et des analyses. Les analystes peuvent effectuer des analyses instantanées à la recherche d'informations détaillées sur le comportement d'un hôte à n'importe quel point dans le temps. En outre, Endpoint peut collecter des logs à partir d'hôtes Windows. NetWitness Endpoint Insights présente deux types d'hôtes, Endpoint Hybrid et Endpoint Log Hybrid. Vous ne pouvez installer qu'une seule instance de type d'hôte dans votre déploiement. Cela signifie que vous pouvez déployer une seule instance de Endpoint Hybrid ou Endpoint Log Hybrid. Vous ne pouvez pas modifier le type après le déploiement.

Endpoint Hybrid collecte et gère les données du point de terminaison (hôte). Il génère des métadonnées pour la procédure d'enquête, l'analyse, l'alerte et le reporting. Il est configuré et géré de manière équivalente à un Log ou Packet Decoder. Endpoint Hybrid exécute un serveur Nginx (en mode proxy inversé) qui reçoit des données de la part de l'agent Endpoint. Les services suivants sont exécutés sur Endpoint Hybrid :

- Endpoint Server gère les données reçues par le biais de Nginx, les stocke dans la base de données Mongo et envoie des métadonnées vers le Log Decoder.
- Log Decoder capture les données à partir du Serveur Endpoint et traite les métadonnées.
- Concentrator regroupe les métadonnées provenant de Log Decoder et les rend disponibles pour tous les composants en amont comme Enquêter, Reporting Engine et Event Stream Analysis, à l'instar d'autres configurations NetWitness Decoder et Concentrator.

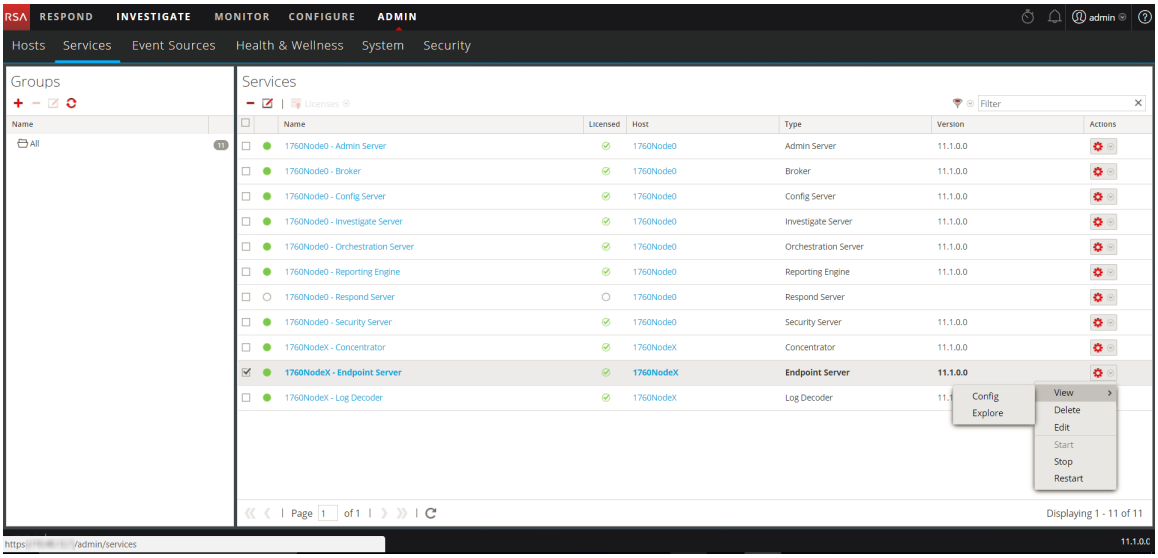
Endpoint Log Hybrid capture à la fois les données de point de terminaison et de log. En plus des services s'exécutant sur Endpoint Hybrid, un service Log Collector s'exécute sur Endpoint Log Hybrid. Il collecte des logs à partir des hôtes Windows et toutes les autres sources d'événements qui sont prises en charge pour la collecte de logs de NetWitness Suite.

Le *Guide de mise en route des hôtes et services* fournit les informations dont vous avez besoin pour comprendre et installer tous les services de NetWitness Suite.

La **configuration de base** implique :

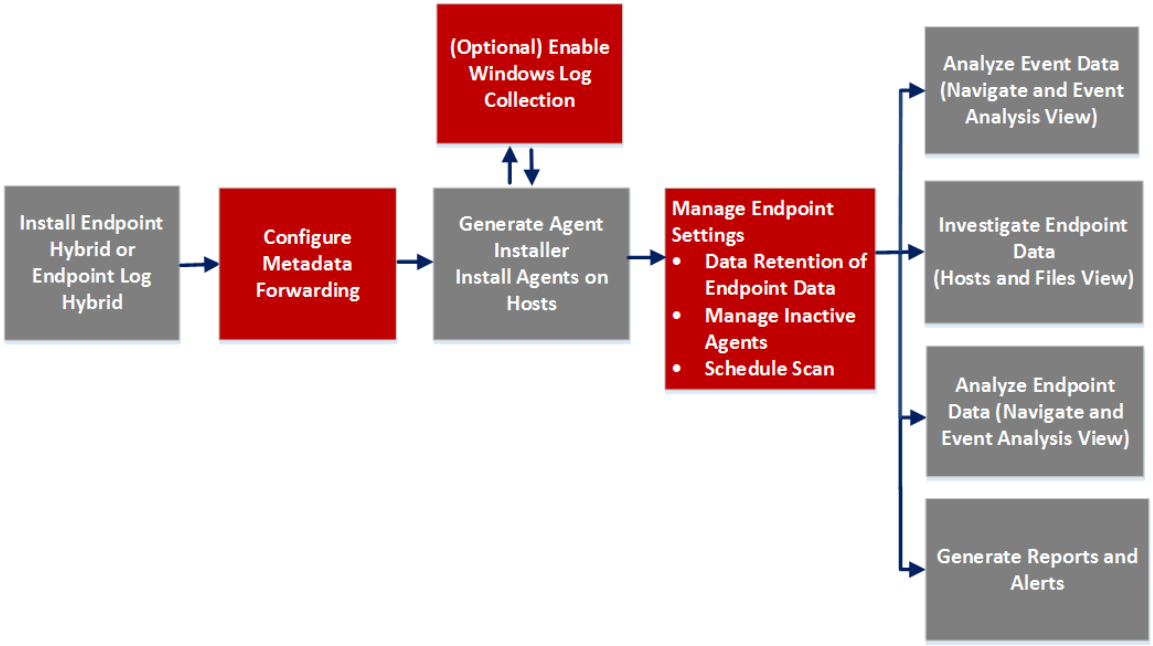
- Installer des agents sur les hôtes
- Configuration du transfert de métadonnées Endpoint, du planning d'analyse et des politiques de rétention
- Définition des politiques de santé et d'intégrité pour surveiller le serveur Endpoint.

Vous pouvez configurer les paramètres requis en utilisant les options dans l'interface utilisateur de NetWitness Suite sous la vue Configuration des services d'administration (**ADMIN > Services > Serveur Endpoint > Config.**).



Configuration du Serveur Endpoint

Cette rubrique décrit les tâches générales nécessaires à la configuration du service Serveur Endpoint.



Tâches	Description

Installer Endpoint Hybrid ou Endpoint Log Hybrid	Consultez le *Guide d'Installation des hôtes physiques* et le *Guide de configuration des hôtes virtuels*.
	
	Remarque : Après avoir installé Endpoint Hybrid ou Endpoint Log Hybrid, enregistrez l'adresse IP de l'hôte du serveur Endpoint sur le serveur NW comme suit :
	1. Ouvrez une session SSH sur le serveur NW.
	2. Accédez au répertoire `/opt/rsa/saTools/bin`.
	`cd /opt/rsa/saTools/bin`
	3. Exécutez le script `register-endpoint` indiquant l'adresse IP de l'hôte Endpoint.
	`./register-endpoint-ip -v --host-addr <ip-address>`
	Le script prend quelques minutes pour mettre à jour l'adresse IP du Serveur Endpoint.

Tâches	Description
Configurer le transfert de métadonnées pour les agents NetWitness Endpoint 11.1	Comme pour les Logs et les Paquets, vous pouvez afficher les métadonnées Endpoint dans la vue Naviguer et Analyse d'événements. Vous pouvez également générer des rapports et des alertes pour les données Endpoint. Par défaut, l'option Métadonnées Endpoint est désactivée. L'agent doit être installé avec l'option Métadonnées Endpoint activée pour pourvoir transférer les métadonnées.
Installer des agents sur les hôtes	Le programme d'installation d'agents Endpoint est généré à l'aide de l'onglet Packager sous **ADMIN > Services > Config > Serveur Endpoint** à partir de l'interface utilisateur de NetWitness Suite. Le Packager est un fichier zip contenant des fichiers exécutables et des fichiers de configuration permettant de générer un programme d'installation d'agent pour les systèmes d'exploitation Linux, Mac et Windows. Vous pouvez installer une seule version de l'agent sur un hôte. Si vous disposez d'une version précédente d'un agent installé (par exemple, 4.4), désinstallez cet agent pour installer l'agent 11.1. Une fois que l'agent est installé, il apparaît dans la vue **Enquêter > Hôtes**. Par défaut, les données Endpoint sont publiées pour la première fois. Pour collecter les données Endpoint ultérieures, vous devez effectuer une analyse ad hoc ou planifier une analyse. Elle récupère des données telles que les pilotes, processus, DLL, fichiers (exécutables), services, autoruns, informations de sécurité, configurations système et scripts disponibles sur l'hôte. Si l'agent est configuré pour la collecte des logs, il collecte les fichiers log depuis des hôtes Windows et les transfère vers un Log Decoder ou Remote Log Collector. Pour plus d'informations sur l'installation de l'agent Endpoint, reportez-vous à la section *Guide d'installation de l'agent Endpoint Insignts*.
Procédure d'enquête sur des données Endpoint	Vous pouvez enquêter sur les données Endpoint dans les vues **Enquêter > Hôtes** et **Enquêter > Fichiers**. Pour plus d'informations, consultez le *Guide d'utilisation Enquêter*.
Configurer la planification de l'analyse	Planifiez une analyse à exécuter de manière quotidienne ou hebdomadaire.
Configurer la rétention de données	Définir des politiques de rétention de données pour stocker et gérer les données Endpoint de manière optimale, en fonction de l'âge des données Endpoint ou de la taille du stockage. Par défaut, 30 jours de données d'agent sont conservées.

Tâches	Description
Gérer les agents inactifs	Par défaut, les agents (y compris toutes les données Endpoint collectées) qui n'ont pas communiqué avec le serveur Endpoint pendant 90 jours sont automatiquement supprimées.

