RSA NETWITNESS® SUITE

Guide de configuration de Context Hub

pour la version 11.0

Informations de contact

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

Marques commerciales

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

Contrat de licence

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

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

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

Licences tierces

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

Remarque sur les technologies de chiffrement

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

Distribution

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

février 2018

Sommaire

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 Suite et fournissent des données enrichies lorsqu'elles sont configurées.

Listes - 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.

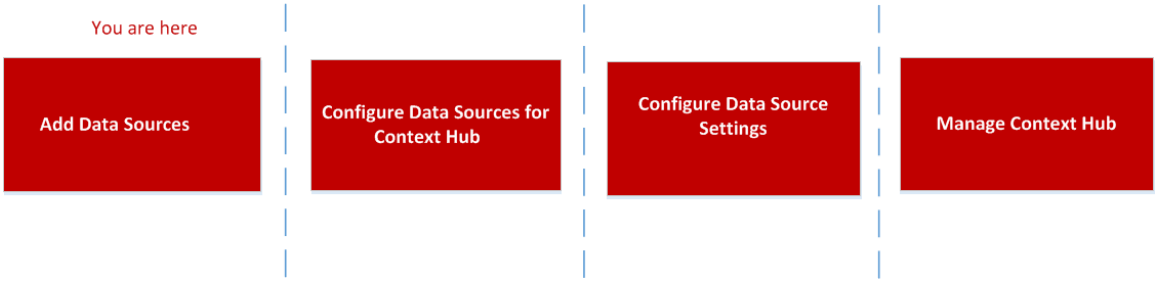
Respond - fournit les informations contextuelles d'une métadonnée spécifique disponible dans Respond et permet à l'analyste de réagir plus vite en fonction des données contextuelles.

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 Suite.

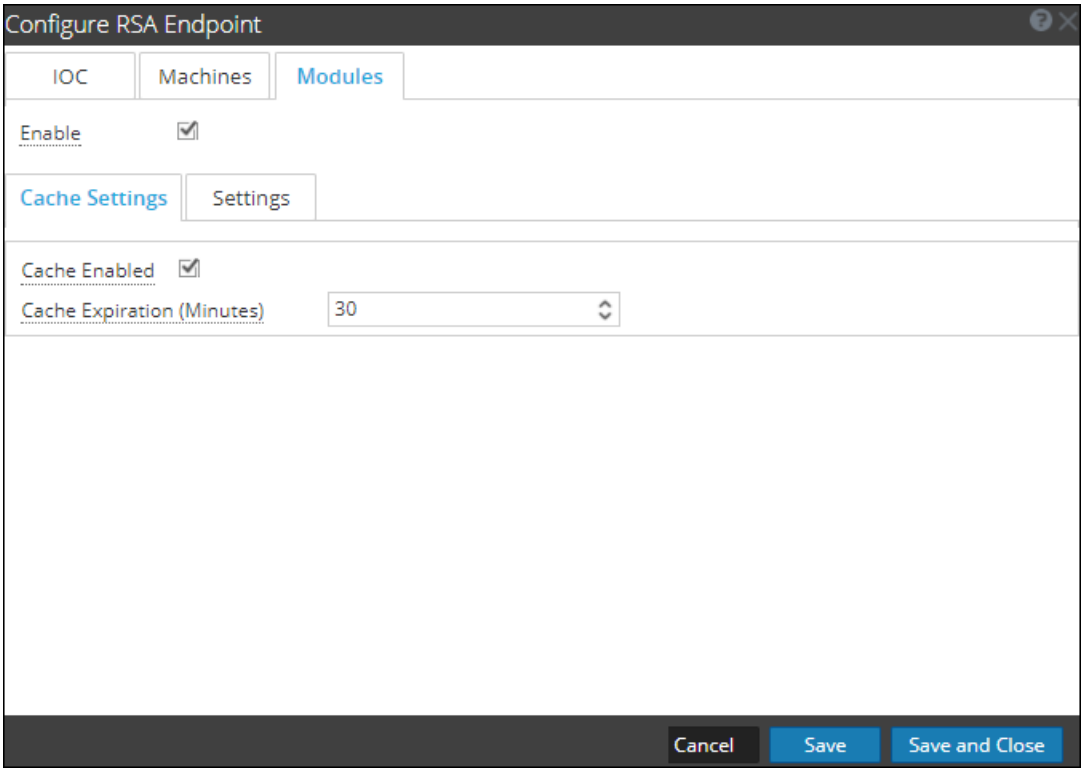
Remarque : Seule une instance de service Context Hub peut être activée dans votre déploiement NetWitness Suite. En cas d'existence de plusieurs services ESA dans NetWitness Suite, vous devez choisir l'hôte ESA approprié au service Context Hub. Un minimum de 8 Go d'espace est requis pour configurer Context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

Configurer 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 ajouté lors de l'ajout de la source de données de 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.

