RSA NETWITNESS® SUITE

Sécurité du système et gestion des utilisateurs

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

Sécurité du système et gestion des utilisateurs

Ce guide fournit des informations sur la configuration de la sécurité et le contrôle des accès utilisateur. L'administrateur système doit maîtriser les paramètres du système, les comptes d'utilisateur, les rôles système, les autorisations et l'accès aux services.

Rubriques

Configurer la sécurité du système

Cette rubrique présente les procédures de bout en bout permettant d'implémenter la sécurité du système. Chaque étape des rubriques suivantes explique un paramètre applicable à l'ensemble du système. Suivez les étapes dans l'ordre pour configurer la sécurité dans NetWitness Suite.

Rubriques

Étape 1. Configurer la complexité des mots de passe

Cette rubrique fournit des instructions pour définir les exigences en matière de complexité des mots de passe NetWitness Suite au niveau du système.

Les mots de passe sont une composante importante de votre stratégie de sécurité réseau. Ils fournissent une protection essentielle de première ligne pour vos systèmes informatiques et aident à prévenir les attaques et l'accès non autorisé aux données confidentielles.

Les stratégies de mots de passe qui visent à améliorer la sécurité des réseaux d'entreprise, varient en fonction des besoins et de la réglementation de l'industrie, ou des entreprises. En raison de ces variations de stratégies de mots de passe, le logiciel NetWitness Suite vous permet de configurer les exigences de complexité des mots de passe pour les utilisateurs NetWitness Suite internes afin de se conformer aux lignes directrices de vos stratégies de mots de passe d'entreprise.

Les exigences en matière de complexité des mots de passe s'appliquent uniquement aux utilisateurs internes et ne sont pas obligatoires pour les utilisateurs externes. Les utilisateurs externes comptent sur leurs propres méthodes et systèmes pour faire respecter les exigences de complexité des mots de passe.

Vous pouvez également spécifier la période d'expiration du mot de passe de l'utilisateur par défaut globale et définir si et quand les utilisateurs internes reçoivent une notification indiquant que leur mot de passe va expirer. La notification d'expiration de mot de passe consiste en un message d'expiration de mot de passe lors de la connexion à NetWitness Suite.

Degré de sécurité du mot de passe

Les mots de passe forts compliquent la tâche des pirates qui cherchent à deviner les mots de passe des utilisateurs et contribuent à empêcher l'accès non autorisé au réseau de votre organisation. Vous pouvez définir le niveau de sécurité approprié des mots de passe pour vos utilisateurs NetWitness Suite. Lorsque vous configurez les paramètres de degré de sécurité du mot de passe, ils s'appliquent aux utilisateurs NetWitness Suite internes, y compris à l'utilisateur administrateur.

Vous pouvez choisir d'appliquer une combinaison des exigences de niveau de sécurité du mot de passe suivantes lorsqu'un utilisateur NetWitness Suite crée ou modifie son mot de passe :

- Longueur minimale du mot de passe
- Nombre minimal de caractères majuscules
- Nombre minimal de caractères minuscules
- Nombre minimal de caractères décimaux (0 à 9)
- Nombre minimal de caractères spéciaux

- Nombre minimal de caractères alphabétiques non latins (y compris les caractères Unicode des langues asiatiques)
- Si le mot de passe contient ou non le nom d'utilisateur

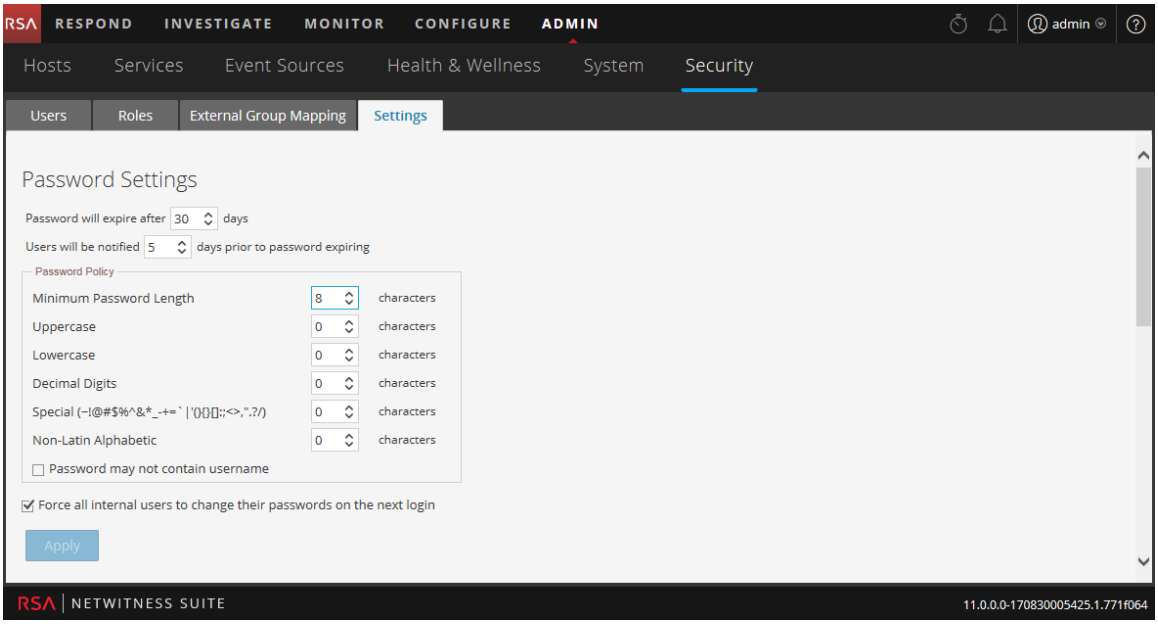
Par exemple, vous pouvez créer des exigences de niveau de sécurité du mot de passe qui comporte un minimum de 8 caractères, qui ne peut pas contenir le nom d'utilisateur de l'utilisateur et qui contient un mélange de lettres majuscules et minuscules, de chiffres et de caractères spéciaux.

Si vous choisissez d'appliquer un nombre minimal de caractères alphabétiques non latins, vérifiez que vos utilisateurs disposent de ces caractères avant de définir leurs mots de passe.

La rubrique « Mots de passe STIG » du *Guide de maintenance du système* fournit un exemple de stratégie de niveau de sécurité du mot de passe.

Configurer le degré de sécurité du mot de passe

1. Dans NetWitness Suite, accédez à **ADMIN > Sécurité**.
   La vue Sécurité s'affiche avec l'onglet **Utilisateurs** ouvert.
2. Cliquez sur l'onglet **Paramètres**.



3. Dans la section **Paramètres de mot de passe**, sélectionnez les exigences de complexité de mot de passe à appliquer lorsque les utilisateurs NetWitness Suite définissent leurs mots de passe et spécifiez le nombre minimal de caractères requis, le cas échéant. Définissez la valeur sur 0 pour répondre aux exigences que vous ne souhaitez pas mettre en œuvre, à l'exception de la longueur minimale du mot de passe, qui a une valeur minimale de

4 caractères.

Exigences	Description
Le mot de passe expirera après <n> jours	Nombre de jours par défaut avant lequel un mot de passe expire pour tous les utilisateurs NetWitness Suite internes. La valeur zéro (0) désactive l'expiration du mot de passe. Pour les nouvelles installations, la valeur par défaut est de 30. Concernant les mises à niveau, la valeur précédente migre automatiquement lors de l'installation de mises à niveau.
Les utilisateurs seront notifiés <n> jours avant l'expiration du mot de passe	Nombre de jours avant la date d'expiration du mot de passe, pour avertir un utilisateur que son mot de passe est sur le point d'expiration. Les utilisateurs voient une boîte de dialogue Message d'expiration de mot de passe lorsqu'ils se connectent à NetWitness Suite. La valeur minimale est de 1 jour.
Longueur minimale du mot de passe	Spécifie une longueur minimale de mot de passe. La longueur minimale du mot de passe empêche les utilisateurs d'utiliser des mots de passe courts qui sont faciles à deviner. La valeur par défaut requise pour la longueur minimale d'un mot de passe est de 4 caractères.
Caractères en majuscules	Indique le nombre minimum de caractères en majuscules contenus dans le mot de passe. Ceci inclut les caractères des langues européennes de A à Z, comprenant des signes diacritiques, des caractères grecs et des caractères cyrilliques. Par exemple : • Lettre majuscule cyrillique : Д Ц • Lettre majuscule grecque : Π Λ
Caractères en minuscules	Indique le nombre minimum de caractères en minuscules contenus dans le mot de passe. Ceci inclut les caractères des langues européennes de a à z, comprenant les eszetts, des signes diacritiques, des caractères grecs et des caractères cyrilliques. Par exemple : • Lettre minuscule cyrillique : д ц • Lettre minuscule grecque : π λ

Exigences	Description
Chiffres décimaux	Indique le nombre minimum de caractères décimaux (compris entre 0 et 9) contenus dans le mot de passe.
Caractères spéciaux (~!@#$%^&*_-+=`|'(){}[]:;<>,".?/)	Indique le nombre minimum de caractères spéciaux contenus dans le mot de passe : `~!@#$%^&*_-+=`|'(){}[]:;<>,".?/`
Caractères alphabétiques non latins	Indique le nombre minimum de caractères alphabétiques Unicode autres que les lettres majuscules et minuscules. Cela inclut les caractères Unicode des langues asiatiques. Par exemple : • Kanji (japonais) : 頁 (feuille) 桜 (arbre)
Le mot de passe ne peut pas contenir le nom d'utilisateur	Indique qu'un mot de passe ne peut pas contenir le nom d'utilisateur non sensible à la casse.

4. Si vous souhaitez que les modifications de stratégie de mot de passe prennent effet dès la prochaine connexion, et non dès la prochaine modification de mot de passe, sélectionnez **Forcer tous les utilisateurs internes à modifier leur mot de passe à la prochaine connexion**. Notez que ce paramètre est activé par défaut.
5. Cliquez sur **Appliquer**.
   Les paramètres de niveau de sécurité du mot de passe prennent effet lorsque les utilisateurs internes créent ou modifient leurs mots de passe. Si vous avez sélectionné **Forcer tous les utilisateurs internes à modifier leur mot de passe à la prochaine connexion**, tous les utilisateurs internes doivent modifier leur mot de passe la prochaine fois qu'ils se connectent à NetWitness Suite.

Étape 2. Modifier les mots de passe d'administrateur par défaut

Cette rubrique fournit des instructions permettant de modifier le mot de passe d'administrateur du service NetWitness Suite et des services Core.

Le compte utilisateur de l'administrateur système est installé avec NetWitness Suite. Le nom d'utilisateur est **admin** et le mot de passe par défaut est le mot de passe qui a été saisi dans l'environnement en mode texte (TUI) au cours du processus d'installation de NetWitness Suite. Le rôle **Administrateurs** est affecté à l'utilisateur admin. Ce rôle détient les privilèges système complets permettant de contrôler les actions de l'utilisateur et les services auxquels il peut accéder. La seule modification possible sur ce compte est le changement du mot de passe. Contrairement aux autres utilisateurs NetWitness Suite, les modifications du mot de passe de l'utilisateur **admin** ne se propagent pas automatiquement aux services en aval. Lorsque vous configurez les paramètres de degré de sécurité du mot de passe, ils s'appliquent à tous les utilisateurs NetWitness Suite, y compris à l'utilisateur admin.

Le mot de passe, aspect important de la sécurité informatique, constitue la première ligne de protection de votre système. L'utilisateur **admin** est pré-installé dans NetWitness Suite et sur chaque service Core. Pour la sécurité, créez les utilisateurs et les rôles de votre organisation dans NetWitness Suite, et sur chaque service Core.

Bonnes pratiques

RSA recommande de suivre les bonnes pratiques suivantes :

- Par défaut, modifiez le mot de passe **admin** de chaque service.
- Créez un mot de passe différent pour le compte **admin** sur chaque service.

Modifiez le mot de passe admin pour NetWitness Suite

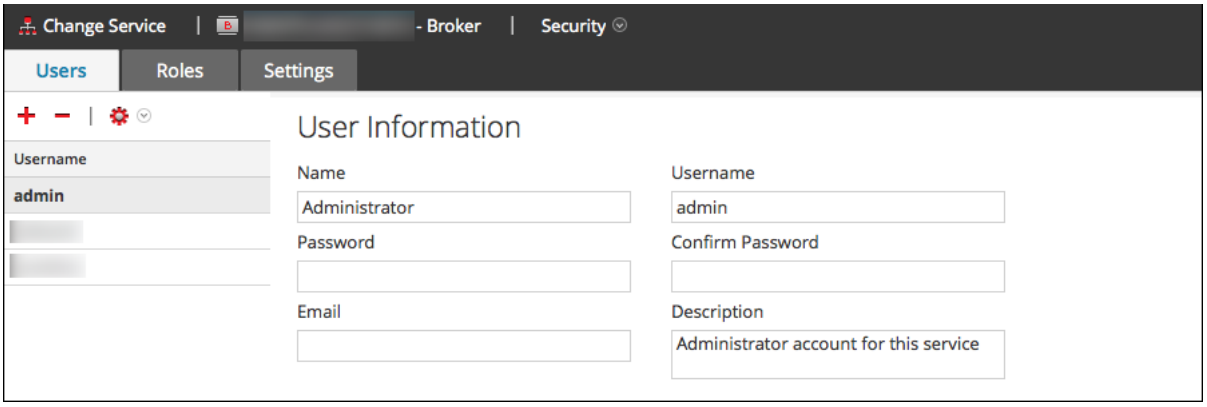
Modifiez le mot de passe **admin** pour NetWitness Suite dans la vue Profil. Reportez-vous à la section « Changement de mot de passe » dans le *Guide de mise en route NetWitness Suite*. Le mot de passe de l'utilisateur **admin** ne se propage pas dans les services Core.

Remarque : Après avoir modifié le mot de passe d'administrateur, vous devez supprimer et ajouter à nouveau une source de données dans Reporting Engine. Pour plus d'informations, reportez-vous à la section **Supprimer et ajouter une nouvelle source de données dans Reporting Engine** ci-dessous.

Modifier le mot de passe admin pour les services Core

Pour modifier le mot de passe admin pour un service Core :

1. Dans NetWitness Suite, accédez à **ADMIN > Services**.
2. Sélectionnez un service, puis > **Vue** > **Sécurité**.
3. Sous l'onglet **Utilisateurs**, sélectionnez l'utilisateur **admin**.



4. Dans le champ **Mot de passe**, saisissez un nouveau mot de passe pour le service sélectionné.
5. Dans le champ **Confirmer le mot de passe**, saisissez une seconde fois le nouveau mot de passe.
6. Cliquez sur **Appliquer**.

Remarque : Après avoir modifié le mot de passe d'administrateur, vous devez supprimer et ajouter à nouveau une source de données dans Reporting Engine. Pour plus d'informations, reportez-vous à la section **Supprimer et ajouter une nouvelle source de données dans Reporting Engine** ci-dessous.

Supprimer et ajouter une nouvelle source de données dans Reporting Engine

Reporting Engine valide une source de données à l'aide du nom d'utilisateur et du mot de passe de la source de données. Si vous changez le nom d'utilisateur ou le mot de passe d'une source de données, vous devez supprimer et ajouter une nouvelle source de données.

Pour supprimer et ajouter une nouvelle source de données dans Reporting Engine :

1. Dans NetWitness Suite, accédez à **ADMIN > Services**.
2. Dans la vue Services, sélectionnez Reporting Engine et **Vue > Config**.
3. Cliquez sur l'onglet **Sources**.
4. Sélectionnez un service à supprimer, puis cliquez sur

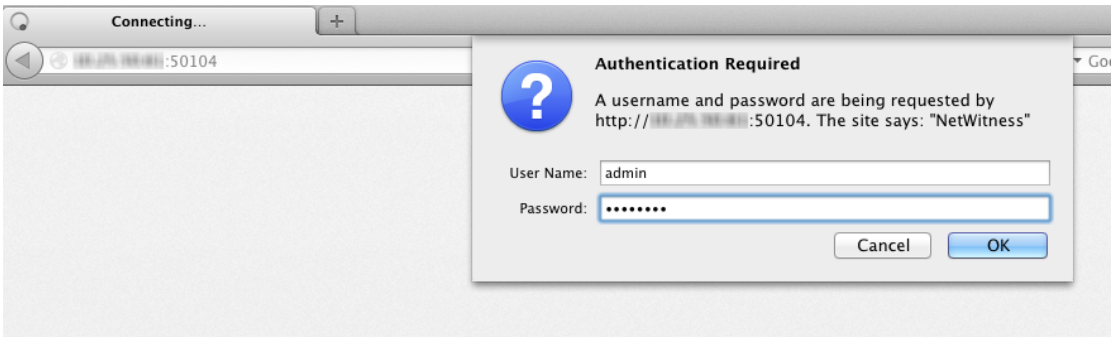
5. Cliquez sur + et sélectionnez **Services disponibles**.
6. Sélectionnez le service que vous avez supprimé à l'étape 4, puis cliquez sur **OK**.
7. Lorsque vous y êtes invité(e), saisissez les nouveaux nom d'utilisateur et mot de passe pour le service.

Modifier le mot de passe admin pour un service à l'aide de l'API REST

Dans certains cas, il peut être nécessaire de modifier le mot de passe admin pour un service Core en dehors de l'interface utilisateur NetWitness Suite. Il s'agit d'une autre façon d'effectuer la modification du mot de passe des services Core, mais ce n'est pas la méthode à privilégier.

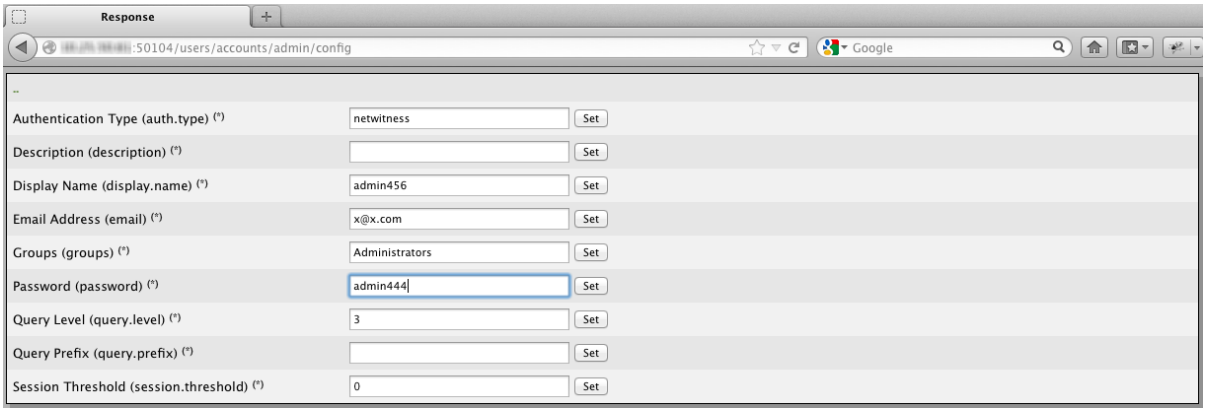
Pour modifier le mot de passe admin pour le service à l'aide de l'interface utilisateur REST :

1. Ouvrez un navigateur web et accédez à l'URL suivante :
   <hostname>:<port>
   où **hostname** est le nom d'un service Core NetWitness Suite et **port** est le port utilisé pour les communications REST. Voici un exemple pour un Decoder :
   `http://10.20.30.40:50104`
   La boîte de dialogue d'authentification s'affiche.



2. Dans la boîte de dialogue, saisissez le nom d'utilisateur et le mot de passe utilisés pour l'authentification en tant qu'administrateur sur le service, puis cliquez sur **OK**. Le nom d'utilisateur par défaut est **admin** et le mot de passe par défaut est **netwitness**.
   La fenêtre REST du service s'affiche.
3. Parcourez la structure des nœuds à l'emplacement **users/accounts/admin/config**.
   Les champs de configuration utilisateur de l'administrateur s'affichent dans la fenêtre du

navigateur.



4. Dans le champ Mot de passe, saisissez un nouveau mot de passe, puis cliquez sur **Définir**.

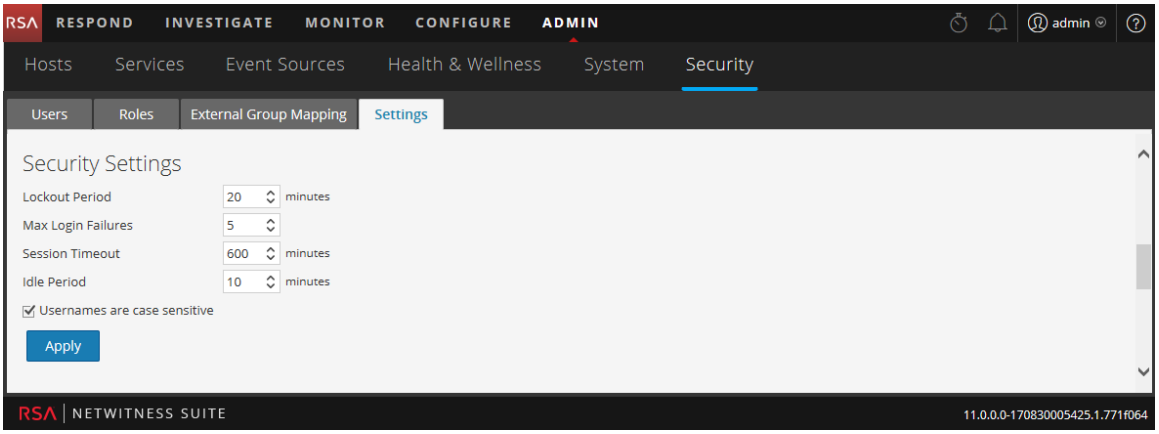
Étape 3. Configurer les paramètres de sécurité au niveau du système

Cette rubrique explique comment définir les paramètres de sécurité au niveau du système.

Les paramètres de sécurité plus généraux, tels que le seuil maximal de tentatives de connexion échouées, s'appliquent à tous les utilisateurs NetWitness Suite et à toutes les sessions. Les paramètres liés aux mots de passe présents dans la section Degré de sécurité du mot de passe, tels que le délai d'expiration du mot de passe et le nombre de jours avant l'expiration des mots de passe utilisateur par défaut, s'appliquent aux utilisateurs internes NetWitness Suite, mais pas aux utilisateurs externes.

Configurer des paramètres de sécurité

1. Dans NetWitness Suite, accédez à **ADMIN > Sécurité**.
   La vue Sécurité s'affiche avec l'onglet **Utilisateurs** ouvert.
2. Cliquez sur l'onglet **Paramètres**.



3. Dans la section **Paramètres de sécurité**, renseignez les valeurs pour les champs comme indiqué dans le tableau suivant.

Champ	Description
Période de blocage	Nombre de minutes durant lesquelles un utilisateur de NetWitness Suite est bloqué si le nombre configuré de tentatives de connexion est dépassé. La valeur par défaut est 20 minutes.

Champ	Description
Nombre maximal d'échecs de la connexion	Nombre maximal d'échecs de la connexion avant le blocage d'un utilisateur. La valeur par défaut est 5.
Expiration de la session	Durée maximale d'une session utilisateur avant expiration, en minutes. La valeur par défaut est 600. La session arrive à expiration lorsque la durée configurée s'est écoulée, après quoi l'utilisateur doit se reconnecter. La valeur maximale autorisée est 30 000. **Remarque :** Si vous avez migré vers NetWitness Suite 11.0 depuis la version 10.6.x et si vous avez précédemment utilisé la valeur 0 pour une durée d'expiration de session illimité, cette valeur est automatiquement rétablie à 30 000 minutes, la valeur 0 n'étant plus pris en charge.
Période d'inactivité	Nombre de minutes d'inactivité avant l'expiration d'une session. La valeur par défaut est 10. La valeur maximale autorisée est 30 000. **Remarque :** Si vous avez migré vers NetWitness Suite 11.0 depuis la version 10.6.x et si vous avez précédemment utilisé une valeur de 0 pour une période d'inactivité illimitée, cette valeur est automatiquement rétablie à la valeur par défaut de 10, la valeur 0 n'étant plus prise en charge.
Les noms d'utilisateur sont sensibles à la casse.	Sélectionnez cette option si vous souhaitez que le champ Nom d'utilisateur soit sensible à la casse sur l'écran de connexion NetWitness Suite . Par exemple, si les noms d'utilisateur sont sensibles à la casse, vous pouvez utiliser admin pour vous connecter à NetWitness Suite, mais vous ne pouvez pas utiliser Administrateur.