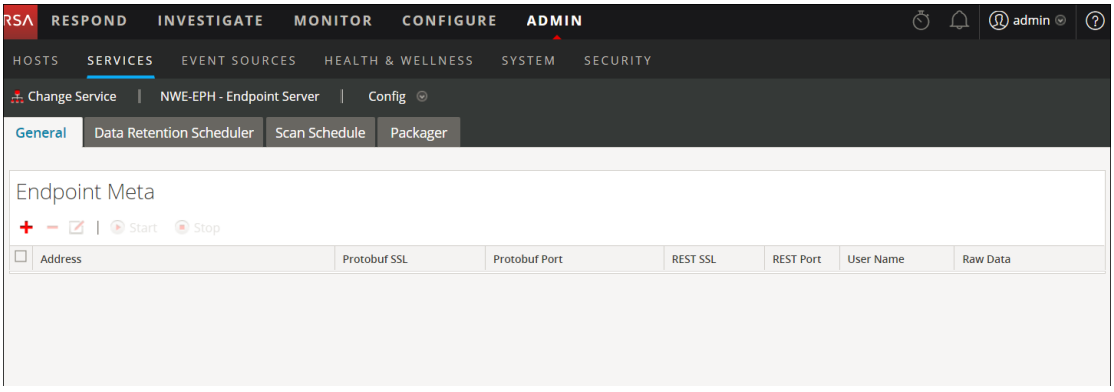
Configurer le transfert de métadonnées pour les agents NetWitness Endpoint 11.1

Vous pouvez afficher les métadonnées Endpoint dans la vue Enquêter de NetWitness Suite (**Naviguer** et **Analyse d'événements**), à l'instar des Logs et des Paquets. Vous devez activer le transfert de métadonnées afin de transférer les catégories suivantes :

Système d'exploitation	Catégories
Windows	Fichier, Service, DLL, Processus, Tâche, Autorun et Machine
Linux	Fichier, Bibliothèque chargée, Systemd, Processus, Cron, Initd et Machine
Mac	Fichier, Daemon, Processus, Tâche, Dylib, Autorun et Machine

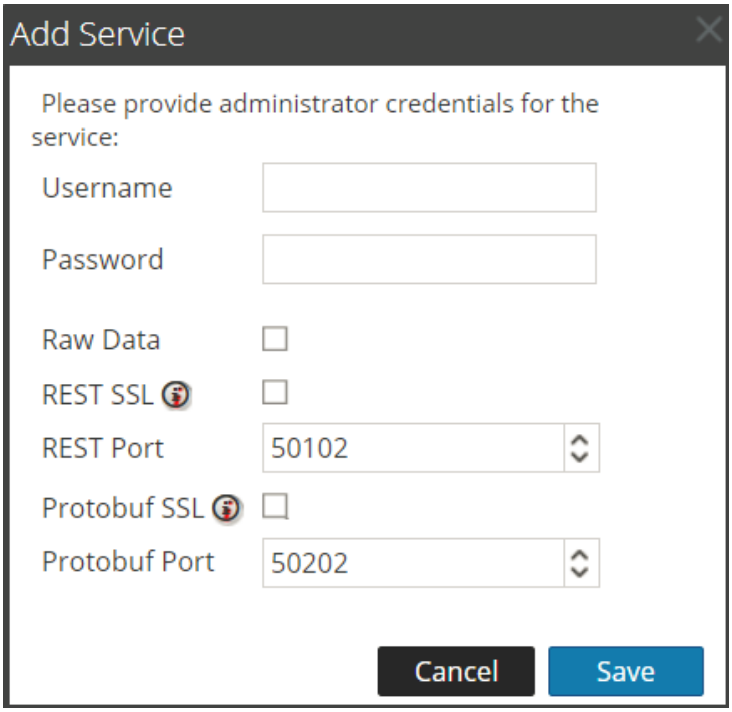
Configuration du transfert de métadonnées

1. Accédez à **ADMIN** > **Services**.
2. Dans la vue Services, sélectionnez le service **Serveur Endpoint**.
3. Cliquez sur  et sélectionnez > **Vue** > **Config**.
4. Cliquez sur l'onglet **Général**.



5. Cliquez sur + dans la barre d'outils.
   La boîte de dialogue Services disponibles s'affiche.
6. Sélectionnez le service Log Decoder et cliquez sur **OK**.

La boîte de dialogue Ajouter un service s'affiche. Vous pouvez ajouter un seul service Log Decoder.



7. Entrez les informations d'identification de l'administrateur pour l'authentification.
8. (Facultatif) Si vous activez les Données brutes, un bref résumé de la session avec les métadonnées est envoyé.
9. (Facultatif) Si vous avez activé SSL sur le port REST du Log Decoder, sélectionnez l'option **REST SSL**. Par défaut, le port REST est 50202 pour non SSL et 56202 pour SSL.
10. Sélectionnez l'option **Protobuf SSL** pour activer SSL sur Protobuf. Le port Protobuf par défaut est 50202.
11. Cliquez sur **Enregistrer**.

Après avoir configuré le transfert de métadonnées, veillez à :

- Démarrer la capture dans le Log Decoder
- Démarrer l'agrégation sur le Concentrator
- Ajouter le Log Decoder en tant que service dans le **Concentrator**

Démarrage du transfert de métadonnées vers le Log Decoder

1. Dans la vue Configuration des métadonnées Endpoint, sélectionnez le service.
2. Cliquez sur Start

   Le Serveur Endpoint commence à transférer les métadonnées vers le Log Decoder.

Arrêt du transfert de métadonnées vers le Log Decoder

1. Dans la vue Configuration des métadonnées Endpoint, sélectionnez le service.
2. Cliquez sur Stop.

   Le Serveur Endpoint arrête de transférer les métadonnées vers le Log Decoder.

Suppression du transfert de métadonnées

Remarque : Assurez-vous d'arrêter le service avant de supprimer le transfert de métadonnées.

1. Dans la vue Configuration des métadonnées Endpoint, sélectionnez le service.
2. Cliquez sur .
3. Cliquez sur **Appliquer**.

Mappages de métadonnées des points de terminaison

Vous pouvez afficher les mappages de métadonnées par défaut ou modifier les mappages de métadonnées pour les points de terminaison.

Schéma JSON pour les mappages de métadonnées

Tous les mappages de métadonnées sont configurés à l'aide du schéma JSON. Vous trouverez ci-dessous un exemple de schéma JSON :

```
{
"metaKeyPairs" : [
     {
     "metaKeyPairsCategory" : "",
     "keyPairs" : [
          {
          "endpointJpath" : "",
          "metaName" : "",
          "type" : "",
          "enabled" : true
          },
          {
```

```
            "endpointJpath" : "",
            "metaName" : "",
            "type" : "",
            "enabled" : true
            }
        ]
        }
]
}
```

Les API suivantes sont utilisées pour afficher ou modifier les mappages de métadonnées :

- `get-default` : affiche les configurations par défaut pour les mappages de métadonnées des points de terminaison.
- `get-custom` : affiche les configurations personnalisées des mappages de métadonnées des points de terminaison.
- `set-custom` : vous pouvez personnaliser les mappages de métadonnées des points de terminaison.

Afficher les mappages de métadonnées

Pour afficher les mappages de métadonnées des points de terminaison :

1. Sur le serveur NW, exécutez la commande `nw-shell` dans l'invite de commandes.
2. Exécutez la commande `login` et saisissez les informations d'identification.
3. Connectez-vous au serveur Endpoint à l'aide de la commande suivante :
   `connect --host <IP address> --port <number>`

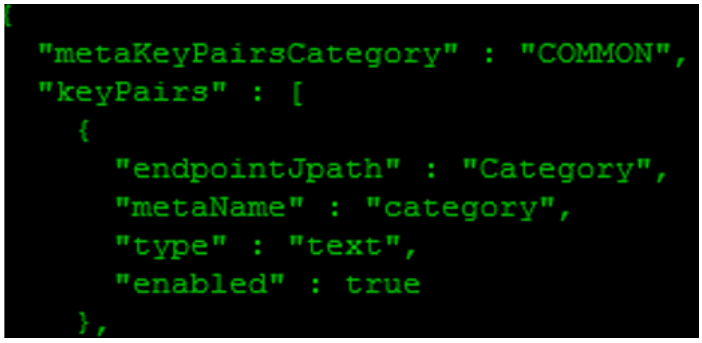
   Remarque : Le port par défaut est le port 7050.
4. Exécutez les commandes suivantes :
   ```
   cd endpoint/meta
   cd get-default
   invoke
   ```

L'écran suivant présente les mappages de métadonnées par défaut :

Pour désactiver un mappage de métadonnées par défaut :

Saisissez la même valeur endpointJpath et définissez le paramètre enabled sur `false`.

Par exemple, si la valeur endpointJpath est `Category` et le paramètre enabled est `true`, saisissez la même valeur endpointJpath et définissez le paramètre enabled sur `false`.



Remarque : Ne modifiez pas la valeur metaKeyPairsCategory du schéma “COMMON”, “COMMON_MACHINE”, “COMMON_MACHINE_FOR_EVENTS”.

Pour modifier le nom ou le type de métadonnées :

Saisissez la même valeur endpointJpath et spécifiez les valeurs metaName et type.

Remarque : La valeur metaName doit exister dans le fichier table-map.xml du Log Decoder, index-concentrator.xml ou index-concentrator-custom.xml du Concentrator pour que metaName apparaisse dans la vue Enquêter.

Ajout ou modification des mappages de métadonnées

Pour ajouter ou modifier les mappages de métadonnées, exécutez l'API `set-custom`. La configuration metaKeyPairs fournie dans le fichier JSON doit correspondre au schéma JSON de la configuration par défaut reçue via l'API `get-default`.

1. Sur le serveur NW, exécutez la commande `nw-shell` dans l'invite de commandes.
2. Exécutez la commande `login` et saisissez les informations d'identification.
3. Connectez-vous au serveur Endpoint à l'aide des commandes suivantes :
   ```
   connect --host <IP address> --port <number>
   ```

   Remarque : Le numéro de port par défaut est 7050)
4. Exécutez les commandes suivantes :
   ```
   cd endpoint/meta
   cd set-custom
   invoke –file <json file>
   ```

Vous pouvez ajouter de nouvelles metaKeys en ajoutant les entrées dans le fichier qui sera téléchargé à l'aide de l'API `set-custom`. L'exemple suivant montre comment ajouter un nouveau mappage de métadonnées :

```
[root@NODE0-1982-SIGNED ~]# nw-shell
RSA NetWitness Shell. Version: 2.9.2
See "help" to list available commands, "help connect" to get started.
offline » login
user: admin
password: **********
admin@offline » connect --host [redacted] --port 7050
Connected to endpoint-server ([redacted])
admin@Folder:/rsa » cd endpoint/meta/set-custom
admin@Method:/rsa/endpoint/meta/set-custom » invoke --file /custom.json
admin@Method:/rsa/endpoint/meta/set-custom » cd ../get-custom
admin@Method:/rsa/endpoint/meta/get-custom » invoke
{
  "metaKeyPairs" : [
    {
      "metaKeyPairsCategory" : "NETWORK",
      "keyPairs" : [
        {
          "endpointJpath" : "file/checksumSha1",
          "metaName" : "checksum",
          "type" : "text",
          "enabled" : true
        }
      ]
    }
  ]
}
admin@Method:/rsa/endpoint/meta/get-custom »
```

Affichage des mappages de métadonnées personnalisées

Pour afficher les mappages de métadonnées personnalisées, exécutez l'API `get-custom`.

Remarque : L'API `get-custom` renvoie des valeurs uniquement si les mappages de métadonnées sont modifiés à l'aide de l'API `set-custom`.