Champ	Description
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)

Source de données (Connexion)	Groupes de réponses pris en charge	Paramètres de champ
Active Directory	Utilisateurs	Mappage de méta 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]
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

Source de données (Connexion)	Groupes de réponses pris en charge	Paramètres de champ
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 Suite.

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

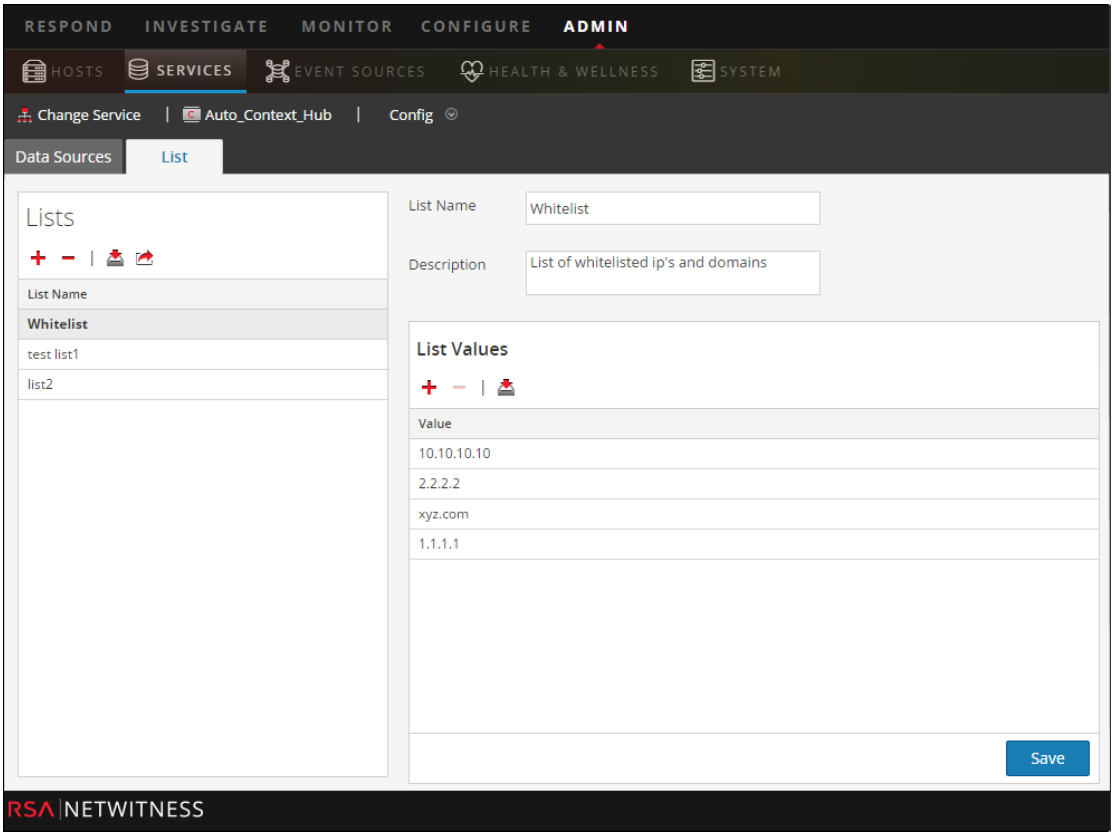
Remarque : Vous devez effectuer les mêmes modifications dans le fichier CSV approprié afin qu'elles soient répercutées à la prochaine récurrence du planning. Sinon, lorsque vous importez des valeurs dans une liste existante à une seule colonne ou plusieurs colonnes, les données sont remplacées à partir du fichier source à la prochaine récurrence du planning.