4. Cliquez sur **Appliquer**. Les paramètres de sécurité prennent effet immédiatement. Si un mot de passe expire, l'utilisateur est invité à modifier le mot de passe lorsqu'il se connecte à NetWitness Suite.

Étape 4. (Facultatif) Configurer l'authentification externe

Cette rubrique présente les méthodes d'authentification externe prises en charge par NetWitness Suite.

Lorsqu'un utilisateur se connecte, NetWitness Suite exécute d'abord l'authentification locale. Si aucun utilisateur local n'est trouvé et que la configuration d'authentification externe est activée, une tentative d'authentification externe est effectuée.

L'authentification externe permet aux utilisateurs ne disposant pas d'un compte utilisateur NetWitness Suite interne de se connecter à NetWitness Suite et de recevoir des autorisations basées sur des rôles.

NetWitness Suite prend en charge deux méthodes d'authentification externe : Active Directory et les modules PAM (Pluggable Authentication Modules, modules d'authentification enfichables). Les rubriques de cette section décrivent la configuration et la procédure de test de chaque méthode.

Rubriques

- Configurer Active Directory
- Configurer la fonctionnalité de connexion PAM

Configurer Active Directory

Cette rubrique explique comment configurer NetWitness Suite pour utiliser Active Directory afin d'authentifier les connexions d'utilisateurs externes.

Lorsqu'un utilisateur se connecte, NetWitness Suite exécute d'abord l'authentification locale. Si aucun utilisateur local n'est trouvé et que la configuration Active Directory est activée, une tentative d'authentification est effectuée avec le service Active Directory. Vous pouvez configurer les paramètres d'Active Directory pour activer l'authentification des groupes externes dans la vue Administrateur > Sécurité > onglet Paramètres.

Dans un environnement avec plusieurs serveurs d'authentification, le transfert LDAP autorise les références LDAP à suivre les recherches de groupes AD. Le transfert LDAP peut augmenter le temps nécessaire à la connexion car les recherches de groupes AD sont étendues aux serveurs d'authentification connectés. Lorsque votre instance AD tente de contacter les contrôleurs de domaine qui sont bloqués par votre pare-feu, le délai pour que les utilisateurs se connectent à NetWitness Suite peut durer plusieurs minutes. NetWitness Suite dispose d'une option de configuration qui spécifie si le transfert LDAP se produit ; par défaut, les références LDAP sont désactivées. Lorsqu'elles sont désactivées, votre instance AD ne tente pas de contacter les contrôleurs de domaine référencés.

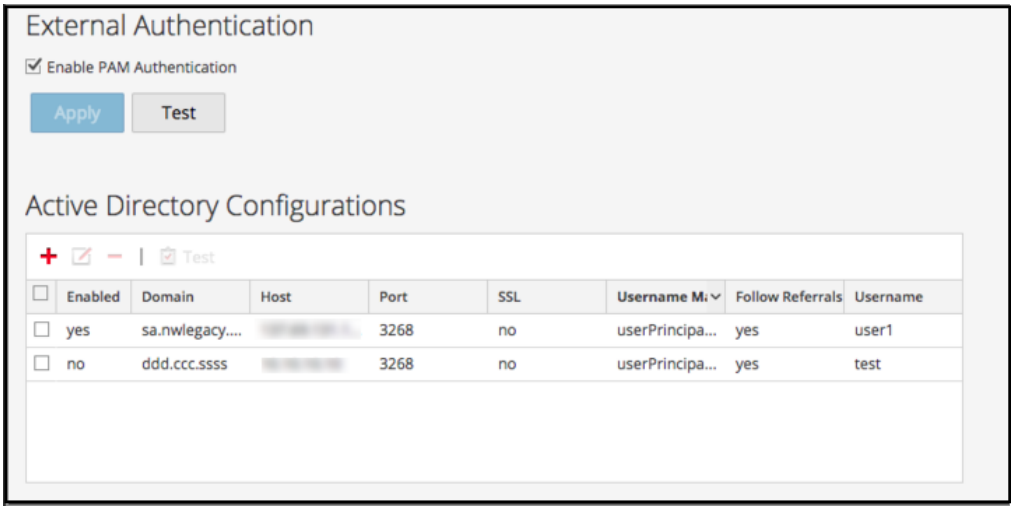
Remarque : L'onglet Paramètres fournit également la possibilité d'activer la configuration PAM, qui peut être utilisée en même temps que des configurations Active Directory. Pour plus d'informations sur l'activation et la configuration de l'authentification PAM, consultez Configurer la fonctionnalité de connexion PAM.

Procédures

Configurer l'authentification Active Directory

1. Accédez à **ADMIN > Sécurité**.
   La vue Sécurité s'affiche avec l'onglet **Utilisateurs** ouvert.
2. Cliquez sur l'onglet **Paramètres**.
   La liste des configurations Active Directory s'affiche dans le panneau afin que vous puissiez

ajouter ou modifier une configuration.



3. Ajoutez, modifiez ou supprimez des domaines comme il convient, comme décrit dans les sections suivantes.

   Les domaines ajoutés à cette liste sont renseignés automatiquement sous l'onglet Mappage de groupe externe afin que vous puissiez mapper les rôles de sécurité à chaque groupe.

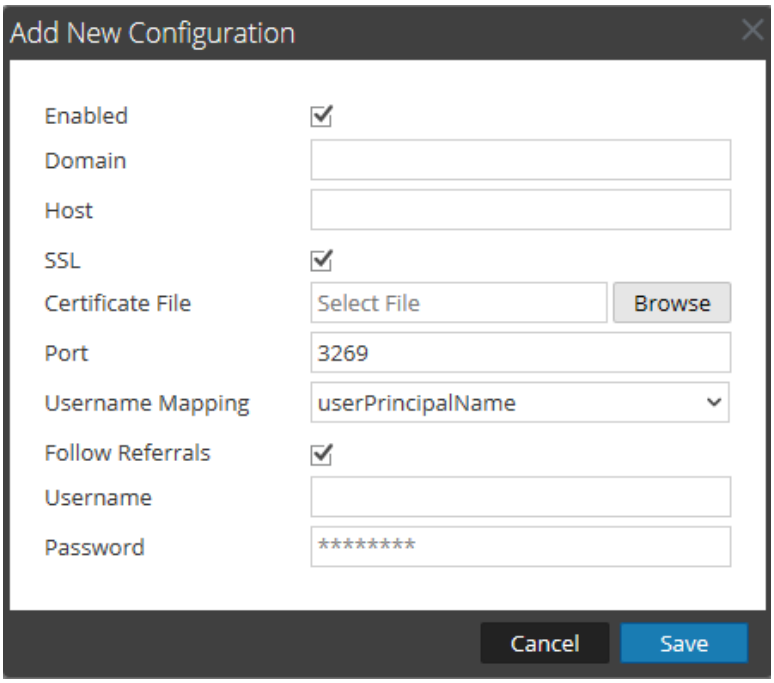
Remarque : Pour configurer les rôles de sécurité utilisés pour l'accès à Active Directory, reportez-vous à l'Étape 5. (Facultatif) Mapper des rôles d'utilisateur aux groupes externes.

Ajouter une nouvelle configuration Active Directory

Pour ajouter une nouvelle configuration Active Directory à la liste des configurations Active Directory :

1. Dans Configurations Active Directory, cliquez sur +.

   La boîte de dialogue Ajouter une nouvelle configuration s'affiche.



2. Cochez la case **Activé**.
3. Saisissez les informations relatives au **domaine**, à l'**hôte** et au **port** pour le service Active Directory.
4. (Facultatif) Pour sélectionner le protocole SSL pour cette configuration, cochez la case **Use SSL**. Vous devez saisir un fichier de certificat en cliquant sur **Parcourir** et en sélectionnant le fichier que vous souhaitez télécharger. Si le serveur Active Directory utilise un certificat signé par une autorité de certification publique, il est inutile de télécharger un certificat. Si le serveur Active Directory utilise un certificat auto-signé, vous devez télécharger soit le certificat d'autorité de certification, soit le certificat auto-signé
5. Dans le champ **Mappage du nom d'utilisateur**, sélectionnez le champ de recherche Active Directory pour utiliser le mappage du nom d'utilisateur. Vous pouvez sélectionner userPrincipalName (UPN) ou sAMAccountName.
6. Pour les sites dotés de plusieurs serveurs d'authentification, cliquez sur **Suivre les références** pour activer ou désactiver la référence LDAP qui suit les recherches de groupes AD.
7. Pour fournir des informations d'identification à lier au service Active Directory lors de la recherche du groupe Active Directory, saisissez les informations d'identification dans les champs **Nom d'utilisateur** et **Mot de passe**.

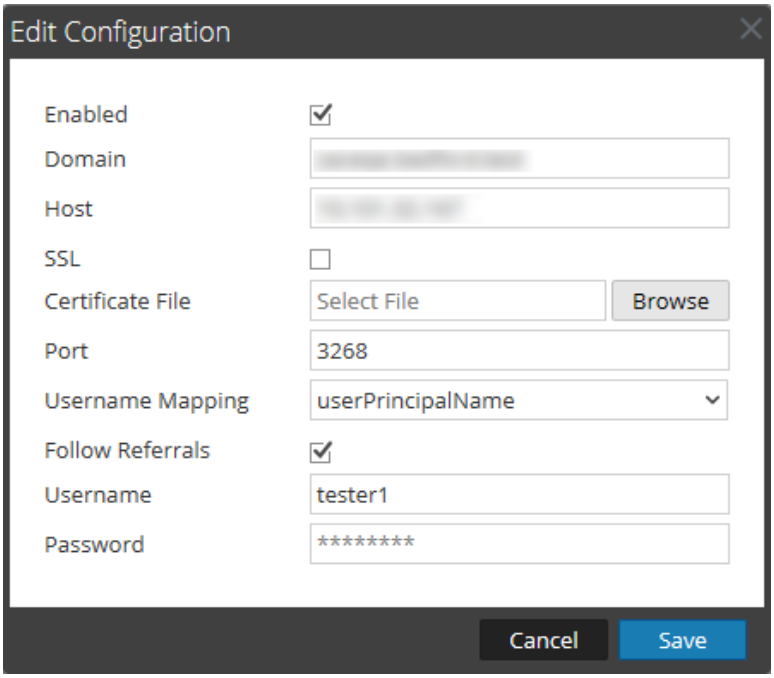
Remarque : Si vous avez sélectionné sAMAccountName dans le champ **Mappage du nom d'utilisateur**, vous devez saisir le nom d'utilisateur au format « domaine\utilisateur » pour vous authentifier.

8. Cliquez sur **Enregistrer**.
   La nouvelle configuration s'affiche dans la liste Configurations Active Directory.

Modifier une configuration Active Directory

Pour modifier une configuration Active Directory dans la liste des configurations Active Directory :

1. Sous **Configurations Active Directory**, sélectionnez la configuration que vous souhaitez modifier, puis cliquez sur .
   La boîte de dialogue Modifier la configuration s'affiche.



2. (Facultatif) Saisissez les informations relatives au **domaine**, à l'**hôte** et au **port** pour le service Active Directory.
3. (Facultatif) Pour sélectionner le protocole SSL pour cette configuration, cochez la case **Use SSL**. Vous devez saisir un fichier de certificat en cliquant sur **Parcourir** et en sélectionnant le fichier de votre choix.
4. (Facultatif) Dans le champ **Mappage du nom d'utilisateur**, sélectionnez le champ de recherche Active Directory pour utiliser le mappage du nom d'utilisateur.

5. Pour spécifier le comportement de l'option Suivre les références LDAP dans les environnements dotés de plusieurs serveurs d'authentification, activez la case à cocher **Suivre les références**.
   a. Si vous souhaitez désactiver le transfert LDAP, décochez la case correspondante.
   b. Si vous souhaitez activer le transfert LDAP, cochez la case.
6. Pour fournir des informations d'identification à lier au service Active Directory lors de la recherche du groupe Active Directory, saisissez les informations d'identification dans les champs **Nom d'utilisateur** et **Mot de passe**.
7. Cliquez sur **Enregistrer**.
   La configuration s'affiche dans la liste Configurations Active Directory.

Tester une configuration Active Directory

Pour tester une configuration Active Directory :

1. Sélectionnez la configuration à tester dans la liste Configurations Active Directory.
2. Dans la barre d'outils, cliquez sur Test.
   Un message s'affiche pour indiquer que le test est concluant.
3. Si le test n'aboutit pas, passez en revue et modifiez la configuration.

Supprimer une configuration Active Directory

Pour supprimer une configuration Active Directory :

1. Sous Configurations Active Directory, sélectionnez la configuration à supprimer dans la liste Configurations Active Directory.
2. Dans la barre d'outils, cliquez sur −.
   Un message s'affiche vous avertissant que tous les utilisateurs de la configuration d'Active Directory sélectionnée ne pourront pas se connecter à NetWitness Suite si celle-ci est supprimée.
3. Exécutez l'une des opérations suivantes :
   a. Pour confirmer la suppression, cliquez sur **Oui**.
   b. Pour annuler la suppression, cliquez sur **Non**.

Configurer la fonctionnalité de connexion PAM

Cette rubrique explique comment configurer NetWitness Suite pour utiliser les modules PAM (Pluggable Authentication Modules) afin d'authentifier les connexions d'utilisateurs externes.

La fonctionnalité de connexion PAM comporte deux composants distincts :

- PAM pour l'authentification de l'utilisateur
- NSS pour l'autorisation de groupe

S'ils sont associés, ils offrent aux utilisateurs externes la fonctionnalité de se connecter à NetWitness Suite sans avoir de compte NetWitness Suite interne, et de recevoir des autorisations ou des rôles déterminés en mappant le groupe externe vers un rôle de sécurité NetWitness Suite. Les deux composants sont requis pour qu'une connexion réussisse.

L'authentification externe est un paramètre au niveau du système. Avant de configurer PAM, examinez attentivement toutes les informations ici.

Modules PAM (Pluggable Authentication Module)

PAM est une bibliothèque fournie par Linux, responsable de l'authentification des utilisateurs auprès des fournisseurs d'authentification tels que RADIUS, Kerberos ou LDAP. Pour la mettre en œuvre, chaque fournisseur d'authentification utilise son propre module, qui se présente sous la forme d'un package de système d'exploitation (OS), tel que pam_ldap. Pour authentifier les utilisateurs, NetWitness Suite utilise la bibliothèque PAM fournie par le système d'exploitation et le module que la bibliothèque PAM est configurée pour utiliser.

Remarque : Le module PAM fournit uniquement la possibilité de s'authentifier.

Name Service Switch

NSS est une fonction Linux qui fournit les bases de données que le système d'exploitation et les applications utilisent pour découvrir des informations comme les noms d'hôtes ; les attributs d'utilisateur comme le répertoire de base, le groupe principal et le shell de connexion ; et pour répertorier des utilisateurs qui appartiennent à un groupe donné. Semblable aux modules PAM, NSS est configurable et utilise des modules pour interagir avec les différents types de fournisseurs. NetWitness Suite utilise les fonctions NSS fournies par le système d'exploitation pour autoriser les utilisateurs PAM externes en recherchant si un utilisateur est connu sur NSS puis en demandant ensuite depuis NSS les groupes dont cet utilisateur est membre. NetWitness Suite compare les résultats de la demande au mappage de groupe externe NetWitness Suite et si un groupe correspondant est trouvé, l'utilisateur obtient un accès pour se connecter à la session NW avec le niveau de sécurité défini dans le mappage de groupe externe.

Remarque : NSS ne fournit pas d'authentification.

Association de PAM et NSS

Les opérations de PAM (authentification) et NSS (autorisation) doivent réussir pour qu'un utilisateur externe soit autorisé à se connecter à NetWitness Suite. La procédure de configuration et de dépannage de PAM est différente de celle de NSS. Les exemples concernant PAM dans ce guide comprennent Kerberos, LDAP et RADIUS. Les exemples de NSS incluent Samba, LDAP et UNIX. L'association de modules PAM et NSS utilisée est déterminée par les besoins du site.

Vue d'ensemble du processus

Pour configurer la fonction de connexion PAM, suivez les instructions de ce document pour effectuer chaque étape :

1. Configurer et tester le module PAM.
2. Configurer et tester le service NSS.
3. Activer PAM dans Serveur NetWitness.
4. Créer des mappages de groupe dans Serveur NetWitness.

Conditions préalables

Avant de commencer la configuration de PAM, passez en revue la procédure et recueillez les détails du serveur d'authentification externe en fonction du module PAM que vous souhaitez mettre en œuvre.

Avant de commencer la configuration de NSS, passez en revue la procédure, identifiez les noms des groupes que vous allez utiliser dans le mappage de groupe externe, puis recueillez les détails du serveur d'authentification externe, selon le service NSS utilisé.

Avant de commencer la configuration de PAM dans NetWitness Suite, identifiez les noms des groupes que vous allez utiliser dans le mappage de groupe externe. Lors du mappage des rôles, le rôle dans NetWitness Suite doit correspondre à un nom de groupe qui existe dans le serveur d'authentification externe.

Configurer et tester le module PAM

Choisissez l'une des sections suivantes pour installer et configurer le composant PAM :

- PAM Kerberos
- PAM LDAP
- PAM Radius
- SecurID

PAM Kerberos

Ports de communication Kerberos - TCP 88

Pour configurer l'authentification PAM avec Kerberos :

1. Exécutez la commande suivante (en vérifiant d'abord que le package `krb5-workstation` est installé dans votre environnement) :
   `yum install krb5-workstation pam_krb5`
2. Modifiez les lignes suivantes dans le fichier de configuration Kerberos `/etc/krb5.conf`. Remplacez les variables, qui sont délimitées par des <crochets>, par vos valeurs et en omettant les crochets. La mise en majuscules est obligatoire aux emplacements indiqués.

```
# Configuration snippets may be placed in this directory as well
includedir /etc/krb5.conf.d/

[logging]
default = FILE:/var/log/krb5libs.log
kdc = FILE:/var/log/krb5kdc.log
admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 dns_lookup_realm = false
 ticket_lifetime = 24h
 dns_lookup_kdc = true
 renew_lifetime = 7d
 forwardable = true
 rdns = false
 default_realm = <DOMAIN.COM>
 default_ccache_name = KEYRING:persistent:%{uid}

[realms]
 <DOMAIN.COM> = {
 kdc = <SERVER.DOMAIN.COM>
 admin_server = <SERVER.DOMAIN.COM>
 }

 [domain_realm]
 <domain.com> = <DOMAIN.COM>
 <.domain.com> = <DOMAIN.COM>
```

3. Testez la configuration Kerberos avec la commande :
   `kinit <user>@<DOMAIN.COM>`
   S'il n'y a aucune sortie après la saisie du mot de passe, c'est que l'opération a réussi.
4. Modifiez le Serveur NetWitnessfichier de configuration PAM`/etc/pam.d/securityanalytics` pour ajouter la ligne suivante. Si le fichier n'existe pas, créez-le et ajoutez la ligne suivante :
   `auth sufficient pam_krb5.so no_user_check`

Ceci termine la configuration de PAM Kerberos. Maintenant, passez à la section suivante, *Configurer et tester le service NSS.*

PAM LDAP

Ports de communication LDAP - TCP 389 or TCP 636

TCP 389 peut être utilisé pour à la fois le trafic déchiffré et dans la plupart des cas, le trafic chiffré, ce qui suffit souvent. La plupart des implémentations LDAP modernes prennent en charge la commande `start_tls` lors de la connexion du port 389, qui met à niveau la connexion d'un état déchiffré en passant à l'état chiffré. Dans cette instance, les URI LDAP commencent toujours avec `ldap://` même en utilisant `start_tls`.

TCP 636 est utilisé uniquement dans les instances où le serveur LDAP ne prend pas en charge la commande `start_tls`. Dans ce cas, les URI LDAP commencent par `ldaps://` et la commande `start_tls` n'est pas utilisée.

Pour configurer l'authentification PAM avec LDAP :

1. Exécutez la commande suivante (en vérifiant d'abord que le package `openldap-clients` est installé dans votre environnement) :
   `yum install nss-pam-ldapd openldap-clients`
2. Modifiez les fichiers de configuration LDAP `/etc/nslcd.conf` comme indiqué dans l'exemple suivant :

Remarque : Remplacez les variables, qui sont délimitées par des <crochets>, par vos valeurs et en omettant les crochets. La mise en majuscules est obligatoire aux emplacements indiqués.

Exemples d'entrées de fichiers `/etc/nslcd.conf` :

```
uri ldap://<server.domain.com>
 base <dc=domain,dc=com>
 binddn <cn=bineuser,dc=domain,dc=com>
 bindpw <secret>
```

3. Après avoir modifié le fichier `/etc/nslcd.conf`, exécutez la commande suivante :
   `systemctl restart nslcd`

4. (Facultatif) Pour activer le transport sécurisé pour la communication LDAP avec vérification de certificat homologue (plus sécurisée), reportez-vous à la page man de Linux pour nslcd sur la modification de code appropriée pour le fichier `/etc/nslcd.conf`.

   Remarque : Les contrôleurs de domaine Windows n'activent pas par défaut le transport LDAP sécurisé. Ils requièrent l'installation d'un certificat de serveur pour l'authentification serveur. L'obtention et l'installation de ce certificat en CC ne sont pas traités dans le cadre de ce document. Quelques indications à ce sujet sont disponibles à l'adresse https://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx.

5. (Facultatif) Pour activer le transport sécurisé pour la communication LDAP sans certificat homologue, reportez-vous à la page man de Linux pour nslcd sur la modification de code appropriée pour le fichier`/etc/nslcd.conf`.

6. Pour dépanner la configuration LDAP, arrêtez d'abord le service `nslcd` en saisissant la commande suivante :
   ```
   systemctl stop nlscd
   ```

7. Pour copier les informations de dépannage et d'état du service à la console, exécutez le service `nslcd` en mode débogage à partir de la ligne de commande :
   ```
   nslcd -d
   ```

8. Modifiez le Serveur NetWitnessfichier de configuration PAM`/etc/pam.d/securityanalytics` pour ajouter la ligne suivante. Si le fichier n'existe pas, créez-le et ajoutez la ligne suivante :
   ```
   auth sufficient pam_ldap.so
   ```

Ceci termine la configuration de PAM LDAP. Maintenant, passez à la section suivante, *Configurer et tester le service NSS*.

PAM Radius

Ports de communication Radius- UDP 1812 ou UDP 1813

Pour configurer l'authentification PAM à l'aide de Radius, vous devez ajouter Serveur NetWitness à votre liste de client de serveur Radius et configurer un code secret partagé. Contactez l'administrateur du serveur Radius pour cette procédure.

Pour configurer l'authentification PAM pour Radius avec LDAP :

1. Exécutez la commande suivante (en vérifiant d'abord que le package `pam_radius` est installé dans votre environnement) :
   ```
   yum install pam_radius
   ```
2. Modifiez le fichier de configuration Radius `/etc/raddb/server` comme suit :
   ```
   # server[:port] shared_secret  timeout (s)
   server    secret     3
   ```
3. Modifiez le Serveur NetWitnessfichier de configuration PAM`/etc/pam.d/securityanalytics` pour ajouter la ligne suivante. Si le fichier n'existe pas, créez-le et ajoutez la ligne suivante :
   ```
   auth sufficient pam_radius_auth.so
   ```

Attention : Pour que PAM RADIUS fonctionne, les fichiers `/etc/raddb/server` doivent disposer d'une autorisation d'écriture. La commande nécessaire pour cela est : `chown netwitness:netwitness /etc/raddb/server`.

Les modules PAM et les services associés information envoient des informations à `/var/log/messages` et `/var/log/secure`. Ces sorties peuvent être utilisées pour aider à résoudre des problèmes de configuration.

La procédure suivante est un exemple des étapes à suivre pour configurer l'authentification PAM pour Radius à l'aide de SecurID :

Remarque : Les exemples de ces tâches utilisent RSA Authentication Manager en tant que serveur Radius.

1. Exécutez la commande suivante (en vérifiant d'abord que le package `pam_radius` est installé dans votre environnement) :
   ```
   yum install pam_radius
   ```
2. Modifiez le fichier de configuration Radius, `/etc/raddb/server` puis mettez-le à jour avec le nom d'hôte de l'instance Authentication Manager, avec le code secret partagé et avec le délai d'expiration :
   ```
   # server[:port] shared_secret timeout (s)
    111.222.33.44         secret        1
    #other-server        other-secret  3
    192.168.12.200:6369 securid       10
   ```

Remarque : Vous devez commenter les lignes `127.0.0.1` et `other-server` puis ajouter l'adresse IP de l'instance Authentication Manager principale avec un numéro de port Radius (par exemple, `192.168.12.200:1812`), un code secret partagé Radius et une valeur d'expiration du délai de 10.