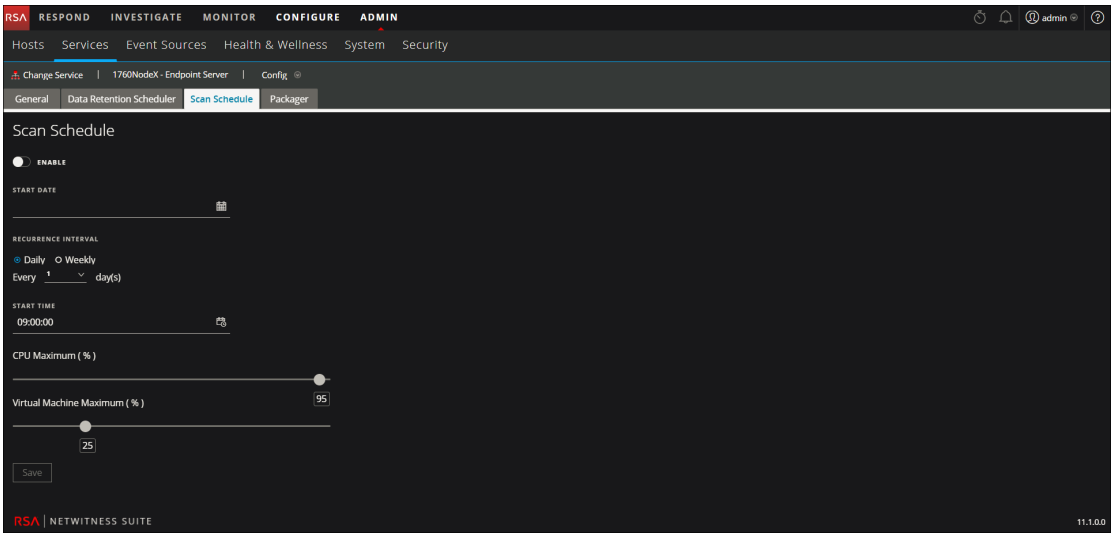
Configurer la planification de l'analyse

Vous pouvez planifier une analyse à exécuter de manière quotidienne ou hebdomadaire.

Remarque : Un seul planning s'appliquant à tous les agents peut être configuré.

Pour configurer la planification de l'analyse :

1. Accédez à **Administrateur** > **Services**.
2. Dans la vue Services, sélectionnez le service **Serveur Endpoint**.
3. Cliquez sur  et sélectionnez > **Vue** > **Config**.
4. Cliquez sur l'onglet **Planning d'analyse**.



5. Cliquez sur le bouton à bascule **Activer** pour configurer l'analyse.
6. Sélectionnez la **Date de début**.
7. Sélectionnez l'intervalle de récurrence : Tous les jours ou Toutes les semaines.

   Remarque : Les valeurs saisies sont spécifiques au fuseau horaire de l'agent.

8. Pour une analyse quotidienne :
   - Sélectionnez l'intervalle de récurrence **Tous les jours**.
   - Spécifiez la fréquence d'analyse en jours.

9. Pour une analyse hebdomadaire :
   - Sélectionnez l'intervalle de récurrence **Toutes les semaines**.
   - Spécifiez la fréquence d'analyse en semaines.
   - Sélectionnez le jour de la semaine.
10. Saisissez l'heure de début de l'analyse.
11. Définissez la valeur maximale du CPU à l'aide du curseur. Cela garantit la limite de CPU de l'agent NetWitness Endpoint. Si les agents sont en cours d'exécution sur les machines virtuelles, définissez la valeur maximale de la machine virtuelle à l'aide du curseur.
12. Cliquez sur **Enregistrer** pour enregistrer la configuration.

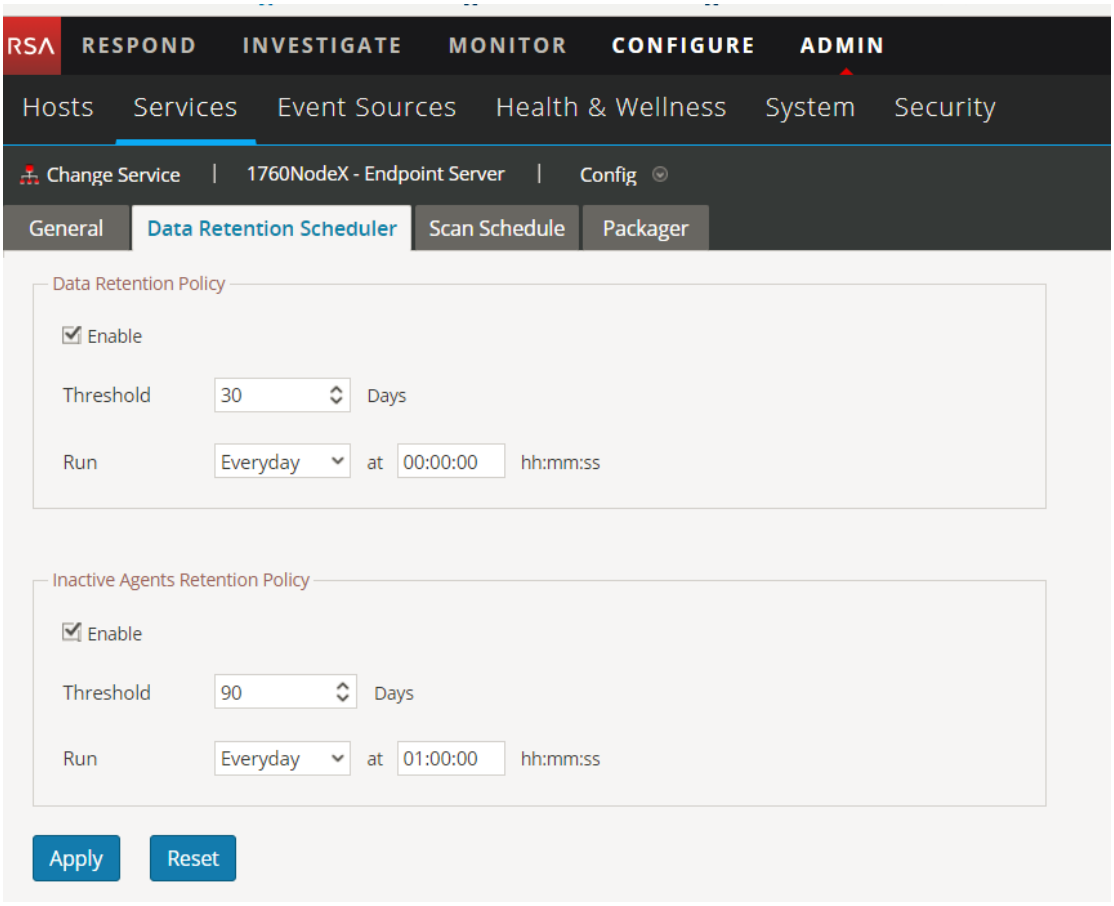
Remarque : Si un agent n'est pas en mesure d'effectuer l'analyse à l'heure programmée car la machine est mise hors tension ou le service de l'agent est arrêté, l'analyse suivante est basée sur la différence de temps écoulé entre l'heure actuelle et l'heure de la prochaine analyse planifiée.
Par exemple, si une analyse est planifiée pour s'exécuter chaque mercredi à 18 h 00, que le service de l'agent est interrompu avant l'heure de début de l'analyse, et qu'il redevient opérationnel le jeudi à 10 h, l'agent attend que le système soit entièrement opérationnel et exécute une analyse immédiatement.
Mais si le service ne redevient opérationnel que le lundi suivant à 13 h, l'analyse s'exécute le mercredi suivant à 18 h 00.

Configurer la rétention de données

Un administrateur peut configurer les stratégies de rétention pour conserver les données Endpoint en fonction de l'âge ou de la taille du stockage. Par défaut, les politiques de rétention basées sur les jours et la taille sont activées.

Pour modifier la configuration de rétention basée sur l'âge :

1. Accédez à **Admin** > **Services**.
2. Dans la vue Services, sélectionnez le service **Serveur Endpoint**.
3. Cliquez sur  et sélectionnez > **Vue** > **Config**.
4. Cliquez sur l'onglet **Planificateur de rétention des données**.

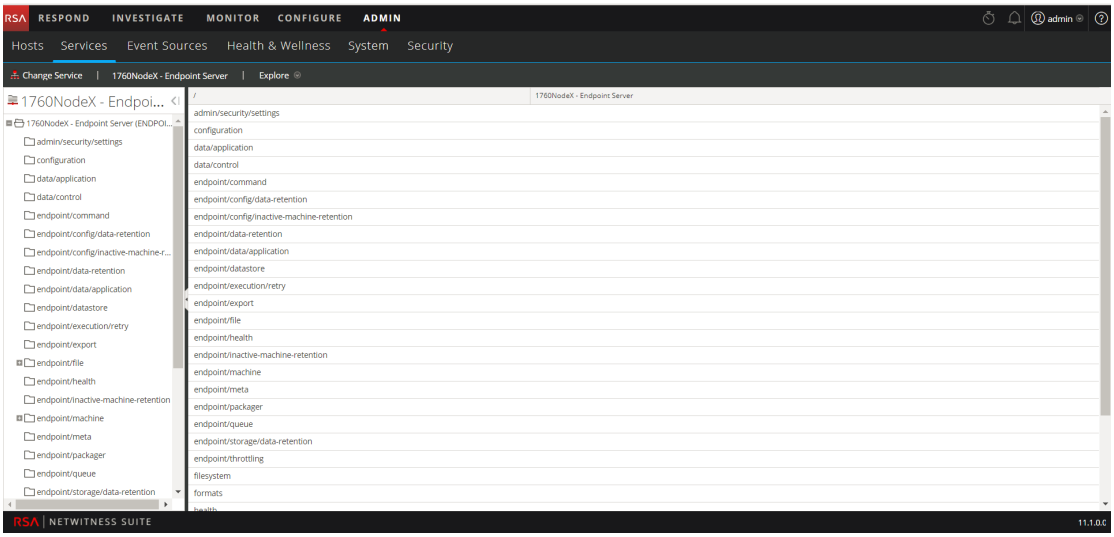


5. Dans le panneau **Politique de rétention des données**, par défaut, le **Seuil** est défini sur 30 jours, et **Exécuter** sur Tous les jours. Cela signifie que 30 jours de données Endpoint sont retenues et les données les plus anciennes sont supprimées de la base de données.
6. Cliquez sur **Appliquer**.

