RSA NETWITNESS® PLATFORM

Guide de configuration de Context Hub

pour la version 11.2

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 de Dell 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 de Dell.

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.

March 2019

Sommaire

7

Fonctionnement de Context Hub **8**

Présentation de la configuration de Context Hub **9**

Configurer des listes en tant que sources de données **10**

Conditions préalables 10

Ajouter une source de données de liste à l'aide d'une zone de stockage de fichiers local 11

Ajouter la source de données de liste à l'aide de HTTP(S) 13

Étapes suivantes : 15

Configurer Archer en tant que source de données **16**

Conditions préalables 16

Configurer la source de donnée Active Directory **23**

Conditions préalables 23

Configurer NetWitness Endpoint comme source de données **27**

Conditions préalables 27

Configurer Respond comme source de données **31**

Conditions préalables 31

Configurer Live Connect comme source de données pour Context Hub **33**

Conditions préalables 33

Activer/désactiver une source de données Live Connect 33

Modifier les paramètres de source de données Live Connect 35

Configurer les paramètres de source de données pour Context Hub **37**

Importer ou exporter des listes pour Context Hub 41

Importer une liste 41

Importer une liste à une seule colonne 41

Importer des valeurs dans une liste existante 43

Exporter une liste pour Context Hub 43

Configurer le mappage du type de méta pour Context Hub 45

Références de Context Hub **47**

Onglet Sources de données de Context Hub 48

Workflow 48

Que voulez-vous faire ? 48

Rubriques connexes 49

Aperçu rapide 49

Onglet Listes de Context Hub 51

Workflow 51
Que voulez-vous faire ? 51
Rubriques connexes 52
Aperçu rapide 52
Résolution des problèmes 55
Problèmes possibles 55

Fonctionnement de Context Hub

Context Hub est un service comportant une fonctionnalité de recherche de fournisseur d'enrichissement dans les vues Répondre et Procédure d'enquête. L'administrateur peut configurer le service Context Hub et les sources de données afin de permettre à l'analyste d'effectuer la recherche contextuelle pour les sources de données requises.

Par défaut, le service Context Hub prend en charge les recherches de fournisseur d'enrichissement pour les types de métadonnées tels que l'adresse IP, l'utilisateur, le domaine, l'adresse MAC, le nom de fichier, le hachage de fichier et l'hôte.

Les sources de données suivantes sont prises en charge par NetWitness Platform et fournissent des données enrichies lorsqu'elles sont configurées.

Lists - fournit des informations contextuelles à partir d'une liste de listes noires, de listes blanches ou de listes de surveillance.

RSA Archer - fournit des informations sur le degré de criticité d'un périphérique ou d'une ressource spécifique en fonction de l'adresse IP ou de l'hôte qui a besoin d'une surveillance constante.

Active Directory - fournit les informations contextuelles d'un utilisateur pour mieux déterminer si l'utilisateur est suspect ou non.

RSA NetWitness® Endpoint - fournit des informations contextuelles pour les indicateurs de module et d'ordinateur de point de terminaison et pour mieux déterminer si l'un des périphériques de point de terminaison est compromis.

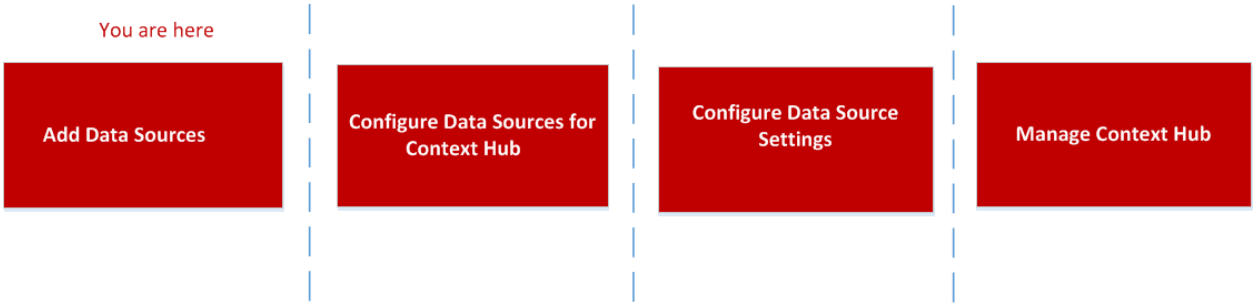
Respond - fournit les informations contextuelles d'une métadonnée spécifique disponible dans Respond et permet à l'analyste de réagir plus vite en fonction des données contextuelles.

Live Connect - fournit des informations contextuelles pour les adresses IP, les domaines et les hachages de fichier dans le serveur de communauté des renseignements sur les menaces RSA Live Connect.

Présentation de la configuration de Context Hub

L'administrateur doit effectuer chaque étape dans l'ordre approprié pour configurer les services de telle manière qu'ils effectuent la recherche contextuelle de manière efficace. Dans la vue **ADMIN> Services**. Configuration des services du service Context Hub, les administrateurs peuvent configurer les sources de données pour le service Context Hub. Les administrateurs peuvent configurer les recherches contextuelles pour les clés méta personnalisées, si nécessaire. Ils peuvent aussi importer ou exporter des listes.

Le workflow ci-dessous présente la manière de configurer le service Context Hub :



Le service Context Hub est préinstallé sur l'hôte ESA primaire et ajouté automatiquement à NetWitness Platform.

Remarque : Seule une instance de service Context Hub peut être activée dans votre déploiement NetWitness Platform. En cas d'existence de plusieurs services ESA dans NetWitness Platform, vous devez choisir l'hôte ESA approprié au service Context Hub. Un minimum de 8 Go d'espace est requis pour configurer Context Hub sur l'hôte ESA.

Configurer des listes en tant que sources de données

Répertorie lorsqu'une source de données utilise le service Context Hub pour extraire des informations contextuelles pour les types de métadonnées qui prennent en charge la recherche contextuelle. Vous pouvez créer une ou plusieurs listes et ajouter des valeurs de liste appropriées à la liste. Veillez à créer une liste significative, par exemple des adresses IP sur liste noire, des adresses IP sur liste blanche, et ainsi de suite. Ces listes peuvent contenir des entités prises en charge, par exemple une adresse IP, une adresse MAC, un nom d'utilisateur, un nom d'hôte, un nom de domaine, un nom de fichier ou un hachage de fichier. Dans l'onglet Source de données, vous pouvez importer une liste à une seule colonne ou à plusieurs colonnes. En outre, tous les flux (à l'exception des flux STIX) qui sont créés sont convertis en listes et affichés dans la recherche contextuelle. Si le Context Hub n'est pas configuré ou si le service est en panne, les flux seront mis à disposition chaque fois que le Context Hub est opérationnel. Pour plus d'informations sur la création de flux, consultez le *Guide de gestion des services Live*.

Remarque : Lorsque vous créez un flux, une liste est générée automatiquement avec le même nom que le flux. Si le nom de la liste existe déjà, le nom de la nouvelle liste est suffixé avec le nombre « 2 ». Par exemple, si le nom de flux existant est le fichier test1.csv, la nouvelle liste sera nommée test2.csv.

Les valeurs de liste sont au format CSV, disponibles dans un emplacement externe et accessibles via les deux méthodes suivantes :

- **Zone de stockage de fichiers local** : Vous pouvez partager un fichier à partir d'un emplacement local.
- **HTTP(S)** : Vous pouvez partager un fichier à l'aide d'un emplacement de serveur Web.

Remarque : Vous pouvez également définir une tâche récurrente pour extraire les données à intervalles réguliers en utilisant les paramètres Lecture préalable lors de la configuration du mappage des métadonnées.

Conditions préalables

Avant de configurer la source de données Lists, vérifiez que :

- L'utilisateur doit disposer des autorisations d'administration.
- Le service Context Hub est disponible dans la vue **ADMIN**> **Services** de NetWitness Platform.
- Si vous utilisez le stockage de fichiers local ou un serveur HTTP(S), le chemin d'accès indiqué doit contenir le fichier CSV.
  En cas de stockage de fichiers locaux distant, le fichier doit être monté ou placé dans l'emplacement du disque local `/var/lib/netwitness/contexthub-server/data`.
- L'utilisateur NetWitness doit avoir des autorisations en lecture pour accéder au fichier.

Attention : Si vous créez une liste Context Hub pour une utilisation comme source d'enrichissement dans l'ESA, le nom de la liste ne peut pas inclure d'espaces ou de caractères spéciaux, ou commencer par un nombre. Si vous ne suivez pas cette convention d'affectation de noms, lorsque vous tentez d'ajouter la liste en tant que source d'enrichissement dans ESA, un message d'erreur s'affiche et vous n'êtes pas autorisé à ajouter la liste.

Ajouter une source de données de liste à l'aide d'une zone de stockage de fichiers local

Pour ajouter une liste en tant que source de données :

1. Accédez à **ADMIN > Services**.

   La vue Services s'affiche.

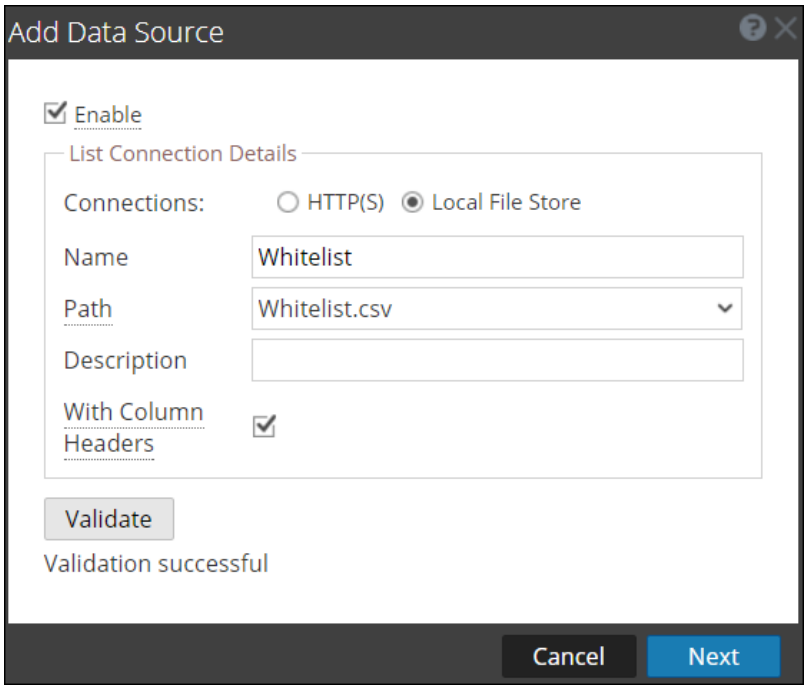
2. Sélectionnez le service Context Hub et cliquez sur > **Vue** > **Config**.

   La vue Configuration des services de Context Hub s'affiche.

3. Sous l'onglet **Sources de données**, cliquez sur > **LISTES**.

   La boîte de dialogue **Ajouter une source de données** s'affiche

4. Par défaut, la case **Activer** est activée. Si cette option est désactivée, le bouton Enregistrer est désactivé, vous ne pouvez pas ajouter la source de données, afficher la liste dans l'onglet des listes liste et afficher les informations contextuelles.
5. Sélectionnez le type de connexion de **Zone de stockage de fichiers local**.



6. Fournissez les détails suivants sur la connexion de la base de données : Renseignez les champs

suivants pour le type de connexion de la zone de stockage de fichiers local :

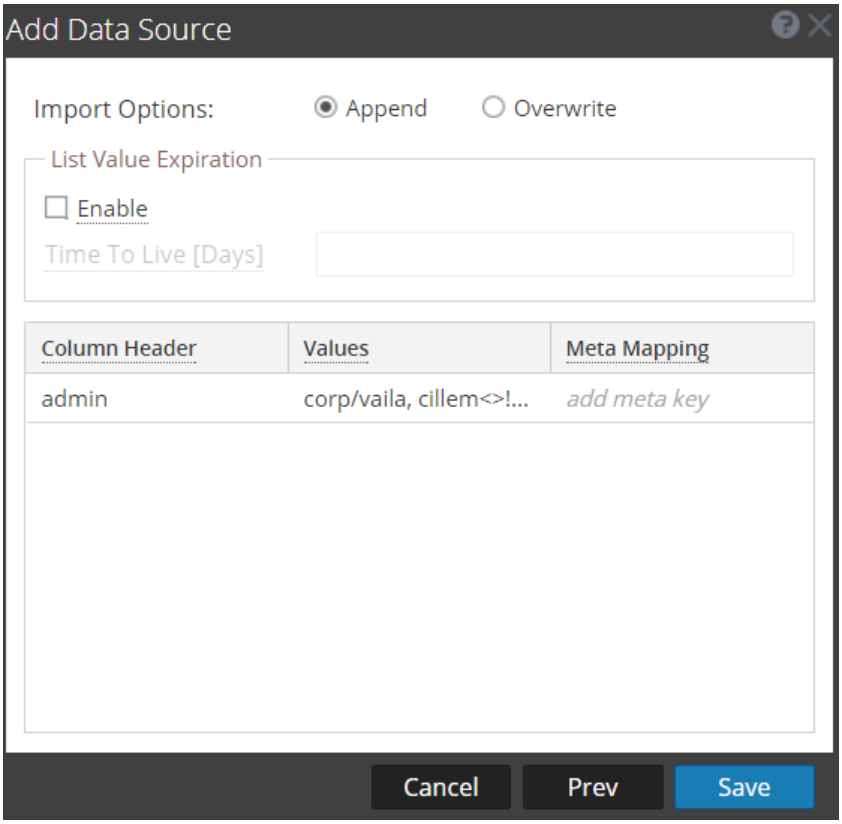
- **Nom :** Indiquez un nom pour la source de données de liste.
- **Chemin :** Ce champ affiche tous les fichiers de données disponibles dans le dossier de données `/var/lib/netwitness/contexthub-server/data`, dans lequel le service Context Hub s'exécute. Sélectionnez le nom du fichier dans la liste déroulante.
  32 colonnes de fichier CSV au maximum sont prises en charge, conformément aux normes qui sont conformes aux normes RFC1480.
- (Facultatif) **Description** : Ajoutez une description pour le fichier sélectionné.
- **Avec en-têtes de colonne** : Sélectionnez cette option pour considérer la première ligne comme les en-têtes de colonne du fichier CSV. Si vous ne sélectionnez pas cette option, vous devrez saisir les en-têtes de colonne dans l'écran suivant.

7. Cliquez sur **Valider**.

   Si la validation échoue, vous ne pouvez pas ajouter la source de données.

8. Cliquez sur **Suivant**.

   La boîte de dialogue suivante s'affiche.



9. Sélectionnez l'une des options suivantes :

   - **Ajouter** : sélectionnez cette option pour ajouter les valeurs importées à une liste existante.
   - **Remplacer** : sélectionnez cette option pour remplacer les valeurs d'une liste existante par les valeurs importées.