3. Modifiez le Serveur NetWitnessfichier de configuration PAM`/etc/pam.d/securityanalytics` pour ajouter la ligne suivante. Si le fichier n'existe pas, créez-le et ajoutez la ligne suivante :

   ```
   auth sufficient pam_radius_auth.so
   ```

   Remarque : Vous pouvez ajouter `debug` à la fin de la ligne ci-dessus dans le fichier `/etc/pam.d/securityanalytics` pour permettre le débogage PAM (par exemple, `auth sufficient pam_radius_auth.so debug`)

Les modules PAM et les services associés envoient des informations à `/var/log/messages` et `/var/log/secure`. Ces sorties peuvent être utilisées pour aider à résoudre des problèmes de configuration.

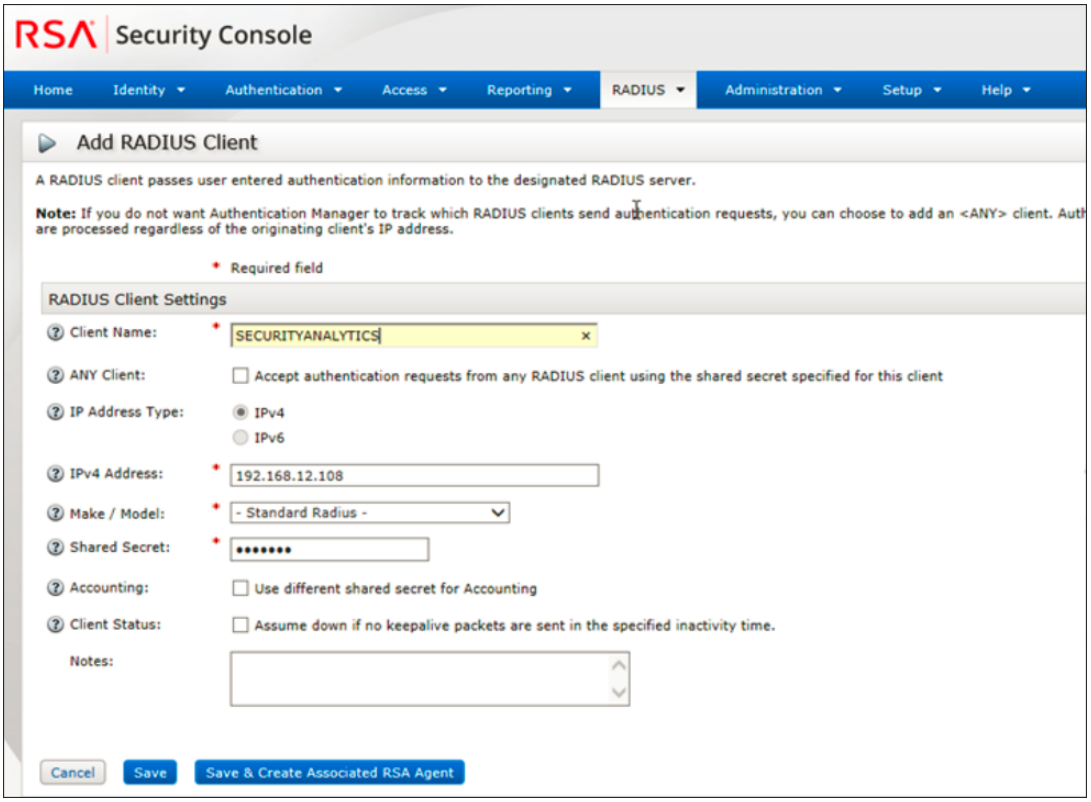
Ajouter un Client Radius et un Agent associé.

Remarque : Les exemples de ces tâches utilisent RSA Authentication Manager en tant que serveur Radius.
Vous devez utiliser les informations d'identification du compte d'administrateur pour vous connecter à la Console de sécurité de RSA Authentication Manager.

Pour ajouter un Client Radius et un Agent associé :

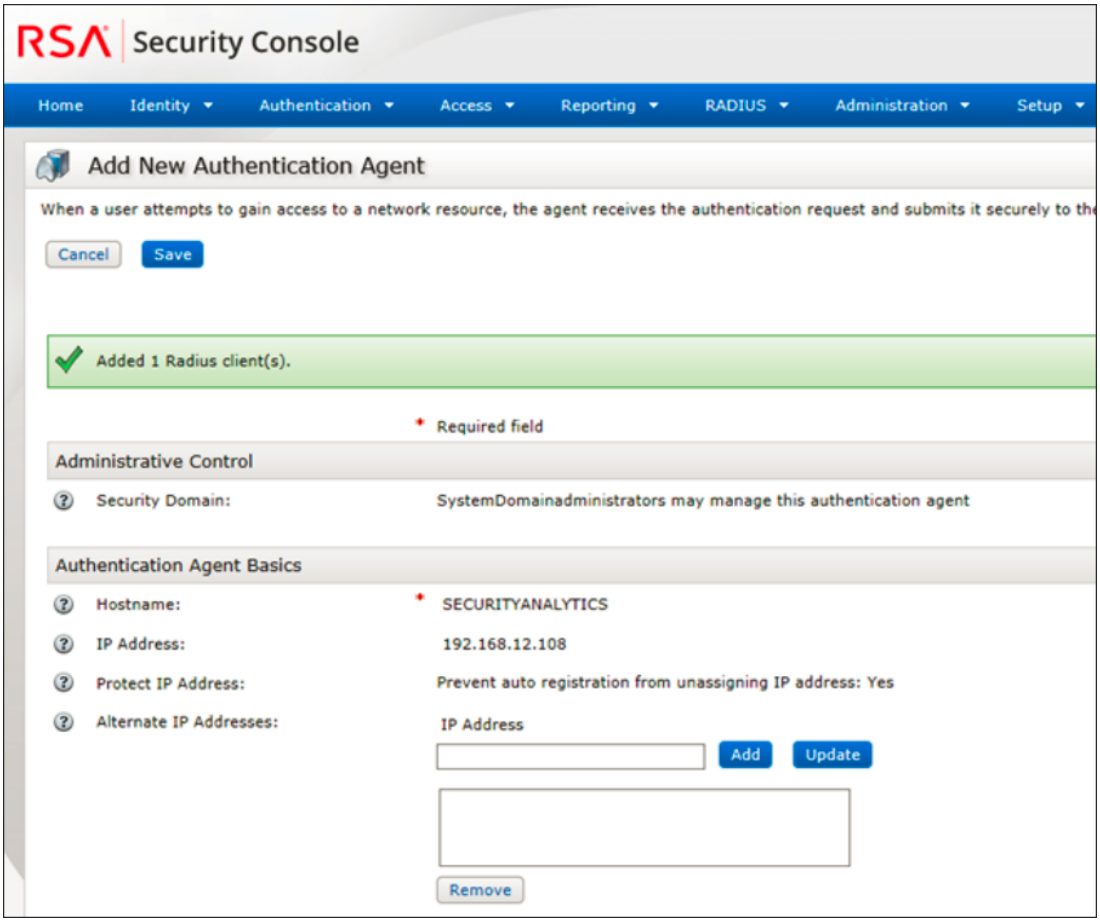
1. Connectez-vous à RSA Authentication Manager.
   La Console de sécurité s'affiche.

2. Dans la Console de sécurité, cliquez sur **RADIUS > Clients RADIUS > Ajouter nouveau**. La page Ajouter un Client RADIUS s'affiche.



3. Dans les paramètres Client RADIUS, fournissez les informations suivantes :
   a. Dans le champ **Nom du client**, saisissez le nom du client, par exemple NetWitness Suite.
   b. Dans le champ **Adresse IPv4**, indiquez l'adresse IPv4 du client Radius, par exemple 192.168.12.108.
   c. Dans la liste déroulante **Marque/Modèle**, sélectionnez le type de client Radius, par exemple Fortinet.
   d. Dans le champ **Code secret partagé**, saisissez le code secret partagé d'authentification.

4. Cliquez sur **Enregistrer et créer un agent RSA associé**.



5. Cliquez sur **Enregistrer**.

Si l'Instance Authentication Manager ne peut pas trouver l'agent d'authentification sur le réseau, une page d'avertissement s'affiche. Cliquez sur **Oui, enregistrer l'Agent**.

Pour plus d'informations, consultez la rubrique Ajouter un client RADIUS du *Guide d'administrateur de RSA Authentication Manager 8.2*.

Ceci termine la configuration de PAM Radius. Maintenant, passez à la section suivante, *Configurer et tester le service NSS*.

Agent PAM pour SecurID

Port de communication PAM - UDP 5500

Conditions préalables

Le module RSA SecurID PAM est pris en charge uniquement dans les conditions suivantes :

1. Les connexions approuvées doivent être activées et fonctionner entre NetWitness Suite et les services de base.

Vue d'ensemble du processus

Voici les étapes générales de configuration du module SecurID PAM :

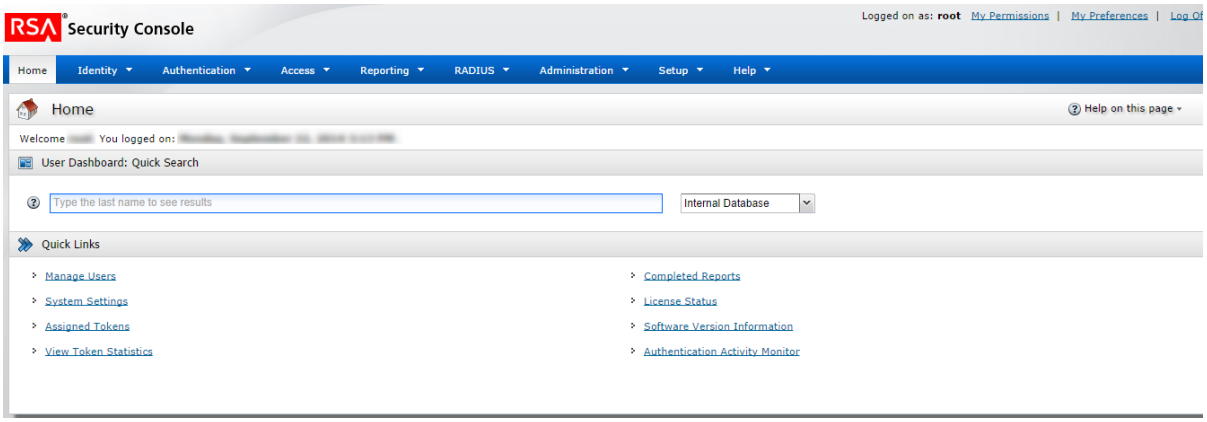
1. Configurez **Authentication Manager** :
   a. Ajouter un agent d'authentification.
   b. Télécharger le fichier de configuration.
2. Configurer **Serveur NetWitness** :
   a. Copiez le fichier de configuration à partir d'Authentication Manager et personnalisez-le.
   b. Installez le module PAM SecurID.
3. Tester la connectivité et l'authentification.

Suivez ensuite les procédures restantes dans les sections qui suivent :

- Configurez NSS.
- Activez PAM dans Serveur NetWitness.
- Configurez les mappages de groupe dans Serveur NetWitness.

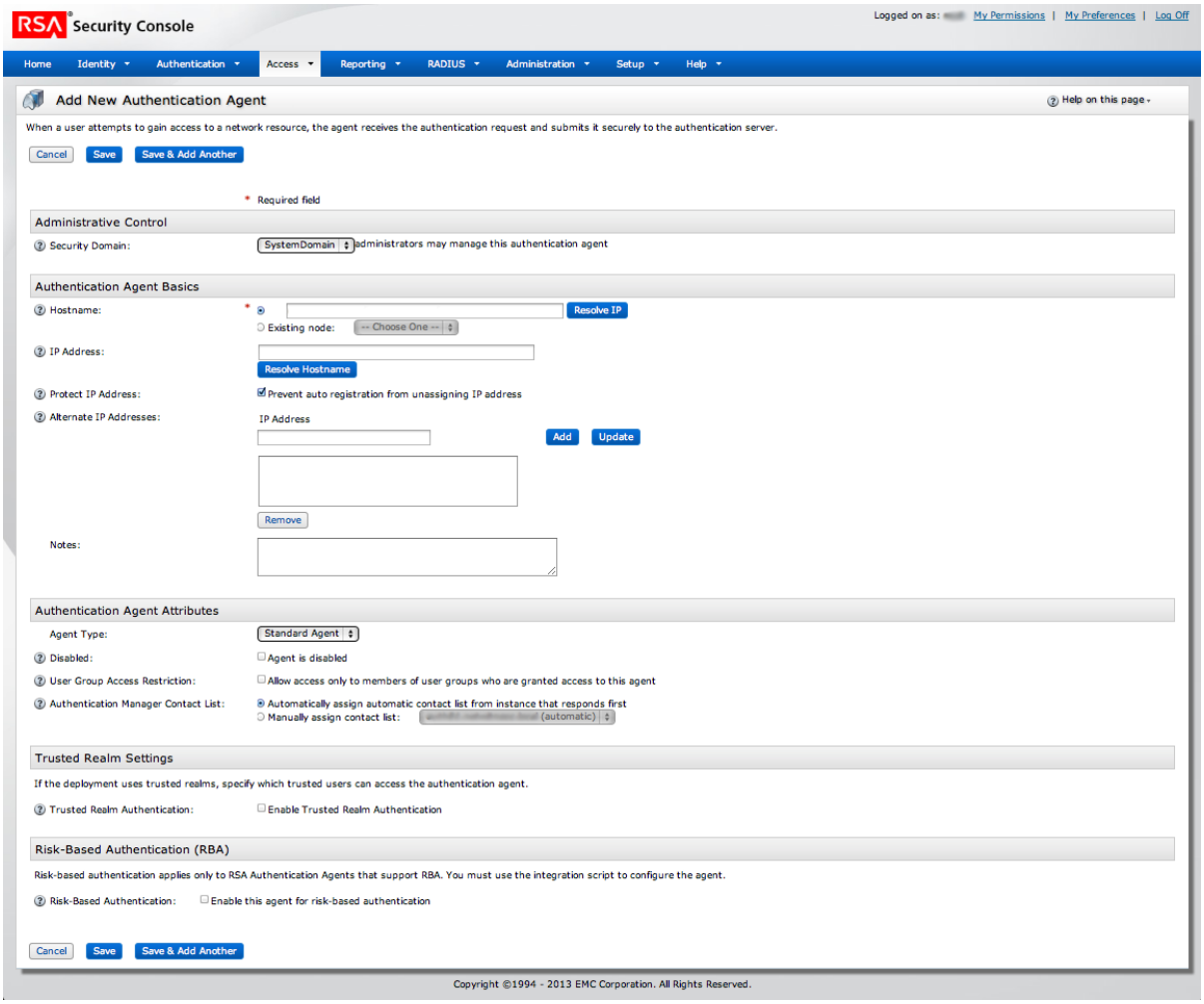
Pour configurer Authentication Manager :

1. Connectez-vous à RSA Authentication Manager.
   La Console de sécurité s'affiche.

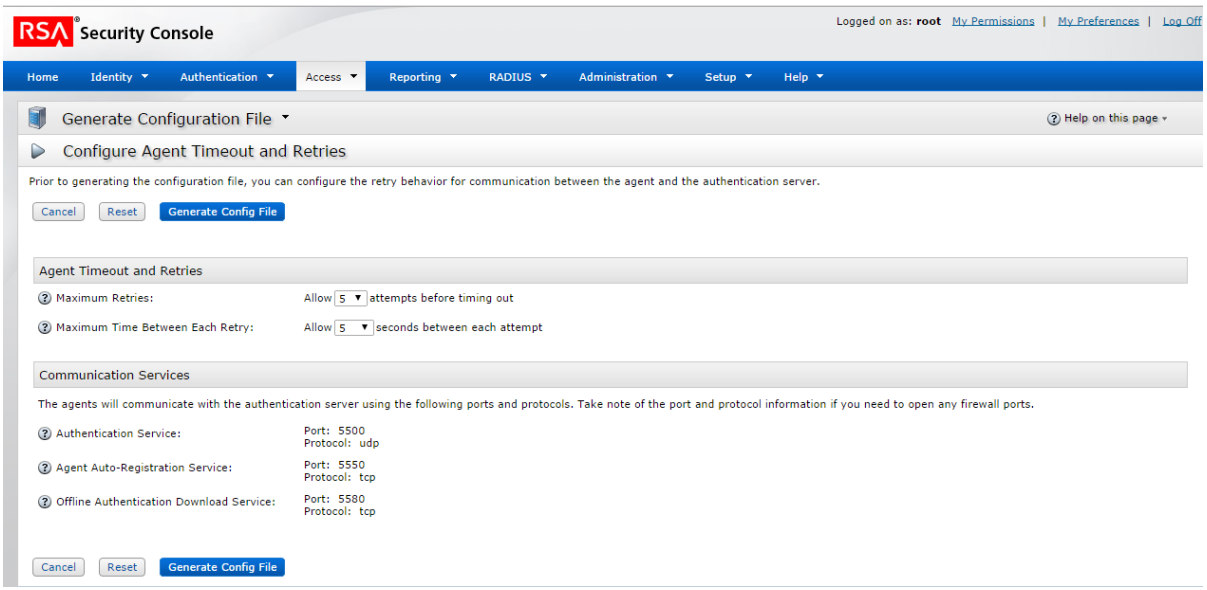


2. Dans la Console de sécurité, ajoutez un nouvel Agent d'authentification.
   Cliquez sur **Accès > Agents d'authentification > Ajouter nouveau.**

La page Ajouter un nouvel agent d'authentification s'affiche.



3. Dans le champ **Nom d'hôte**, saisissez le nom d'hôte de Serveur NetWitness.
4. Cliquez sur **Résoudre l'adresse IP**.
   L'adresse IP de Serveur NetWitness s'affiche automatiquement dans le champ **Adresse IP**.
5. Conservez les paramètres par défaut et cliquez sur **Enregistrer**.
6. Générer un fichier de configuration.
   Cliquez sur **Accès > Agents d'authentification > Générer le fichier de configuration**.
   La page Générer le fichier de configuration s'affiche.



7. Conservez les valeurs par défaut et cliquez sur **Générer le fichier de configuration**. Cela crée **AM_Config.zip**, qui contient deux fichiers.
8. Cliquez sur **Téléchargez maintenant**.

Pour installer et configurer le module SecurID PAM :

1. Sur Serveur NetWitness, créez un répertoire :
   `mkdir /var/ace`
2. Sur Serveur NetWitness, copiez `sdconf.rec` à partir du fichier .zip dans `/var/ace`.
3. Créez un fichier texte `sdopts.rec` dans le répertoire `/var/ace`.
4. Insérez la ligne suivante :
   `CLIENT_IP=<IP address of Serveur NetWitness>`
5. Installez l'Agent d'autorisation SecurID pour PAM, qui est disponible dans le dépôt yum :
   `yum install sid-pam-installer`
6. Exécutez le script d'installation :
   `/opt/rsa/pam-agent-installer/install_pam.sh`
7. Suivez les instructions pour accepter ou modifier les valeurs par défaut.
8. Modifiez le Serveur NetWitnessfichier de configuration PAM`/etc/pam.d/securityanalytics` pour ajouter la ligne suivante. Si le fichier n'existe pas, créez-le et ajoutez la ligne suivante :
   `auth sufficient pam_securid.so`

Ceci termine l'installation du module PAM SecurID. Ensuite, testez la connectivité et l'authentification. Puis suivez les procédures de Configurer et tester le service NSS.

Remarque : Si la configuration de PAM SecurID n'est pas terminée, il est probable que le serveur Jetty se bloque et l'interface utilisateur NetWitness Suite ne s'affiche pas. Vous devez attendre que la configuration de l'authentification PAM soit terminée, puis redémarrer le serveur Jetty.

Pour tester la connectivité et l'authentification :

1. Exécutez `/opt/pam/bin/64bit/acetest`, saisissez le **nom d'utilisateur** et le **code secret**.
2. (Facultatif) Si acetest échoue, activez le débogage :
   ```
   vi/etc/sd_pam.conf
   RSATRACELEVEL=15
   ```
3. Exécutez `/opt/pam/bin/64bit/acestatus`. Sortie ci-dessous
   ```
   RSA ACE/Server Limits
    ---------------------
    Configuration Version : 15 Client Retries : 5
    Client Timeout : 5 DES Enabled : Yes

   RSA ACE/Static Information
    --------------------------
    Service : securid Protocol : udp Port Number : 5500

   RSA ACE/Dynamic Information
    ---------------------------
    Server Release : 8.1.0.0 Communication : 5

   RSA ACE/Server List
    -------------------
    Server Name :  auth81.netwitness.local
    Server Address :  192.168.100.10
    Server Active Address : 192.168.100.10
    Master : Yes Slave : No Primary : Yes
    Usage : Available for Authentications
   ```
4. (Facultatif) Pour dépanner le serveur Authentication Manager,
   cliquez sur **Reporting > Moniteurs d'activité en temps réel > Moniteur d'activité d'authentification.**
   Ensuite, cliquez sur **Démarrer le moniteur**.
5. Si vous avez modifié le paramètre, réinitialisez RSATRACELEVEL sur 0 :
   ```
   vi/etc/sd_pam.conf
   RSATRACELEVEL=0
   ```

Attention : Après l'installation, vérifiez que VAR_ACE dans le fichier `/etc/sd_pam.conf` pointe vers l'emplacement correct du fichier sdconf.rec. Il s'agit du chemin vers les fichiers de configuration. La commande nécessaire pour cela est : `chown -R netwitness:netwitness /var/ace`.

Ceci termine la configuration de l'agent PAM pour SecurID. Maintenant, passez à la section suivante, *Configurer et tester le service NSS*.

Configurer et tester le service NSS

Choisir un service NSS

Il existe trois options de service NSS : Samba, LDAP et UNIX. Les trois comportent des avantages et des inconvénients.

Avantages de NSS Samba	Inconvénients de NSS Samba
Objectif construit pour Active Directory	Ne peut être utilisé avec des back-ends non-AD
Peu ou pas de configuration doit être effectuée dans Active Directory	Potentiellement plus difficile à configurer et dépanner
Pas de comptes utilisateurs spéciaux nécessaires	Nécessite que la machine Serveur NW soit associée au domaine Active Directory
	Utilise de nombreux ports pour communiquer avec Active Directory ; plus difficile à mettre en œuvre au travers des pare-feux et proxys

Avantages de NSS LDAP	Inconvénients de NSS LDAP
La configuration de base est simple	Peut nécessiter une configuration et des rôles supplémentaire à l'intérieur de Active Directory
Peut communiquer avec toute mise en œuvre de LDAP	Nécessite la configuration d'un compte de liaison LDAP

Avantages de NSS LDAP	Inconvénients de NSS LDAP
Utilise un seul port TCP pour la communication - plus facile de travailler avec des pare-feux et proxy	Plus difficile d'activer le transport sécurisé à moins de le configurer pour ne pas valider les certificats de serveur
Ne nécessite pas d'associer un hôte NW au domaine AD	

NSS UNIX

Aucune configuration n'est nécessaire pour activer le module NSS UNIX ; il est activé dans le système d'exploitation hôte par défaut. Pour autoriser un utilisateur pour un groupe spécifique, il suffit de l'ajouter au système d'exploitation et de l'ajouter à un groupe :

1. Créez un groupe de systèmes d'exploitation à ajouter à votre utilisateur externe avec cette commande :
   `groupadd <groupname>`
2. Ajoutez l'utilisateur externe au système d'exploitation avec cette commande :
   `adduser -G <groupname> -M -N <externalusername>`

Remarque : Notez que cette opération ne permet PAS ni autorise l'accès à la console Serveur NW.

Ceci termine la configuration de NSS UNIX. Ensuite, passez à la section Tester la fonctionnalité NSS.

NSS Samba

Ports de communication Winbind AD

Les ports suivants sont les ports minimums. Les tests internes indiquent qu'ils doivent être ouverts pour autoriser la fonctionnalité NSS Samba. Ces informations sont fournies uniquement à titre de référence.