Pour modifier la configuration de rétention basée sur l'âge :

Par défaut, pour la rétention basée sur la taille, la valeur `rollover-after` est définie sur 80 et `rollover-chunk-size` est définie sur 10. Cela signifie que lorsque la taille du stockage dépasse 80 % de l'espace alloué sur la partition de disque, 10 % de données Endpoint plus anciennes sont supprimées de la base de données. Toutefois, vous pouvez modifier ces valeurs comme suit :

1. Dans le menu principal, accédez à **Admin** > **Services**.
2. Dans la vue Services, sélectionnez le service **Serveur Endpoint**.
3. Cliquez sur  et sélectionnez > **Vue** > **Explorer**. La vue Explorer s'affiche :



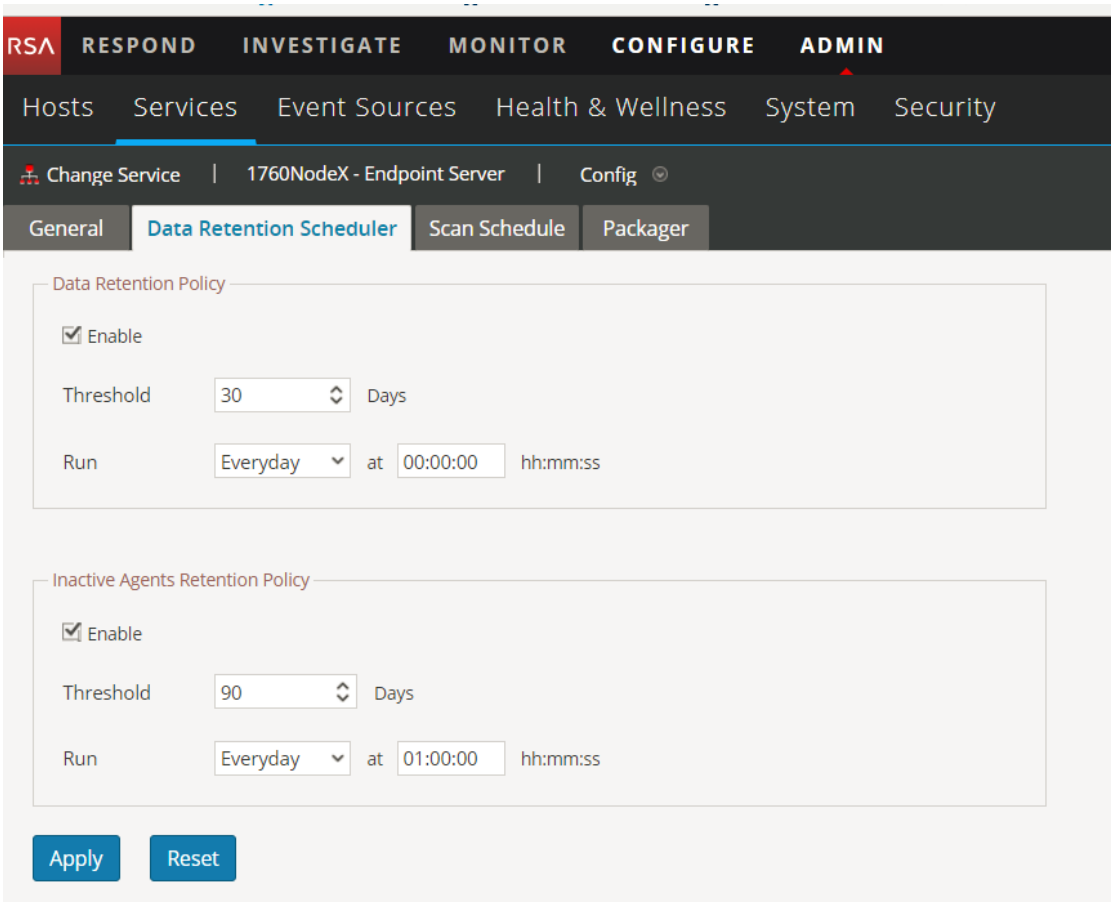
4. Dans le volet de gauche, sélectionnez **endpoint/config/data-retention**.
5. Modifiez les configurations en fonction de vos besoins.

Gérer les agents inactifs

Un administrateur peut configurer une politique de rétention des agents inactifs pour supprimer les données des agents qui sont inactifs, à partir du Serveur Endpoint. Lors de la suppression, le Serveur Endpoint cesse de collecter des données provenant de ces agents. Cette option est activée par défaut.

Pour configurer la politique de rétention des agents inactifs :

1. Accédez à **Administrateur** > **Services**.
2. Dans la vue Services, sélectionnez **Serveur Endpoint**.
3. Cliquez sur  et sélectionnez > **Vue** > **Config**.
4. Cliquez sur l'onglet **Planificateur de rétention des données**.



5. Dans le panneau **Politique de rétention des agents inactifs**, par défaut, le **Seuil** est défini sur 90 jours, et **Exécuter** sur Tous les jours. Cela signifie que les données des agents qui n'ont pas communiqué avec le Serveur Endpoint depuis 90 jours sont supprimées de la base

de données.

6. Cliquez sur **Appliquer**.

Remarque : La Politique de rétention des agents inactifs n'est pas applicable pour les agents NetWitness Endpoint 4.4.0.2 ou version ultérieure.

Intégration de NetWitness Endpoint 4.4.0.2 ou une version ultérieure à NetWitness Endpoint 11.1

Vous pouvez configurer les métadonnées Endpoint pour NetWitness Endpoint 4.4.0.2 de l'une des manières suivantes :

- **(Option 1) Intégrer le serveur de Console NetWitness Endpoint 4.4.0.2 à Endpoint Hybrid ou Endpoint Log Hybrid** - Les données des agents NetWitness Endpoint 4.4.0.2 ou version ultérieure sont disponibles dans la vue **Enquêter > Hôtes** et **Fichiers**, et vous pouvez afficher les métadonnées Endpoint dans la vue **Enquêter > Naviguer** et **Analyse d'événements**. Pour cette option, assurez-vous que le serveur Endpoint est configuré pour le transfert des métadonnées.
- **(Option 2) Intégrer le service Meta Integrator à NetWitness 4.4.0.2 directement vers un Log Decoder** - Vous pouvez afficher les métadonnées Endpoint dans la vue **Enquêter > Naviguer** et **Analyse d'événements**. Les données d'agents NetWitness Endpoint 4.4 ne sont pas disponibles dans la vue **Enquêter > Hôtes** et **Fichiers**.

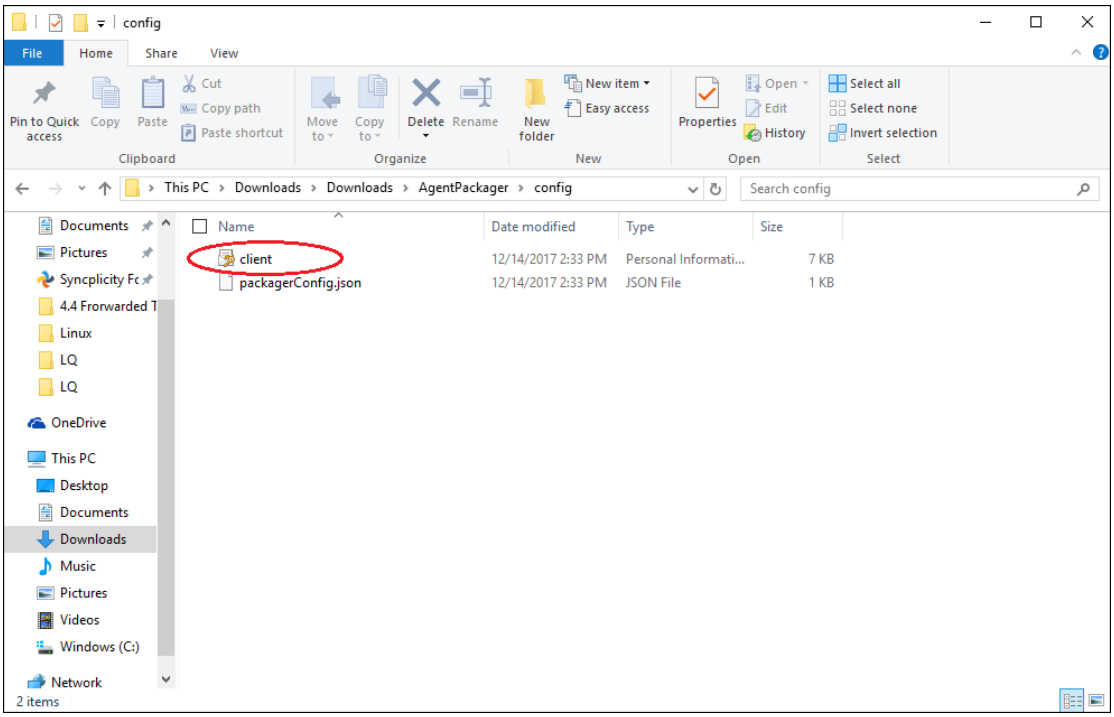
Outre les catégories mentionnées pour les agents NetWitness Endpoint 11.1, les catégories suivantes sont également transmises aux agents NetWitness Endpoint 4.4.0.2 ou version ultérieure : Événement de fichiers, Événement réseau, Événement de registre et Événement de processus.

Configuration du serveur de Console NetWitness Endpoint 4.4.0.2

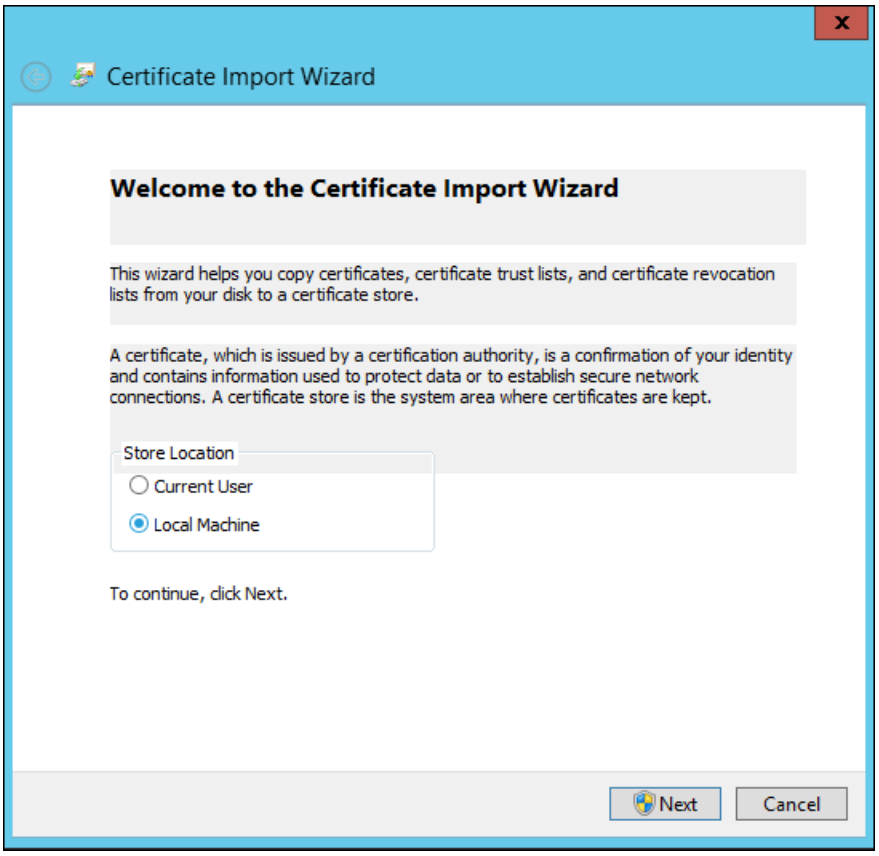
Configuration du certificat client sur le serveur de Console NetWitness Endpoint 4.4.0.2 (pour l'Option 1)

Le serveur de Console NetWitness Endpoint 4.4.0.2 doit utiliser le même certificat client que les agents NetWitness Endpoint 11.1 utilisent pour transférer les métadonnées sur le Serveur Endpoint.