10. Dans la section **Expiration des valeurs de liste**, l'option **Activer** est par défaut désactivée. Si vous souhaitez stocker les valeurs de liste consultées dans le cache pendant un nombre de jours spécifié,activez la case à cocher **Activer** et indiquez le nombre de jours dans le champ **durée de vie (jours)** pour les valeurs de liste à conserver.
11. Dans l'écran suivant, mappez au moins une clé méta à un ou plusieurs types de métadonnées en mappant un en-tête de colonne à une métadonnée. La description de chaque champ est comme suit :
    - **En-tête de colonne** : Affiche les en-têtes du fichier CSV à mapper à un type de métadonnée.
    - **Mappage de métadonnée** : Mappez un champ d'en-tête de colonne à un type de métadonnée.
    - **Valeurs** : Affiche les trois premières valeurs de la liste importée.
12. Cliquez sur **Enregistrer**.

Ajouter la source de données de liste à l'aide de HTTP(S)

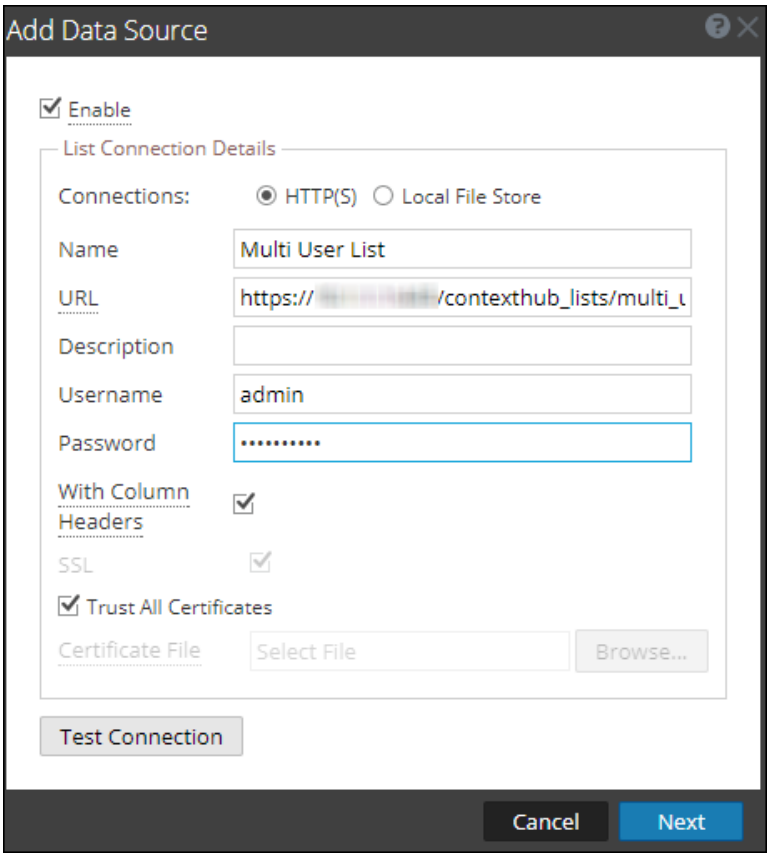
Pour ajouter une liste en tant que source de données :

1. Sélectionnez **ADMIN** > **Services**.

   La vue Services s'affiche.
2. Sélectionnez le service Context Hub et cliquez sur  > **Vue** > **Config**.

   La vue Configuration des services de Context Hub s'affiche.
3. Sous l'onglet **Sources de données**, cliquez sur  > **LISTES**.

   La boîte de dialogue **Ajouter une source de données** s'affiche.
4. Sélectionnez le type de connexion HTTP(S).

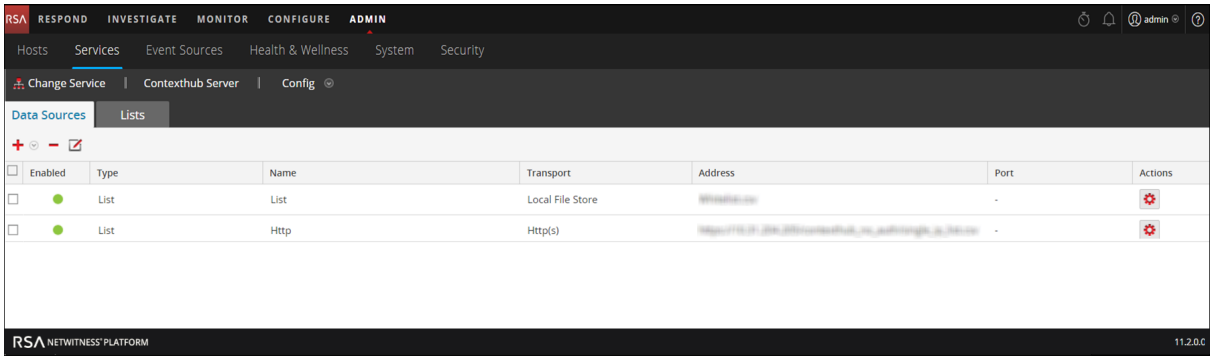


- Renseignez les champs suivants pour le type de connexion HTTP(S).
  - **Nom :** Indiquez un nom pour la source de données liste.
  - **URL** : Saisissez le chemin d'accès du fichier CSV disponible à l'emplacement HTTP(S), ainsi que le nom d'hôte ou l'adresse IP de l'ordinateur distant sur lequel se trouve la liste. L'URL doit être au format : `https://<Hostname or IP-address of the HTTP (S)server>:<Port on which the HTTP(S) server is hosted>/<Absolute path of CSV file>`. Par exemple, `https://10.1.1.1:443/contexthub_lists/multi_user_list.csv`
  - (Facultatif) **Description** : Ajoutez une description pour le fichier sélectionné.
  - (Facultatif) **Nom d'utilisateur :** Saisissez le nom d'utilisateur nécessaire pour se connecter au serveur HTTP(S) qui requiert une authentification de base.
  - (Facultatif) **Mot de passe :** Saisissez le mot de passe nécessaire pour se connecter au serveur HTTP(S) qui requiert une authentification de base.
  - **Avec en-têtes de colonne** : Sélectionnez cette option si vous souhaitez importer un fichier CSV avec des en-têtes. Si cette option est sélectionnée et que vous importez le fichier CSV sans les en-têtes, la première ligne sera considérée comme un en-tête modifiable.
  - **SSL :** Si vous saisissez une URL avec le protocole HTTPS dans ce champ, cette option est sélectionnée automatiquement. Si vous saisissez une URL avec le protocole HTTP, cette case est désactivée.

- **Approuver tous les certificats** : Activez cette case pour ajouter la source de données sans valider le certificat. Si vous désactivez cette option, vous devez télécharger un certificat de serveur HTTP(S) au format .cer ou .crt valide pour que la connexion soit établie.

5. Cliquez sur **Tester la connexion** pour tester la connexion entre Context Hub et la source de données.
6. Cliquez sur **Enregistrer** pour enregistrer les paramètres.

   La liste est ajoutée comme source de données pour le Context Hub configuré et s'affiche dans l'onglet **Sources de données**.



Étapes suivantes :

- Ajouter, modifier ou supprimer des valeurs d'une liste spécifique.
- Configurer les paramètres de source de données afin de déterminer les champs de source de données à afficher dans le panneau Contexte. Pour savoir comment procéder, reportez-vous à la rubrique Configurer les paramètres de source de données pour Context Hub .
- Importer et exporter une liste. Pour plus d'informations, reportez-vous à Importer ou exporter des listes pour Context Hub.
- Affichez les données contextuelles dans le panneau Récapitulatif du contexte de la vue Répondre ou Enquêter. Pour plus d'informations, reportez-vous au *Guide d'utilisation RSA NetWitness Respond* et au *Guide d'utilisation RSA NetWitness Investigation et Malware Analysis*.

Configurer Archer en tant que source de données

Vous pouvez configurer Archer comme source de données pour Context Hub et utiliser le service Context Hub pour récupérer des informations contextuelles à partir d'Archer. Utilisez les procédures de cette rubrique pour ajouter Archer comme source de données pour le service Context Hub et configurer les paramètres (si nécessaire) pour Archer.

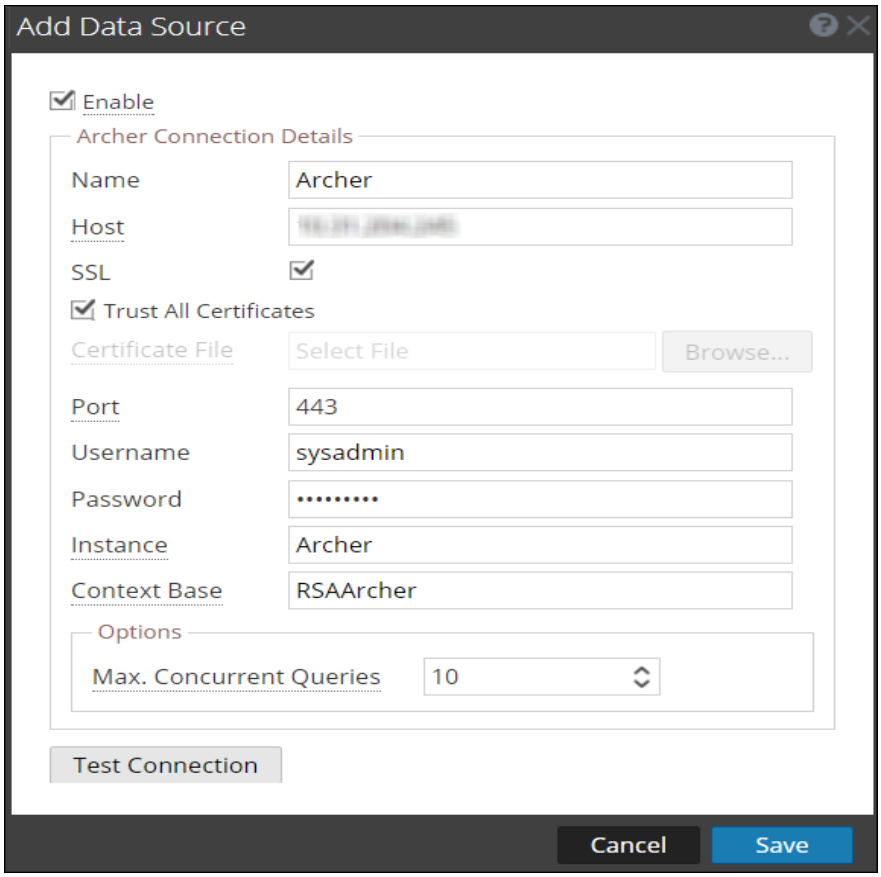
Conditions préalables

Avant de configurer la source de données Archer, vérifiez que :

- le service Context Hub est disponible dans la vue **ADMIN**> **Services** de NetWitness Platform.
- Archer est installé avec une licence pour l'application Périphériques.

Pour ajouter Archer comme source de données pour Context Hub :

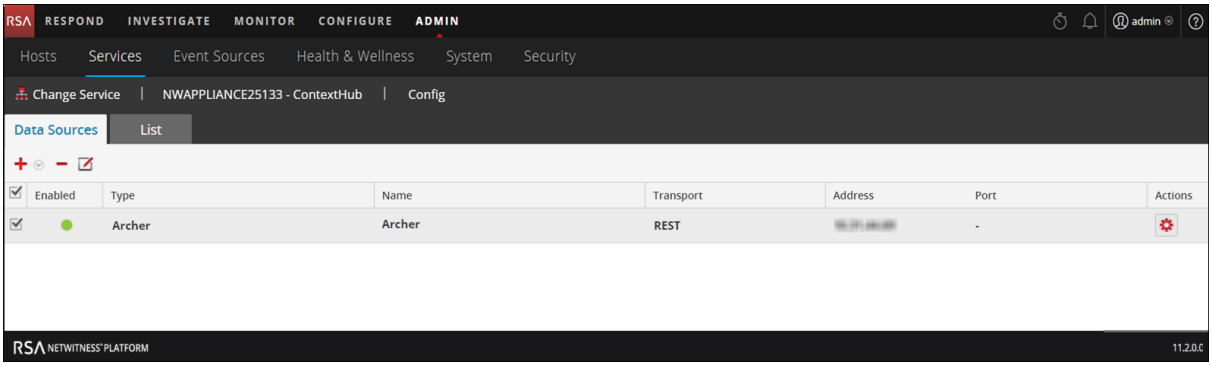
1. Accédez à **ADMIN** > **Services**.
   La vue Services s'affiche.
2. Sélectionnez le service Context Hub, puis cliquez sur > **Vue** > **Config**
   La vue Configuration des Services s'affiche.
3. Sous l'onglet **Sources de données**, cliquez sur > **Archer**.
   La boîte de dialogue **Ajouter une source de données** s'affiche.



4. Fournissez les informations suivantes :

- Par défaut, la case **Activer** est activée. Si cette option est désactivée, le bouton Enregistrer est désactivé et vous ne pouvez pas ajouter la source de données et afficher les informations contextuelles.
- Renseignez les champs suivants :
  - **Nom** : Indiquez le nom de la source de données Archer.
  - **Hôte** : Indiquez le nom d'hôte ou l'adresse IP où le serveur Archer est installé.
  - **SSL**: Par défaut, cette option est sélectionnée et permet d'établir une communication SSL avec Archer.
  - **Approuver tous les certificats** : Activez cette case pour ajouter la source de données sans valider le certificat. Si vous désactivez cette option, vous devez télécharger un certificat de serveur Endpoint valide pour que la connexion soit établie.
  - **Port** : Le port par défaut est 443.
  - **Nom d'utilisateur** : Saisissez le nom d'utilisateur du serveur Archer.
  - **Mot de passe**: Saisissez le mot de passe du serveur Archer.
  - **Instance** : Saisissez le nom de l'instance à partir de laquelle vous souhaitez extraire des données. Une instance de RSA Archer est une configuration unique qui inclut un contenu unique dans une base de données, la connexion à la base de données, l'interface et la connexion. Vous pouvez avoir des instances individuelles pour chaque emplacement ou région, ou pour les environnements de développement, de test et de production. La base de données de l'instance stocke le contenu de RSA Archer pour une instance spécifique.
  - **Base contextuelle** : Saisissez le nom du répertoire virtuel où les fichiers sont stockés. Par exemple, rsaarcher situé à l'adresse Web RSA Archer https://archer.company.com/**rsaarche**r/default.aspx. Si les fichiers sont stockés dans l'adresse Web par défaut IIS https://archer.company.com/default.aspx, ce champ doit être vide.
  - **Nbre max. Requêtes simultanées** : Vous pouvez configurer le nombre maximum de requêtes simultanées définies par le service Context Hub à exécuter sur les sources de données configurées. La valeur par défaut est 10.
5. Cliquez sur **Tester la connexion** pour tester la connexion entre la source de données Archer et Context Hub.

6. Cliquez sur **Enregistrer**.
   Archer est ajouté comme source de données pour Context Hub et s'affiche dans l'onglet **Sources de données**.



Après avoir ajouté la source de données, vous pouvez configurer les paramètres de cette source de données. Pour savoir comment procéder, reportez-vous à la section Configurer les paramètres de source de données pour Context Hub . Vous pouvez afficher les données contextuelles dans le panneau Récapitulatif du contexte de la vue Répondre ou Enquêter. Pour savoir comment procéder, reportez-vous au *Guide d'utilisation de NetWitness Respond* et au *Guide d'utilisation Investigation et Malware Analysis*.