TCP 88 - Kerberos
TCP 139 - Netbios
TCP 389 - LDAP
UDP 53 - DNS
UDP 88 - Kerberos
UDP 389 - LDAP

Des ports supplémentaires peuvent être nécessaires, en fonction des exigences propres sur site de la mise en œuvre. Des ports supplémentaires peuvent être nécessaires, en fonction des exigences propres sur site de la mise en œuvre : http://technet.microsoft.com/en-us/library/dd772723%28ws.10%29.aspx

Pour configurer NSS Samba :

1. Modifiez le fichier de configuration Samba, `/etc/samba/smb.conf`, comme suit. Remplacez les variables, qui sont délimitées par des <crochets>, par vos valeurs et en omettant les crochets. La mise en majuscules est obligatoire aux emplacements indiqués.

```
[global]
workgroup = domain
netbios name = <NW_APPLIANCE_HOSTNAME>
password server = <ADSERVER.DOMAIN.COM>
realm = <DOMAIN.COM>

local master = no
security = ads
syslog only = yes
log file = /var/log/samba/log.%m
max log size = 5120
idmap config * : range = 16777216-33554431
template shell = /bin/bash
winbind use default domain = true
winbind offline logon = false
winbind enum groups = yes
```

2. Pour activer et démarrer le service de liaison de Windows, `winbind`, saisissez les commandes suivantes :

```
systemctl enable winbind
systemctl start winbind
```

3. Modifiez le fichier de configuration NSS, `/etc/nsswitch.conf`. Mettez à jour uniquement les 2 entrées ci-dessous et laissez le reste sur les valeurs par défaut :

```
passwd:     files winbind
group:      files winbind
```

4. Pour associer le domaine, saisissez la commande suivante :

```
net ads join -U <DomainAdminUser>
```

5. Pour stocker le SID du contrôleur de domaine, saisissez la commande suivante :

```
net rpc getsid -S <SERVER.DOMAIN.COM>
```

6. Testez la fonctionnalité NSS comme décrit dans la section *Tester la fonctionnalité NSS*.

7. Lorsque vous avez confirmé que NSS fonctionne correctement à partir de la ligne de commande, pour redémarrer l'hôte pour que les modifications NSS prennent effet, saisissez la commande suivante.
   `reboot`

Pour dépanner NSS Samba :

Pour vérifier si NSS Winbind peut communiquer avec succès avec Active Directory :

1. Saisissez les commandes suivantes :
   `wbinfo -u` pour renvoyer la liste des utilisateurs AD
   `wbinfo -g` pour retourner une liste des groupes AD
2. Si aucune commande ne fonctionne, exécutez `winbind` dans la console en mode de débogage en saisissant les commandes suivantes :
   ```
   systemctl stop winbind
   winbindd -S -F -d <optional debugleve 0-10>
   ```
3. À partir d'une session ssh séparée, répétez l'étape 1 et vérifiez la sortie `winbindd` pour obtenir l'indication du problème.
   Augmentez le degré d'explicitation du débogage de `winbindd` le cas échéant.
4. Effectuez les ajustements nécessaires pour `/etc/samba/smb.conf`.
5. Dans la fenêtre de débogage `winbindd` de l'étape 2, arrêtez `winbindd` en saisissant `CTRL-C`.
   Répétez les étapes 1 et 2 et continuez le dépannage jusqu'à ce que les commandes `wbinfo` réussissent.
6. Après le succès des commandes `wbinfo`, utilisez les commandes `getent` de la section Test de la fonctionnalité NSS de ce guide pour tester NSS.
   ```
   getent passwd <pamUser>
   getent group <groupOfPamUser>
   ```
7. Lorsque la commande `getent` réussit, arrêtez la ligne de commande `winbindd` en saisissant `CTRL-C` et saisissez la commande suivante pour démarrer le processus du service :
   `systemctl start winbind`

Si `wbinfo -g` réussit depuis la ligne de commande, mais que la recherche du mappage de groupe externe ne présente aucun des groupes Active Directory :

1. Ajoutez les lignes suivantes à `/etc/samba/smb.conf` :
   `allow trusted domains = no`
2. Saisissez `systemctl restart winbind .`

Ceci termine la configuration de NSS Samba. Ensuite, passez à la section Tester la fonctionnalité NSS.

NSS LDAP

Remarque : Ces instructions exigent que tous les utilisateurs PAM et les objets des groupes NSS de Active Directory comportent la valeur de leurs attributs `uidNumber` et `gidNumber` sur des numéros UID et GID de style UNIX afin d'être utilisés par NSS LDAP. Les anciens schémas Active Directory peuvent ne pas avoir ces attributs par défaut. Les nouveaux schémas AD peuvent comporter ces attributs, mais ils ne peuvent pas être définis dans chaque objet. La configuration correcte de ces attributs n'entre pas dans le cadre du présent document. Contactez votre administrateur Active Directory pour que ces attributs soient définis pour les utilisateurs PAM et les groupes NSS.

Un utilisateur de liaison LDAP doit être créé dans Active Directory pour utiliser NSS. Cet utilisateur doit être configuré pour que son mot de passe n'expire pas. Étant donné que ces informations d'identification doivent être spécifiées pour le service NSS LDAP en clair, les autorisations de `/etc/nslcd.conf` doivent être laissées sur 600 (leur valeur par défaut) de sorte que le fichier ne puisse être lu par des utilisateurs du système autres que racine.

LDAP Communication Ports - TCP 389 or TCP 636

TCP 389 peut être utilisé pour à la fois le trafic déchiffré et dans la plupart des cas, le trafic chiffré, ce qui suffit souvent. La plupart des implémentations LDAP modernes prennent en charge la commande `start_tls` lors de la connexion du port 389, qui met à niveau la connexion d'un état déchiffré en passant à l'état chiffré. Dans cette instance, les URI LDAP commencent toujours avec `ldap://` même en utilisant `start_tls`.

TCP 636 est utilisé uniquement dans les instances où le serveur LDAP ne prend pas en charge la commande `start_tls`. Dans cette instance, les URI LDAP commencent par `ldaps://` et la commande `start_tls` n'est pas utilisée.

Pour configurer le module NSS pour LDAP avec Active Directory :

1. Obtenez le package `nss-pam-ldapd` à partir du référentiel SMCUPDATE ou à partir du référentiel des mises à jour Serveur NetWitness si le serveur est synchronisé avec SMCUPDATE. Cela nécessite un compte Live configuré dans NetWitness Suite.
2. Pour installer le package, exécutez la commande suivante :
   ```
   yum install nss-pam-ldapd
   ```
3. Modifiez `/etc/nslcd.conf` pour inclure les lignes ci-dessous, en vous assurant que les lignes existantes dans le fichier commencent d'abord par un caractère dièse # au début de la ligne :
   ```
   uid nslcd
   gid ldap
   uri ldap://<server.domain.com>
   base <dc=domain,dc=com>
   binddn <cn=binduser,dc=domain,dc=com
   bindpw <secret>
   ```
   Remarque : Vous devrez ajouter des mappages supplémentaires entre les recherches NSS et recherches LDAP pour votre environnement spécifique. Reportez-vous à la page man de Linux pour nslcd pour obtenir des informations spécifiques.
4. (Facultatif) Pour activer le transport sécurisé pour la communication LDAP avec vérification de certificat homologue (plus sécurisée), reportez-vous à la page man de Linux pour nslcd sur la modification de code appropriée pour le fichier `/etc/nslcd.conf`.

Remarque : Les contrôleurs de domaine Windows n'activent pas par défaut le transport LDAP sécurisé. Ils requièrent l'installation d'un certificat de serveur pour l'authentification serveur. L'obtention et l'installation de ce certificat en CC ne sont pas traités dans le cadre de ce document. Quelques indications à ce sujet sont disponibles à l'adresse https://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx

5. (Facultatif) Pour activer le transport sécurisé pour la communication LDAP sans certificat homologue, reportez-vous à la page man de Linux pour nslcd sur la modification de code appropriée pour le fichier `/etc/nslcd.conf`.
6. Modifiez le fichier de configuration de NSS `/etc/nsswitch.conf`. Mettez à jour uniquement les deux entrées ci-dessous et laissez le reste sur les valeurs par défaut :
   ```
   passwd:files ldap
   group:files ldap
   ```

7. Pour activer et démarrer le service NSLCD, saisissez ces commandes :
   ```
   systemctl enable nslcd
   systemctl start nslcd
   ```
8. Testez la fonctionnalité NSS à l'aide des conseils de la section *Tester la fonctionnalité NSS*. Si les tests NSS échouent, dépannez NSS LDAP comme décrit dans *Dépanner NSS LDAP*.
9. Lorsque vous avez confirmé que NSS fonctionne correctement à partir de la ligne de commande, redémarrez l'hôte pour que les modifications NSS prennent effet.
   ```
   reboot
   ```

Pour dépanner NSS LDAP :

1. Pour dépanner NSS LDAP, arrêtez d'abord le service nslcd en saisissant la commande suivante :
   ```
   systemctl stop nslcd
   ```
2. Pour copier les informations de dépannage et d'état du service sur la console, exécutez le service nslcd en mode débogage à partir de la ligne de commande.
   ```
   nslcd -d
   ```
3. (Facultatif) Pour augmenter le degré d'explicitation du débogage, ajoutez un d supplémentaire plusieurs fois à la fin de nslcd -d, par exemple, saisissez la commande suivante :
   ```
   nslcd -ddd
   ```
4. À partir d'une session ssh distincte, utilisez les commandes `getent` de la section Test de la fonctionnalité NSS de ce guide pour tester NSS. Surveillez la sortie de débogage à partir de nslcd pour obtenir les indications de l'endroit où l'échec se produit. Augmentez le degré d'explicitation du débogage de nslcd le cas échéant.
   ```
   getent passwd <pamUser>
   getent group <groupOfPamUser>
   ```
5. Effectuez les ajustements nécessaires dans `/etc/nslcd.conf` en fonction de la sortie de l'étape 2 ou 3.
6. Dans la fenêtre de débogage nslcd de l'étape 2 ou 3, arrêtez `nslcd` avec `CTRL-C`. Répétez l'étape 2 ou 3 et continuez le dépannage jusqu'à ce que les commandes `getent` réussissent.
7. Lorsque `getent` réussit, arrêtez la ligne de commande `nslcd` et démarrez le processus du service :
   ```
   systemctl start nslcd
   ```

Les problèmes courants peuvent comprendre :

- Le certificat SSL de transport sécurisé LDAP qui n'est pas installé sur le serveur LDAP/AD.
- Échec de vérification de certificat d'autorité de certification : commentez la ligne `tls_cacert` dans `/etc/nslcd.conf` et essayez `tls_reqcert never`. Si elle réussit, vous savez quelle vérification du certificat est un échec.
  - Le certificat CA racine n'est pas au format PEM.
  - Utilisez le certificat de l'autorité de certification émettrice plutôt que le certificat de l'autorité de certification racine.
  - Le nom du certificat SSL du serveur LDAP ne correspond pas à son nom d'hôte.
- Nom unique de base incorrect.
- L'utilisateur ou le mot de passe de liaison LDAP n'est pas spécifié correctement.
- En spécifiant de façon incorrecte `ldaps://` au lieu de `ldap://` dans la ligne `uri` de `/etc/nslcd.conf`. `ldaps://` doit uniquement être utilisé avec LDAPS mais pas la commande `start_tls`.
- Les utilisateurs et les groupes Active Directory ne disposent pas d'attributs `uidNumber` ou `gidNumber` définis.
- Le pare-feu réseau bloque les communications.
- Le nom d'hôte du serveur LDAP spécifié ne peut pas être résolu
  - Paramètres DNS incorrects dans `/etc/resolv.conf`.
  - Nom d'hôte incorrect spécifié à la ligne `uri` de `/etc/nslcd.conf`.

Ceci termine la configuration de NSS LDAP. Ensuite, passez à la section Tester la fonctionnalité NSS.

Tester la fonctionnalité NSS

Pour tester si NSS fonctionne avec l'un des services NSS précédents, utilisez les commandes suivantes :

```
getent passwd <pamUser>
 getent group <groupOfPamUser>
```

La sortie doit être similaire à :

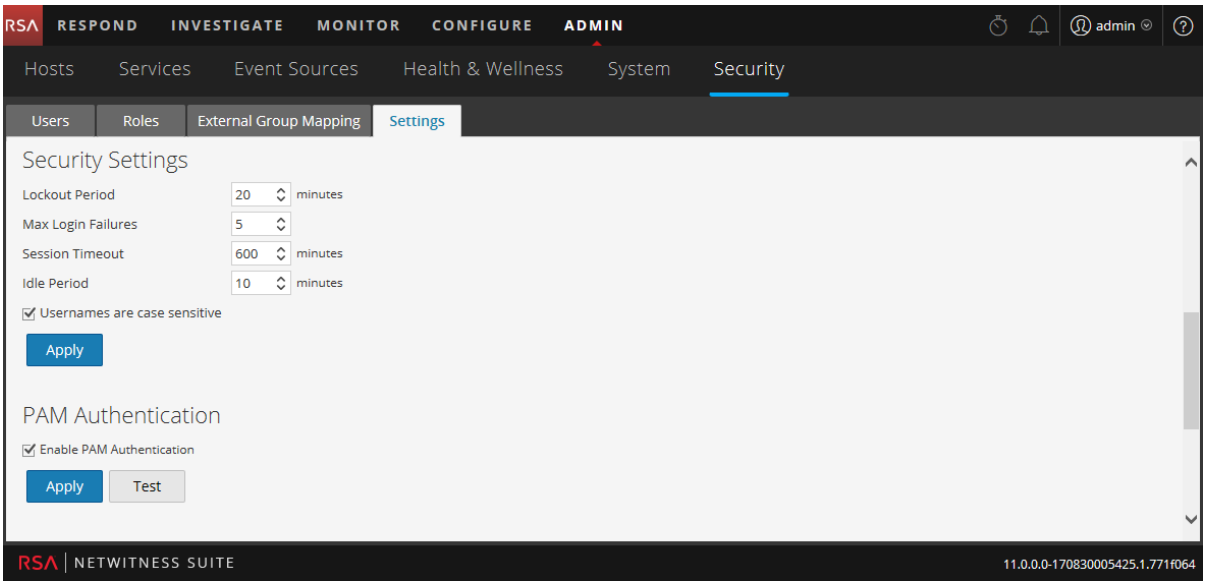
```
[root@~]# getent passwd myuser
 myuser:*:10000:10000::/home/myuser:/bin/sh
[root@~]# getent group mygroup
 mygroup:*:10000:myuser3
```

- Si aucune commande ne produit de sortie, l'autorisation externe ne fonctionne pas correctement sur NSS. Reportez-vous aux conseils de dépannage de votre module NSS fournis dans ce document.
- Si les commandes `getent` fonctionnent et que la réussite de l'authentification est confirmée dans `/var/log/secure` mais que NetWitness Suite ne parvient toujours pas à autoriser les utilisateurs externes à se connecter :
  - Est-ce que le nom de groupe correct a été spécifié pour le groupe NSS dans le mappage de groupe externe NW ? Reportez-vous aux sections ci-dessous Activer PAM et Créer des mappages de groupe.
  - Il se peut que la configuration NSS ait changé et que NetWitness Suite n'ait pas relevé le changement. Un redémarrage de l'hôte NetWitness Suite entraînera l'application des modifications de configuration NSS par NetWitness Suite. Un redémarrage de `jetty` n'est pas suffisant.

Passez à la section suivante, Activer PAM dans Serveur NetWitness.

Activer PAM dans Serveur NetWitness

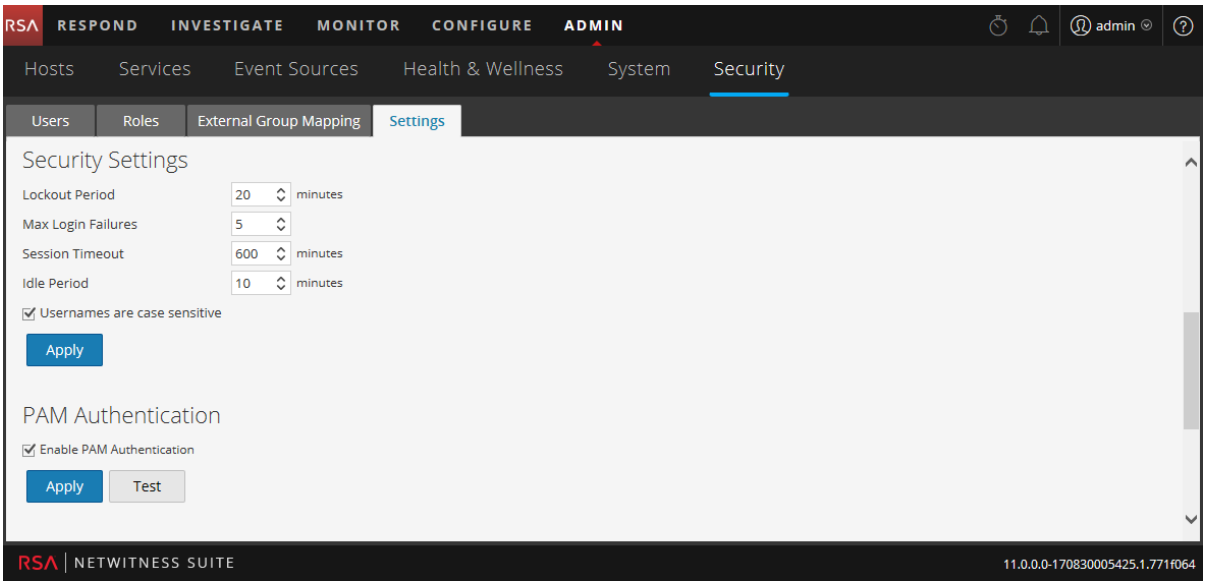
1. Dans NetWitness Suite, accédez à **ADMIN > Sécurité**.
   La vue Administrateur > Sécurité s'ouvre avec l'onglet Utilisateurs ouvert.
2. Cliquez sur l'onglet **Paramètres**.
3. Sous **Authentification PAM**, sélectionnez **Activer l'authentification PAM** , puis cliquez sur **Appliquer**.



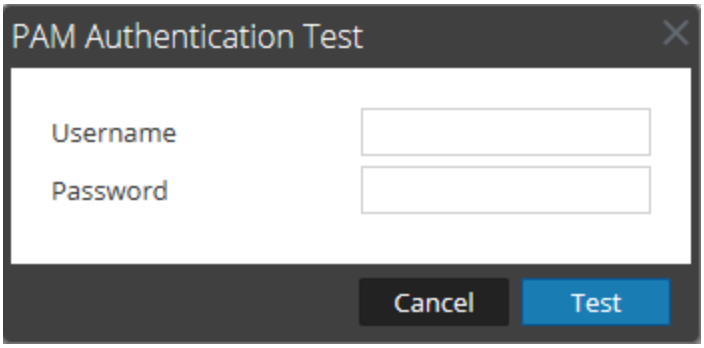
Tester l'authentification PAM

Pour tester l'authentification externe PAM :

1. Accédez à **ADMIN > Sécurité**.
   La vue Sécurité s'affiche avec l'onglet **Utilisateurs** ouvert.
2. Cliquez sur l'onglet **Paramètres**.
3. Sous **Authentification PAM**, sélectionnez **Activer l'authentification PAM**.



4. Sous les options **Authentification PAM**, cliquez sur **Tester**.
   La boîte de dialogue **Test d'authentification PAM** s'affiche.



5. Saisissez un nom d'utilisateur et un mot de passe que vous voulez tester pour l'authentification avec la configuration PAM actuelle.
6. Cliquez sur **Tester**.
   La méthode d'authentification externe est testée pour assurer la connectivité.
7. Si le test n'aboutit pas, passez en revue et modifiez la configuration.

L’authentification PAM est activée, et les configurations Active Directory restent également activées. Les configurations PAM sont automatiquement renseignées dans l’onglet Mappage de groupe externe pour vous permettre de mapper des rôles de sécurité pour chaque groupe. Pour configurer les rôles de sécurité utilisés pour accéder à PAM, reportez-vous à l’Étape 5. (Facultatif) Mapper des rôles d'utilisateur aux groupes externes.

Mode de fonctionnement du contrôle d'accès basé sur un rôle

Cette rubrique explique le fonctionnement du contrôle d'accès basé sur un rôle lorsqu'une connexion approuvée est établie entre Serveur NetWitness et un service Core.

Dans RSA NetWitness® Suite , les rôles déterminent ce que les utilisateurs sont autorisés à faire. Un rôle dispose d'autorisations et il convient d'attribuer un rôle à chaque utilisateur. Les autorisations de l'utilisateur dépendent alors de son rôle.

Rôles préconfigurés

Pour simplifier le processus de création des rôles et l'attribution des autorisations, il existe des rôles préconfigurés dans NetWitness Suite. Vous pouvez également ajouter des rôles personnalisés pour votre organisation.

Le tableau suivant répertorie chaque rôle préconfiguré et les autorisations qui lui sont attribuées. Toutes les autorisations sont attribuées au rôle Administrateurs. Un sous-ensemble d'autorisations est attribué à chacun des autres rôles.

Rôle	Autorisation
Administrateurs	Accès complet au système Le profil Administrateurs système se voit accorder toutes les autorisations par défaut.
Opérateurs	Accès aux configurations, mais pas au contenu méta ni de session. Le profil Opérateurs système est axé sur la configuration système, mais pas sur l'Investigation, ni sur Alerting ESA, Reporting et Répondre.
Analystes	Accès au contenu méta et de session, mais pas aux configurations. Le profil Analystes du centre des opérations de sécurité (SOC) est axé sur l'Investigation, sur Alerting ESA, Reporting et Répondre, mais pas sur la configuration système.
Administrateur de réponse	Accès à toutes les autorisations Répondre

Rôle	Autorisation
Responsables de SOC	Même accès que les Analystes avec des autorisations supplémentaires pour gérer les incidents Le profil Responsables de SOC est identique à celui des Analystes, mais dispose des autorisations nécessaires pour configurer Répondre.
Analystes du malware	Accès aux investigations et aux événements de malware. Le seul accès accordé au profil Analystes du malware est celui du module Malware Analysis.
Responsables de la confidentialité des données	Le profil Spécialiste de la confidentialité des données est semblable à celui des administrateurs, mais davantage axé sur les options de configuration qui gèrent l'obfuscation et la visualisation des données sensibles au sein du système (voir *Gestion de la confidentialité des données*). Les utilisateurs qui se voient attribuer le rôle de Spécialiste de la confidentialité_ des données peuvent voir quelles métaclés sont marquées pour obfuscation. Ils voient également les métaclés obfusquées et les valeurs créées pour les métaclés marquées.

Connexions approuvées entre le serveur et le service

Dans une connexion approuvée, un service fait explicitement confiance à Serveur NetWitness pour gérer et authentifier les utilisateurs. Cela réduit l'administration sur chaque service puisque les utilisateurs authentifiés n'ont pas à être définis localement dans chaque service Core.

Comme le montre le tableau ci-dessous, vous effectuez toutes les tâches de gestion des utilisateurs sur le serveur.

Tâche	Emplacement
Ajouter un utilisateur	Serveur
Gérer les noms d'utilisateur	Serveur
Gérer les mots de passe	Serveur
Authentifier les utilisateurs NetWitness Suite internes	Serveur

Tâche	Emplacement
(Facultatif) Authentifier les utilisateurs externes avec :	
- Active Directory	Serveur
- PAM	Serveur
Installer et configurer PAM	Serveur

Les avantages d'une connexion approuvée et de la gestion centralisée des utilisateurs sont les suivants :

- Vous effectuez toutes les tâches d'administration des utilisateurs en même temps, uniquement sur Serveur NetWitness.
- Vous contrôlez l'accès aux services, mais vous n'avez pas besoin de configurer ni d'authentifier les utilisateurs sur les services.
- Les utilisateurs saisissent leur mot de passe une seule fois au moment de la connexion à NetWitness Suite et sont authentifiés par le serveur.
- Les utilisateurs, déjà authentifiés par le serveur, accèdent à chaque service Core dans ADMIN > Services sans saisir de mot de passe.