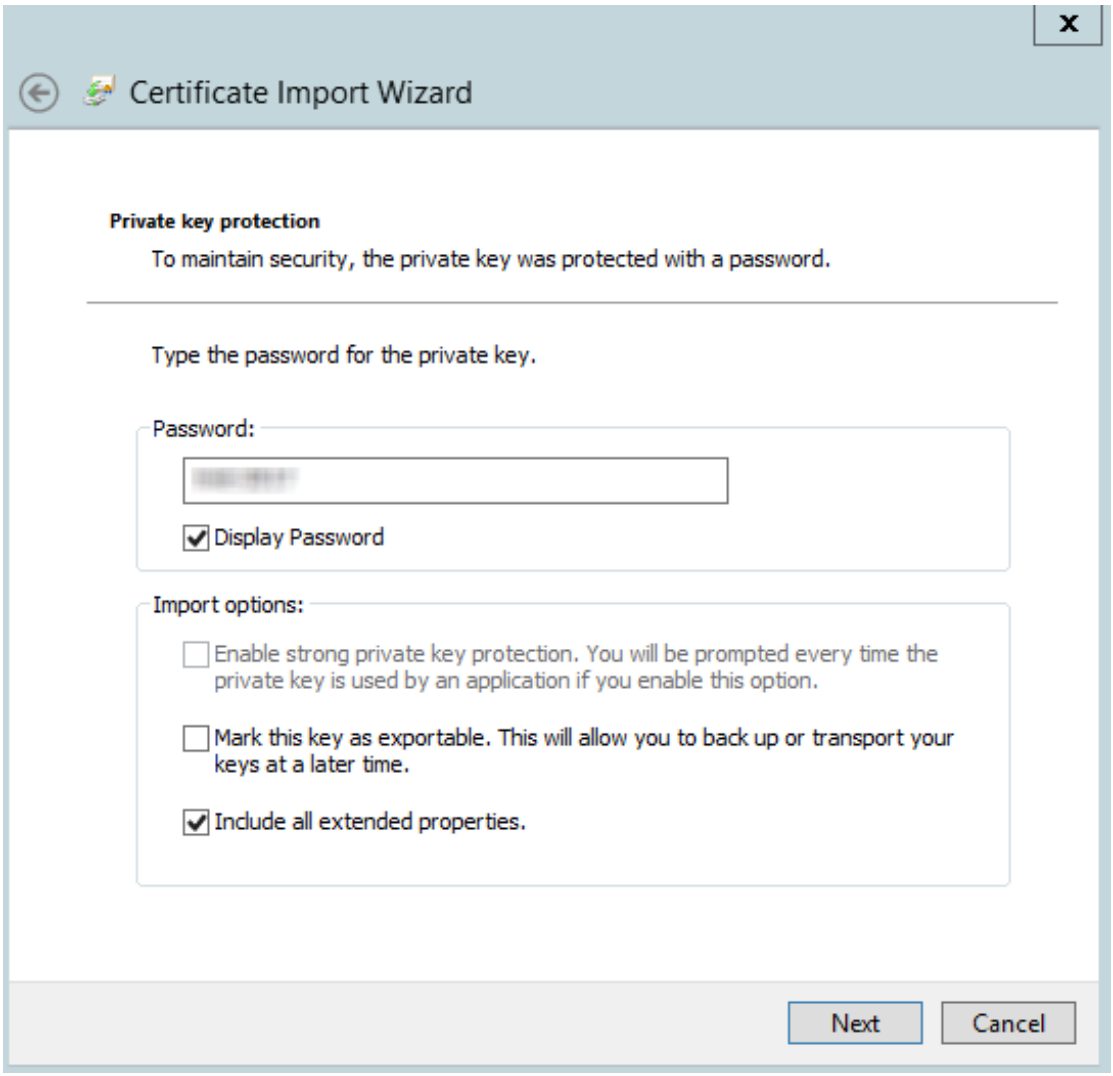
1. Téléchargez le packager d'agent. Pour plus d'informations, reportez-vous au *Guide d'installation de l'agent Endpoint Insights*.
2. Extrayez **AgentPackager.zip** et dans le dossier Config, récupérez le certificat client.
3. Copiez le certificat client dans le serveur de Console NetWitness Endpoint 4.4.



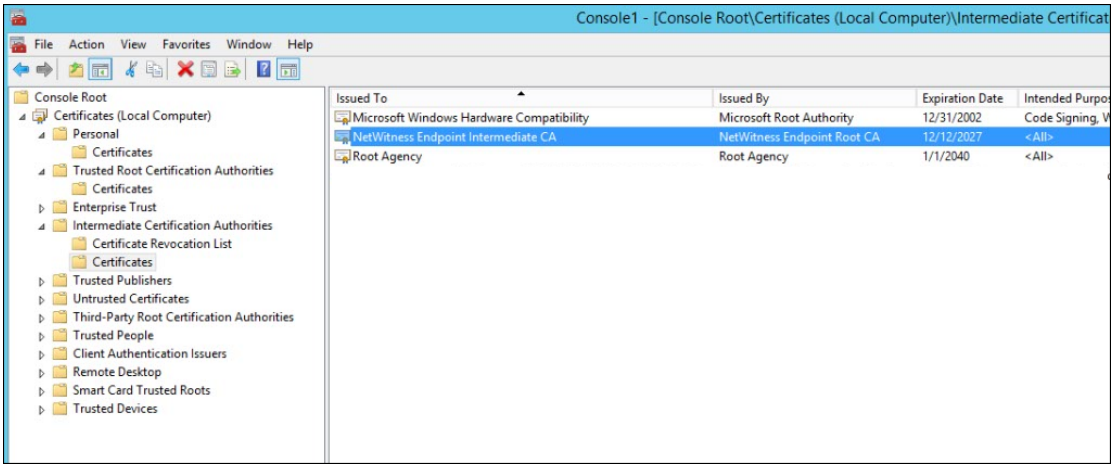
4. Double-cliquez sur le fichier **client**.
   La boîte de dialogue **Assistant d'importation de certificat** s'affiche.
5. Sélectionnez l'emplacement de stockage en tant que **Machine locale**, puis cliquez sur **Suivant**.



6. Sélectionnez le fichier à importer, puis cliquez sur **Suivant**.
7. Saisissez le mot de passe utilisé lors de la génération du packager de l'agent.



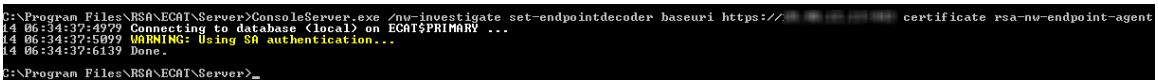
8. Cliquez sur **Suivant** et **Terminer**.
Le certificat est répertorié sous **Personnel**, **Autorités de certification intermédiaires** > **Certificat** et **Autorités de certification racines de confiance** dans le serveur de Console.



Activation du transfert de métadonnées dans NetWitness Endpoint 4.4.0.2 (pour l'Option 1)

Pour activer le transfert de métadonnées pour les agents NetWitness Endpoint 4.4.0.2 sélectionnés, exécutez la commande suivante :

`ConsoleServer.exe /nw-investigate set-endpointdecoder baseuri <ENDPOINT HOST> certificate <CERTIFICATE DISPLAY NAME>.`



Par exemple, `ConsoleServer.exe /nw-investigate set-endpointdecoder baseuri https://<Ip Address>:443 certificate rsa-nw-endpoint-agent`

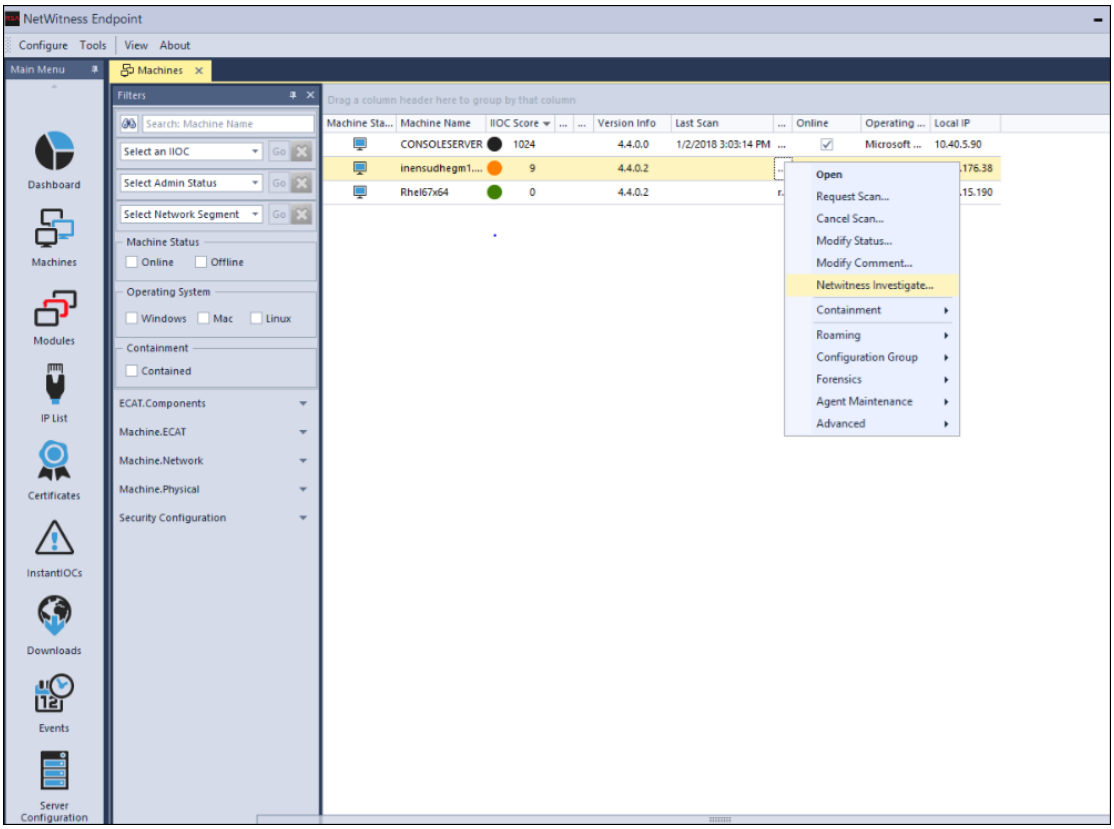
Activation du transfert de métadonnées dans NetWitness Endpoint 4.4.0.2 vers le Log Decoder (pour l'Option 2)

Pour activer le service Metadata Integrator pour les agents NetWitness Endpoint 4.4.0.2, exécutez la commande suivante :
`ConsoleServer.exe /nw-investigate enable.`

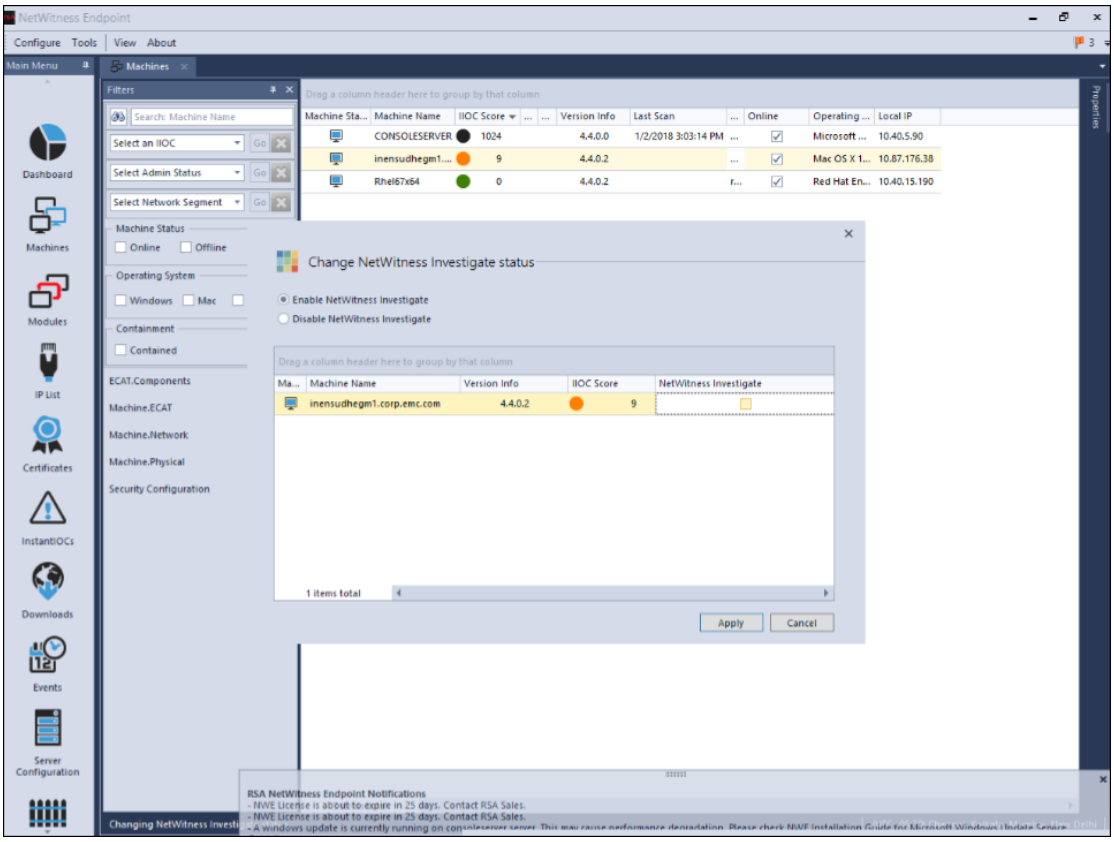
Activation de machines pour transférer les métadonnées de NetWitness Endpoint 4.4.0.2 vers le serveur NetWitness Endpoint (pour les Options 1 et 2)

Après avoir activé le transfert des métadonnées à l'aide de l'une des options ci-dessus, procédez comme suit pour permettre aux ordinateurs de transférer les métadonnées.