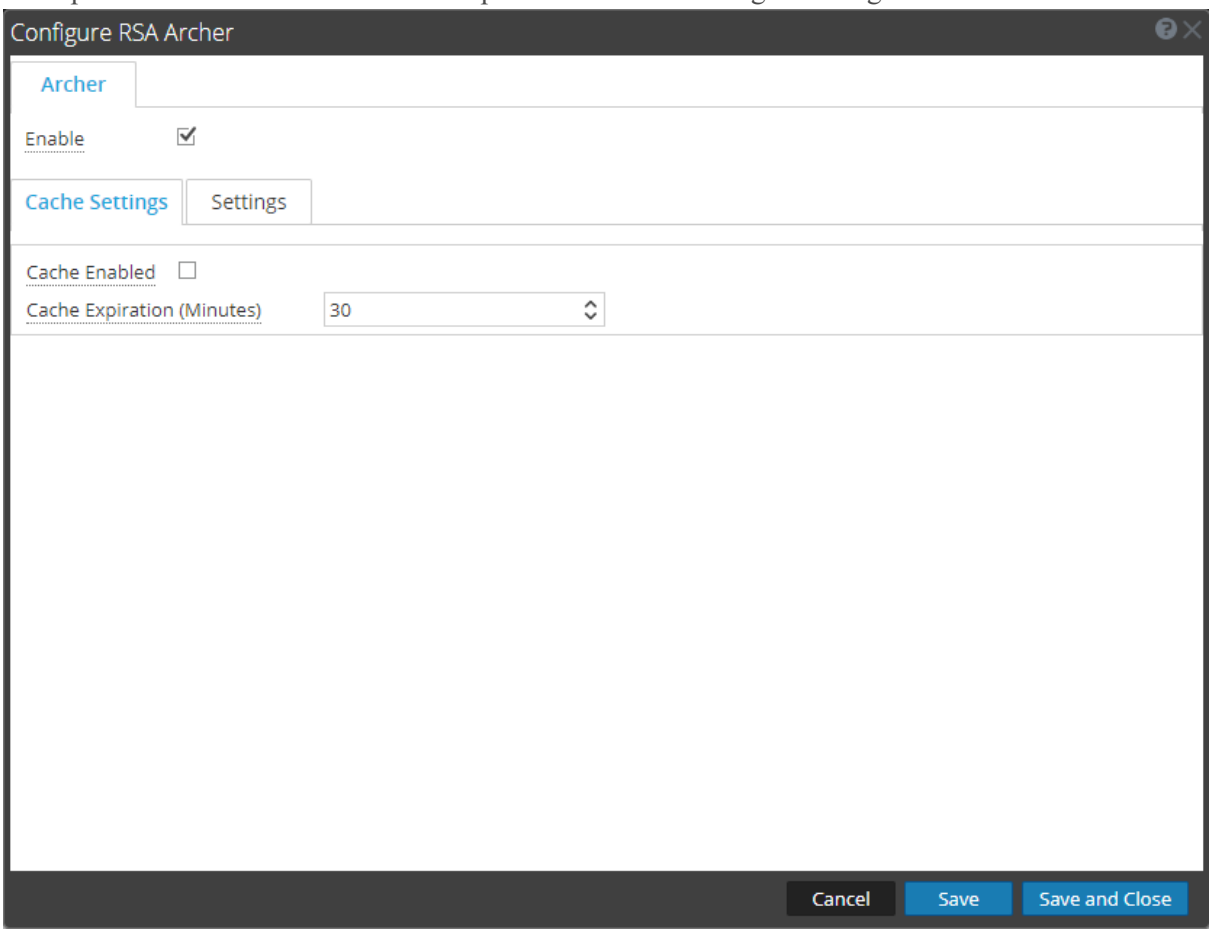
Configurer la source de données Archer

Une fois que vous avez configuré les sources de données requises, vous pouvez personnaliser les paramètres des sources de données en fonction de vos besoins.

Pour accéder aux paramètres et les configurer :

1. Accédez à **ADMIN**> **Services**.
   La vue Services s'affiche.
2. Dans le panneau Services, sélectionnez le service Context Hub, puis cliquez sur > **Vue** > **Config**.
   La vue Configuration des services de Context Hub s'affiche.
3. Sélectionnez la source de données pour laquelle vous souhaitez configurer les paramètres, puis cliquez sur dans la colonne Actions.

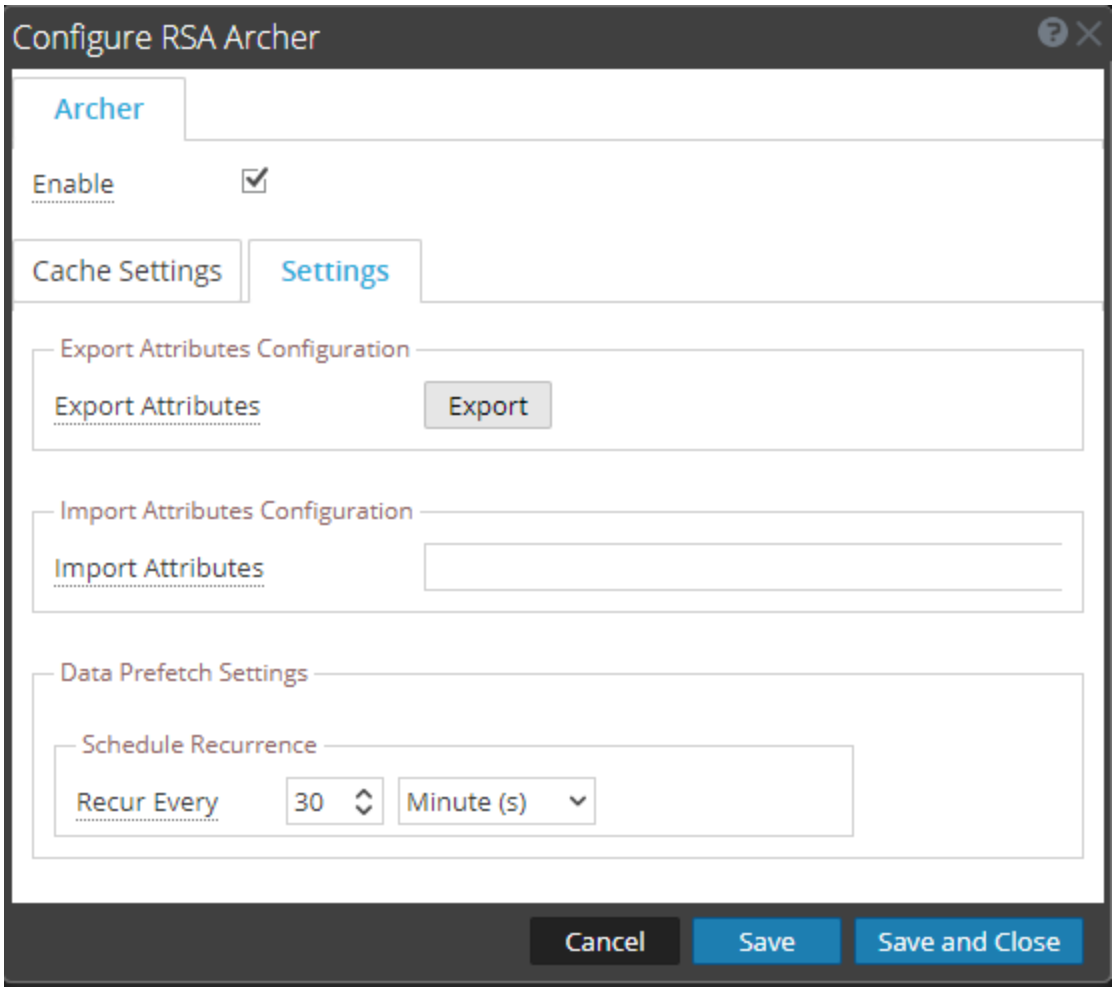
La capture d'écran suivante est un exemple de la boîte de dialogue Configuration de RSA Archer :



4. Dans l'onglet **Paramètres**. Configurez les champs suivants :

Champ	Description
Activer	Cette option est activée par défaut (cochée) et peut être utilisée pour activer ou désactiver la réponse de la source de données sélectionnée.
Paramètres du cache	Toute recherche de Context Hub peut être stockée dans le cache de Context Hub pour une durée configurée. La réponse à toute demande ultérieure correspondante sera extraite à partir du cache de Context Hub. Cette section permet de définir les paramètres de cache suivants pour la requête : • **Cache activé** : Par défaut, cette case est cochée et la réponse à la requête est mise en cache. • **Expiration du cache (minutes)** : Durée maximale de conservation de la requête dans le cache. La durée par défaut est de 30 minutes et la durée maximale de 7 200 minutes. Vous pouvez les configurer.

5. Cliquez sur **Paramètres du cache**. Configurez les champs suivants



Champ	Description
Exporter la configuration des attributs	Dans **Paramètres**, **Exporter la configuration des attributs**, cliquez sur **Exporter** pour exporter la configuration des attributs Archer. Il s'agit des attributs visibles dans la recherche contextuelle lors de l'affichage des détails d'Archer pour une adresse IP, un hôte ou un Mac. Un fichier de configuration JSON est téléchargé et l'ordre des attributs synchronisés avec la liste dans le panneau contextuel est conservé dans le fichier JSON.
Configuration des attributs d'importation	Si vous souhaitez mettre à jour ou modifier les paramètres de configuration dans **Paramètres**, **Importer la configuration des attributs**, cliquez sur **Parcourir**. Sélectionnez le fichier JSON contenant les attributs de configuration. Les attributs apparaissent dans le panneau Recherche contextuelle lorsqu'un utilisateur affiche le contexte, dans l'ordre dans lequel ils ont été importés. **Remarque** : Vous pouvez sauvegarder les attributs précédents avant d'importer les modifications apportées aux attributs existants.

Champ	Description
Paramètres de la lecture préalable des données	Dans **Paramètres**, **Paramètres de la lecture préalable des données** permet d'effectuer une lecture préalable des données. Configurez la **Récurrence régulière** pour fournir des données plus rapidement lorsque vous survolez avec la souris l'entité souhaitée dans Respond.
Récurrence régulière	Dans le champ **Répéter tous les**, entrez une valeur ou utilisez la liste déroulante pour configurer la périodicité de la prérécupération. La durée de temps par défaut peut être sélectionnée dans la liste déroulante pour configurer la durée de la périodicité. Les valeurs disponibles sont les minutes, les heures, les jours ou les semaines.

6. Cliquez sur l'une des options suivantes :

- **Annuler** - Sélectionnez cette option pour annuler les modifications.
- **Enregistrer** - Sélectionnez cette option pour enregistrer les modifications.
- **Enregistrer et fermer** - Sélectionnez cette option pour enregistrer et fermer la boîte de dialogue.

Remarque : Une fois les paramètres de source de données configurés, vous pouvez configurer les paramètres de configuration de Context Hub en accédant à **ADMIN**> **Services**> **Vue** > **Explorer**. Veillez à redémarrer le service Context Hub si vous apportez des modifications de configuration dans la vue Explorer.

Configurer la source de donnée Active Directory

Vous pouvez configurer Active Directory (AD) comme source de données pour Context Hub à l'aide de LDAP et utiliser le service Context Hub pour récupérer des informations contextuelles à partir d'Active Directory. Utilisez les procédures de cette rubrique pour ajouter AD comme source de données pour le service Context Hub et configurer les paramètres (si nécessaire) pour AD.

Conditions préalables

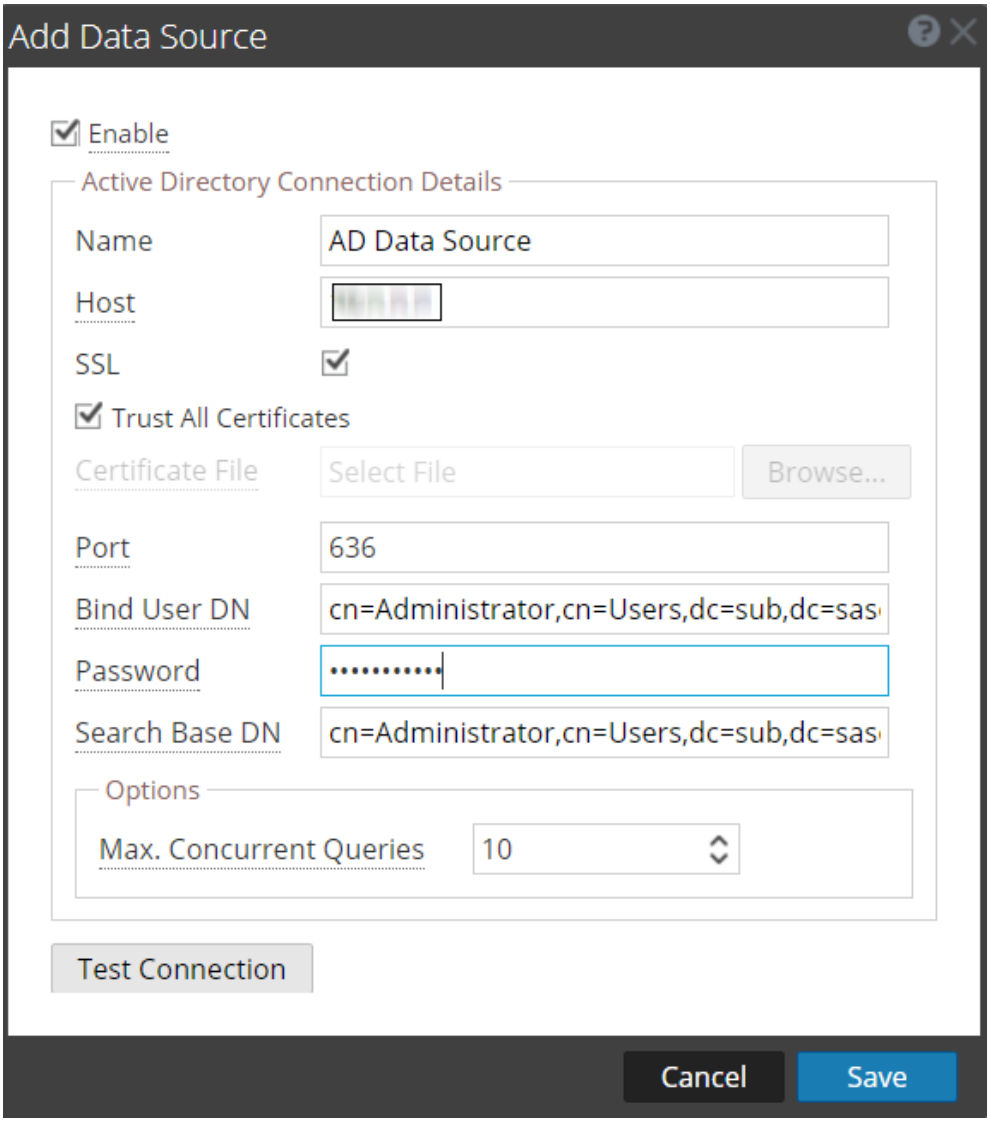
Avant de configurer la source de données Active Directory, vérifiez que :

- le service Context Hub est disponible dans la vue **ADMIN** > **Services** de NetWitness Platform.
- Active Directory est disponible et fonctionne sur Windows 2003, 2008 et 2012.