Importer une liste à une seule colonne

Pour importer une liste :

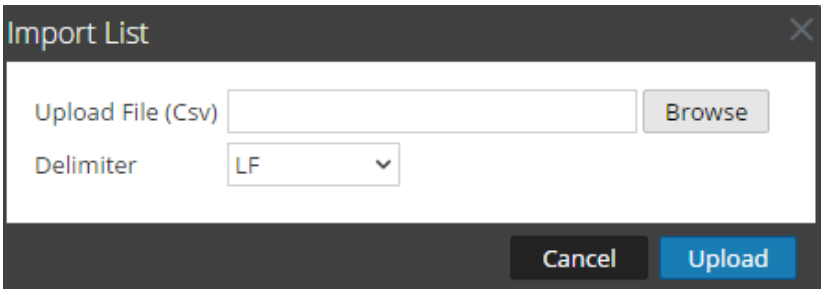
1. Sélectionnez ADMIN > **Services**.
   La vue Services s'affiche.
2. Dans le **panneau Services**, sélectionnez le service  Context Hub, puis cliquez sur > **View** > **Config**.
   La vue Configuration des services du service Context Hub s'affiche.
3. Cliquez sur l'onglet **Listes**.
   L'onglet Listes comprend le panneau **Listes** et le panneau **Valeurs de la liste**.

L'image ci-dessous illustre un exemple de liste à une seule colonne.



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 effectuant une importation. Pour plus d'informations sur la façon d'importer une liste à plusieurs colonnes, reportez-vous à la rubrique Configurer des sources de données de listes pour Context Hub.

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 Suite.

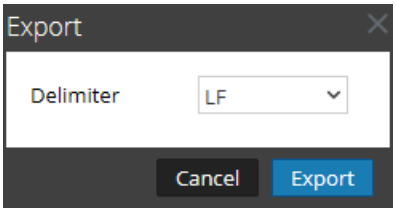
Les valeurs de liste sont importées dans la liste sélectionnée. Ces listes sont considérées comme des sources de données permettant de récupérer des informations contextuelles. Mais vous pouvez ajouter une liste existante à plusieurs colonnes. Les données ne sont ajoutées que si le nombre de colonnes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

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 Suite 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 :

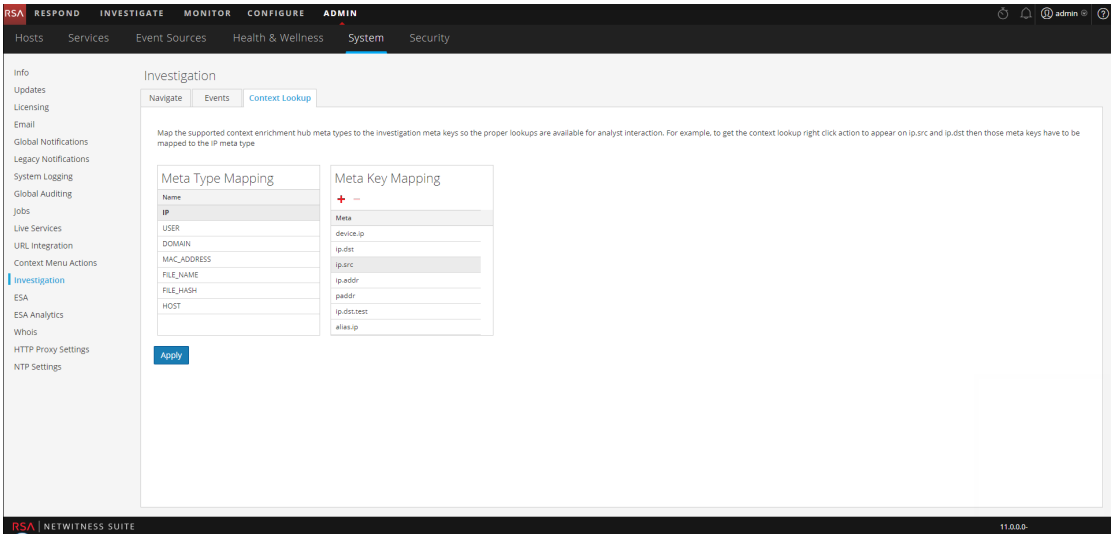
Nom de type de métadonnées	Clés méta
IP	device.ip, ip.src, ip.dst, ip.addr,ipv6.src, alias.ip, ipv6.addr, device.ipv6,forward.ip, forward.ipv6,ipv6.dst, ipv6.addr, stransaddr, transaddr
USER	user.src, user.dst, username, event user
DOMAIN	domain.src, domain.dst,fqdn, web.domain, domain, sdomain, ddomain
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