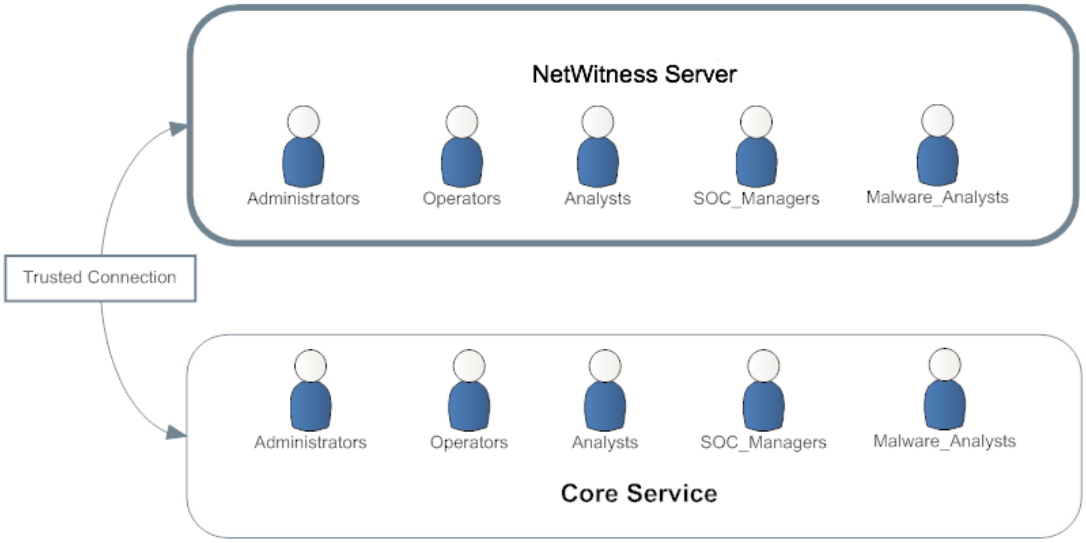
Établissement des connexions approuvées

Lorsque vous installez la version 11.0 ou que vous procédez à la mise à niveau vers cette version, les connexions approuvées sont établies par défaut avec deux paramètres :

1. SSL est activé.
2. Le service Core est connecté à un port SSL chiffré.

Noms de rôles courants sur le serveur et les services

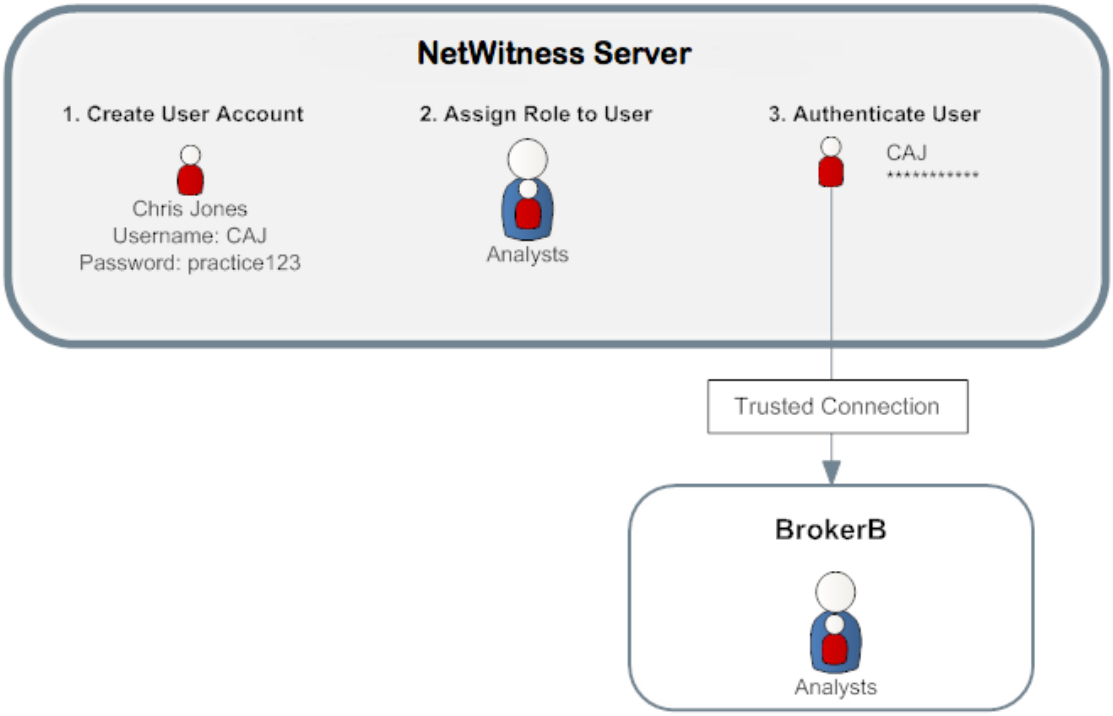
Les connexions approuvées reposent sur des noms de rôles courants sur le serveur et le service. Lors d'une installation, NetWitness Suite installe les cinq rôles préconfigurés sur le serveur et sur chaque service Core.



Si vous ajoutez un rôle personnalisé tel que le rôle Analystes_juniors, vous devez l'ajouter à chaque service comme ArchiverA et BrokerB. Les noms de rôles sont sensibles à la casse, ne peuvent pas contenir d'espace et doivent être identiques. Par exemple, Analyste_junior (singulier) et Analystes_juniors (pluriel) ne répondent pas aux exigences des noms de rôles courants.

Workflow de bout en bout pour la configuration d'utilisateurs et l'accès à un service

Ce workflow montre comment fonctionne le contrôle d'accès basé sur un rôle lorsqu'une connexion approuvée est établie entre Serveur NetWitness et le service BrokerB.



1. Sur Serveur NetWitness, créez un compte pour un nouvel utilisateur :
   Nom : Chris Jones
   Nom d'utilisateur : CAJ
   Mot de passe : practice123
2. Déterminez si vous souhaitez attribuer un rôle préconfiguré ou personnalisé à Chris Jones :
   - **Rôle préconfiguré**
     a. Conservez ou modifiez les autorisations par défaut attribuées au **rôle Analystes** qui comprend des autorisations telles que l'accès aux modules Alerting, Investigation et Malware.
     b. Attribuez le rôle Analystes à Chris Jones.
   - **Rôle personnalisé**
     a. Créez le rôle personnalisé, par exemple Analystes_juniors.
     b. Attribuez les autorisations au **rôle Analystes_juniors**.
     c. Attribuez le rôle Analystes_juniors à Chris Jones.
     d. Ajoutez le rôle Analystes_juniors au service, par exemple BrokerB.
3. L'utilisateur, Chris Jones, se connecte à Serveur NetWitness:
   Nom d'utilisateur : CAJ

Mot de passe : practice123

4. Le serveur authentifie Chris Jones.
5. La connexion approuvée autorise l'utilisateur authentifié, Chris Jones, à accéder à BrokerB sans saisir d'autre mot de passe.

Pour obtenir des descriptions et des procédures plus détaillées, reportez-vous à la rubrique Gérer les utilisateurs à l'aide de rôles et d'autorisations.

Rubrique connexe

- Autorisations du rôle

Autorisations du rôle

Cette rubrique décrit l'accès à l'interface utilisateur à la disposition des utilisateurs attribués aux NetWitness Suite rôles intégrés.

Dans NetWitness Suite, l'accès des utilisateurs à chaque module, dashlet et vue est restreint en fonction des autorisations attribuées décrites dans cette rubrique. Vous pouvez trouver ces autorisations de rôle dans les boîtes de dialogue Ajouter ou modifier les rôles, accessibles à partir de l'onglet Administrateur > Sécurité > Attribution de rôles.

Dans les boîtes de dialogue Ajouter ou modifier les rôles, les onglets de la section Autorisation représentent les différentes zones deNetWitness Suite et affichent les autorisations disponibles pour ces domaines. Par exemple, l'onglet Administration présente les autorisations disponibles dans la vue Administrateur.

Remarque : Dans les boîtes de dialogue Ajouter ou modifier un rôle, il n'existe aucun onglet de configuration correspondant à la vue Configuration. Pour attribuer des autorisations dans la vue Configuration, attribuez des autorisations pour les vues contenues dans la vue Configuration : Contenu Live (Live), Règles de l'incident (Incidents), Règles ESA (Alerting), Abonnements (Live) et Feeds personnalisés (Live).

Remarque : À gauche de l'onglet Administration se trouve un onglet marqué d'un astérisque (*). Cet onglet indique l'accès à la gestion des services back-end uniquement.

Les tableaux qui suivent présentent les autorisations par défaut attribuées à chaque NetWitness Suite rôle d'utilisateur :

- Administrateurs
- Opérateurs
- Analystes
- Administrateur de réponse
- Responsables du SOC (Gest. SOC)
- Analystes Malware (MA)
- Responsables de la confidentialité des données (DPO)

Étant donné que le rôles d'Administrateurs possède toutes les autorisations par défaut, ils ne sont pas inclus dans les tableaux.

Format des autorisations de service des nouveaux services

Les autorisations de service inhérentes à certains nouveaux NetWitness Suite services sont divisées en trois parties, au format suivant :

<nom du service> <ressource>.<action>

Par exemple, pour l'autorisation **investigate-server.metrics.read** :

- nom du service = **investigate-server** (serveur Rechercher)
- ressource = **metrics** (statistiques)
- action = **read** (lire)

Les utilisateurs alloués à cette autorisation peuvent lire les statistiques exposées par le service de serveur Rechercher.

Administration

Le tableau suivant décrit les autorisations disponibles pour chaque rôle dans l'onglet Administration : Les Administrateurs disposent de toutes les autorisations par défaut et ne sont pas répertoriés.

Autorisation	Opérateurs	Analystes	Gest. SOC	MA	DPO
Accéder au module Administration	Oui	Oui	Oui	Oui	Oui
Accéder à l'intégrité	Oui	Oui	Oui	Oui	Oui
Appliquer les mises à jour du système	Oui				
Possibilité d'adhérer à Live Intelligence Sharing	Oui				
Gérer les audits globaux	Oui				Oui
Gérer la politique d'intégrité	Oui				
Gérer les paramètres avancés	Oui				
Gérer les audits	Oui				Oui
Gérer les e-mails	Oui				
Gérer les LLS	Oui				

Autorisation	Opérateurs	Analystes	Gest. SOC	MA	DPO
Gérer les logs	Oui				Oui
Gérer les notifications	Oui				
Gérer les plug-ins	Oui				
Gérer les prédicats	Oui				
Gérer la reconstruction	Oui				
Gérer la sécurité	Oui				Oui
Gérer les services	Oui				Oui
Gérer les paramètres du système	Oui				
Modifier les paramètres ESA	Oui				
Modifier les sources d'événements	Oui				
Modifier les hôtes	Oui				
Modifier les services	Oui				Oui
Afficher les sources d'événements	Oui		Oui		
Afficher la politique d'intégrité	Oui	Oui	Oui		
Afficher le navigateur des statistiques d'intégrité	Oui	Oui	Oui		Oui
Afficher les hôtes	Oui				Oui
Afficher les services	Oui				Oui

Serveur Administrateur

Le tableau suivant décrit les autorisations disponibles dans l'onglet Administrateur. Les Administrateurs disposent de toutes les ;autorisations ; en outre, il s'agit du seul rôle bénéficiant des autorisations par défaut.

Autorisation	Description
admin-server.configuration.manage	Autorisation d'afficher et de modifier tous les paramètres de configuration de service
admin-server.health.read	Autorisation de lire les notifications d'intégrité qu'expose le service
admin-server.logs.manage	Autorisation de modifier la configuration des logs
admin-server.metrics.read	Autorisation de lire les statistiques qu'expose le service
admin-server.process.manage	Autorisation de démarrer et d'arrêter le service
admin-server.security.manage	Autorisation de modifier les ressources liées à la sécurité (mots de passe, clés, etc.)
admin-server.security.read	Autorisation de lire les ressources liées à la sécurité

Alerting

Le tableau suivant décrit les autorisations disponibles pour chaque rôle dans l'onglet Alerting : Les Administrateurs disposent de toutes les autorisations par défaut et ne sont pas répertoriés.

Autorisation	Opérateurs	Analystes	Gest. SOC	MA	DPO
Accéder au module Alerting	Oui	Oui	Oui		Oui
Gérer les règles	Oui		Oui		Oui
Afficher les alertes		Oui	Oui		Oui

Autorisation	Opérateurs	Analystes	Gest. SOC	MA	DPO
Afficher les règles	Oui		Oui		Oui

Serveur de configuration

Le tableau suivant décrit les autorisations disponibles dans l'onglet Serveur de configuration : Les Administrateurs disposent de toutes les autorisations ; en outre, il s'agit du seul rôle bénéficiant des autorisations par défaut.

Autorisation	Description
config-server.*	Toutes les autorisations (tous les éléments ci-dessous)
config-server.configuration.manage	Autorisation d'afficher et de modifier tous les paramètres de configuration de service
config-server.health.read	Autorisation de lire les notifications d'intégrité qu'expose le service
config-server.logs.manage	Autorisation de modifier la configuration des logs
config-server.metrics.read	Autorisation de lire les statistiques qu'expose le service
config-server.process.manage	Autorisation de démarrer et d'arrêter le service
config-server.security.manage	Autorisation de modifier les ressources liées à la sécurité (mots de passe, clés, etc.)
config-server.security.read	Autorisation de lire les ressources liées à la sécurité

Tableau de bord

Le tableau suivant décrit les autorisations disponibles pour chaque rôle dans l'onglet Tableau de bord : Les Administrateurs disposent de toutes les autorisations par défaut et ne sont pas répertoriés.

Autorisation	Opérateurs	Analystes	Gest. SOC	MA	DPO
Accès au dashlet - Dashlet Liste de périphériques Administrateur	Oui	Oui	Oui		Oui
Accès au dashlet - Dashlet Surveillance des périphériques Administrateur	Oui				Oui
Accès au dashlet - Dashlet Actualité Administrateur	Oui	Oui	Oui		Oui
Accès au dashlet - Dashlet Variance d'alerte		Oui	Oui		Oui
Accès au dashlet - Dashlet Alertes récentes d'Alerting		Oui	Oui		Oui
Accès au dashlet - Dashlet Tâches liées à Investigation		Oui	Oui		Oui
Accès au dashlet - Dashlet Valeurs principales Investigation		Oui	Oui		Oui
Accès au dashlet - Dashlet Ressources proposées dans Live	Oui	Oui	Oui		Oui
Accès au dashlet - Dashlet Nouvelles ressources dans Live	Oui	Oui	Oui		Oui
Accès au dashlet - Dashlet Abonnements Live	Oui	Oui	Oui		Oui
Accès au dashlet - Dashlet Ressources mises à jour dans Live	Oui	Oui	Oui		Oui

Autorisation	Opérateurs	Analystes	Gest. SOC	MA	DPO
Accès au dashlet - Dashlet Tâches Malware		Oui	Oui		Oui
Accès au dashlet - Dashlet Rapports récents de Reporting		Oui	Oui		Oui
Accès au dashlet - Dashlet Graphiques de Reporting		Oui	Oui		Oui
Accès au dashlet - Dashlet Alertes principales		Oui	Oui		Oui
Accès au dashlet - Dashlet RSA First Watch Unified	Oui	Oui	Oui		Oui
Accès au dashlet - Dashlet Raccourcis Unified	Oui	Oui	Oui		Oui

Serveur ESA analytics

Le tableau suivant décrit les autorisations disponibles dans l'onglet Serveur ESA analytics. Les Administrateurs et Opérateurs disposent de toutes les autorisations ; en outre, il s'agit des seuls rôles bénéficiant des autorisations par défaut.

Autorisation	Description
esa-analytics-server.*	Toutes les autorisations (tous les éléments ci-dessous)
esa-analytics-server.analytics.manage	Autorisation d'afficher et de modifier l'analytique de l'ESA
esa-analytics-server.analytics.read	Autorisation d'afficher l'analytique de l'ESA
esa-analytics-server.configuration.manage	Autorisation d'afficher et de modifier tous les paramètres de configuration de service

Autorisation	Description
esa-analytics-server.health.read	Autorisation de lire les notifications d'intégrité qu'expose le service
esa-analytics-server.logs.manage	Autorisation de modifier la configuration des logs
esa-analytics-server.metrics.read	Autorisation de lire les statistiques qu'expose le service
esa-analytics-server.model.manage	Autorisation d'afficher et de modifier les modèles ESA
esa-analytics-server.model.read	Autorisation d'afficher les modèles ESA
esa-analytics-server.process.manage	Autorisation de démarrer et d'arrêter le service
esa-analytics-server.security.read	Autorisation de lire les ressources liées à la sécurité

Incidents

Le tableau suivant décrit les autorisations disponibles pour chaque rôle dans l'onglet Incidents : Les Administrateurs disposent de toutes les autorisations par défaut et ne sont pas répertoriés.

Autorisation	Opérateurs	Analystes	Gest. SOC	MA	DPO
Accéder au module Incident		Oui	Oui	Oui	Oui
Configurer l'intégration Incident Management			Oui		Oui
Supprimer les alertes et incidents					Oui

Autorisation	Opérateurs	Analystes	Gest. SOC	MA	DPO
Gérer les règles de gestion des alertes			Oui		Oui
Afficher et gérer les incidents		Oui	Oui	Oui	Oui

Rechercher

Le tableau suivant décrit les autorisations disponibles pour chaque rôle dans l'onglet Rechercher : Les Administrateurs disposent de toutes les autorisations par défaut et ne sont pas répertoriés.

Autorisation	Opérateurs	Analystes	Gest. SOC	MA	DPO
Accéder au module Investigation		Oui	Oui	Oui	Oui
Recherche contextuelle		Oui	Oui	Oui	
Créer des incidents à partir d'Investigation		Oui	Oui	Oui	
Gérer la liste à partir d'Investigation		Oui	Oui	Oui	
Parcourir les événements		Oui	Oui	Oui	Oui
Parcourir les valeurs		Oui	Oui	Oui	Oui

Serveur Rechercher

Le tableau suivant décrit les autorisations disponibles dans l'onglet Serveur Rechercher :

Autorisation	Description
investigate-server.*	Toutes les autorisations (tous les éléments ci-dessous)

Autorisation	Description
investigate-server.configuration.manage	Autorisation de modifier les propriétés de configuration du serveur
investigate-server.health.read	Autorisation de lire les notifications d'intégrité qu'expose le service
investigate-server.logs.manage	Autorisation de modifier la configuration des logs
investigate-server.metrics.read	Autorisation de lire les statistiques qu'expose le service
investigate-server.process.manage	Autorisation de démarrer et d'arrêter le service
investigate-server.security.manage	Autorisation de modifier les ressources liées à la sécurité (mots de passe, clés, etc.)
investigate-server.security.read	Autorisation de lire les ressources liées à la sécurité

Le tableau suivant décrit les autorisations disponibles pour chaque rôle dans l'onglet Rechercher : Les Administrateurs disposent de toutes les autorisations par défaut et ne sont pas répertoriés.

Autorisation	Opérateurs	Analystes	Gest. SOC	MA	DPO
investigate-server.*		Oui	Oui	Oui	Oui
investigate-server.configuration.manage					
investigate-server.health.read					
investigate-server.logs.manage					
investigate-server.metrics.read					

Autorisation	Opérateurs	Analystes	Gest. SOC	MA	DPO
investigate-server.process.manage					
investigate-server.security.manage					
investigate-server.security.read					

Live

Le tableau suivant décrit les autorisations disponibles pour chaque rôle dans l'onglet Live : Les Administrateurs disposent de toutes les autorisations par défaut et ne sont pas répertoriés.

Autorisation	Opérateurs	Analystes	Gest. SOC	MA	DPO
Live					
Accéder au module Live	Oui	Oui	Oui		Oui
Gérer les paramètres du système Live	Oui				
Ressources					
Déployer les ressources Live	Oui				Oui
Gérer les feeds Live	Oui				Oui
Gérer les ressources Live	Oui				Oui
Rechercher des ressources Live	Oui	Oui	Oui		Oui
Afficher les détails des ressources Live	Oui	Oui	Oui		Oui

Serveur d'orchestration

Le tableau suivant décrit les autorisations disponibles dans l'onglet Serveur d'orchestration. Les Administrateurs, les Opérateurs et les Responsables de la confidentialité des données disposent de toutes les autorisations ; en outre, il s'agit des seuls rôles bénéficiant des autorisations par défaut.

Autorisation	Description
Serveur d'orchestration*	Toutes les autorisations (tous les éléments ci-dessous)
orchestration-server.configuration.manage	Autorisation d'afficher et de modifier tous les paramètres de configuration de service
orchestration-server.health.read	Autorisation de lire les notifications d'intégrité qu'expose le service
orchestration-server.logs.manage	Autorisation de modifier la configuration des logs
orchestration-server.metrics.read	Autorisation de lire les statistiques qu'expose le service
orchestration-server.process.manage	Autorisation de démarrer et d'arrêter le service
orchestration-server.security.manage	Autorisation de modifier les ressources liées à la sécurité (mots de passe, clés, etc.)
orchestration-server.security.read	Autorisation de lire les ressources liées à la sécurité

Malware

Le tableau suivant décrit les autorisations disponibles pour chaque rôle dans l'onglet Malware : Les Administrateurs disposent de toutes les autorisations par défaut et ne sont pas répertoriés.

Autorisation	Opérateurs	Analystes	Gest. SOC	MA	DPO
Télécharger le ou les fichiers de malware		Oui	Oui	Oui	Oui
Lancer une analyse Malware Analysis		Oui	Oui	Oui	Oui
Afficher les événements Malware Analysis		Oui	Oui	Oui	Oui

Rapports

Le tableau suivant décrit les autorisations disponibles pour chaque rôle dans l'onglet Rapports : Les Administrateurs disposent de toutes les autorisations par défaut et ne sont pas répertoriés.

Autorisation	Opérateurs	Analystes	Gest. SOC	MA	DPO
Alerte					
Définir l'alerte RE		Oui	Oui		Oui
Exporter la définition d'alerte RE		Oui	Oui		Oui
Gérer les alertes RE		Oui	Oui		Oui
Afficher les alertes RE		Oui	Oui		Oui
Afficher les alertes RE planifiées		Oui	Oui		Oui
Graphique					
Définir le graphique		Oui	Oui		Oui
Supprimer le graphique		Oui	Oui		Oui
Exporter la définition de graphique		Oui	Oui		Oui
Gestions des graphiques		Oui	Oui		Oui

Autorisation	Opérateurs	Analystes	Gest. SOC	MA	DPO
Afficher les graphiques		Oui	Oui		Oui
Liste					
Définir les listes		Oui	Oui		Oui
Supprimer la liste		Oui	Oui		Oui
Exporter la liste		Oui	Oui		Oui
Gérer les listes		Oui	Oui		Oui
Rapport					
Définir le rapport		Oui	Oui		Oui
Supprimer le rapport		Oui	Oui		Oui
Exporter le rapport		Oui	Oui		Oui
Gérer les rapports		Oui	Oui		Oui
Afficher les rapports		Oui	Oui		Oui
Rapports					
Accéder à la configuration		Oui	Oui		Oui
Accéder au module Reporter		Oui	Oui		Oui
Accéder à la recherche Reporter		Oui	Oui		Oui
Accéder à la vue		Oui	Oui		Oui
Règle					
Ajouter la définition d'alerte à partir de la règle		Oui	Oui		Oui
Définir la règle		Oui	Oui		Oui

Autorisation	Opérateurs	Analystes	Gest. SOC	MA	DPO
Supprimer la règle		Oui	Oui		Oui
Exporter la règle		Oui	Oui		Oui
Gérer les règles		Oui	Oui		Oui
Afficher l'utilisation de la règle		Oui	Oui		Oui
Planning					
Définir le planning		Oui	Oui		Oui
Supprimer le planning		Oui	Oui		Oui
Afficher les plannings		Oui	Oui		Oui
Warehouse Analytics					
Définir les tâches		Oui	Oui		Oui
Supprimer les tâches		Oui	Oui		Oui
Gérer les tâches		Oui	Oui		Oui
Afficher les tâches		Oui	Oui		Oui

Serveur Répondre

Le tableau suivant décrit les autorisations disponibles dans l'onglet Serveur Répondre.

Autorisation	Description
respond-server.*	Toutes les autorisations (tous les éléments ci-dessous)
respond-server.alert.delete	Autorisation de supprimer des alertes
respond-server.alert.manage	Autorisation de créer, de mettre à jour ou de supprimer des alertes

Autorisation	Description
respond-server.alert.read	Autorisation d'afficher des alertes
respond-server.alertrule.manage	Autorisation de créer, de mettre à jour ou de supprimer des règles d'agrégation des alertes
respond-server.alertrule.read	Autorisation d'afficher les règles d'agrégation des alertes
respond-server.configuration.manage	Autorisation de modifier les propriétés de configuration de service
respond-server.health.read	Autorisation de lire les notifications d'intégrité qu'expose le service
respond-server.incident.delete	Autorisation de supprimer des incidents
respond-server.incident.manage	Autorisation de créer, de mettre à jour ou de supprimer des incidents
respond-server.incident.read	Autorisation d'afficher les incidents
respond-server.journal.manage	Autorisation de créer, de mettre à jour ou de supprimer des entrées de journal pour un incident
respond-server.journal.read	Autorisation d'afficher les entrées de journal pour un incident
respond-server.logs.manage	Autorisation de modifier la configuration des logs
respond-server.metrics.read	Autorisation de lire les statistiques qu'expose le service
respond-server.process.manage	Autorisation de démarrer et d'arrêter le service
respond-server.remediation.manage	Autorisation de créer, de mettre à jour ou de supprimer des tâches de correction

Autorisation	Description
respond-server.remediation.read	Autorisation d'afficher les tâches de correction
respond-server.security.manage	Autorisation de modifier les ressources liées à la sécurité (mots de passe, clés, etc.)
respond-server.security.read	Autorisation de lire les ressources liées à la sécurité

Le tableau suivant répertorie les autorisations pour chaque rôle dans l'onglet Serveur Répondre. Les Administrateurs et les Administrateurs de réponse disposent de toutes les autorisations par défaut et ne sont pas répertoriés.