Pour ajouter AD comme source de données pour Context Hub :

1. Accédez à **ADMIN** > **Services**.
   La vue Services s'affiche.
2. Sélectionnez le service Context Hub et cliquez sur  > **Vue** > **Config**.
   La vue Configuration des services de Context Hub s'affiche.

3. Sous l'onglet **Sources de données**, cliquez sur + > **AD**.
   La boîte de dialogue **Ajouter une source de données** s'affiche.



Vous devez configurer le schéma Active Directory pour répliquer les attributs suivants afin d'afficher les données dans la page RÉPONDRE :

- ID de l'employé
- Département
- Entreprise
- Titre
- Code postal

Tous les autres attributs sont répliqués automatiquement.

6. Fournissez les détails suivants sur la connexion de la base de données :

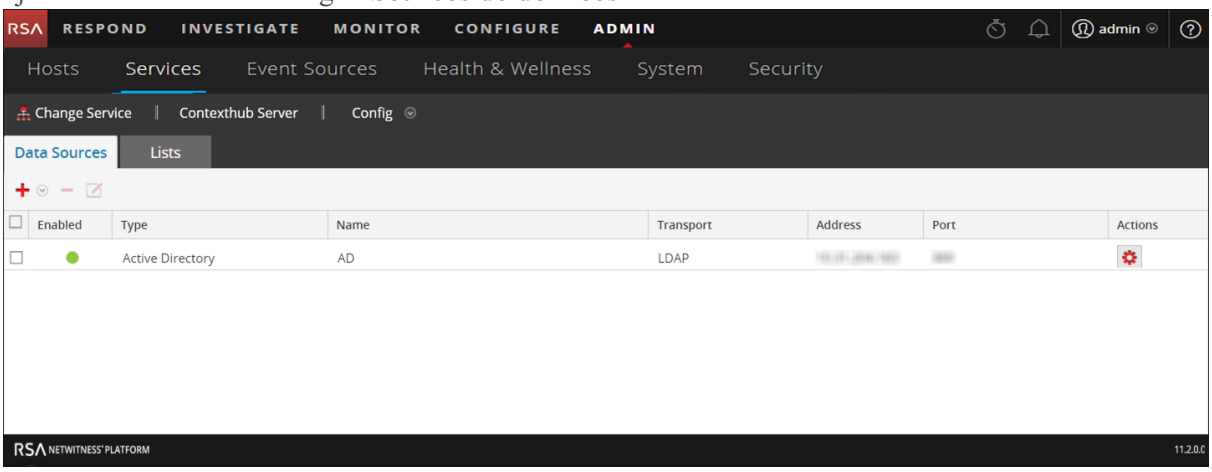
- Par défaut, la case **Activer** est activée. Si cette option est désactivée, le bouton Enregistrer est désactivé et vous ne pouvez pas ajouter la source de données et afficher les informations contextuelles.
- Renseignez les champs suivants :
  - **Nom :** Indiquez le nom de la source de données AD.
  - **Hôte :** Indiquez l'adresse IP ou le nom d'hôte du serveur AD.
  - **SSL :** Par défaut, il est vérifié avec le numéro de port 636, qui se connecte à la source de données avec une connexion Secure Sockets Layer (SSL).
  - **Approuver tous les certificats** : Activez cette case pour ajouter la source de données sans valider le certificat. Si vous désactivez cette option, vous devez télécharger un certificat de serveur Active Directory au format .cer ou .crt valide pour que la connexion soit établie. Si vous ajoutez plusieurs sources de données Active Directory avec SSL, vous devez configurer toutes ces sources de données avec un certificat valide ou l'option Approuver tous les certificats.
  - **Port :** le port par défaut est 636 avec SSL et 389 sans SSL.
    Si vous souhaitez extraire des données de plusieurs domaines, vous pouvez configurer une seule source de données avec le port de catalogue global (3269 avec SSL ou 3268 sans SSL).

    Pour couvrir plusieurs domaines, vous pouvez également configurer une seule source de données pour chaque domaine avec le port par défaut (389 avec SSL ou 636 sans SSL).

    Une multi-forêt est un ensemble de plusieurs domaines. Si vous souhaitez extraire des données d'une multi-forêt, vous devez configurer chaque forêt avec le port de catalogue global (3269 avec SSL ou 3268 sans SSL).
  - **Mot de passe :** Saisissez le mot de passe du nom unique de l'utilisateur utilisé pour la liaison avec Active Directory.
  - **Lier le nom unique de l'utilisateur :** Nom unique de l'utilisateur qui s'authentifie auprès du répertoire de recherche. Par exemple, cn=Administrator,cn=Users,dc=sub,dc=saserver,dc=local.
  - **Rechercher le nom unique de base :** Le nom unique de base ou DN de base identifie l'entrée dans le répertoire à partir duquel les recherches sont déclenchées. Le DN de base est souvent désigné comme étant la base de recherche. Par exemple, dc=sub,dc=saserver,dc=local.

7. Cliquez sur **Tester la connexion** pour tester la connexion entre Context Hub et la source de données.
8. Cliquez sur **Enregistrer**.
   AD est ajouté comme source de données pour le Context Hub configuré. La source de données AD

ajoutée s'affiche dans l'onglet **Sources de données**.



Après avoir ajouté la source de données, vous pouvez configurer les paramètres de cette source de données. Pour savoir comment procéder, reportez-vous à la rubrique Configurer les paramètres de source de données pour Context Hub .

Étapes suivantes

Une fois la configuration effectuée, vous pouvez afficher les données contextuelles dans le panneau Récapitulatif du contexte de la vue Répondre ou Enquêter. Pour savoir comment procéder, consultez la rubrique **Navigate to Context Summary Panel and View Additional Context** du manuel *Investigation and Malware Analysis Guide*.

Configurer NetWitness Endpoint comme source de données

Vous pouvez configurer NetWitness Endpoint comme source de données pour Context Hub et utiliser le serveur Context Hub pour récupérer des informations contextuelles à partir de NetWitness Endpoint. Utilisez les procédures de cette rubrique pour ajouter NetWitness Endpoint comme source de données pour le service Context Hub et configurer les paramètres (si nécessaire) pour NetWitness Endpoint.

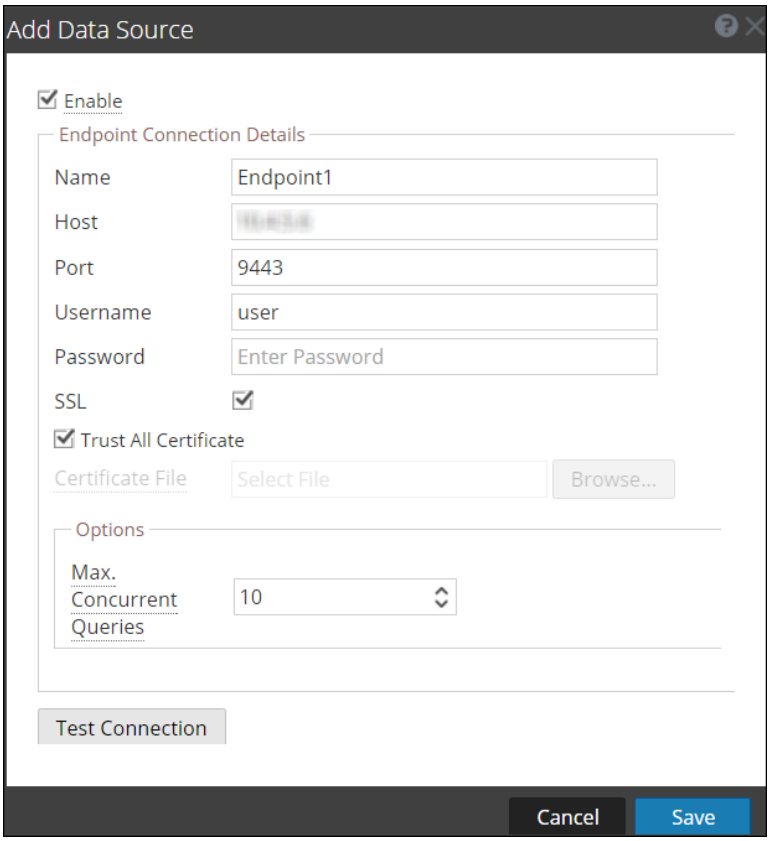
Conditions préalables

Avant de configurer la source de données NetWitness Endpoint, vérifiez que :

- le service Context Hub est disponible dans la vue **ADMIN** > **Services** de NetWitness Platform.
- NetWitness Endpoint (v4.1.1 à 4.3.0.5) est installé et configuré.
  Pour plus d'informations sur l'installation, la configuration de NetWitness Endpoint, et pour plus d'informations sur ce service, reportez-vous aux documents NetWitness Endpoint disponibles dans RSA Link.

Pour ajouter NetWitness Endpoint comme source de données pour Context Hub :

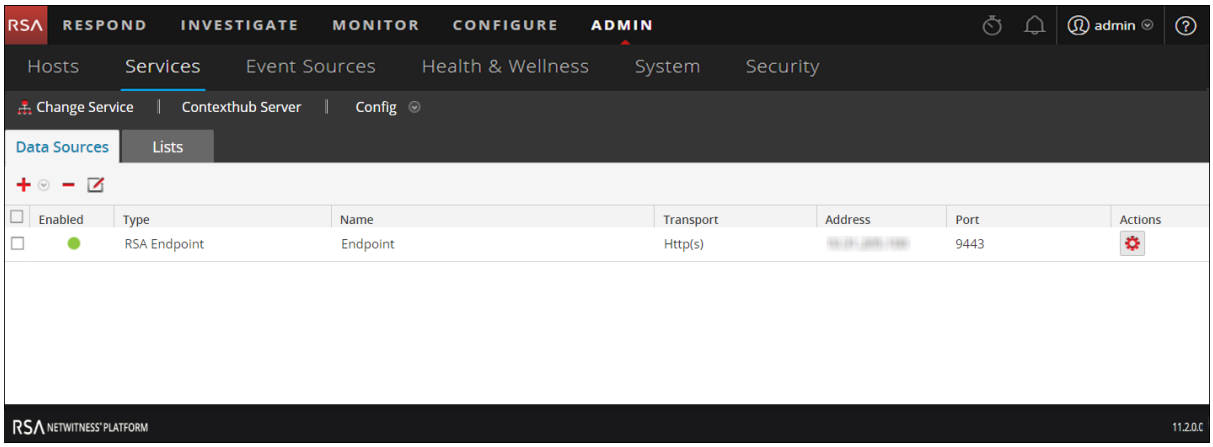
1. Accédez à **ADMIN** > **Services**.
   La vue Services s'affiche.
2. Sélectionnez le service Context Hub et cliquez sur >**Vue** > **Config**.
   La vue Configuration des services s'affiche.
3. Sous l'onglet **Sources de données**, cliquez sur + > **RSA Endpoint**.
   La boîte de dialogue **Ajouter une source de données** s'affiche.



4. Fournissez les informations suivantes :

- Par défaut, la case **Activer** est activée. Si cette option est désactivée, le bouton Enregistrer est désactivé et vous ne pouvez pas ajouter la source de données et afficher les informations contextuelles.
- Renseignez les champs suivants :
  - **Nom :** Indiquez le nom de la source de données NetWitness Endpoint.
  - **Hôte** : Saisissez le nom ou l'adresse IP de l'hôte sur lequel le serveur API NetWitness Endpoint est installé.
  - Port **:** Le port par défaut est le port 9443.
  - **SSL**: Sélectionnez SSL si vous souhaitez que NetWitness Platform communique avec l'hôte qui utilise le protocole SSL. Cette option est activée par défaut.
  - **Nom d'utilisateur** : Saisissez le nom d'utilisateur du serveur API NetWitness Endpoint.
  - **Mot de passe** : Saisissez le mot de passe du serveur API NetWitness Endpoint.
  - **Approuver tous les certificats** : Activez cette case pour ajouter la source de données sans valider le certificat. Si vous désactivez cette option, vous devez télécharger un certificat valide généré par un serveur ou une autorité de certification pour authentifier la connexion avec les formats pris en charge : .cer ou .crt chiffrés Base64 [PEM] ou DER.
  - **Nbre max. Requêtes simultanées** : Vous pouvez configurer le nombre maximal de requêtes simultanées à exécuter sur les sources de données configurées. La valeur par défaut est 10.

5. Cliquez sur **Tester la connexion** pour tester la connexion entre Context Hub et NetWitness Endpoint.
6. Cliquez sur **Enregistrer**.
   NetWitness Endpoint est ajouté comme source de données pour Context Hub et s'affiche dans l'onglet **Sources de données**.



Étapes suivantes

Après avoir ajouté la source de données, vous pouvez en configurer les paramètres. Pour plus d'informations, reportez-vous à la rubrique Configurer les paramètres de source de données pour Context Hub .

Vous pouvez aussi afficher les données contextuelles dans le panneau Récapitulatif du contexte de la vue Répondre ou Enquêter. Pour plus d'informations, reportez-vous au *Guide d'utilisation RSA NetWitness Respond* et au *Guide RSA NetWitness Investigation et Malware Analysis*.

Configurer Respond comme source de données

Vous pouvez configurer Respond comme source de données pour Context Hub et utiliser le service Context Hub pour récupérer des informations contextuelles à partir du service Respond. Si le service Respond est déjà configuré, les détails de configuration sont pré-remplis lors de l'ajout de Respond comme source de données. Utilisez les procédures de cette rubrique pour ajouter Respond comme source de données pour le service Context Hub et configurer les paramètres.

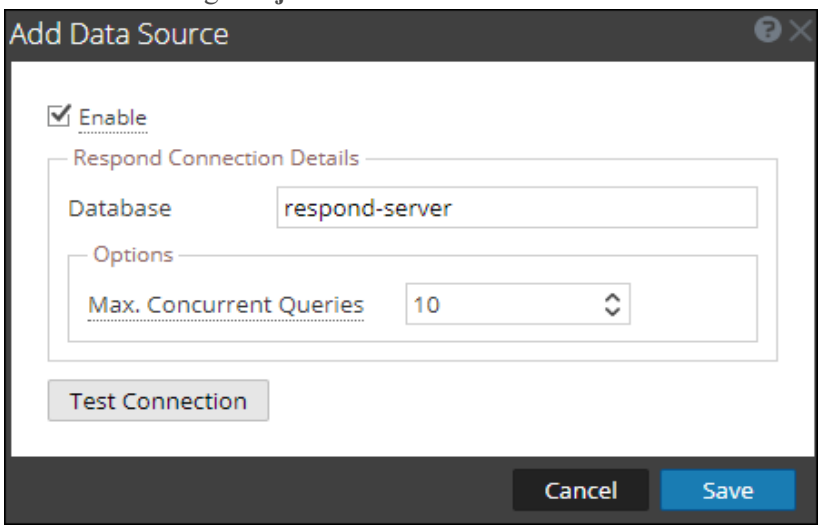
Conditions préalables

Avant de configurer la source de données Respond, vérifiez que :

- le service Context Hub est disponible dans la vue **ADMIN**> **Services** de NetWitness Platform.
- le service Respond est disponible.