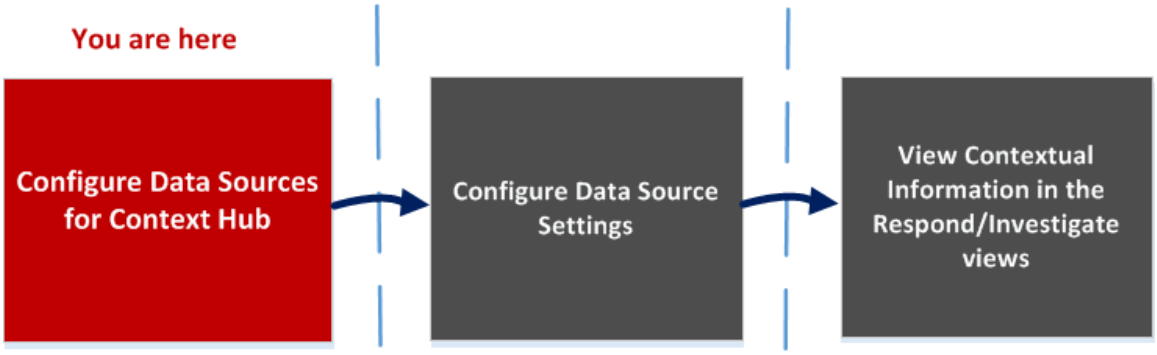
Une fois que vous avez configuré le service Context Hub et la source de données requise, vous pouvez gérer les paramètres de chaque source de données. Cela vous aidera à optimiser et personnaliser les résultats de recherche.

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 sources 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*.

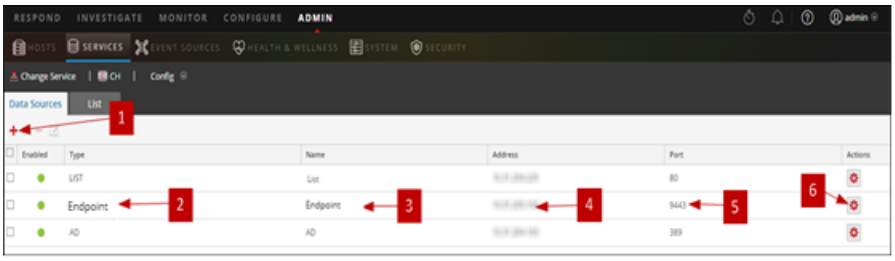
*Vous pouvez effectuer cette tâche (qui se trouve sous l'onglet Sources de données Context Hub.)

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 la source de données NetWitness Endpoint
- Configurer la source de données Répondre
- Configurer la source de données Live Connect

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 sources de données pour Context Hub.

Fonctionnalité	Description
	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 des sources 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 des sources de données.

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.

Fonctionnalité	Description
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**.

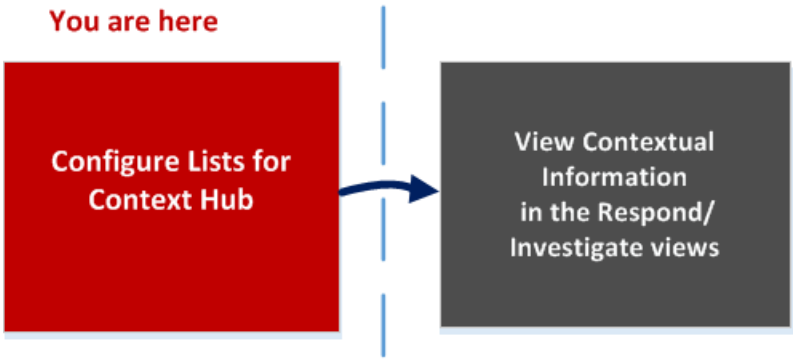
À l'aide de l'onglet Listes du service Context Hub, vous pouvez créer une ou plusieurs listes, et y ajouter les valeurs de liste appropriées. Ces listes sont automatiquement considérées comme des sources de données pour le service Context Hub.