Autorisation	Opérateurs	Analystes	Gest. SOC	MA	DPO
respond-server.*					Oui
respond-server.alert.delete					
respond-server.alert.manage		Oui	Oui	Oui	
respond-server.alert.read		Oui	Oui	Oui	
respond-server.alertrule.manage			Oui		
respond-server.alertrule.read			Oui		
respond-server.configuration.manage					
respond-server.health.read					
respond-server.incident.delete					
respond-server.incident.manage		Oui	Oui	Oui	
respond-server.incident.read		Oui	Oui	Oui	
respond-server.journal.manage		Oui	Oui	Oui	

Autorisation	Opérateurs	Analystes	Gest. SOC	MA	DPO
respond-server.journal.read		Oui	Oui	Oui	
respond-server.logs.manage					
respond-server.metrics.read					
respond-server.process.manage					
respond-server.remediation.manage		Oui	Oui	Oui	
respond-server.remediation.read		Oui	Oui	Oui	
respond-server.security.manage					
respond-server.security.read					

Serveur de sécurité

Le tableau suivant décrit les autorisations disponibles dans l'onglet Serveur de sécurité. Les Administrateurs, les Opérateurs et les Responsables de la confidentialité des données disposent de toutes les autorisations ; en outre, il s'agit des seuls rôles bénéficiant des autorisations par défaut.

Autorisation	Description
security-server.*	Toutes les autorisations (tous les éléments ci-dessous)
security-server.account.manage	Autorisation d'afficher, de créer, de modifier ou de supprimer NetWitness Suite comptes locaux
security-server.account.read	Autorisation d'afficher NetWitness Suite comptes locaux
security-server.configuration.manage	Autorisation d'afficher et de modifier tous les paramètres de configuration de service

Autorisation	Description
security-server.health.read	Autorisation de lire les notifications d'intégrité qu'expose le service
security-server.logs.manage	Autorisation de modifier la configuration des logs
security-server.metrics.read	Autorisation de lire les statistiques qu'expose le service
security-server.permission.manage	Autorisation de créer ou de supprimer NetWitness Suite autorisations
security-server.process.manage	Autorisation de démarrer et d'arrêter le service
security-server.role.manage	Autorisation de créer, de modifier ou de supprimer NetWitness Suite rôles (par exemple, d'ajouter des autorisations de rôle)
security-server.role.read	Autorisation d'afficher NetWitness Suite définitions de rôle
security-server.security.manage	Autorisation de modifier les ressources liées à la sécurité (mots de passe, clés, etc.)
security-server.security.read	Autorisation de lire les ressources liées à la sécurité
security-server.user.manage	Autorisation d'afficher, de créer, de modifier ou de supprimer NetWitness Suite profils utilisateur
security-server.user.read	Autorisation d'afficher NetWitness Suite détails du profil utilisateur (par exemple, les rôles, les heures de connexion, etc.)

Gérer les utilisateurs à l'aide de rôles et d'autorisations

Cette rubrique présente un ensemble de procédures complètes pour gérer les utilisateurs dans NetWitness Suite. Ces étapes expliquent comment ajouter un utilisateur dans NetWitness Suite, puis comment contrôler ses activités autorisées.

Rubriques

Étape 1. Passer en revue les rôles préconfigurés NetWitness

Pour simplifier le processus de création des rôles et l'attribution des autorisations, il existe des rôles préconfigurés dans NetWitness Suite.

Rôle	Autorisation
Administrateurs	Accès complet au système
Opérateurs	Accès aux configurations, mais pas au contenu méta ni de session
Analystes	Accès au contenu méta et de session mais pas aux configurations
Administrateur de réponse	Accès à toutes les autorisations des onglets Serveur Répondre et Incidents.
Responsables de SOC	Même accès que les Analystes avec des autorisations supplémentaires pour gérer les incidents
Analystes du malware	Accès aux événements de malware et au contenu méta et de sessions
Responsables de la confidentialité des données	Accès au contenu méta et de session ainsi qu'aux options de configuration qui gèrent l'obscurcissement et l'affichage des données sensibles dans le système (voir Gestion de la confidentialité des données).

L'administrateur peut également ajouter des rôles personnalisés.

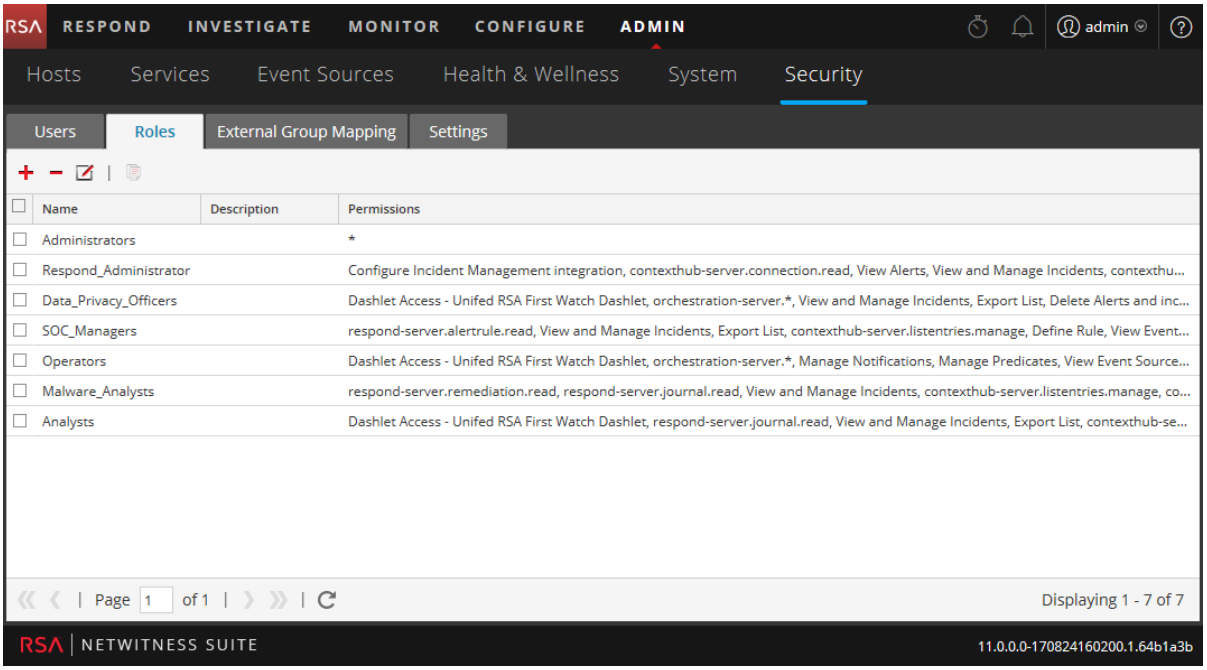
Étape 2. (Facultatif) Ajouter un rôle et attribuer des autorisations

Bien que NetWitness Suite inclue des rôles préconfigurés, vous pouvez ajouter des rôles personnalisés. Par exemple, parallèlement au rôle préconfiguré Analystes, vous pouvez ajouter les rôles personnalisés AnalystesEurope et AnalystesAsia. Pour obtenir la liste détaillée des autorisations, reportez-vous à la rubrique Autorisations du rôle.

Chacune des procédures suivantes commence sous l'onglet **Rôles**.

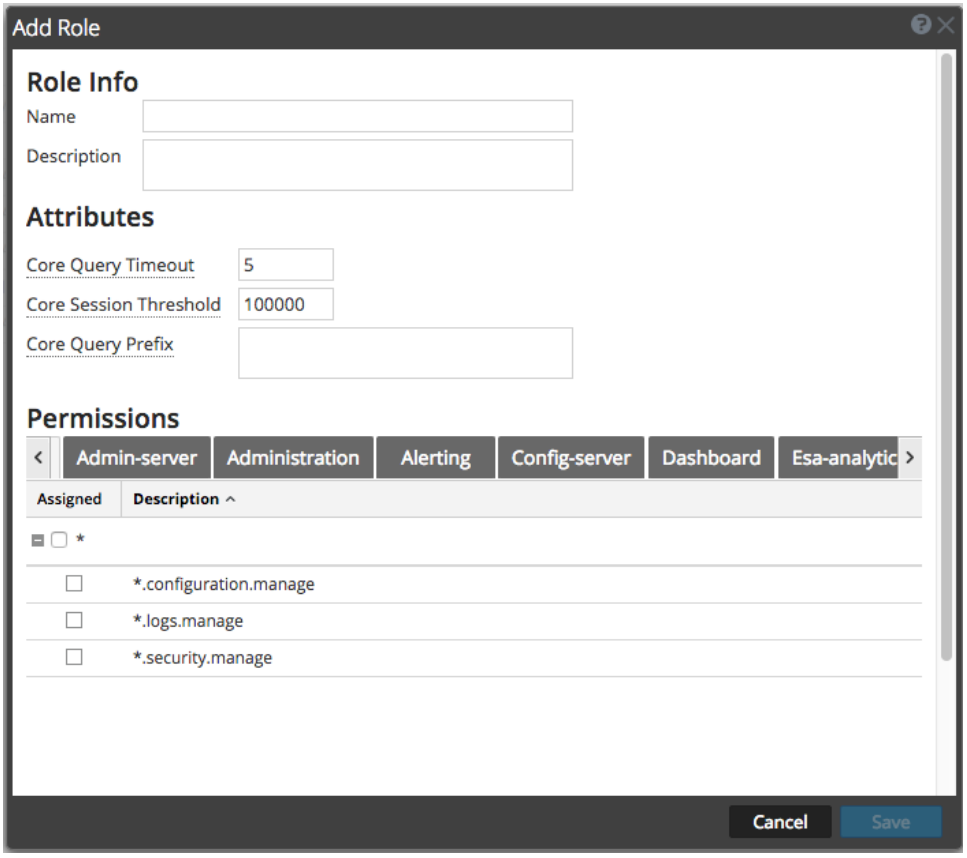
Pour accéder à cet onglet :

1. Accédez à **ADMIN Sécurité**.
   La vue Sécurité s'affiche avec l'onglet **Utilisateurs** ouvert.
2. Cliquez sur l'onglet **Rôles**.



Ajouter un rôle et attribuer des autorisations

1. Sous l'onglet **Rôles**, cliquez sur ✚ dans la barre d'outils.
2. La boîte de dialogue **Ajouter un Rôle** apparaît.



3. Dans la section **Attributs**, saisissez les informations suivantes pour le rôle :
   - **Nom**
   - (Facultatif) **Description**
4. Dans la section **Attributs**, entrez les valeurs souhaitées pour chaque attribut. Pour plus d'informations sur les attributs, reportez-vous à l'Étape 3. Vérifier les attributs Requête (Query) et Session par rôle.
5. Dans la section **Autorisations** :
   - Cliquez sur ‹ et › pour parcourir les modules.
   - Sélectionnez le module auquel le rôle accèdera.
   - Sélectionnez chacune des autorisations dont disposera le rôle.

6. Répétez les étapes précédentes jusqu'à ce que vous sélectionniez toutes les autorisations à attribuer au rôle.
7. Cliquez sur **Enregistrer** pour ajouter le nouveau rôle, qui est effectif immédiatement. Vous pouvez maintenant attribuer le nouveau rôle aux utilisateurs.

Dupliquer le rôle

Un moyen efficace d'ajouter un nouveau rôle est de dupliquer un rôle similaire, de l'enregistrer sous un nouveau nom et de réviser les autorisations qui sont déjà attribuées.

1. Sous l'onglet **Rôles**, sélectionnez le rôle à dupliquer, puis cliquez sur .
2. Saisissez le nom du nouveau rôle et cliquez sur **Enregistrer**.
3. Pour modifier les autorisations, suivez les étapes de la procédure suivante.

Modifier les autorisations attribuées à un rôle

1. Dans l'onglet **Rôles**, sélectionnez le rôle souhaité et cliquez sur .
   La boîte de dialogue **Modifier un rôle** apparaît.
2. Dans la section **Autorisations** :
   - Cliquez sur et pour parcourir les modules.
   - Sélectionnez un module pour réviser ses autorisations.
   - Sélectionnez ou désélectionnez chaque autorisation.
3. Répétez l'étape précédente jusqu'à ce que le rôle dispose des autorisations nécessaires.
4. Cliquez sur **Enregistrer**. Les autorisations révisées prennent effet immédiatement.

Supprimer un rôle

Vous pouvez supprimer un rôle s'il n'est attribué à aucun utilisateur.

1. Sous l'onglet **Rôles**, sélectionnez le rôle, puis cliquez sur .
2. Vous êtes ensuite invité à confirmer la suppression du rôle. Cliquez sur **Oui**.

Étape 3. Vérifier les attributs Requête (Query) et Session par rôle

Cette rubrique décrit les attributs Requête (Query) et Session, et fournit des instructions pour configurer ces attributs pour les rôles d'utilisateur. Cette rubrique décrit également comment ces paramètres de rôles ont un impact sur chaque paramètre utilisateur, et ce qui se produit si un utilisateur détient plusieurs rôles.

Après avoir défini vos rôles d'utilisateur, vous devez vérifier les attributs de requête et de session configurés pour chacun. Vous pouvez les ajuster en fonction de vos exigences.

Attributs Requête (Query) et Session

Les attributs de requête et de session déterminent la façon dont les requêtes exécutées par un utilisateur sont gérées. Ces attributs vous permettent de verrouiller les informations que les utilisateurs peuvent récupérer. Ces attributs s'appliquent à toutes les sessions des utilisateurs affectés à un rôle.

En fonction de vos exigences, vous pouvez préciser les attributs de gestion des requêtes suivants pour un rôle d'utilisateur :

- **Expiration du délai de requête de base** est un paramètre facultatif qui s'applique aux services de base de NetWitness Suite 10.5 et à toute version ultérieure. Il spécifie le nombre maximal de minutes durant lesquelles un utilisateur peut exécuter une requête. Si cette valeur est définie, elle doit correspondre à zéro (0) ou une valeur supérieure. Une valeur zéro signifie qu'il n'y a aucun délai.
- **Seuil de session de base** est un paramètre obligatoire. Cette valeur doit être égale à zéro (0) ou une valeur supérieure. Si le seuil est supérieur à zéro, une optimisation de requête extrapole le nombre total de sessions qui dépasse le seuil. Si la valeur des métadonnées renvoyée par la requête atteint le seuil, le système :
  - Arrête la détermination du nombre de sessions
  - Affiche le seuil et le pourcentage du temps de requête utilisé pour atteindre le seuil
- **Préfixe de requête de base** est un filtre facultatif appliqué aux requêtes exécutées par l'utilisateur. Le préfixe restreint les résultats des requêtes accessibles à l'utilisateur. Par exemple, le préfixe de requête `'service' = 80` précède les requêtes exécutées par l'utilisateur et ce dernier ne peut accéder qu'aux métadonnées des sessions HTTP.

Les paramètres des attributs de gestion des requêtes appliqués à un utilisateur dépendent des appartenances aux rôles de l'utilisateur. Il est important de vérifier les paramètres des attributs de gestion des requêtes pour vos rôles.

Comment les paramètres des attributs de gestion des requêtes s'appliquent aux utilisateurs individuels

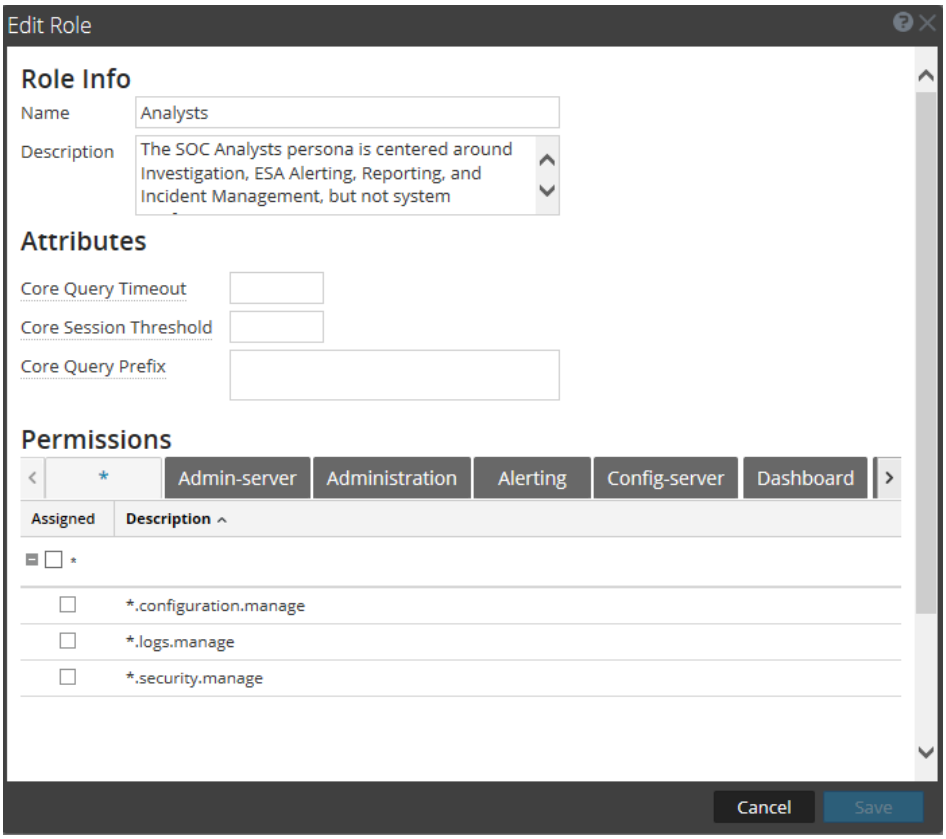
Si un utilisateur a plusieurs rôles, la logique suivante s'applique :

- **Délai d'expiration de la requête :** La valeur la plus permissive (élevée) de tous les rôles attribués s'applique à l'utilisateur.
- **Préfixe de requête :** Les préfixes de requête de chacun des rôles d'utilisateur sont associés.
- **Seuil de session :** La valeur la plus élevée de tous les rôles attribués s'applique à l'utilisateur.

Procédure

Pour définir des attributs de gestion des requêtes pour un rôle d'utilisateur :

1. Accédez à **ADMIN > Sécurité**.
   La vue Sécurité s'affiche avec l'onglet **Utilisateurs** ouvert.
2. Cliquez sur l'onglet **Rôles**. Si vous ajoutez un rôle, cliquez sur . Si vous modifiez un rôle, sélectionnez le rôle, puis cliquez sur .
   La boîte de dialogue Ajouter ou modifier un rôle s'affiche.



3. Pour définir les attributs pour le rôle, dans la section **Attributs** :
   - (Facultatif) Dans le champ **Expiration du délai de requête de base**, saisissez le nombre maximal de minutes pendant lesquelles un utilisateur peut exécuter une requête. La valeur par défaut est 5 minutes. Ce délai s'applique uniquement aux requêtes exécutées depuis Investigation. Les services de base de NetWitness Suite 10.5 et des versions ultérieures utilisent ce champ.
     Lors de la migration vers NetWitness Suite 10.5 et versions ultérieures, s'il n'y a aucune valeur définie pour les rôles, 5 minutes est la valeur définie par défaut.
   - Saisissez un **seuil de session de base** pour le système afin d'arrêter la détermination du nombre de sessions. L'option par défaut est *100000*. La limite que vous renseignez ici remplace la valeur du **Nb Max exports de session** définie dans les paramètres de la vue ENQUÊTER.
   - (Facultatif) Saisissez un **Préfixe de requête de base** pour filtrer les résultats de requête vus par les membres de rôle. Par défaut, le champ est vide.

   Remarque : Une valeur en italique indique une valeur par défaut, par exemple *5*. Une valeur qui n'est pas en italique indique un changement de la valeur par défaut, par exemple `1200`.

4. Cliquez sur **Enregistrer**.

Étape 4. Configurer un utilisateur

Cette rubrique présente les procédures permettant de configurer un nouvel utilisateur.

Rubriques

- Ajouter un utilisateur et attribuer un rôle
- Activer, déverrouiller et supprimer des comptes d'utilisateur

Ajouter un utilisateur et attribuer un rôle

Cette rubrique explique comment ajouter un nouvel utilisateur pour chaque type de compte d'utilisateur, local et externe. Elle explique également comment attribuer un rôle à un utilisateur local.

Tous les utilisateurs NetWitness Suite doivent disposer d'un compte utilisateur local ou externe.

Les éléments suivants doivent être pris en compte lors de la gestion de comptes utilisateur locaux et externes.

Compte utilisateur local	Compte utilisateur externe
Géré au sein de NetWitness Suite	Géré en externe et en dehors du cadre de ce document.
Rôles attribués directement	Rôles attribués par le mappage de groupe externe
Autorisations issues de chaque rôle attribué à l'utilisateur, comme expliqué dans cette rubrique	Autorisations issues de chaque rôle mappé au groupe d'utilisateurs externe du compte, comme expliqué dans l'Étape 5. (Facultatif) Mapper des rôles d'utilisateur aux groupes externes.
NetWitness Suite gère toutes les informations utilisateur.	NetWitness Suite gère uniquement l'identification utilisateur. Cela comprend le nom d'utilisateur, le nom complet et l'e-mail.

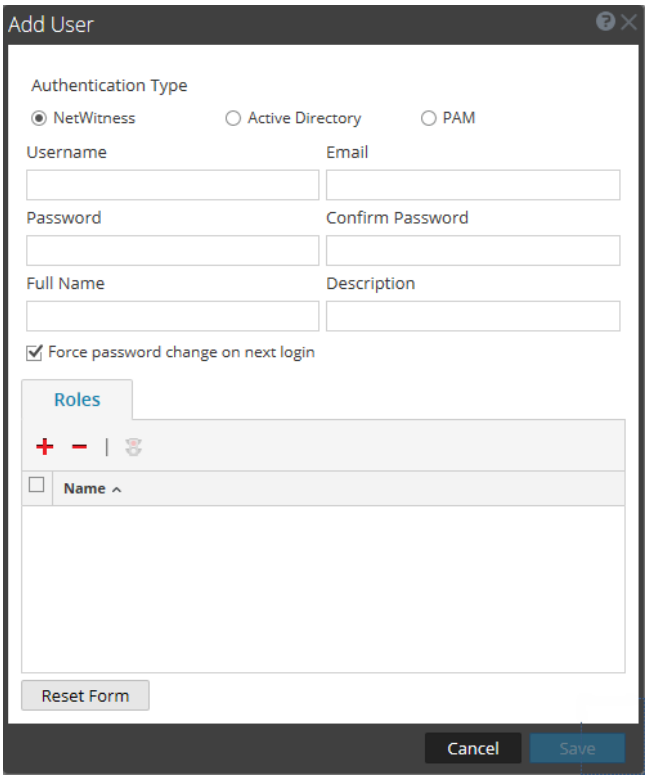
Procédures

Chacune des procédures suivantes commence sous l'onglet Utilisateurs. Pour accéder à l'onglet Utilisateurs, accédez à **ADMIN > Sécurité**. La vue Sécurité s'affiche avec l'onglet Utilisateurs ouvert.