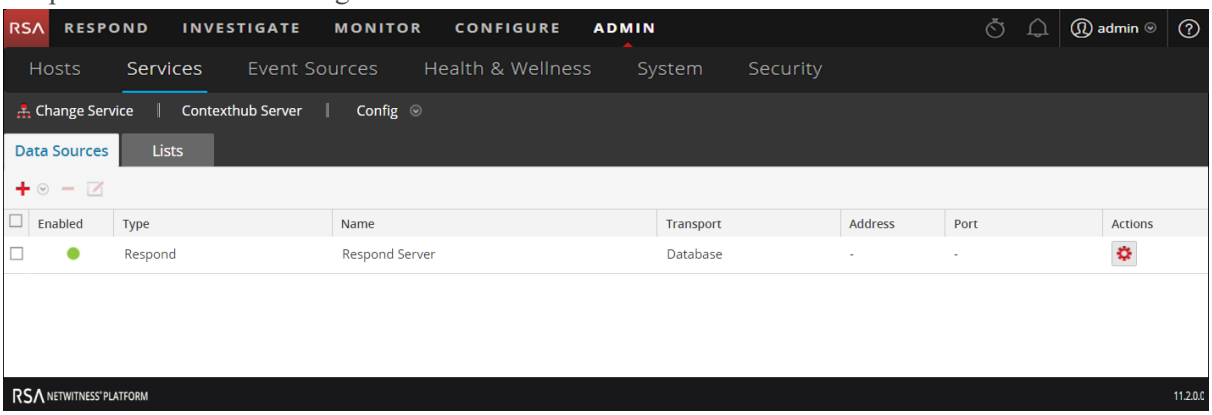
Pour ajouter Respond comme source de données pour Context Hub :

1. Accédez à **ADMIN** > **Services**.
   La vue Services s'affiche.
2. Sélectionnez le service Context Hub et cliquez sur > **Vue** > **Config**.
   La vue Configuration des services de Context Hub s'affiche.
3. Sous l'onglet **Sources de données**, cliquez sur + > **Respond**.
   La boîte de dialogue **Ajouter une source de données** s'affiche.



   Les champs requis pour configurer la source de données Respond sont mis à jour automatiquement.
4. Cliquez sur **Tester la connexion** pour tester la connexion entre Context Hub et la source de données.
5. Cliquez sur **Enregistrer**.
   Respond est ajouté comme source de données pour le Context Hub configuré. La source de données

Respond s'affiche dans l'onglet **Sources de données**.



Après avoir ajouté la source de données, vous pouvez en configurer les paramètres. Pour plus d'informations, reportez-vous à la rubrique Configurer les paramètres de source de données pour Context Hub .

Étapes suivantes

Une fois la configuration effectuée, vous pouvez afficher les données contextuelles dans le panneau Récapitulatif du contexte de la vue Répondre ou Enquêter. Pour plus d'informations, reportez-vous au *Guide d'utilisation RSA NetWitness Respond* et au *Guide RSA Netwitness Investigation et Malware Analysis*.

Configurer Live Connect comme source de données pour Context Hub

Cette rubrique décrit la procédure de configuration d'une source de données Live Connect pour Context Hub.

RSA Live Connect est un service de renseignements sur les menaces basé sur le Cloud. Ce service collecte, analyse et évalue les renseignements sur les menaces (adresses IP, domaines, fichiers,etc.) qui sont collectés à partir de différentes sources, y compris la communauté de clients RSA NetWitness® Platform et RSA NetWitness® Endpoint.

RSA Live Connect fait partie des Services Live et peut être configuré dans la vue Système > panneau Configuration des services Live. Pour plus d'informations sur la configuration des services Live, consultez la section **Configurer les paramètres des services Live** dans le Guide de *configuration système*.

RSA Live Connect Threat Insights fournit aux analystes la possibilité d'extraire des données de renseignement sur les menaces, telles que des informations liées à la propriété intellectuelle, du service Live Connect, qui seront exploitées par les analystes pendant la procédure d'enquête. Par défaut, **Threat Insights** est activé dans **Services Live supplémentaires**. Si le service Context Hub est configuré, Live Connect est ajouté automatiquement comme source de données pour Context Hub.

Conditions préalables

Assurez-vous que :

- Context Hub est activé et que le service est disponible dans la vue ADMIN > Services de NetWitness Platform.
- Le compte RSA Live est disponible.

Remarque : Pour créer un compte Live, reportez-vous à la section **Étape 1. Créer un compte Live** dans le *Guide de gestion des services Live*.

Par défaut, **Threat Insights** est activé dans la section **Services Live supplémentaires**. Avant de configurer la source de données Live Connect, vérifiez que vous êtes connecté à votre compte Live avec vos informations d'identification de compte Live et que Context Hub est activé. Live Connect est ajouté automatiquement en tant que source de données pour le service Context Hub.

Pour plus d'informations sur la configuration du compte Live et des services Live, consultez la section **Configurer les paramètres des services Live** dans le *Guide de configuration système*.

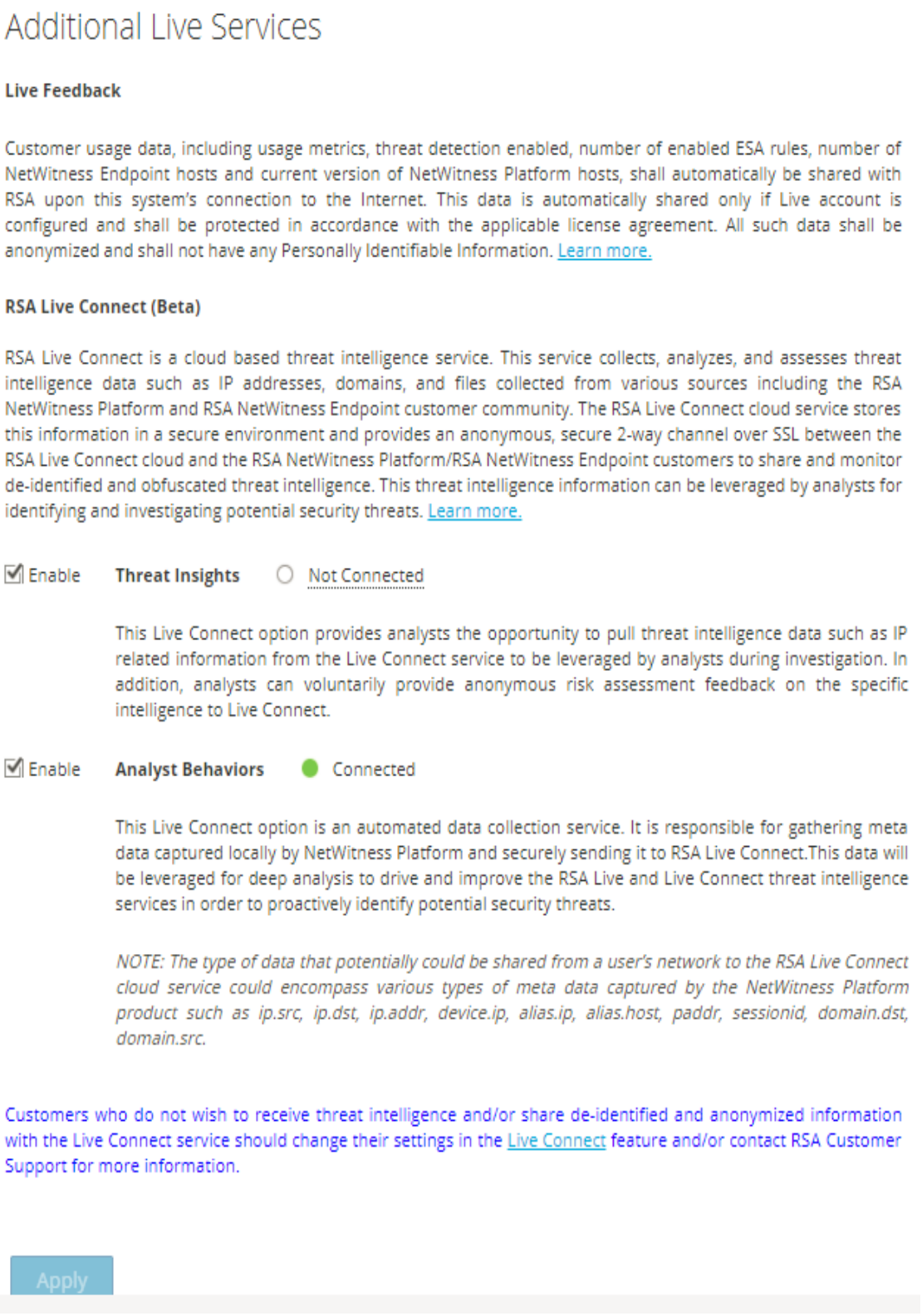
Pour plus d'informations sur la configuration du service Context Hub, reportez-vous à la section **Étape1. Ajouter le service Context Hub** du *Guide de configuration de Context Hub*.

Activer/désactiver une source de données Live Connect

Pour activer/désactiver une source de données Live Connect pour Context Hub

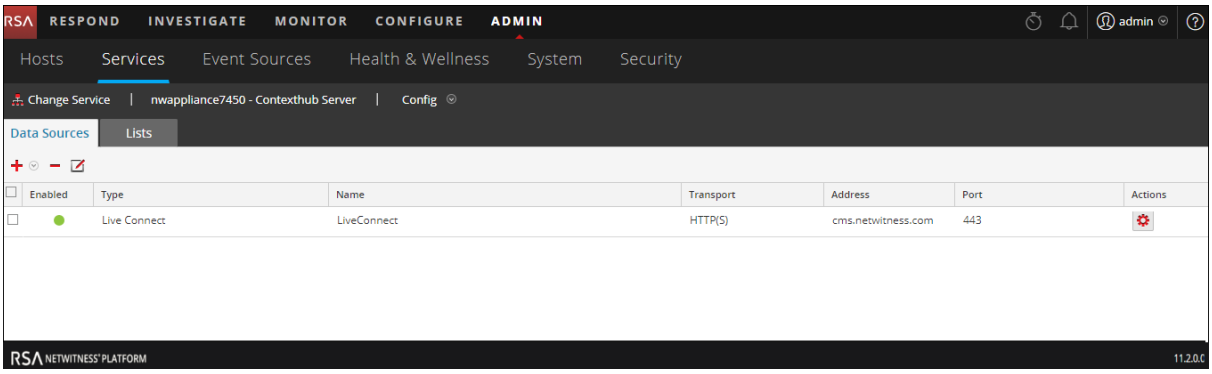
1. Accédez à **ADMIN > Système**.
2. Dans le volet de navigation de gauche, sélectionnez **Services Live**.

3. Dans la section **Services Live supplémentaires**, activez **Threat Insights**.



4. Cliquez sur **Appliquer**.
   La source de données Live Connect est activée pour le service Context Hub.

5. Pour vérifier, accédez à l'onglet **Sources de données** et affichez les sources disponibles.
   La source Live Connect doit être ajouté à la liste des sources disponibles et le champ **Activé** doit être un cercle vert plein ( ).



6. Pour désactiver la source de données Live Connect, désactivez **Threat Insights** dans le panneau Services Live supplémentaires et cliquez sur **Appliquer**.

   La source de données Live Connect est désactivée pour le service Context Hub.

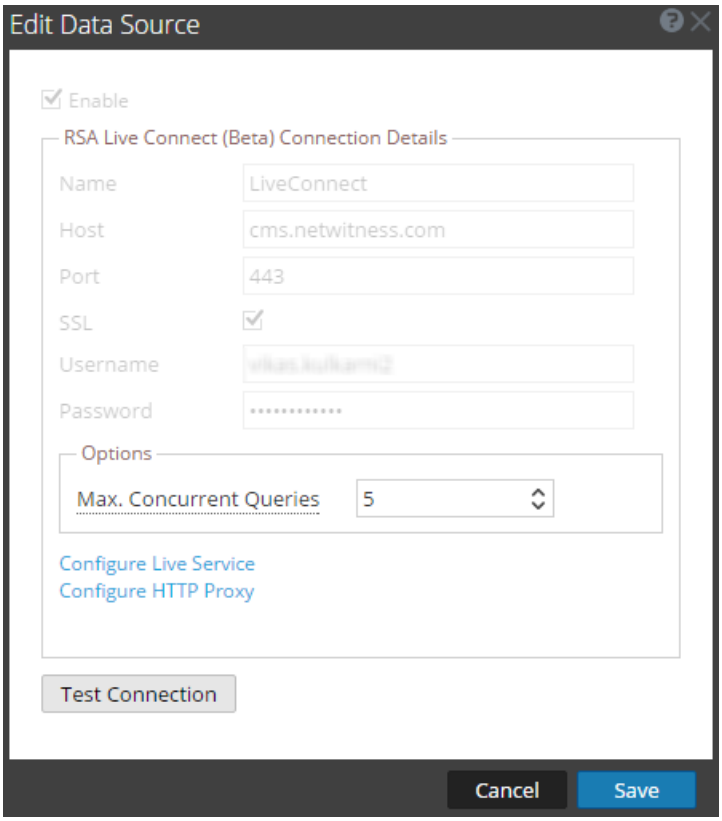
> **Remarque :** Si Threat Insights est désactivé, le panneau Recherche contextuelle pour Live Connect (dans les vues Naviguer et Événements de Procédure d'enquête) affiche un message pour configurer la source de données Live Connect. Pour afficher les données contextuelles pour Live Connect, vous devez activer Threat Insights.

Modifier les paramètres de source de données Live Connect

Pour modifier une source de données Live Connect pour Context Hub :

1. Dans le menu Menu principal, sélectionnez **Admin > Services**.
   La vue Services s'affiche.
2. Dans le panneau **Services**, sélectionnez le service Context Hub, puis cliquez sur > **Vue** > **Config**.
   La vue Configuration des services s'affiche.
3. Dans l'onglet **Sources de données**, sélectionnez la source de données Live Connect et cliquez sur .

   La boîte de dialogue **Modifier la source de données** s'affiche.



4. Modifier les champs obligatoires :

Champ	Description
Nbre max. Requêtes simultanées	Vous pouvez configurer le nombre maximal de requêtes simultanées définies par le service Context Hub à exécuter sur les sources de données configurées. La valeur par défaut est 25.

5. Pour modifier les paramètres de connexion de Live et les paramètres de proxy, procédez comme suit :
   - Pour modifier les paramètres de connexion de Live, consultez la section **Panneau de Configuration des Services Live** dans le *Guide de Configuration système*.
   - Pour modifier les paramètres de proxy, consultez la section **Panneau Paramètres proxy HTTP** dans le *Guide de Configuration système*.
6. Cliquez sur **Tester la connexion** pour tester la connexion entre Context Hub et la source de données.
7. Cliquez sur **Enregistrer** pour enregistrer les paramètres.