Vous pouvez remplir ces listes à l'aide d'éléments, soit par l'importation de fichiers CSV, 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 pour Context Hub
Administrateur/analyste	Afficher les informations contextuelles dans la vue Répondre	Consultez le *Guide d'utilisation de NetWitness Respond.*
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).

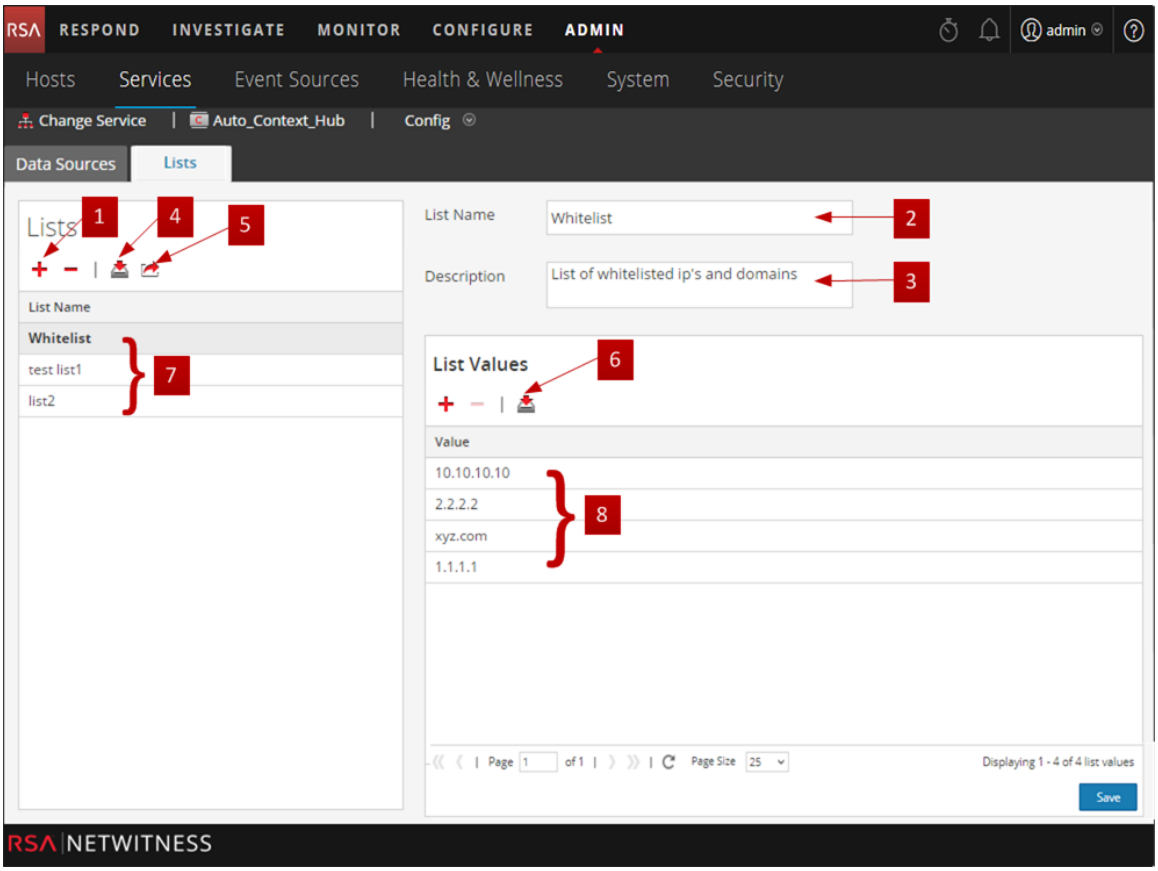
Rubriques connexes

- Onglet Sources de données de Context Hub

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

8 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.

Fonctionnalité	Description
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*.

Dépannage

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

Problèmes possibles

Problème	Solutions
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 la fonction Enquêter de la page Répondre ne permet pas d'accéder au lien correct.	Lorsque vous arrêtez et redémarrez le serveur RabbitMQ, l'option Pivoter vers la fonction Enquêter disponible dans l'écran de réponse n'est pas visible. Et le panneau contextuel de Pivoter vers la fonction Enquêter rouvre la même page. Vous devez redémarrer le service jetty sur le serveur Netwitness, vous connecter à l'hôte de serveur Netwitness et exécuter la commande de redémarrage du service jetty.