Ajouter un utilisateur et attribuer un rôle

Pour ajouter un compte utilisateur local et attribuer un rôle à l'utilisateur :

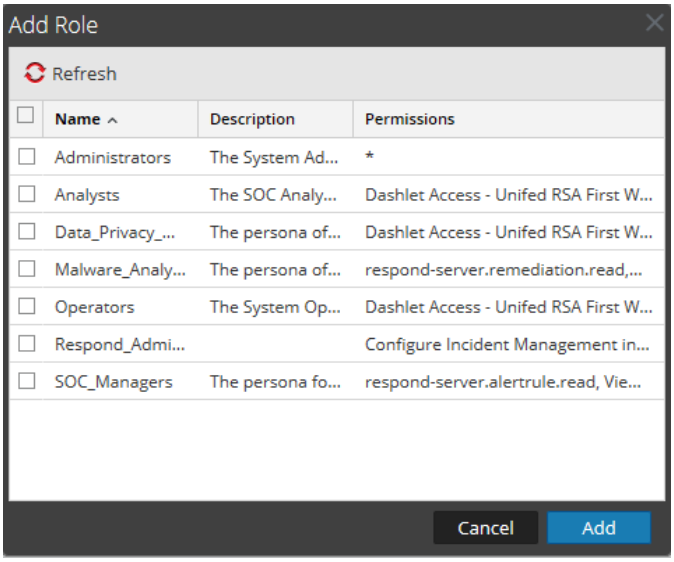
1. Sous l'onglet **Utilisateurs**, cliquez sur  dans la barre d'outils.
   La boîte de dialogue **Ajouter un utilisateur** s'affiche.



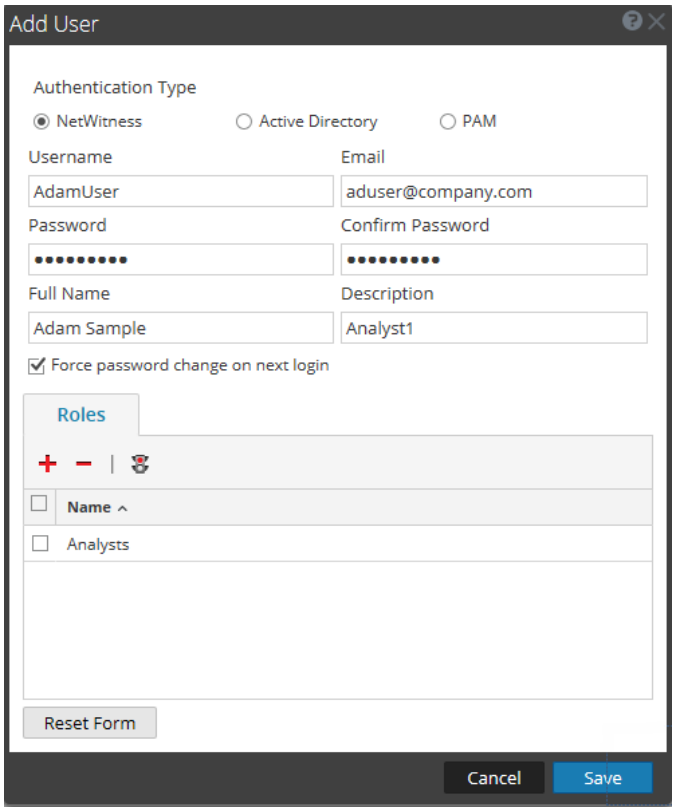
2. Indiquez les informations de compte suivantes pour le nouvel utilisateur :
   - **Type d'authentification** : **NetWitness** est sélectionné par défaut et est le bon choix lors de l'ajout d'un utilisateur local. Cette option s'affiche uniquement lorsqu'il existe des configurations Active Directory ou PAM définies afin de permettre la sélection de ce type d'authentification. S'il n'existe aucune configuration Active Directory ou PAM, le type d'authentification est défini automatiquement sur NetWitness et il n'existe pas d'autres options disponibles.
   - **Nom d'utilisateur** pour la consignation dans NetWitness Suite
   - **Adresse e-mail**
   - Mot de passe pour la connexion à NetWitness Suite, dans les champs**Mot de passe** et **Confirmer le mot de passe**
   - **Nom complet** du nouvel utilisateur
   - (Facultatif) **Description** du compte d'utilisateur
3. Pour faire expirer le mot de passe de l'utilisateur avant la prochaine connexion, sélectionnez **Forcer le changement du mot de passe à la prochaine connexion**.
   Cela n'affecte pas les sessions utilisateur actives. L'icône s'affiche dans la ligne de

l'utilisateur pour montrer que le mot de passe de l'utilisateur a expiré. Une fois le mot de passe expiré, il est impossible de l'annuler. Cette case est décochée à la prochaine modification du compte d'utilisateur.

4. Pour attribuer un rôle à l'utilisateur, cliquez sur + sous l'onglet **Rôles**.
   La boîte de dialogue de sélection **Ajouter un rôle** affiche la liste des rôles disponibles.

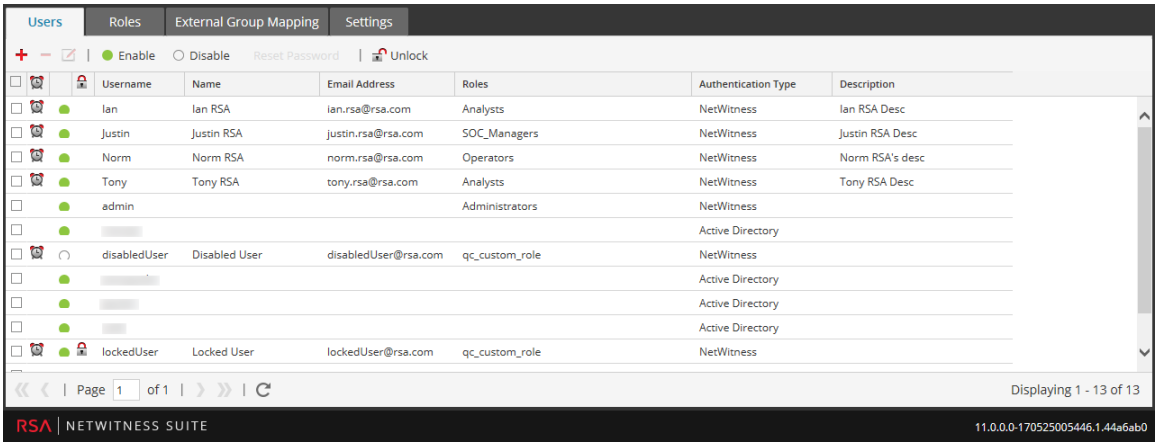


5. Sélectionnez chaque rôle à attribuer, puis cliquez sur **Ajouter**.
   La boîte de dialogue **Ajouter un utilisateur** affiche chaque rôle à attribuer à l'utilisateur.



6. (Facultatif) Sélectionnez un rôle et cliquez sur pour **Afficher toutes les autorisations** pour le rôle.

7. Cliquez sur **Enregistrer**.
   L'onglet **Utilisateurs** affiche le nouvel utilisateur et chaque rôle qui lui est attribué. Le compte est immédiatement actif.

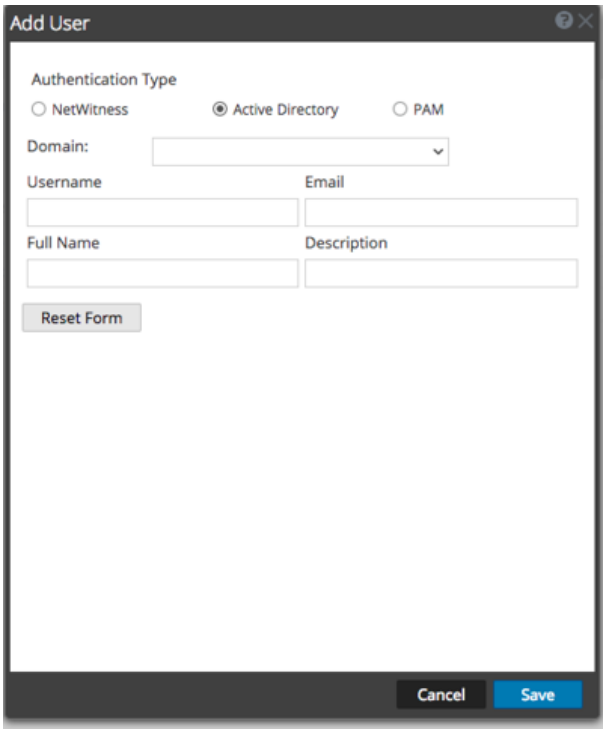


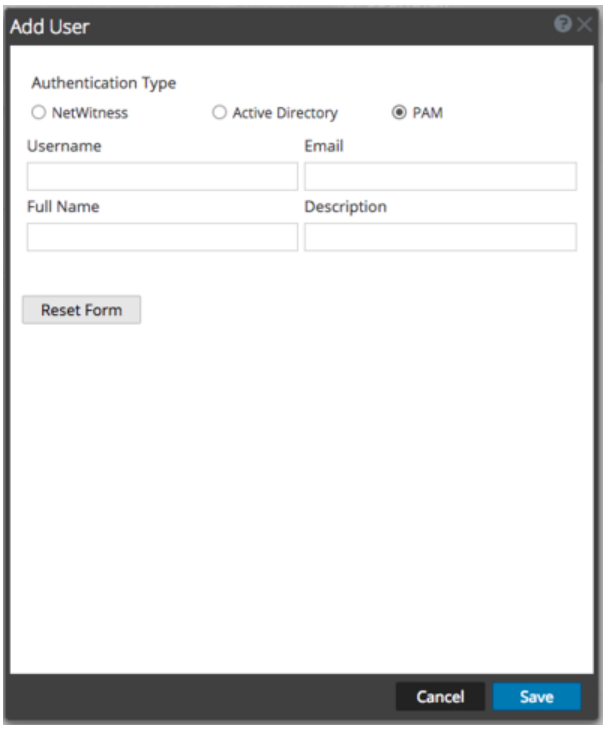
Ajouter un utilisateur pour authentification externe

Condition préalable : L'authentification externe doit être configurée. Reportez-vous à l'Étape 4. (Facultatif) Configurer l'authentification externe.

Pour ajouter un utilisateur authentifié de façon externe, en dehors de NetWitness Suite :

1. Sous l'onglet **Utilisateurs**, cliquez sur + dans la barre d'outils.
   La boîte de dialogue **Ajouter un utilisateur** s'affiche.
2. Pour **Type d'authentification**, sélectionnez soit **Active Directory** soit **PAM**. La boîte de dialogue s'actualise pour afficher les champs obligatoires pour le type d'authentification externe sélectionné.





3. Indiquez les informations suivantes :
   - **Domaine** (si vous sélectionnez l'authentification Active Directory uniquement) : Sélectionnez le domaine Active Directory pour l'utilisateur dans la liste déroulante des domaines disponibles.
   - **Nom d'utilisateur** pour la consignation dans NetWitness Suite
   - **Adresse e-mail**
   - **Nom complet** du nouvel utilisateur
   - (Facultatif) **Description** du compte d'utilisateur
4. Cliquez sur **Enregistrer.** L'onglet Utilisateurs affiche le nouveau compte utilisateur auquel un rôle et des autorisations doivent être attribués.
5. Pour mapper un rôle vers le nouvel utilisateur, reportez-vous à l'Étape 5. (Facultatif) Mapper des rôles d'utilisateur aux groupes externes.

Modifier les informations utilisateur ou les rôles

Pour modifier les informations de compte d'un utilisateur ou les rôles qui lui sont attribués :

1. Sous l'onglet **Utilisateurs**, sélectionnez un utilisateur, puis cliquez sur dans la barre d'outils.La boîte de dialogue **Modifier l'utilisateur** s'affiche.

2. Pour modifier les informations utilisateur, modifiez l'un des champs suivants :
   - **E-mail**
   - **Nom complet**
   - **Description**
3. Pour faire expirer le mot de passe d'un utilisateur **interne** avant la prochaine connexion, sélectionnez **Forcer le changement du mot de passe à la prochaine connexion**.
   Cela n'affecte pas les sessions utilisateur actives. L'icône  s'affiche dans la ligne de l'utilisateur pour montrer que le mot de passe de l'utilisateur a expiré. Une fois le mot de passe expiré, il est impossible de l'annuler. Cette case est décochée à la prochaine modification du compte d'utilisateur.
4. Dans la section **Rôles** :
   - Pour attribuer un autre rôle, cliquez sur +, sélectionnez un rôle, puis cliquez sur **Ajouter**.
   - Pour retirer un rôle attribué, sélectionnez le rôle, puis cliquez sur −.
5. Cliquez sur **Enregistrer**.

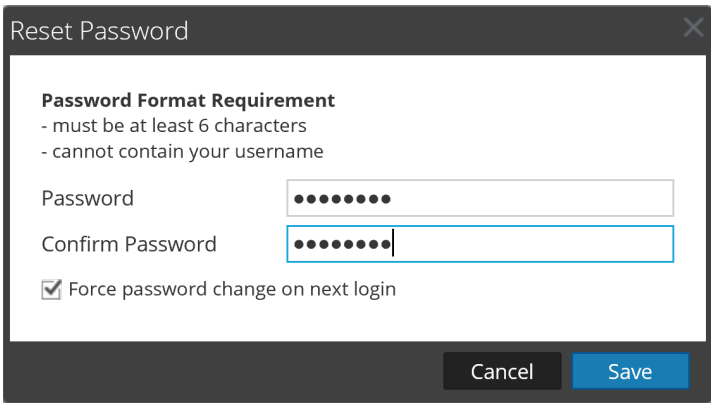
Supprimer un utilisateur

1. Sous l'onglet **Utilisateurs**, sélectionnez un utilisateur.
2. Dans la barre d'outils, cliquez sur −.
3. Cliquez sur **Enregistrer**.

Remarque : Pour supprimer complètement un utilisateur authentifié de façon externe par Active Directory, vous devez également supprimer l'utilisateur du groupe AD.

Réinitialiser le mot de passe de l'utilisateur

1. Sous l'onglet **Utilisateurs**, sélectionnez un utilisateur.
2. Dans la barre d'outils, cliquez sur **Réinitialiser le mot de passe**.



   La section **Exigence de format de mot de passe** répertorie les exigences spécifiques pour le mot de passe. Les administrateurs peuvent modifier ces exigences pour tous les utilisateurs internes dans la stratégie de mot de passe. Reportez-vous à l'Étape 1. Configurer la complexité des mots de passe.

3. Indiquez si vous souhaitez imposer un changement de mot de passe lors de la prochaine connexion d'un utilisateur à NetWitness Suite.
4. Cliquez sur **Enregistrer**.

Activer, déverrouiller et supprimer des comptes d'utilisateur

Cette rubrique fournit des instructions pour activer, déverrouiller et supprimer des comptes d'utilisateur.

Tous les utilisateurs de NetWitness Suite doivent avoir un compte utilisateur local avec un nom d'utilisateur et un mot de passe, ou avoir un compte utilisateur externe. Dans NetWitness Suite, vous pouvez activer, désactiver et supprimer des comptes utilisateur locaux.

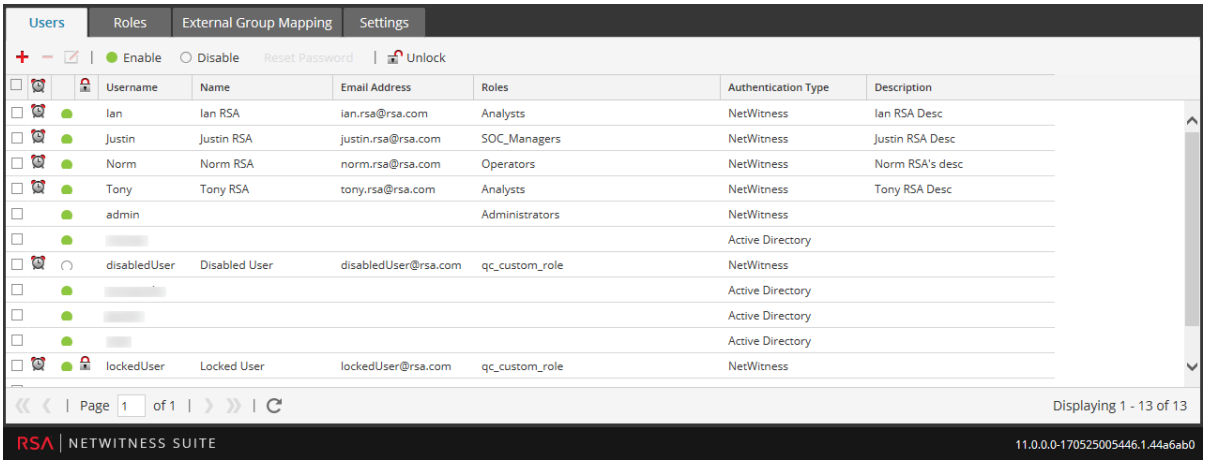
La première fois qu'un utilisateur externe se connecte à NetWitness Suite, une nouvelle entrée d'utilisateur est automatiquement créée avec NetWitness Suite. NetWitness Suite gère uniquement les informations d'identification utilisateur ; par exemple, son nom complet et son adresse e-mail.

Vous pouvez déverrouiller des comptes verrouillés pour les utilisateurs locaux et externes.

Activer les comptes utilisateur NetWitness Suite désactivés

Pour activer les comptes utilisateur NetWitness Suite qui ont été désactivés :

1. Dans NetWitness Suite, accédez à **ADMIN Sécurité**.
   La vue Sécurité s'affiche avec l'onglet **Utilisateurs** ouvert.



2. Dans la grille **Utilisateurs**, sélectionnez un ou plusieurs comptes.
3. Cliquez sur Enable.
   Une boîte de dialogue demande confirmation.
4. Si vous voulez activer les comptes, cliquez sur **Oui**.
   Les comptes sont activés et l'utilisateur peut se connecter à NetWitness Suite.

Désactiver les comptes utilisateur NetWitness Suite

Vous pouvez bloquer l'accès utilisateur en désactivant des utilisateurs. La désactivation de l'utilisateur ne supprime pas les préférences de l'utilisateur. Cette action bloque l'accès des utilisateurs sans supprimer les préférences utilisateur, de sorte qu'au moment de leur réactivation, les préférences des utilisateurs sont intactes. Vous pouvez réactiver les utilisateurs pour restaurer l'accès utilisateur. La désactivation d'utilisateurs s'applique uniquement aux utilisateurs locaux et non à ceux externes.

Pour désactiver des comptes utilisateur NetWitness Suite :

1. Dans la grille **Utilisateurs**, sélectionnez un ou plusieurs comptes.
2. Cliquez sur Disable.

   Une boîte de dialogue demande confirmation.
3. Si vous voulez désactiver les comptes, cliquez sur **Oui**.

   Les comptes sont désactivés et l'utilisateur ne peut plus se connecter à NetWitness Suite.

Déverrouiller les comptes utilisateur NetWitness Suite verrouillés

Un utilisateur est verrouillé pour une certaine période de temps après un certain nombre d'échecs de tentatives de connexion consécutifs. Pour déverrouiller des comptes utilisateur NetWitness Suite qui sont verrouillés en raison d'un nombre trop important d'échecs de tentatives de connexion :

1. Dans la grille **Utilisateurs**, sélectionnez un ou plusieurs comptes.
2. Cliquez sur Unlock.

   Une boîte de dialogue demande confirmation.
3. Si vous voulez déverrouiller les comptes, cliquez sur **Oui**.

   Les comptes sont débloqués et l'utilisateur peut se connecter à NetWitness Suite.

Supprimer des comptes utilisateur NetWitness Suite

Si vous n'utilisez pas l'authentification externe, un utilisateur peut se connecter à NetWitness Suite à l'aide d'un compte local. Ces comptes locaux sont gérés directement avec NetWitness Suite. Pour révoquer l'accès à un utilisateur local, désactivez le compte ou supprimez-le entièrement du système.

Remarque : Cela supprime tous les préférences utilisateur pour le compte à partir de NetWitness Suite. Si telle n'est pas votre intention, désactivez l'utilisateur au lieu de le supprimer.

Pour supprimer des comptes utilisateur NetWitness Suite :

1. Accédez à **ADMIN > Sécurité**.
   La vue Sécurité s'affiche avec l'onglet **Utilisateurs** ouvert.
2. Dans la grille Utilisateurs, sélectionnez un ou plusieurs comptes.
3. Cliquez sur .
   Une boîte de dialogue d'avertissement demande confirmation.
4. Si vous voulez supprimer les comptes, cliquez sur **Oui**.
   Les comptes sont supprimés de NetWitness Suite et les utilisateurs ne peuvent plus se connecter à NetWitness Suite.

Étape 5. (Facultatif) Mapper des rôles d'utilisateur aux groupes externes

Cette rubrique décrit les méthodes permettant de mapper les rôles d'utilisateur NetWitness Suite à des groupes externes.

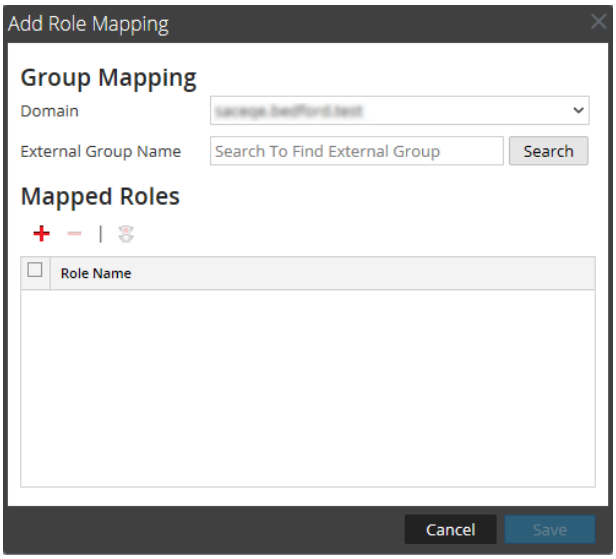
Dans NetWitness Suite, les groupes externes font dériver des autorisations pour différents modules et vues de rôles d'utilisateur NetWitness Suite, qui possèdent les autorisations qui leur sont attribuées. Pour fournir l'accès à un groupe externe, mappez-y les rôles d'utilisateur. Pour modifier l'accès d'un groupe externe, modifiez les rôles qui y sont mappés. Ajoutez et supprimez des rôles jusqu'à ce que le groupe externe possède l'accès nécessaire. Les modifications prennent effet immédiatement.

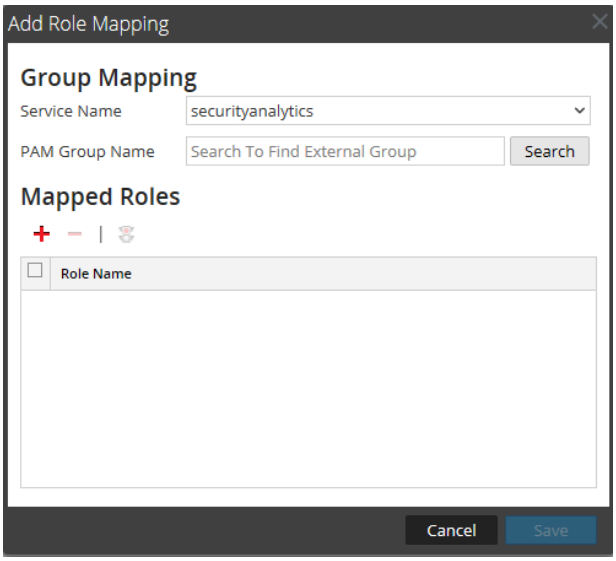
Conditions préalables

Sous l'onglet Paramètres, vous devez définir une méthode pour que l'authentification d'utilisateur externe rende les groupes externes visibles pour NetWitness Suite.

Ajouter un mappage de rôle à un groupe externe

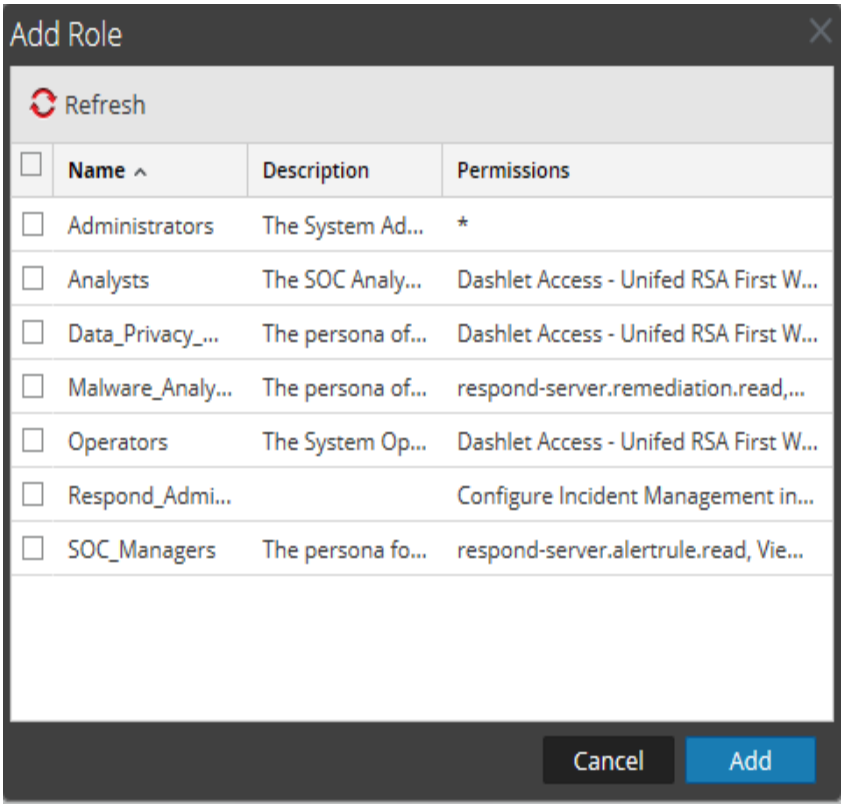
1. Dans NetWitness Suite, accédez à **ADMIN > Sécurité**.
   La vue Sécurité s'affiche avec l'onglet **Utilisateurs** ouvert.
2. Cliquez sur l'onglet **Mappage de groupe externe**.
3. Dans la barre d'outils cliquez sur +.
   La boîte de dialogue **Ajouter un mappage de rôle** pour la méthode d'authentification externe que vous avez sélectionnée s'affiche.