1. Ouvrez l'interface utilisateur NetWitness Endpoint 4.4.0.2.
2. Dans le volet de gauche, cliquez sur **Machines**. La liste de machines disponibles s'affiche.



3. Sélectionnez les machines pour lesquelles vous souhaitez transférer les métadonnées vers le serveur NetWitness Endpoint.
4. Cliquez avec le bouton droit et sélectionnez l'option **NetWitness Enquêter**.
   La boîte de dialogue Modifier l'état NetWitness Enquêter s'affiche.



5. Sélectionnez l'option **Activer NetWitness Enquêter**.
6. Cliquez sur **Appliquer**.
7. Pour vérifier si l'option **Activer NetWitness Enquêter** est activée, répétez l'étape 4.

Références Endpoint

Cette section est destinée à vous aider à comprendre l'objectif de la vue Configuration des Services du serveur Endpoint. Chaque configuration fait l'objet d'une brève introduction et comporte un tableau Que voulez-vous faire, contenant des liens vers les procédures associées. En outre, elle comprend des workflows et des recherches rapides pour mettre en évidence des fonctions importantes de l'interface utilisateur.

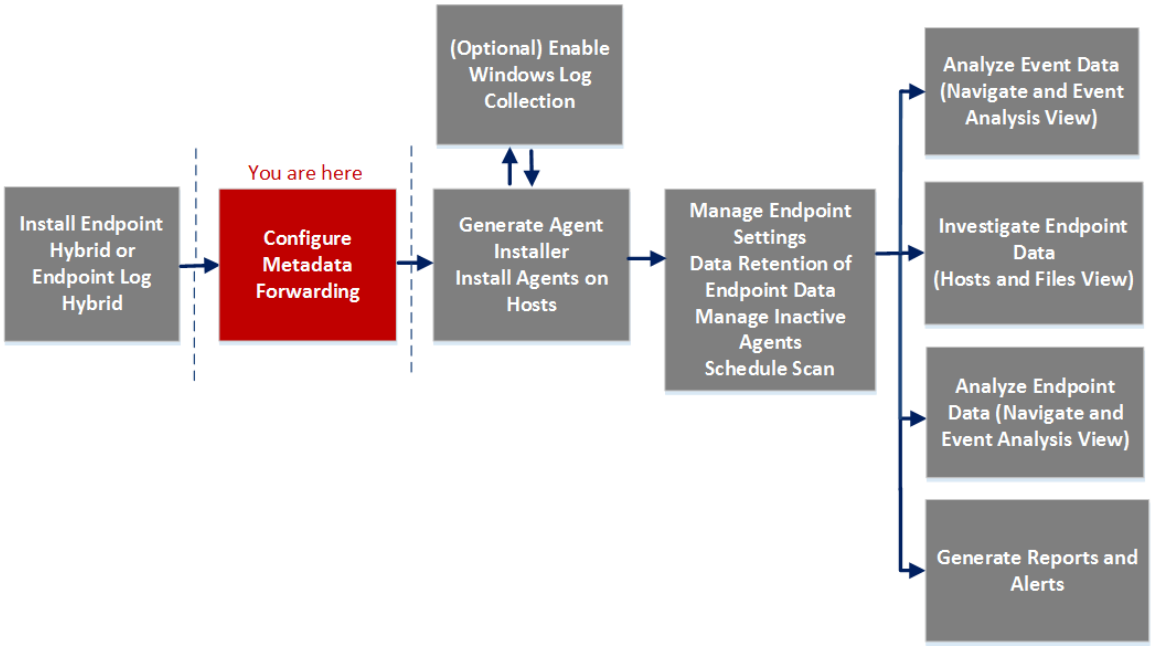
Vous pouvez afficher les nœuds de service complets sous forme d'arborescence dans la vue Explorer les services. Pour plus d'informations, reportez-vous à la rubrique « Vue Explorer les services » du *Guide de mise en route de l'hôte et des services*.

Onglet Général

Dans l'onglet **Général**, vous pouvez configurer le transfert des métadonnées Endpoint. Pour accéder à cette vue :

1. Accédez à **Administrateur** > **Services**.
2. Dans la vue Services, sélectionnez **Serveur Endpoint**.
3. Cliquez sur  et sélectionnez > **Vue** > **Config**.
4. Cliquez sur l'onglet **Général**.

Workflow



Que voulez-vous faire ?

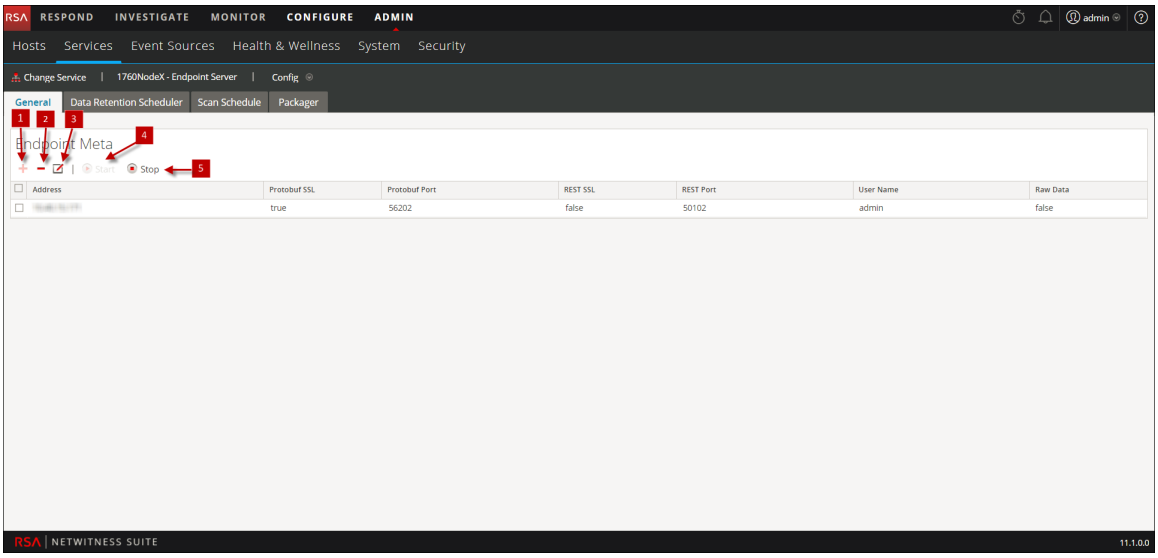
Rôle	Je souhaite...	Me montrer comment
Administrateur	Configurer le transfert de métadonnées Endpoint pour les agents NetWitness Endpoint 11.1	Configuration du transfert de métadonnées

Rôle	Je souhaite...	Me montrer comment
Administrateur	Configurer le transfert de métadonnées Endpoint pour les agents NetWitness Endpoint 4.4.0.2 ou de version ultérieure	Intégration de NetWitness Endpoint 4.4.0.2 ou une version ultérieure à NetWitness Endpoint 11.1

*Vous pouvez effectuer cette tâche dans la vue actuelle.

Aperçu rapide

La figure suivante donne un exemple de l'onglet Général.



1. Cliquez sur + pour afficher la boîte de dialogue **Services disponibles**.
2. Cliquez sur − pour supprimer le service ajouté.
3. Cliquez sur pour modifier les informations relatives au service ajouté.
4. Cliquez sur Start pour démarrer le transfert des métadonnées Endpoint.
5. Cliquez sur Stop pour arrêter le transfert des métadonnées Endpoint.

Le tableau suivant décrit les champs de l'onglet Général.

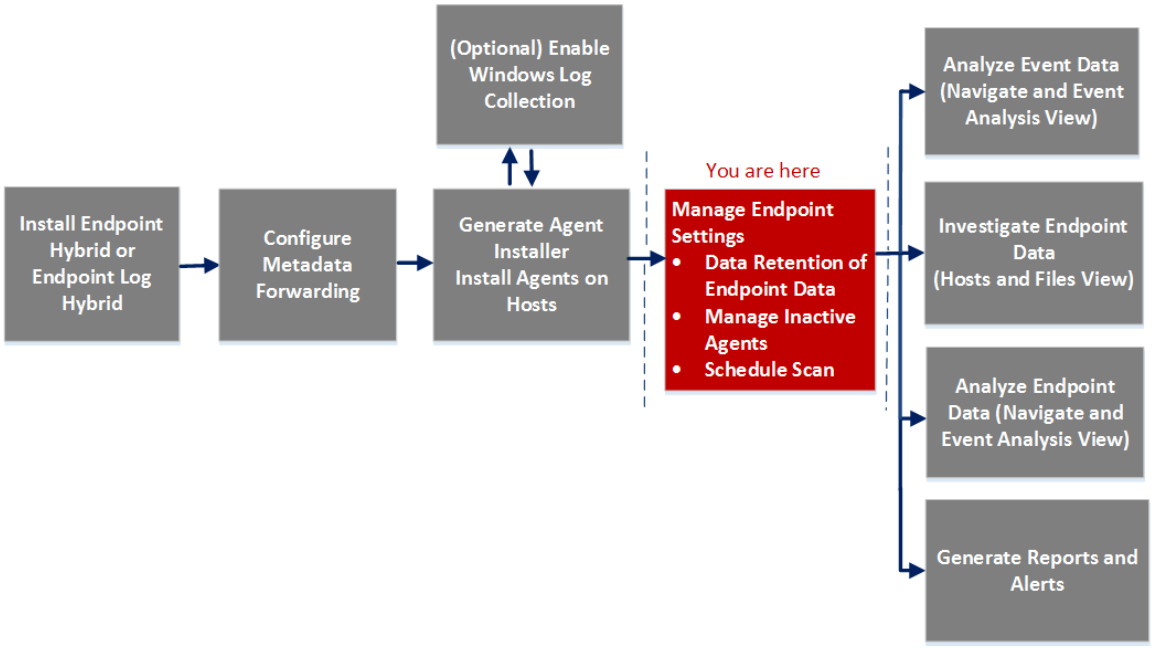
Champ	Description
Adresse	Affiche l'adresse IP du service Log Decoder.
Protobuf SSL	Indique si SSL est activé sur Protobuf Cette option est désactivée par défaut.
Port Protobuf	Affiche le port utilisé pour Protobuf. Le port par défaut est 50202.
REST SSL	Indique si SSL est activé sur le port REST dans le service Log Decoder. Cette option est désactivée par défaut.
Port REST	Affiche le port utilisé pour les communications REST. La valeur par défaut est 50202 (pour autre que SSL) et 56202 (pour SSL).
Nom d'utilisateur	Affiche le nom d'utilisateur.
Données brutes	Envoie un bref résumé de la session ainsi que les métadonnées en cas d'activation. Cette option est désactivée par défaut.