Étapes suivantes

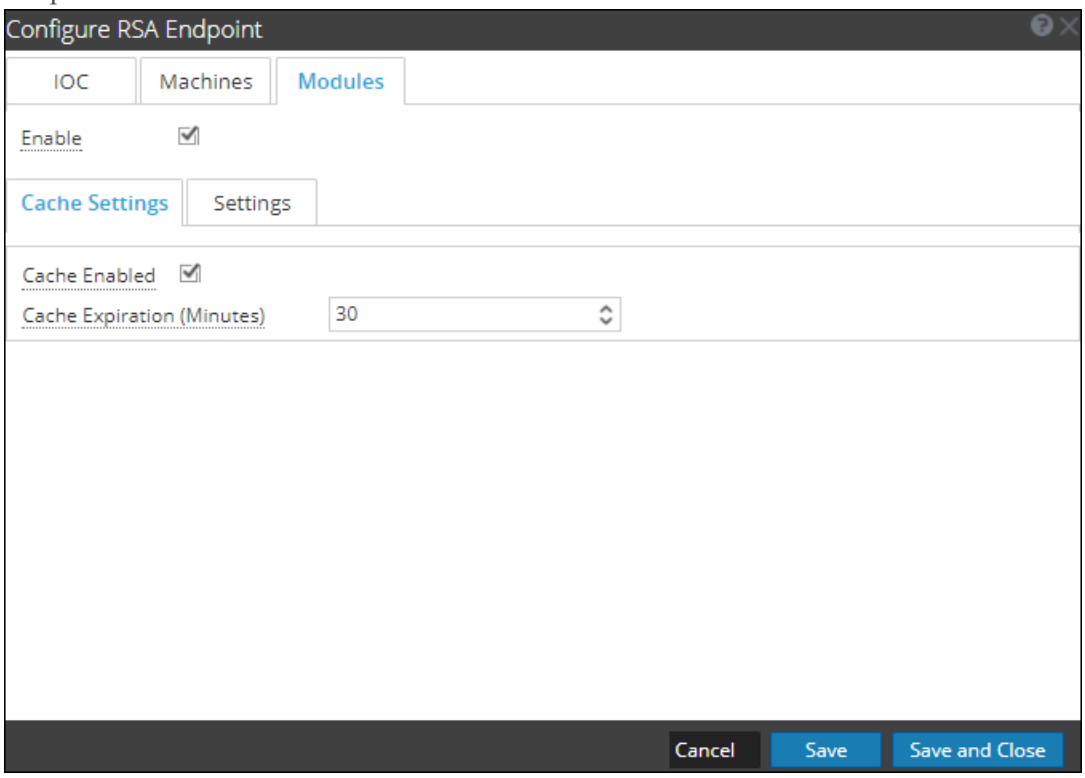
Une fois la configuration effectuée, vous pouvez afficher les données contextuelles dans le panneau Récapitulatif du contexte de la vue Répondre ou Enquêter. Pour plus d'informations, reportez-vous au *Guide d'utilisation RSA NetWitness Respond* et au *Guide RSA NetWitness Investigation et Malware Analysis*.

Configurer les paramètres de source de données pour Context Hub

Une fois que vous avez configuré les sources de données requises, vous pouvez personnaliser les paramètres des sources de données en fonction de vos besoins.

Pour accéder aux paramètres et les configurer :

1. Accédez à **ADMIN**> **Services**.
   La vue Services s'affiche.
2. Dans le panneau Services, sélectionnez le service Context Hub, puis cliquez sur > **Vue** > **Config**.
   La vue Configuration des services de Context Hub s'affiche.
3. Sélectionnez la source de données pour laquelle vous souhaitez configurer les paramètres, puis cliquez sur dans la colonne Actions.
   La capture d'écran suivante est un exemple de la boîte de dialogue des paramètres NetWitness Endpoint :



4. Configurez les champs suivants :

Champ	Description
Activer	Cette option est activée par défaut (cochée) et peut être utilisée pour activer ou désactiver la réponse de la source de données sélectionnée.
Paramètres du cache	Toute recherche de Context Hub peut être stockée dans le cache de Context Hub pour une durée configurée. La réponse à toute demande ultérieure correspondante sera extraite à partir du cache de Context Hub. Cette section permet de définir les paramètres de cache suivants pour la requête : • **Cache activé** : Par défaut, cette case est cochée et la réponse à la requête est mise en cache. • **Expiration du cache (minutes)** : Durée maximale de conservation de la requête dans le cache. La durée par défaut est de 30 minutes et la durée maximale de 7 200 minutes. Vous pouvez les configurer.
Expiration des valeurs de liste	**Activer** : Sélectionner Activer pour définir le nombre de jours de disponibilité des valeurs de liste. Par défaut, cette option est désactivée et les valeurs sont conservées. **Durée de vie (jours)** : Saisissez le nombre de jours de conservation des valeurs de liste.
Mappage de méta	N'importe quelle liste stockée dans Context Hub doit être accessible via une recherche. La recherche dans Context Hub est effectuée en fonction du type de méta ou d'entités. Exemples : IP, HOST, MAC ADDRESS, DOMAIN, FILE_NAME, FILE_HASH, USER. **Type de métadonnées** : Entités disponibles dans Context Hub. **Champs Context Hub** : En-têtes de colonne à partir du fichier CSV que vous avez ajoutés lors de la création d'une liste.
Valeur IIOC minimale	Score minimum de l'indicateur de compromission instantané (IIOC) à prendre en compte pour extraire les informations contextuelles des modules NetWitness Endpoint.
Durée de la requête (jours)	Durée (en jours) sur laquelle va porter la requête des données contextuelles.
Limite	Nombre maximum d'enregistrements à afficher lors d'une recherche de contexte.
Répéter tous les	Configurez le planning récurrent pour extraire et stocker des données contextuelles sur les intervalles requis.

5. Cliquez sur l'une des options suivantes :
   - **Annuler** - Sélectionnez cette option pour annuler les modifications.
   - **Enregistrer** - Sélectionnez cette option pour enregistrer les modifications.
   - **Enregistrer et fermer** - Sélectionnez cette option pour enregistrer et fermer la boîte de dialogue.

En fonction de la source de données que vous sélectionnez, les groupes de réponses varient. Le tableau suivant décrit les groupes de réponses pour chaque source de données.

Source de données (Connexion)	Groupes de réponses pris en charge	Paramètres de champ
Liste	Liste	Mappage de méta Type de méta Champs Context Hub Paramètres Paramètres de lecture préalable des données Récurrence régulière Expiration des valeurs de liste Paramètres de cache Cache activé Expiration du cache (minutes) [Min. : 30 minutes et Max. : 7 200 minutes]
RSA Archer	Archer	Paramètres de cache Cache activé Expiration du cache (minutes) Paramètres Exporter la configuration des attributs Exporter les paramètres de la lecture préalable des données Gestion de la protection des données personnelles Récurrence régulière
Active Directory	Utilisateurs	Mappage de métadonnée Type de métadonnées Champs Context Hub Paramètres Paramètres de la lecture préalable des données Récurrence régulière Expiration des valeurs de liste Paramètres du cache Cache activé Expiration du cache (minutes) [Min. : 30 minutes et Max. : 7 200 minutes]

Source de données (Connexion)	Groupes de réponses pris en charge	Paramètres de champ
RSA Endpoint	IOC Machines Modules	Paramètres de cache Cache activé Expiration du cache (minutes) Paramètres Paramètres du panneau contextuel Paramètres de cache Cache activé Expiration du cache (minutes) Paramètres Paramètres du panneau contextuel Paramètres de cache Cache activé Expiration du cache (minutes) Paramètres Valeur IIOC minimale Paramètres du panneau contextuel
Répondre	Alertes Incidents	Paramètres du panneau contextuel Paramètres de lecture préalable des données Durée de la requête (jours) Paramètres de cache Cache activé Expiration du cache (minutes)
Live Connect	Domaine Fichier IP	Paramètres de cache Cache activé Expiration du cache (minutes) Paramètres Paramètres du panneau contextuel

Remarque : Une fois les paramètres de source de données configurés, vous pouvez configurer les paramètres de configuration de Context Hub en accédant à **ADMIN**> **Services**> **Vue** > **Explorer**. Veillez à redémarrer le service Context Hub si vous apportez des modifications de configuration dans la vue Explorer.

Importer ou exporter des listes pour Context Hub

En tant qu'administrateur, vous pouvez importer ou exporter une liste configurée dans le service Context Hub, qui peut être utilisée par un analyste. Le fichier à importer ou exporter est un fichier CSV, et vous pouvez ajouter plusieurs listes comme sources de données.

Conditions préalables

Assurez-vous que Context Hub est activé et que le service est disponible dans la vue **Admin** > **Services** de NetWitness Platform.

Importer une liste

Une fois que vous avez importé une liste, vous pouvez effectuer les tâches suivantes :

- Importer des valeurs dans une liste existante
- Ajouter une ligne à une liste
- Modifier le nom et la description d'une liste
- Modifier une valeur dans une liste
- Supprimer une liste
- Supprimer une ligne dans une liste

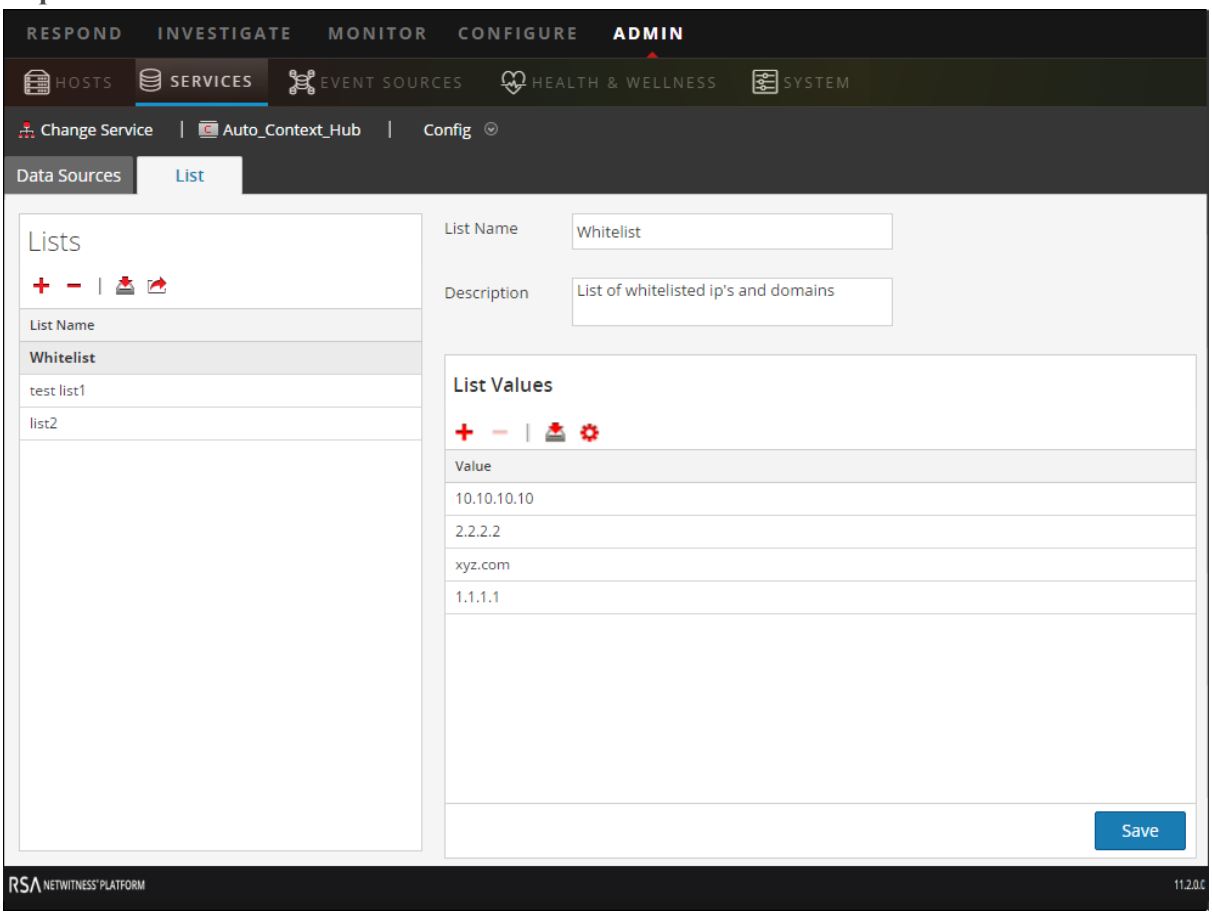
Remarque : Vous devez effectuer les mêmes modifications dans le fichier CSV approprié afin qu'elles soient répercutées à la prochaine récurrence du planning. Sinon, lorsque vous importez des valeurs dans une liste existante à une seule colonne ou plusieurs colonnes, les données sont remplacées à partir du fichier source lors du renouvellement du planning. Dans le cas d'une liste de flux personnalisée, si le flux est modifié ou supprimé, la liste du Context Hub correspondante est également modifiée ou supprimée.

Importer une liste à une seule colonne

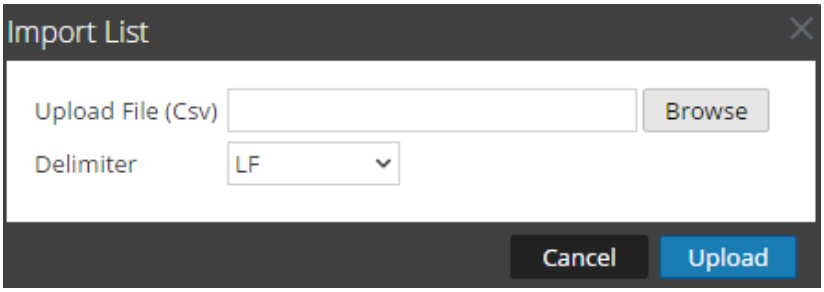
Pour importer une liste :

1. Sélectionnez ADMIN > **Services**.
   La vue Services s'affiche.
2. Dans le **panneau Services**, sélectionnez le service  Context Hub, puis cliquez sur > **View** > **Config**.
   La vue Configuration des services du service Context Hub s'affiche.
3. Cliquez sur l'onglet **Listes**.
   L'onglet Listes comprend le panneau **Listes** et le panneau **Valeurs de la liste**.
   L'image ci-dessous illustre un exemple de liste à une seule colonne.**<capture d'écran actualisée**

requise>



4. Cliquez sur dans le panneau **Listes**.
   La boîte de dialogue **Importer la liste** s'affiche.



5. Dans la boîte de dialogue **Importer la liste**, effectuez les étapes suivantes :
   a. Dans le champ **Télécharger le fichier (csv)**, recherchez et sélectionnez le fichier `CSV`.
   b. Dans le champ **Délimiteur**, sélectionnez le délimiteur des valeurs de liste parmi les options **Virgule**, **CR** (Retour chariot) et **LF** (Saut de ligne).
6. Cliquez sur **Télécharger** pour télécharger le fichier CSV dans Context Hub.