Onglet Planificateur de rétention des données

Dans l'onglet **Planificateur de rétention des données**, vous pouvez configurer les politiques de rétention des données et des agents inactifs. Pour accéder à cette vue :

1. Accédez à **Administrateur** > **Services**.
2. Dans la vue Services, sélectionnez **Serveur Endpoint**.
3. Cliquez sur  et sélectionnez > **Vue** > **Config**.
4. Cliquez sur l'onglet **Planificateur de rétention des données**.

Workflow



Que voulez-vous faire ?

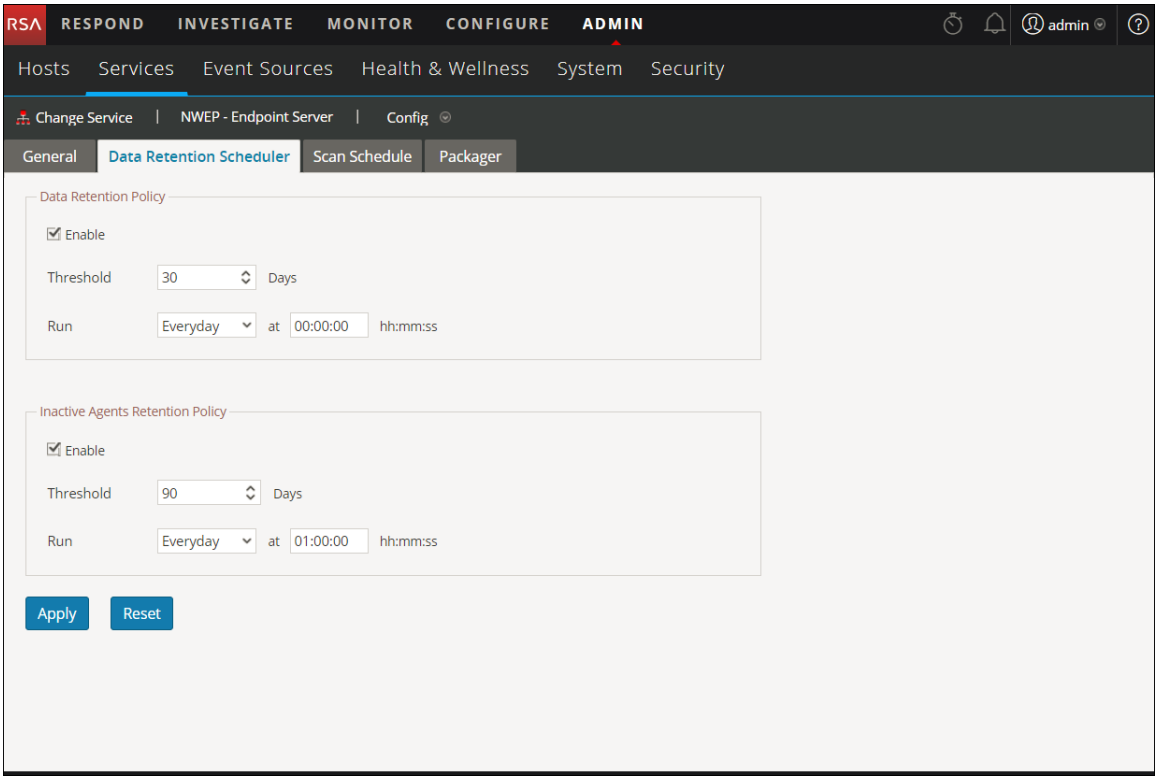
Rôle	Je souhaite...	Me montrer comment
Administrateur	Configurer la politique de rétention des données*	Configurer la rétention de données

Rôle	Je souhaite...	Me montrer comment
Administrateur	Configurer la politique de rétention des agents inactifs*	Gérer les agents inactifs

*Vous pouvez effectuer cette tâche dans la vue actuelle

Aperçu rapide

La figure suivante donne un exemple de l'onglet Planificateur de rétention des données.



Fonctionnalités

Le tableau suivant répertorie les champs de la politique de rétention des données.

Champ	Description
Activer	Active la configuration de la politique de rétention des données. Cette option est activée par défaut.

Champ	Description
Seuil	Affiche le nombre de jours de rétention des données Endpoint dans la base de données. Par défaut, le seuil est défini à 30 jours. Les données datant de plus de 30 jours sont supprimées de la base de données.
Exécuter	Affiche le planning d'exécution de la tâche de rétention des données. Par défaut, la vérification de la base de données a lieu tous les jours à 00:00:00. Vous pouvez sélectionner la fréquence dans la liste déroulante (Tous les jours, Jours de la semaine, Week-end ou Personnalisé, Personnalisé vous permettant de sélectionner un ou plusieurs jours spécifiques de la semaine) et l'heure d'exécution de la tâche.
Appliquer	Remplace les calendriers précédents pour ce service et applique immédiatement le nouveau calendrier.
Réinitialiser	Réinitialise le calendrier avec les paramètres par défaut.

Le tableau suivant répertorie les champs de la politique de rétention des agents inactifs.

Champs	Description
Activer	Active la configuration de la politique des agents inactifs. Cette option est activée par défaut.
Seuil	Affiche le nombre de jours pendant lesquels les agents inactifs sont conservés sur le serveur Endpoint. Par défaut, la valeur de seuil est définie à 90 jours.
Exécuter	Affiche le calendrier d'exécution de la tâche de rétention des agents inactifs. Par défaut, la vérification de la base de données a lieu tous les jours à 00:00:00. Vous pouvez sélectionner la fréquence dans la liste déroulante (Tous les jours, Jours de la semaine, Week-end ou Personnalisé, Personnalisé vous permettant de sélectionner un ou plusieurs jours spécifiques de la semaine) et l'heure d'exécution de la tâche.
Appliquer	Remplace les calendriers précédents pour ce service et applique immédiatement les nouveaux paramètres.

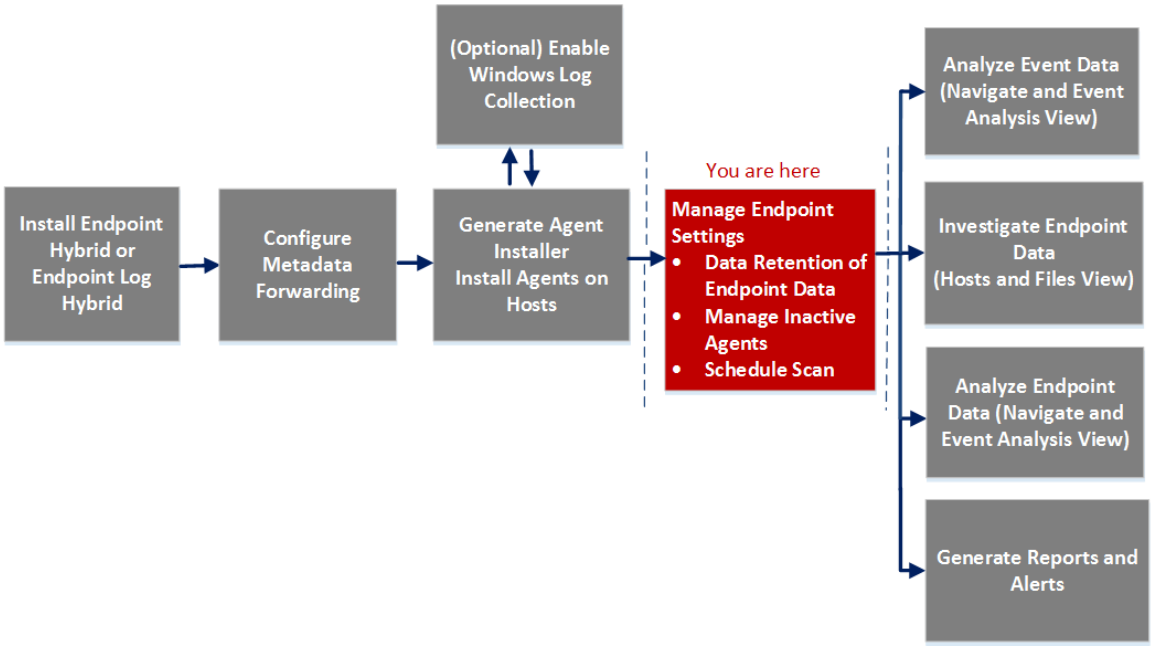
Champs	Description
Réinitialiser	Réinitialise le calendrier avec les paramètres par défaut.

Onglet Planning d'analyse

Dans l'onglet **Planning d'analyse**, vous pouvez configurer la planification de l'analyse Pour accéder à cette vue :

1. Accédez à **Administrateur** > **Services**.
2. Dans la vue Services, sélectionnez **Serveur Endpoint**.
3. Cliquez sur  et sélectionnez > **Vue** > **Config**.
4. Cliquez sur l'onglet **Planning d'analyse**.

Workflow



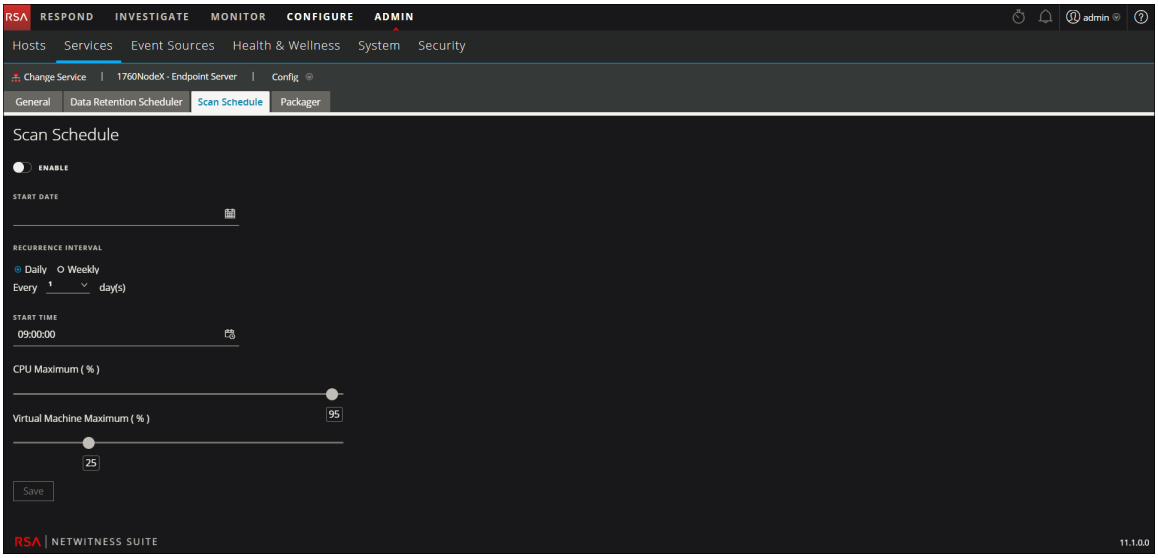
Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur	Configurer la planification de l'analyse*	Configurer la planification de l'analyse

*Vous pouvez effectuer cette tâche dans la vue actuelle

Aperçu rapide

La figure suivante donne un exemple de l'onglet Planning d'analyse.



Le tableau suivant décrit les champs de l'onglet Planning d'analyse. Les valeurs saisies sont spécifiques au fuseau horaire de l'agent.

Champ	Description
Activer	Sélectionnez l'option pour configurer l'analyse. Cette option est désactivée par défaut.
Date de début	Spécifiez la date de début de l'analyse.
Intervalle de récurrence	Sélectionnez l'intervalle de récurrence quotidienne ou hebdomadaire et définissez la fréquence en jours.
Heure de début	Spécifiez l'heure de début de l'analyse.
CPU max.	Définissez la valeur à l'aide du curseur. Cela garantit la limite de CPU de l'agent NetWitness Endpoint.

Champ	Description
Nb max. VM	Définissez la valeur à l'aide du curseur. **Remarque :** Utilisez cette option si des agents sont en cours d'exécution sur les machines virtuelles. Cela s'applique uniquement aux agents Windows.

Onglet Package

Dans l'onglet **Packager**, vous pouvez générer un packager d'agent et un programme d'installation d'agent. Pour accéder à cette vue :

1. Accédez à **Administrateur** > **Services**.
2. Dans la vue Services, sélectionnez **Serveur Endpoint**.
3. Cliquez sur  et sélectionnez > **Vue** > **Config**.
4. Cliquez sur l'onglet **Packager**.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur	Générer un packager d'agent pour Endpoint Data Collection*	*Guide d'installation de l'agent Endpoint Insights*
Administrateur	Génération d'un packager d'agent pour Windows Log Collection*	
Administrateur	Générer un programme d'installation d'agent*	

*Vous pouvez effectuer cette tâche dans la vue actuelle

Pour plus d'informations sur la génération d'un agent, consultez le *Guide d'installation de l'agent Endpoint Insights*.

Résolution des problèmes

Cette section fournit des informations sur les problèmes rencontrés lors de l'utilisation de RSA NetWitness Endpoint Insights.

Problèmes de communication liés à l'agent

Problème	L'agent ne peut pas communiquer avec le serveur Endpoint.

Explication	Le problème peut avoir l'une des origines suivantes :
	• Dans le packager d'agent :
	  • L'adresse IP du serveur est incorrecte
	  • Le port spécifié n'est pas disponible pour la communication avec le serveur Endpoint
	• Le serveur Endpoint ou le serveur Nginx ne fonctionne pas
	• Les règles de pare-feu ou de table IP bloquent la connexion entre l'hôte et le serveur Endpoint
	• L'agent est inactif ou supprimé manuellement de l'interface utilisateur

Solution	• Vérifiez si le serveur Endpoint et le serveur Nginx sont accessibles • Désinstallez l'agent, redémarrez l'hôte, puis réinstallez l'agent • Effectuez une mise à jour des règles de pare-feu ou de table IP, si nécessaire

Problème	L'agent met beaucoup de temps à effectuer l'analyse.
Explication	Dans certains cas, l'analyse de NetWitness Endpoint prend beaucoup de temps. Cela est dû à l'utilisation du processeur par d'autres programmes antivirus (tels que Windows Defender, McAfee, Norton, etc.) qui peuvent être installés sur les machines de l'agent.
Solution	Il est recommandé de mettre en liste blanche le fichier NWEAgent.exe dans l'antivirus Windows Suite.

Problèmes liés au packager

Message	`Failed to load the client certificate.`
Problème	Mot de passe de certificat incorrect.
Explication	Lors de la génération du programme d'installation de l'agent, le mot de passe du certificat ne correspond pas à celui fourni lors du téléchargement du packager de l'agent à partir de l'interface utilisateur.
Solution	Spécifie le mot de passe du certificat correct.

Message	`An unexpected error has occurred attempting to retrieve this data.`
Problème	Lorsque vous tentez d'accéder à l'onglet Packager, il s'ouvre avec le message d'erreur.
Explication	Le serveur Endpoint est peut-être arrêté ou n'est pas accessible.
Solution	Vérifiez l'état du serveur Endpoint sous **Admin > Service**. Si le service n'est pas exécuté, démarrez le serveur Endpoint.

Problèmes liés au planning d'analyse

Message	`An unexpected error has occurred attempting to retrieve this data.`
Problème	Lorsque vous tentez d'accéder à l'onglet Planification d'analyse, il s'ouvre avec le message d'erreur.
Explication	Le serveur Endpoint est peut-être arrêté ou n'est pas accessible.
Solution	Vérifiez l'état du serveur Endpoint sous **Admin > Service**. Si le service n'est pas exécuté, démarrez le serveur Endpoint.

Problèmes liés au service Intégrité

Comportement	Les métadonnées Endpoint ne sont pas disponibles dans la vue **Enquêter** > **Naviguer** ou **Analyse d'événements**
Problème	La vérification du fonctionnement du Meta-Ld-Buffer indique un état **Défectueux** pour le service Intégrité avec les exceptions suivantes : `dataprocessor-5] WARN MetaManagement|Meta Forwarding waiting for free buffer in Log decoder`
Solution	Vérifiez que : • La fonctionnalité de capture est activée sur le Log Decoder • Les métadonnées sont configurées correctement.

Comportement	Pour NetWitness Endpoint 4.4.0.2, les métadonnées n'atteignent pas le serveur Endpoint.
Problème	Le fonctionnement du Meta-Ld-Buffer indique un état **Défectueux** pour le service Intégrité avec les exceptions suivantes : `dataprocessor-5] WARN MetaManagement|Meta Forwarding waiting for free buffer in Log decoder`
Explication	Vérifiez que : • Le certificat est obtenu et importé sur le serveur de Console NetWitness 4.4.0.2 • L'option Enquêter de NetWitness est activée dans l'interface utilisateur de NetWitness Endpoint • Le transfert de métadonnées est configuré sur le serveur de Console NetWitness 4.4.0.2

Comportement	La vérification du fonctionnement de Data.Application.Connection-Health pour le serveur Endpoint indique un état **Défectueux**.

Problème	Le service Mongo ou le serveur Endpoint est arrêté.
Explication	Pour plus d'informations sur les erreurs, consultez les logs Endpoint Server dans /var/log/netwitness/endpoint-server/endpoint-server.log.
Solution	Redémarrez le service Mongo ou le service Endpoint.

Comportement	La vérification des statistiques de fonctionnement de Endpoint.Health.Overall-Health indique un état **Défectueux**.
Problème	Le service Mongo ou le serveur Endpoint est arrêté.
Explication	Vérifiez les autres statistiques de fonctionnement du serveur Endpoint (par exemple, Data.Application.Connection-Health, Endpoint.Health.Ld-Buffer-Health) pour identifier les statistiques présentant un état Défectueux. Si l'une d'entre elles indique l'état Défectueux, le fonctionnement global du serveur Endpoint indiquera également l'état Défectueux.
Solution	Consultez la solution applicable à ces statistiques dans la section Problèmes liés au service Intégrité.

Problème	Le nombre de rejets de l'agent est supérieur au seuil d'alarme.
Explication	Le nombre d'éléments rejetés par l'agent est supérieur à une limite spécifique et votre règle personnalisée est déclenchée. Par exemple, le nombre de rejets effectués par l'agent au cours des 5 dernières heures correspond à 10 % des agents déployés.
Solution	Vérifiez l'état de fonctionnement global du serveur Endpoint et consultez les instructions de dimensionnement.

Problème	La taille de stockage des statistiques de Data.Application a dépassé le seuil d'alarme.
Explication	La taille de stockage de Data.Application a dépassé le seuil (par exemple, 75 %) et la règle personnalisée est déclenchée. **Remarque :** Par défaut, le serveur supprime automatiquement les anciennes données lorsqu'il atteint 80 % de l'espace disque.

Solution	Vérifiez le seuil défini dans la politique de rétention des données.

Problème	La vérification du fonctionnement de Data.Application.Connection-Health indique un état Défectueux ou Fatal.
Explication	Le service Mongo est désactivé.
Solution	Vérifiez que le service Mongo est actif et consultez les logs du serveur Endpoint pour connaître les détails de l'erreur.

Problème	Le nombre de requêtes d'agent indique un seuil d'alarme égal à 0.

Explication	Le nombre de requêtes d'agent indique 0 pour toute la journée ou la semaine. Le problème peut avoir l'une des origines suivantes :
	• Dans le packager d'agent :
	  • L'adresse IP du serveur est incorrecte
	  • Le port spécifié n'est pas disponible pour la communication avec le serveur Endpoint
	• Le serveur Endpoint ou le serveur Nginx ne fonctionne pas
	• Les règles de pare-feu ou de table IP bloquent la connexion entre l'hôte et le serveur Endpoint
	• L'agent est inactif ou supprimé manuellement de l'interface utilisateur

Solution	• Vérifiez si le serveur Endpoint et le serveur Nginx sont accessibles • Désinstallez l'agent, redémarrez l'hôte, puis réinstallez l'agent • Effectuez une mise à jour des règles de pare-feu ou de table IP, si nécessaire

Problème de configuration des métadonnées

Comportement	Le serveur de Console affiche un message.
Problème	Le serveur de Console affiche le message suivant : *Le serveur de Console consignera le traitement par lots sous la forme 1. "rsa-nw-endpoint-agent afin d'établir une connexion SSL avec Netwitness Suite.*

Explication	Lorsque vous exécutez une analyse rapide sur le serveur NetWitness Endpoint 4.4 pour un agent ou une machine, un message s'affiche.
Solution	Vérifiez la configuration des métadonnées.

Problème d'installation

Comportement	NetWitness Suite permet d'installer plusieurs instances d'Endpoint Hybrid ou d'Endpoint Log Hybrid.
Problème	Une seule instance d'Endpoint Hybrid ou d'Endpoint Log Hybrid peut être utilisée pour les données de point de terminaison.
Explication	Au cours de l'installation d'Endpoint Hybrid ou d'Endpoint Log Hybrid, vous pouvez procéder à l'installation d'une autre instance sans aucun problème.
Solution	Vous devez supprimer toutes les instances d'Endpoint Hybrid ou d'Endpoint Log Hybrid, à l'exception de celle que vous souhaitez utiliser pour les données de point de terminaison.

Problème lié aux agents inactifs

Problème	L'agent peut être inactif ou ne pas avoir communiqué avec le serveur Endpoint depuis longtemps.
Explication	Une liste des agents inactifs est disponible dans la base de données Mongo avec l'ID de l'agent. En utilisant ces informations, vous pouvez rechercher des détails supplémentaires sur les agents inactifs.
Solution	Pour rechercher des agents inactifs dans votre déploiement, procédez comme suit : 1. Ouvrez le fichier log du serveur Endpoint dans `/var/log/netwitness/endpoint-server/endpoint-server.log` et recherchez l'<ID> de l'agent. 2. Copiez l'ID de l'agent affiché dans le fichier log. 3. Recherchez l'ID de l'agent dans le fichier log d'accès NGINX (`/var/log/nginx/access.log`) pour récupérer les détails suivants relatifs à un agent inactif :

	• Adresse IP • Date et heure auxquelles l'agent est devenu inactif • Emplacement