Ces listes sont considérées comme des sources de données permettant de récupérer des informations contextuelles. Mais vous pouvez effectuer un ajout à une liste à plusieurs colonnes existante. Les données ne sont ajoutées que si le nombre de colonnes concorde.

Remarque : Vous ne pouvez pas créer une nouvelle liste à plusieurs colonnes en important directement un fichier CSV. Toutefois, tous les flux qui sont convertis en listes à plusieurs colonnes s'afficheront dans l'onglet Liste. Pour plus d'informations sur la façon d'importer une liste à plusieurs colonnes, reportez-vous à la rubrique Configurer des listes en tant que sources de données.

Importer des valeurs dans une liste existante

Lorsque vous importez des valeurs dans une liste existante à plusieurs colonnes, les données sont remplacées à partir du fichier source à la prochaine récurrence du planning.

Pour importer des valeurs dans une liste :

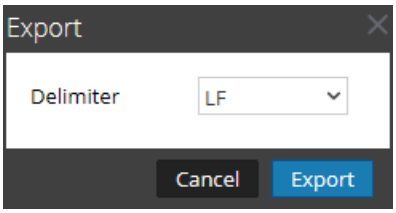
1. Accédez à **ADMIN** > **Services**.
   La vue Services s'affiche.
2. Sélectionnez un service et cliquez sur  > **Vue** > **Config**.
   La vue Configuration des services du service Context Hub s'affiche.
3. Cliquez sur l'onglet **Listes**.
   L'onglet Liste comprend le panneau **Listes** et le panneau **Valeurs de la liste**.
4. Dans le panneau Listes, sélectionnez la liste dont vous souhaitez importer les valeurs.
5. Cliquez sur  dans le panneau **Valeurs de la liste**.
   La boîte de dialogue **Importer la liste** s'affiche.
6. Dans la boîte de dialogue **Importer la liste**, effectuez les étapes suivantes :
   a. Dans le champ **Télécharger le fichier (csv)**, recherchez et sélectionnez le fichier `CSV`.
   b. Dans le champ **Délimiteur**, sélectionnez le délimiteur des valeurs de liste parmi les options **Virgule**, **CR** (Retour chariot) et **LF** (Saut de ligne).
7. Cliquez sur **Télécharger** pour télécharger le fichier CSV dans NetWitness Platform.

Les valeurs de liste sont importées dans la liste sélectionnée. Ces listes sont considérées comme des sources de données permettant de récupérer des informations contextuelles. Mais vous pouvez ajouter une liste existante à plusieurs colonnes. Les données ne sont ajoutées que si le nombre de colonnes concorde.

Exporter une liste pour Context Hub

Pour exporter une liste :

1. Sous l'onglet **Listes** de la vue Configuration des services du service Context Hub, cliquez sur  .
   La boîte de dialogue **Exporter** s'affiche.



2. Dans le champ **Délimiteur**, sélectionnez le délimiteur des valeurs d'une liste exportée dans la liste déroulante [**Virgule**, **CR** (Retour chariot) et **LF** (Saut de ligne).
3. Cliquez sur **Exporter**.

Pour une liste à une seule colonne, vous pouvez sélectionner le délimiteur. Et, dans le cas d'une liste à plusieurs colonnes, la liste est exportée sur la machine locale, sous forme d'un fichier CSV.

Remarque : Lorsqu'un flux personnalisé est converti en une liste Context Hub, vous devez mapper au moins une clé méta avec un ou plusieurs mappage d'entité pour un en-tête de colonne avec un méta. Toutefois, si vous souhaitez ajouter ou modifier d'autres entités, vous pouvez le faire en cliquant sur ⚙ .

Configurer le mappage du type de méta pour Context Hub

En tant qu'administrateur, vous gérez le mappage des types de méta Context Hub avec les clés méta NetWitness.

Le service Context Hub fournit une recherche contextuelle des métavaleurs dans les vues Répondre et Procédure d'enquête. Ces métavaleurs sont regroupées en types de métadonnées selon la catégorie à laquelle ils appartiennent. Les clés méta de NetWitness Platform Respond et Investigation, par exemple `ip.src` et `ip.dst`, sont regroupées dans le type de métadonnées `IP` dans Context Hub. Le type de métadonnées `IP` est mappé à son tour à des métadonnées telles que `alert.events.source.device.ip_address` et `alert.events.destination.device.ip_address` dans la base de données RÉPONDRE.

Dans la vue **ADMIN**> **Système** > **Procédure d'enquête**, l'onglet Recherche contextuelle permet à l'administrateur de configurer le mappage des clés méta et du type de méta dans NetWitness. L'administrateur peut ajouter ou supprimer des clés méta à la liste des types de métadonnées pris en charge par Context Hub.

Le service Context Hub est préconfiguré avec un mappage par défaut des types de métadonnées aux clés méta. Il est censé fonctionner pour la plupart des déploiements, sauf si des mappages personnalisés sont créés pour votre déploiement spécifique.

Remarque : Vous ne pouvez pas ajouter un nouveau type de métadonnées.

Le mappage par défaut est indiqué ci-dessous :

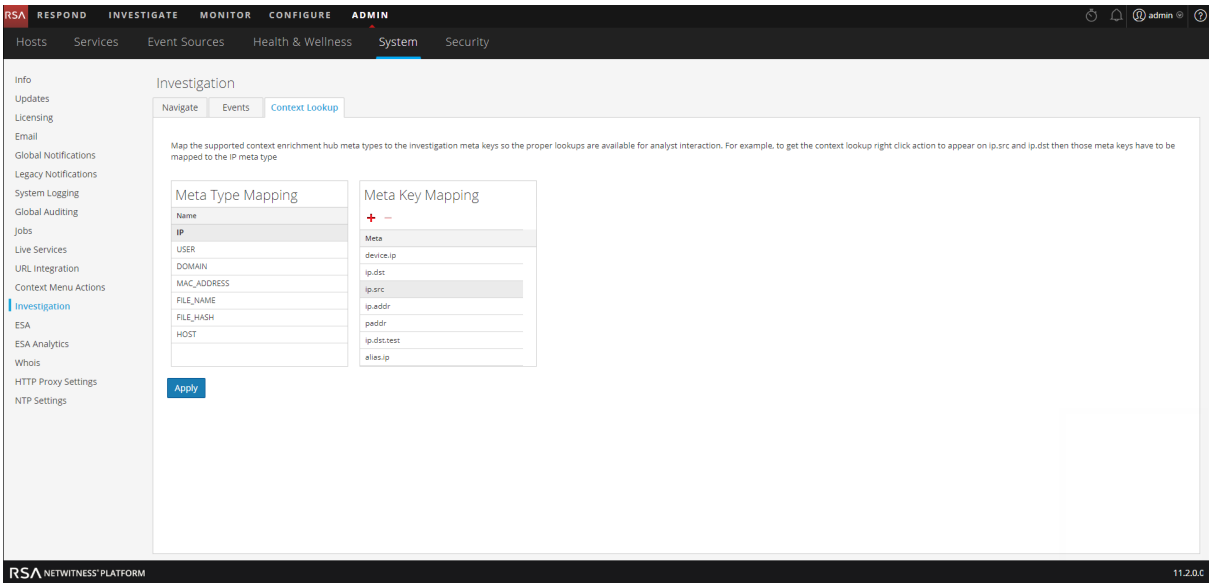
Nom de type de métadonnées	Clés méta
IP	device.ip, ip.src, ip.dst, ip.addr,ipv6.src, alias.ip, ipv6.addr, device.ipv6,forward.ip, forward.ipv6,ipv6.dst, ipv6.addr, stransaddr, transaddr
USER	user.src, user.dst, username, event user
DOMAIN	domain.src, domain.dst,fqdn, web.domain, domain, sdomain, ddomain
MAC_ADDRESS	eth.dst, eth.src, alias.mac
FILE_NAME	filename, sourcefile
FILE_HASH	checksum
HÔTE	device.host, alias.host, host.src, host.dst

Procédure

Pour gérer le mappage des clés méta Investigation :

1. Accédez à ADMIN > **Système**.
2. Dans le panneau des options, sélectionnez **Procédure d'enquête**.

   Le panneau Configuration des procédures d'enquête s'affiche.
3. Sélectionnez l'onglet **Recherche contextuelle**.



4. Sélectionnez un type de métadonnées pour visualiser les clés méta par défaut mappées à ce type de métadonnées.
5. Pour ajouter une clé méta, cliquez sur +, puis saisissez la clé méta.
6. Pour supprimer une clé méta, sélectionnez-la, puis cliquez sur −.
7. Pour enregistrer les modifications, cliquez sur **Appliquer**.
8. Pour ajouter un nouveau méta, il doit être inclus dans le fichier d'index personnalisé du Concentrator. Par exemple, si vous souhaitez ajouter un méta **nom de domaine complet**, vous aurez besoin ajouter une nouvelle entrée : **key name="fqdn" description="Fully Qualified Domain Name="IndexValues" form-at="Text" valueMax="100" />** dans le fichier d'index. Pour plus d'informations sur l'ajout d'un nouveau méta dans le fichier d'index, consultez la rubrique Index Customization dans le document*Core Database Tuning Guide*. Une fois que vous avez ajouté le nouveau méta, vous pouvez afficher les informations contextuelles en cliquant sur l'option Pivoter vers la fonction Enquêter dans la vue Répondre.

Si une nouvelle clé méta est ajoutée, l'option de menu Recherche contextuelle est activée pour les métavaleurs situées sous la clé méta. Pour plus d'informations, consultez la rubrique Panneau Configuration des procédures d'enquête dans le *Guide de configuration système*.

Références de Context Hub

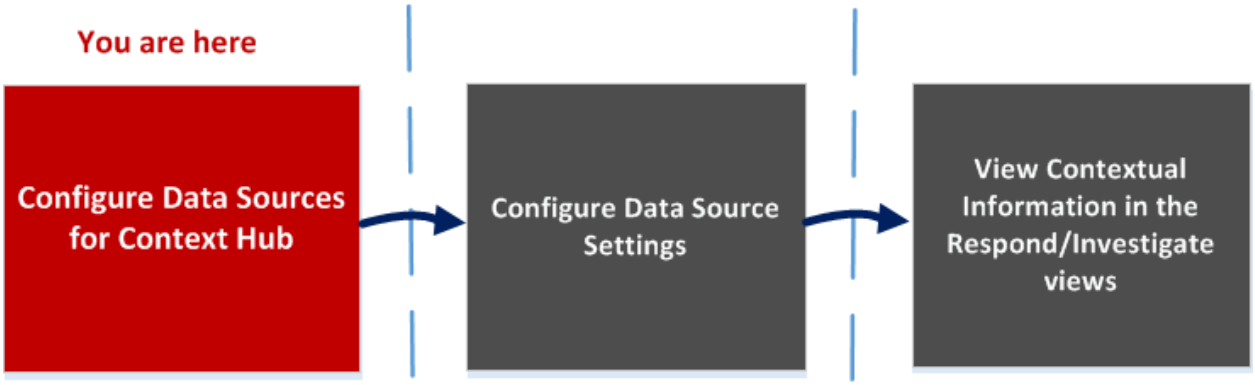
Une fois que vous avez configuré le service Context Hub et la source de données requise, vous pouvez gérer les paramètres de chaque source de données. Cela vous aidera à optimiser et personnaliser les résultats de recherche.

Onglet Sources de données de Context Hub

Sous l'onglet **Sources de données**, vous pouvez configurer une ou plusieurs sources de données pour le service Context Hub. Accédez à **ADMIN** > **SERVICES** > Sélectionnez le service Context Hub > **Vue** > **Config** > **Sources de données**.

Workflow

Ce workflow présente la procédure de configuration des sources de données pour le service Context Hub pour afficher des informations contextuelles dans les vues Répondre et Enquêter.



- La première tâche consiste à ajouter une source de données
- La deuxième tâche consiste à configurer les paramètres des sources de données pour améliorer votre déploiement. Cette tâche est facultative car les paramètres de chaque source de données sont déjà configurés avec des valeurs par défaut afin d'optimiser les performances.
- La troisième tâche consiste à visualiser et analyser les informations contextuelles dans le panneau Récapitulatif du contexte des vues Répondre et Enquêter.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur	Configurer des sources de données pour Context Hub*	Configurer des listes en tant que sources de données Configurer Archer en tant que source de données Configurer la source de donnée Active Directory Configurer NetWitness Endpoint comme source de données Configurer Respond comme source de données Configurer Live Connect comme source de données pour Context Hub

Rôle	Je souhaite...	Me montrer comment
Administrateur	Configurer des paramètres de données Hub*	Configurer les paramètres de source de données pour Context Hub
Analyste	Afficher les informations contextuelles dans la vue Répondre	Consultez le *Guide d'utilisation de NetWitness Respond.*
Analyste	Ajouter, créer et supprimer la liste à partir des vues Répondre ou Enquêter	Consultez le *Guide d'utilisation de NetWitness Respond.* Consultez le *Guide d'utilisation Investigation et Malware Analysis*.
Analyste	Ajouter ou supprimer une entrée dans une liste existante	Consultez le *Guide d'utilisation de NetWitness Respond.*

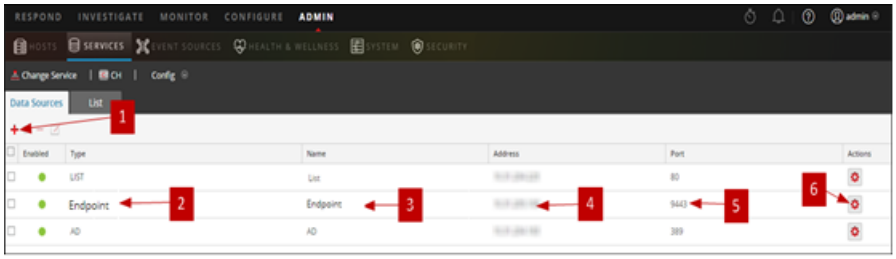
*Vous pouvez effectuer cette tâche (qui se trouve sous l'onglet Sources de données Context Hub.)

Rubriques connexes

- Configurer des listes en tant que sources de données
- Configurer Archer en tant que source de données
- Configurer la source de donnée Active Directory
- Configurer NetWitness Endpoint comme source de données
- Configurer Respond comme source de données
- Configurer Live Connect comme source de données pour Context Hub

Aperçu rapide

L'exemple suivant illustre comment ajouter une source de données pour le service Context Hub.



1. Cliquez sur + pour afficher la boîte de dialogue **Ajouter une source de données**.
2. Affiche le type de source de données.
3. Nom qui identifie la source de données.
4. Adresse IP ou nom d'hôte de la source de données.
5. Port de connexion de la source de données.
6. Ouvre la boîte de dialogue **Configurer les paramètres**. Vous pouvez afficher et modifier les paramètres à afficher dans le panneau Récapitulatif du contexte dans les vues Répondre ou

Enquêter.
7 Cliquez sur **Tester la connexion** pour vérifier que l'hôte est connecté au service Context Hub.

Barre d'outils

Le tableau suivant décrit les actions de la barre d'outils.

Fonctionnalité	Description
	Ouvre la boîte de dialogue Ajouter une source de données pour vous permettre d'ajouter une source de données. Vous ne pouvez ajouter qu'une seule source de données de chaque type. Exceptions : les sources de données Liste et Active Directory qui peuvent être ajoutées plusieurs fois. Pour obtenir des instructions détaillées sur l'ajout d'une source de données, reportez-vous à la section Configurer des listes en tant que sources de données.
	Supprimer une source de données. Si vous supprimez une source de données, Context Hub ne considère pas le service supprimé comme une source de données. Toutes les informations contextuelles extraites précédemment cessent d'être disponibles.
	Ouvre la boîte de dialogue Modifier une source de données. Pour obtenir une description de chaque champ du panneau Modifier une source de données, reportez-vous à la section Configurer Live Connect comme source de données pour Context Hub.
	Ouvre la boîte de dialogue Configurer les paramètres. Vous pouvez afficher et modifier les paramètres des sources de données. Pour obtenir une description de chaque champ de la boîte de dialogue Configurer les réponses, reportez-vous à la section Configurer les paramètres de source de données pour Context Hub .

Configurations des sources de données

Le tableau ci-dessous décrit les configurations listées.

Fonctionnalité	Description
Activé	Indique si la source de données est activée ou désactivée. Un cercle vert plein indique que la source de données est activée ( ). Un cercle blanc vide indique que la source de données est désactivée.
Type	Type de source de données. Par exemple, Lists, Archer, Active Directory, Endpoint, Répondre ou Live Connect.
Nom	Nom unique qui identifie la source de données. Par exemple, Répondre \.
Adresse	Adresse IP ou nom d'hôte de la source de données.
Port	Port de connexion de la source de données varie en fonction de la source de données en cours d'ajout. Par exemple, pour Endpoint le port est 9443, pour Lists le port est 80, etc.

Onglet Listes de Context Hub

Sous l'onglet **Listes**, vous pouvez créer et configurer des listes pour Context Hub. Accédez à **ADMIN** > **SERVICES** > Sélectionnez le service Context Hub > **Vue** > **Config** > **Listes**.

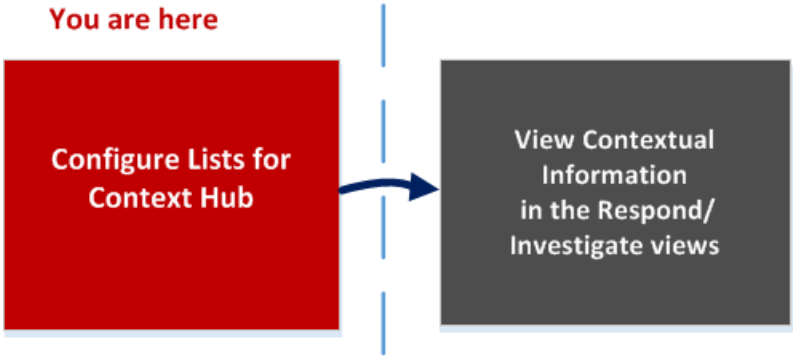
À l'aide de l'onglet Listes du service Context Hub, vous pouvez créer une ou plusieurs listes, et y ajouter les valeurs de liste appropriées. Ces listes sont automatiquement considérées comme des sources de données pour le service Context Hub.

Vous pouvez remplir ces listes à l'aide d'éléments, soit par l'importation de fichiers CSV externes ou de feeds personnalisés, soit par l'ajout de métadonnées via l'option Ajouter à la liste/Supprimer de la liste des vues Répondre et Investigation.

Remarque : Vous pouvez également créer des listes et ajouter des valeurs de liste à partir des vues Répondre et Investigation. Pour plus d'informations, reportez-vous au *Guide d'utilisation RSA NetWitness Respond* et au *Guide RSA Netwitness Investigation et Malware Analysis*.

Workflow

Ce workflow présente la procédure de configuration des listes pour le service Context Hub pour afficher des informations contextuelles dans les vues Répondre et Enquêter.



La création d'une ou de plusieurs listes est la première tâche de ce workflow. Les listes peuvent contenir des métas prises en charge, telles que : Adresse IP, Utilisateur, Hôte, Domaine, Adresse MAC, Nom du fichier ou Hachage de fichier. La tâche suivante consiste à analyser ou utiliser les données de listes pour afficher des données contextuelles dans les vues Répondre et Enquêter.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur	Configurer des sources de données de listes pour Context Hub*	Configurer des listes en tant que sources de données
Administrateur/analyste	Afficher les informations contextuelles dans la vue Répondre	Consultez le *Guide d'utilisation de NetWitness Respond*.

Rôle	Je souhaite...	Me montrer comment
Administrateur/analyste	Gérer les listes et les valeurs de liste dans Investigation	Consultez le *Guide d'utilisation Investigation et Malware Analysis*.
Administrateur/analyste	Créer une liste	Reportez-vous au *Guide d'utilisation de NetWitness Respond* et au *Guide d'utilisation Investigation et Malware Analysis*.
Administrateur/analyste	Mettre à jour une liste	Reportez-vous au *Guide d'utilisation de NetWitness Respond* et au *Guide d'utilisation Investigation et Malware Analysis*.
Administrateur/analyste	Supprimer la liste	Reportez-vous au *Guide d'utilisation de NetWitness Respond* et au *Guide d'utilisation Investigation et Malware Analysis*.
Administrateur/analyste	Importer une liste	Importer ou exporter des listes pour Context Hub
Administrateur/analyste	Exporter une liste	Importer ou exporter des listes pour Context Hub

*Vous pouvez effectuer cette tâche ici (c'est-à-dire sous l'onglet Listes de Context Hub).

Rubriques connexes

- Onglet Sources de données de Context Hub
- « Dépannage de NetWitness Investigate » dans le *Guide de l'utilisateur de NetWitness Investigate*

Aperçu rapide

L'exemple suivant montre comment ajouter des listes pour le service Context Hub.

L'onglet Liste contient les panneaux **Listes** et **Valeurs de la liste**. Le panneau **Listes** contient une barre d'outils avec les options permettant d'ajouter, de supprimer, d'importer et d'exporter des listes. Les entrées situées sous **Nom de la liste** sont des listes ajoutées ou importées pour le service Context Hub.

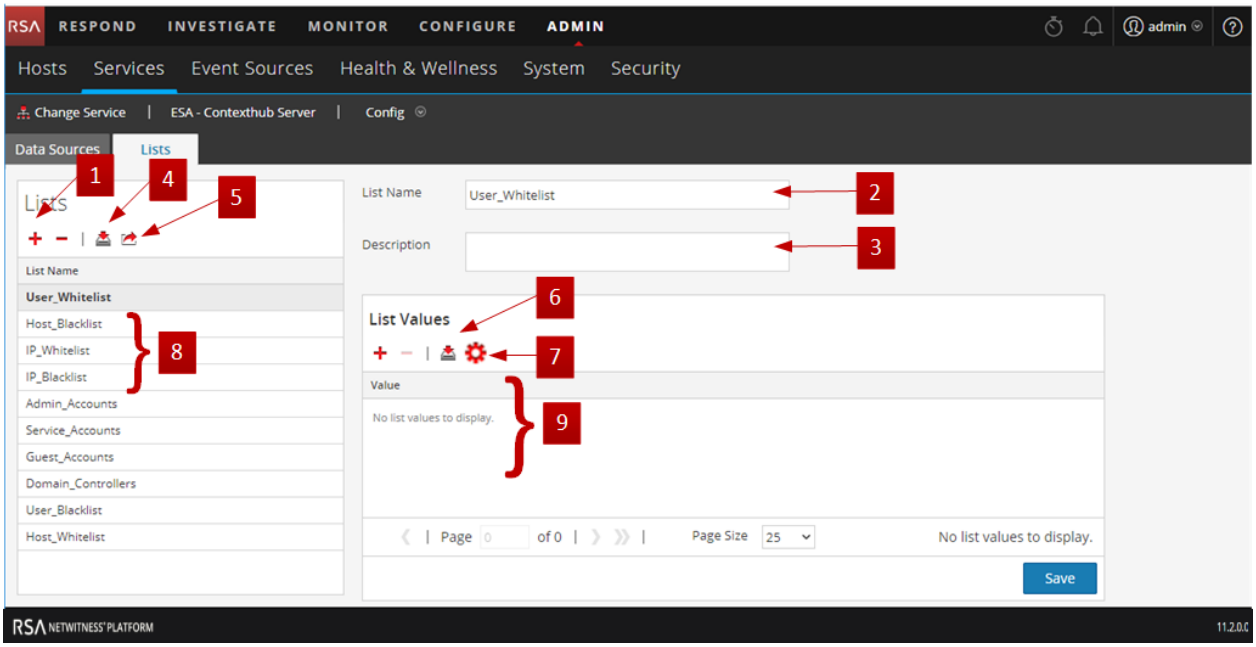
Par défaut, 10 listes vides à colonne unique sont disponibles dans RSA NetWitness Platform11.1. Ces listes sont vides et vous devez y ajouter des informations. Les 10 noms de liste préconfigurés sont utilisés dans les règles ESA ; pour plus d'informations sur les règles ESA, consultez *Lancer des alertes avec le Guide d'utilisation des règles de corrélation de l'ESA*. Les utilisateurs qui rétrogradent vers des versions antérieures verront ces nouvelles listes en plus des listes créées précédemment. Les listes disponibles par défaut sont les suivantes :

- Admin_Accounts
- Guest_Accounts
- Service_Accounts
- User_Blacklist
- User_Whitelist
- Host_Whitelist

- Domain_Controllers
- IP_Blacklist
- IP_Whitelist
- Host_Blacklist

Remarque : Si une liste avec le même nom existe déjà avant la mise à jour ou l'installation de RSA NetWitness Platform 11.2, cette liste sera conservée. Renommez cette liste avant d'effectuer la mise à jour vers la version 11.1, ou mettez à jour le contenu de sorte qu'il puisse être utilisé dans les règles de l'ESA.

Les listes sont disponibles dans l'onglet Règles de l'ESA dans CONFIGURER > Règles ESA > Paramètres > Sources d'enrichissement. Pour plus d'informations sur les règles de l'ESA, consulteztez *Lancer des alertes à l'aide du guide de l'ESA pour la version 11.1*.
Le panneau **Valeurs de la liste** comporte une barre d'outils avec des options permettant d'ajouter, de supprimer et d'importer des valeurs de liste dans la liste sélectionnée. Les entrées situées sous **Valeur** identifient chaque entrée de la liste.



1	Pour ajouter une nouvelle liste, cliquez sur +.
2	Nom identifiant la liste.
3	Description de la liste.
4	Cliquez sur pour importer des listes dans Context Hub.
5	Cliquez sur pour exporter une liste vers la machine locale.
6	Cliquez sur pour importer des valeurs de liste dans la liste sélectionnée.

7 Cliquez sur pour ajouter ou modifier l'adressage d'entité.

8 Affiche les listes personnalisées qui sont ajoutées à Context Hub.

9 Affiche les valeurs de liste qui sont ajoutées à la liste sélectionnée.

Barre d'outils

Le tableau suivant décrit les actions de la barre d'outils.

Fonctionnalité	Description
	Ajoutez une nouvelle liste. Pour plus d'informations, reportez-vous à Configurer des listes en tant que sources de données.
	Supprimez une liste. Si vous supprimez une liste de Context Hub, elle n'est plus considérée comme une source de données permettant de récupérer des informations contextuelles.
	Importez des listes dans Context Hub. Pour plus d'informations, reportez-vous à Importer ou exporter des listes pour Context Hub.
	Exportez une liste vers la machine locale. Pour plus d'informations, reportez-vous à Importer ou exporter des listes pour Context Hub.

Options de la vue Liste

Le tableau ci-dessous décrit les configurations des listes.

Fonctionnalité	Description
Nom de la liste	Nom unique permettant d'identifier la liste.
Description	Description de la liste.
Enregistrer	Enregistrer les modifications apportées à la liste.

Étapes suivantes

Une fois la configuration effectuée, vous pouvez afficher les données contextuelles dans le panneau Récapitulatif du contexte de la vue Répondre ou Enquêter. Pour savoir comment procéder, consultez les rubriques **Accéder au panneau Récapitulatif du contexte et Afficher un contexte supplémentaire** du *Guide d'utilisation Investigation et Malware Analysis*.

Résolution des problèmes

Cette rubrique fournit des informations sur les problèmes que les utilisateurs de NetWitness Platform peuvent rencontrer lors de la configuration du service Context Hub.

Problèmes possibles

Problème	Solution
La lecture préalable échoue si la liste est créée en mode ajout. Le message d'erreur suivant s'affiche dans les journaux indiquant que, les entrées dans la liste dépassent le maximum autorisé. `Error setting data source entries com.rsa.asoc.contexthub.exception.ContextHubException: total.entries.exceed.max` En outre, l'intégrité définit les statistiques suivantes : `Contexthub.Datasource.Health.Data-Sources-Health` à `Unhealthy` et affiche les noms des listes pour lesquelles la lecture préalable a échoué. Par exemple, le nombre d'entrées dans la liste est 50001 et le nombre d'enregistrements dans le fichier CSV est 50001, car l'utilisateur n'a pas modifié le CSV depuis la dernière lecture préalable. La limite supérieure du nombre d'entrées dans la liste est 100 000. Maintenant, lors de la lecture préalable, Context Hub essaie d'ajouter 50001 entrées à la liste, mais puisque 50001 + 50001 > 100 000, la lecture préalable échoue.	Dans le fichier CSV, ajoutez uniquement les entrées que vous souhaitez ajouter au fichier. csv existant. Si vous ne souhaitez pas ajouter d'entrées à la liste, appliquez l'une des options suivantes, selon le cas : • Si vous avez créé la liste avec des en-têtes, supprimez toutes les lignes du fichier CSV à l'exception de l'en-tête. • Si vous avez créé la liste sans en-têtes, vous devez avoir 0 ligne dans le fichier CSV.
L'établissement de la liaison SSL avec un certificat d'Archer échoue lors de son ajout comme source de données.	Utilisez un certificat généré par Archer avec l'option Approuver tous les certificats configurée.
L'option Pivoter vers Investigate de la vue Répondre ne permet pas d'accéder à l'emplacement correct.	Redémarrez le service jetty sur le serveur Netwitness, connectez-vous à l'hôte de serveur Netwitness et exécutez la commande `service jetty restart`.

Problème	Solution
Lorsque vous importez une liste dans laquelle il manque des guillemets, comme « 172.16.0.0, la liste est enregistrée sans données à afficher. Cela est dû au bug Apache (CSV-141) qui n'analyse pas les fichiers csv au format incorrect.	Importez une liste avec des guillemets corrects pour éviter d'afficher un fichier vide. Par exemple, « 172.16.0.0 », « host.mycompany.com », etc.
L’augmentation de la limite pour les alertes et les incidents entraîne une erreur de recherche. Par défaut, le nombre d’alertes et d’incidents est limité à 50.	Si la limite est augmentée, la plus grande quantité de métadonnées cherchées pour les alertes et les incidents peut conduire à une erreur de recherche due à une restriction de la base de données interne. Pour résoudre cela, il faut revenir aux paramètres par défaut qui limitent le nombre d’alertes et d’incidents affichés à 50.