4. Cliquez sur **Rechercher** et recherchez le nom de groupe externe dans Rechercher les groupes externes, puis sélectionnez un nom de groupe externe.

5. Pour ajouter des rôles au mappage de groupe, cliquez sur + dans la section **Rôles mappés**.
   La boîte de dialogue **Ajouter un Rôle** apparaît.



6. Cochez la case dans la barre de titre pour sélectionner tous les rôles ou sélectionner des rôles individuellement.
7. Pour ajouter les rôles à la section **Rôles mappés** dans la boîte de dialogue Ajouter un mappage de rôle, cliquez sur **Ajouter**.
   La boîte de dialogue se ferme et les rôles sélectionnés s'affichent dans la section Rôles mappés.
8. Si vous souhaitez supprimer des rôles de la section **Rôles mappés**, sélectionnez les rôles et cliquez sur − .
9. Lorsque la boîte de dialogue **Ajouter un mappage de rôles** reflète le mappage de rôle que vous souhaitez définir pour le groupe, cliquez sur **Enregistrer**.
   La boîte de dialogue Ajouter un mappage de rôle se ferme, et le nouveau mappage de rôle est répertorié dans la liste de l'onglet Mappage de groupe externe.

Modifier un mappage de rôle pour un groupe

1. Dans la barre d'action **Mappage de groupe externe**, cliquez sur **Modifier**.
   La boîte de dialogue **Modifier le mappage de rôle** s'affiche avec le nom du groupe dans le champ **Nom du groupe externe**.
2. Pour ajouter des rôles au mappage, cliquez sur + dans la section **Rôles mappés**.
   La boîte de dialogue Ajouter un rôle apparaît.
3. Cochez la case dans la barre de titre pour sélectionner tous les rôles ou sélectionner des rôles individuellement.
4. Pour ajouter les rôles à la section **Rôles mappés** dans la boîte de dialogue **Ajouter un mappage de rôle**, cliquez sur **Ajouter**.
   La boîte de dialogue se ferme et les rôles sélectionnés s'affichent dans la section Rôles mappés.
5. Si vous souhaitez supprimer des rôles de la section **Rôles mappés**, sélectionnez les rôles et cliquez sur − .
6. Lorsque la boîte de dialogue **Modifier le mappage de rôle** reflète le mappage de rôle que vous souhaitez définir pour le groupe, cliquez sur **Enregistrer**.
   La boîte de dialogue se ferme, et le mappage de rôle modifié est répertorié dans l'onglet Mappage de groupe externe.

Rubrique connexe

- Rechercher les groupes externes

Rechercher les groupes externes

Cette rubrique donne des instructions sur la façon de rechercher les groupes externes auxquels sont mappés des rôles d'utilisateur NetWitness Suite.

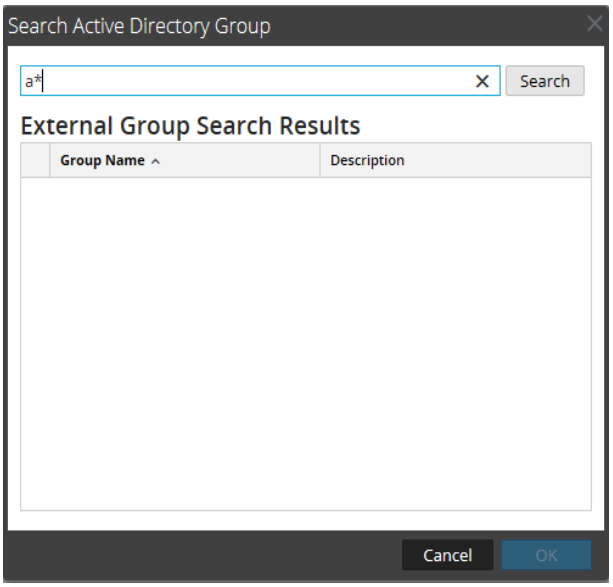
Conditions préalables

Une méthode d'authentification d'utilisateur externe doit être activée.

Procédure

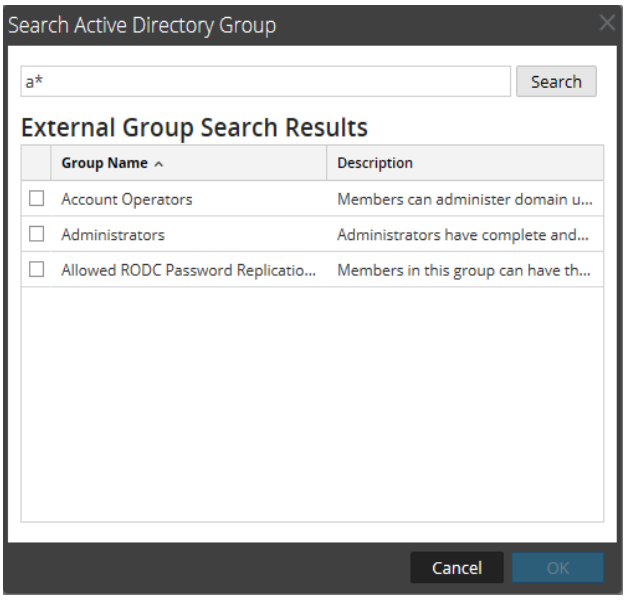
Pour rechercher un groupe externe :

1. Dans NetWitness Suite, accédez à **ADMIN > Sécurité**.
   La vue Sécurité s'affiche avec l'onglet **Utilisateurs** ouvert.
2. Cliquez sur l'onglet **Mappage de groupe externe**.
3. Dans la barre d'outils, cliquez sur + ou .
   La boîte de dialogue **Ajouter un mappage de rôle** pour la méthode d'authentification externe que vous avez sélectionnée s'affiche.
4. La section **Mappage de groupes** dépend de la méthode d'authentification externe sélectionnée.
   - Pour **Active Directory**, sélectionnez un **Domaine**. Cliquez ensuite sur **Rechercher** à côté de **Nom du groupe externe**.
   - Pour **PAM**, cliquez sur **Rechercher** à côté de **Nom du groupe PAM**.
     La boîte de dialogue **Rechercher les groupes externes** s'affiche.
5. Dans **Nom de domaine complet**, saisissez un nom de groupe ou une partie de nom de groupe en y ajoutant le caractère générique (*).



6. Cliquez sur **Rechercher**.

   Les résultats s'affichent dans la section **Résultats de la recherche de groupes externes**.



7. Sélectionnez le groupe auquel attribuer les rôles et cliquez sur **OK**.

Références

Cette rubrique regroupe des références pour la sécurité du système et la gestion des utilisateurs dans NetWitness Suite.

Rubriques

Vue Admin - Sécurité

Cette rubrique décrit tous les éléments d'interface utilisateur de la vue Administration > Sécurité et de tous les onglets et boîtes de dialogue qui lui sont associés. Les composants de l'interface sont répertoriés par ordre alphabétique.

La vue Administration - Sécurité permet de gérer les comptes utilisateur et les rôles d'utilisateur, de mapper les groupes externes aux rôles NetWitness Suite et de modifier les autres paramètres du système liés à la sécurité. Ces paramètres s'appliquent au système NetWitness Suite et sont utilisés parallèlement aux paramètres de sécurité des différents services.

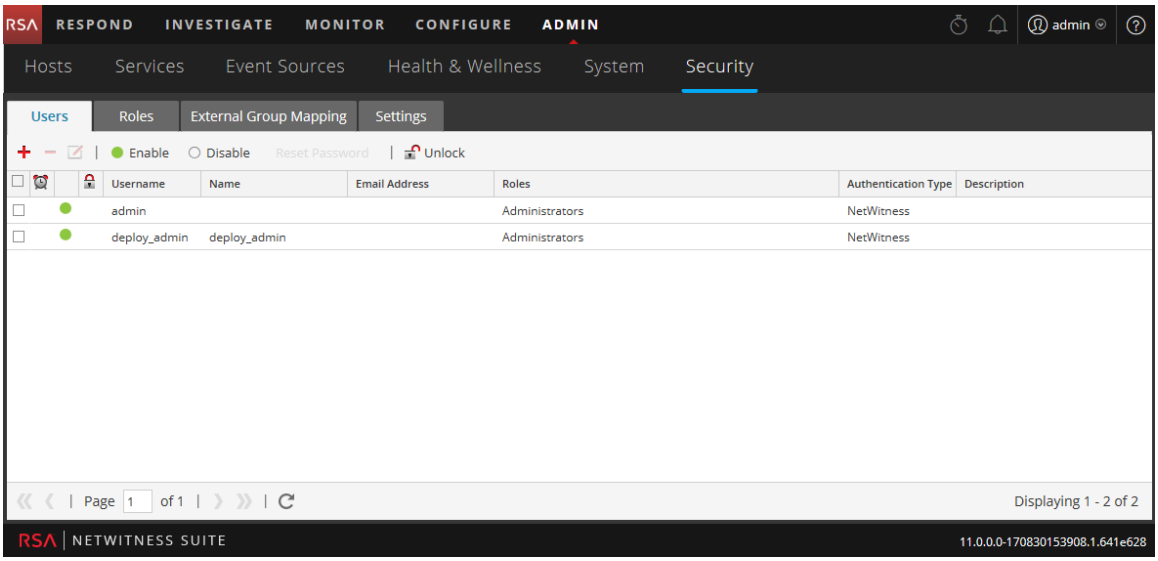
Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Admin	Gérer les utilisateurs	Étape 4. Configurer un utilisateur
Admin	Gérer les rôles	Étape 1. Passer en revue les rôles préconfigurés NetWitness Étape 2. (Facultatif) Ajouter un rôle et attribuer des autorisations
Admin	(Facultatif) Configurer les mappages de groupes externes	Étape 5. (Facultatif) Mapper des rôles d'utilisateur aux groupes externes
Admin	Configurer les paramètres	Étape 3. Configurer les paramètres de sécurité au niveau du système

Rubriques connexes

- Onglet Utilisateurs
- Onglet Rôles
- Onglet Mappage de groupe externe
- Onglet Paramètres

Pour afficher la vue de la sécurité de l'administrateur, accédez à **ADMIN > sécurité**.



La vue Admin > Sécurité contient quatre onglets :

- L'onglet **Utilisateurs** permet de gérer les comptes utilisateur.
- L'onglet **Rôles** permet de définir les rôles de sécurité et de les attribuer aux comptes utilisateur.
- L'onglet **Mappage de groupe externe** permet de gérer les paramètres d'accès aux groupes LDAP.
- L'onglet **Paramètres** permet de configurer la complexité et l'expiration des mots de passe des utilisateurs NetWitness Suite internes, ainsi que le comportement du système face aux échecs de connexion et à l'inactivité. Cet onglet permet aussi de configurer l'authentification externe.

Onglet Utilisateurs

Cette rubrique présente les caractéristiques et les fonctions de configuration d'un compte utilisateur dans la vue Admin > Sécurité > onglet Utilisateurs.

Chaque utilisateur NetWitness Suite doit disposer d'un compte utilisateur. Sous l'onglet Utilisateurs, vous pouvez créer, modifier, supprimer, activer/désactiver et déverrouiller un compte utilisateur.

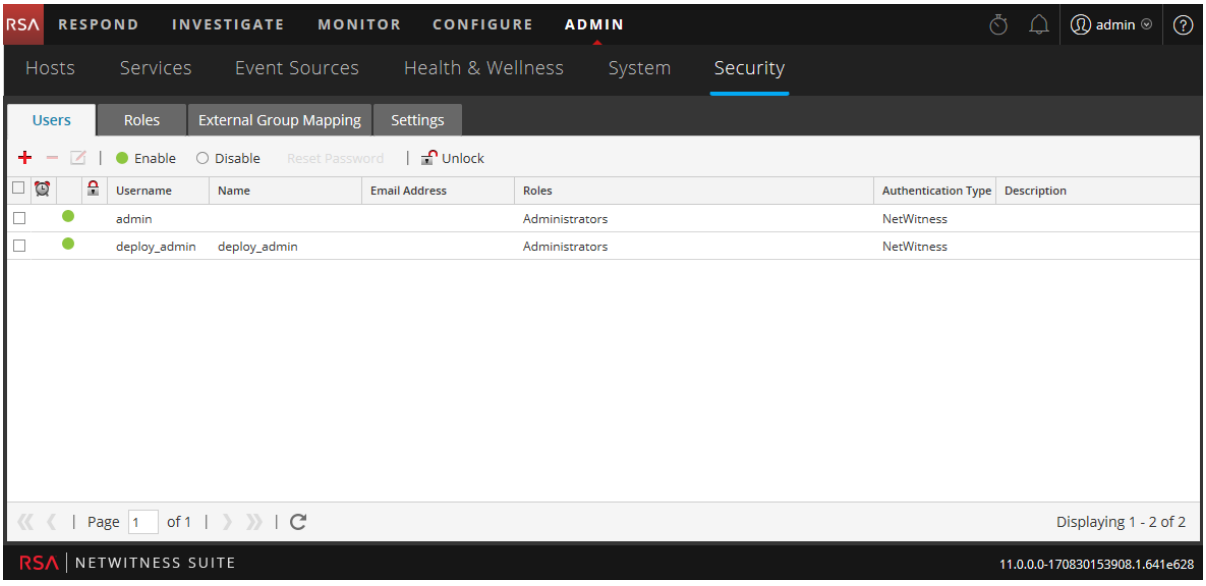
Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Admin	Configurer un nouvel utilisateur	Étape 4. Configurer un utilisateur Ajouter un utilisateur et attribuer un rôle
Admin	Gérer les comptes utilisateurs	Activer, déverrouiller et supprimer des comptes d'utilisateur

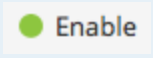
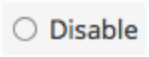
Rubriques connexes

- Boîte de dialogue Ajouter ou modifier un utilisateur

Pour accéder à cette vue, accédez à **ADMIN > sécurité**. La vue sécurité s'ouvre sur le **utilisateurs** onglet par défaut.



L'onglet Utilisateurs se compose de la liste Utilisateurs avec une barre d'outils en haut. Voici les fonctions de la barre d'outils.

Fonctionnalité	Description
	Ouvrez la boîte de dialogue Ajouter un utilisateur.
	Supprime l'utilisateur sélectionné.
	Ouvre la boîte de dialogue Modifier l'utilisateur de l'utilisateur sélectionné.
	Active un compte utilisateur désactivé avec toutes les préférences utilisateur intactes.
	Bloque l'accès des utilisateurs sans supprimer les préférences utilisateur de sorte qu'au moment de leur réactivation, les préférences des utilisateurs sont intactes.
Réinitialiser le mot de passe	Ouvre la boîte de dialogue Réinitialiser le mot de passe qui vous permet de modifier le mot de passe de l'utilisateur sélectionné. Cette boîte de dialogue répertorie les exigences de format du mot de passe nécessaires de modifier le mot de passe et permet de forcer l'utilisateur à modifier leur mot de passe à la prochaine connexion.
 Déverrouiller	Débloque un compte utilisateur qui a été verrouillé en raison d'un nombre trop important de tentatives de connexion infructueuses.

La liste **Utilisateurs** comporte ces colonnes.

Colonne	Description
	Si cette icône apparaît dans une ligne d'utilisateur, elle indique que le mot de passe de l'utilisateur a expiré.
Nom d'utilisateur	Nom d'utilisateur pour la connexion à NetWitness Suite.
Nom	Nom de l'utilisateur auquel le compte appartient.

Colonne	Description
Adresse e-mail	Adresse e-mail de l'utilisateur.
Rôles	Rôle attribué à l'utilisateur.
Externe	Méthode d'authentification, qui peut être externe par Active Directory, PAM ou interne par NetWitness Suite.
Description	Description du compte utilisateur

Boîte de dialogue Ajouter ou modifier un utilisateur

Cette rubrique présente les boîtes de dialogue Ajouter un utilisateur et Modifier l'utilisateur, accessibles à partir de la vue Admin > Sécurité > onglet Utilisateurs.

Tous les utilisateurs doivent avoir un compte utilisateur local avec nom d'utilisateur et mot de passe, ou un compte utilisateur externe mappé à NetWitness Suite.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur	Ajouter un utilisateur et attribuer un rôle	Étape 2. (Facultatif) Ajouter un rôle et attribuer des autorisations
Administrateur	Modifier les informations utilisateur	Étape 2. (Facultatif) Ajouter un rôle et attribuer des autorisations
Administrateur	Réinitialiser le mot de passe de l'utilisateur	Étape 2. (Facultatif) Ajouter un rôle et attribuer des autorisations
Administrateur	Ajouter un utilisateur pour authentification externe	Étape 2. (Facultatif) Ajouter un rôle et attribuer des autorisations

Rubriques connexes

- Gérer les utilisateurs à l'aide de rôles et d'autorisations
- Activer, déverrouiller et supprimer des comptes d'utilisateur

Préférences utilisateur

Pour afficher la boîte de dialogue **Ajouter un utilisateur** ou **Modifier l'utilisateur** :

1. Dans NetWitness Suite, accédez à **ADMIN> Sécurité**.
   La vue Sécurité s'affiche avec l'onglet **Utilisateurs** ouvert.
2. Exécutez l'une des opérations suivantes :
   - Dans la barre d'action, cliquez sur  .
     La boîte de dialogue **Ajouter un utilisateur** s'affiche.

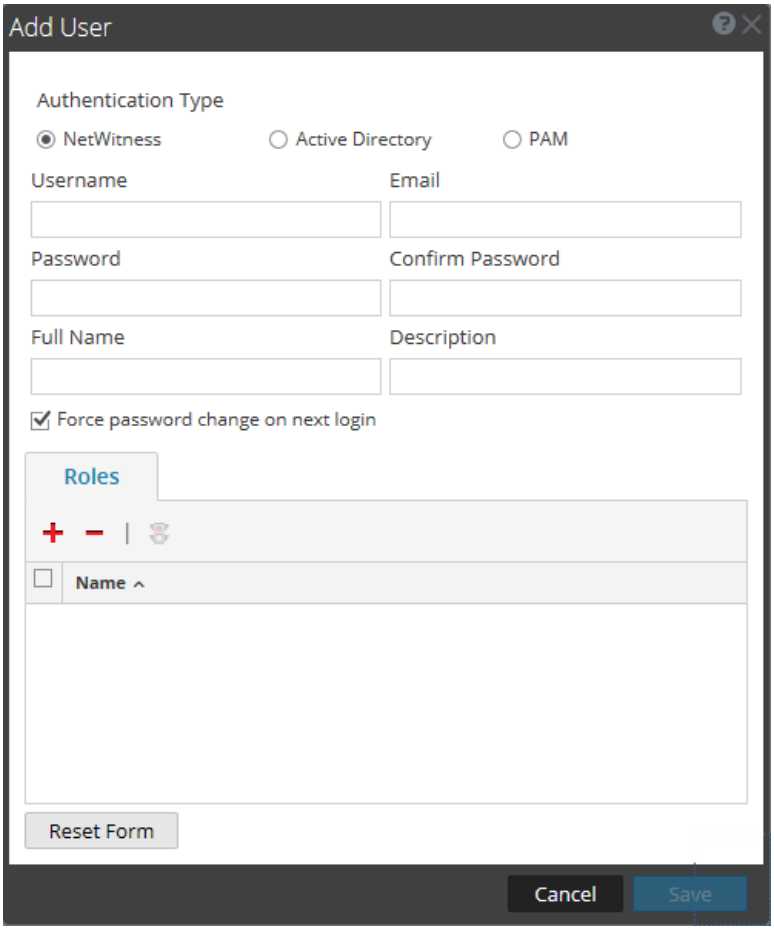
- Sélectionnez un utilisateur dans la barre d'action, cliquez sur .

  La boîte de dialogue **Modifier l'utilisateur** apparaît.

Les boîtes de dialogue Ajouter un utilisateur et Modifier l'utilisateur sont les mêmes, à ceci près que la boîte de dialogue Ajouter un utilisateur contient en plus les champs **Mot de passe** et **Confirmer le mot de passe**. Vous pouvez ajouter un mot de passe pour un nouvel utilisateur dans la boîte de dialogue Ajouter un utilisateur. Les utilisateurs peuvent changer leurs propres mots de passe dans les préférences utilisateur. Vous pouvez réinitialiser le mot de passe d'un utilisateur directement à partir de l'onglet Utilisateurs.

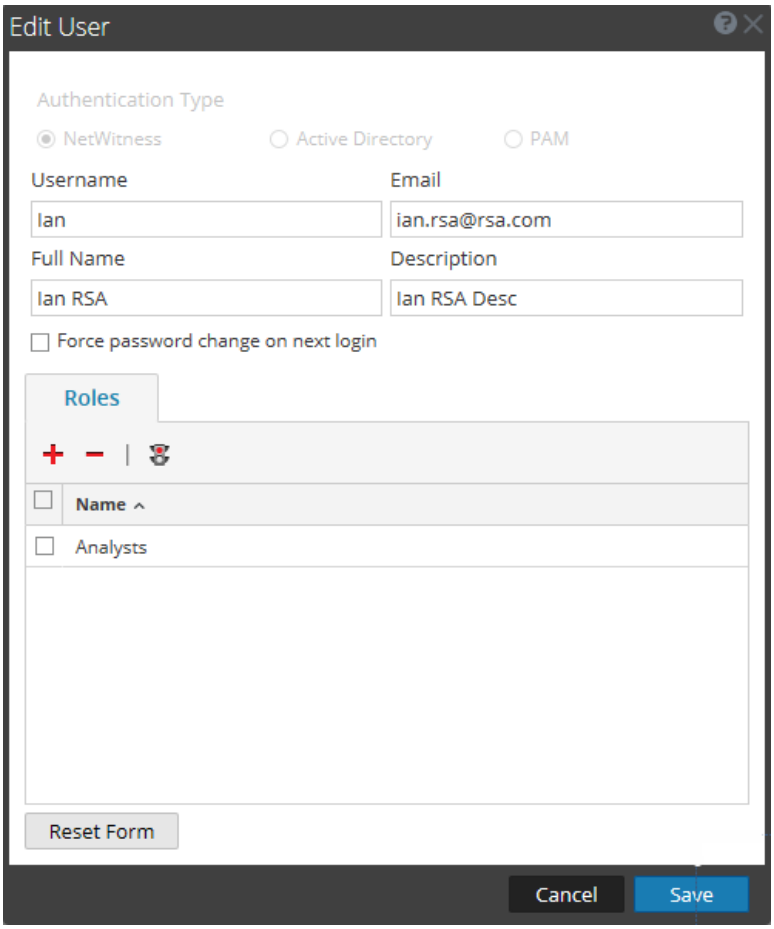
Boîte de dialogue Ajouter un utilisateur

Il s'agit de la boîte de dialogue Ajouter un utilisateur pour un utilisateur interne.



Boîte de dialogue Modifier l'utilisateur

Il s'agit de la boîte de dialogue Modifier l'utilisateur pour un utilisateur interne.



Les boîtes de dialogue Ajouter un utilisateur et Modifier l'utilisateur présentent les éléments suivants :

- Type d'authentification
- Informations utilisateur
- Rôles auxquels appartient l'utilisateur

Informations utilisateur

Le tableau suivant fournit les descriptions des informations utilisateur.

Champ	Description
Type d'authentification	Type d'authentification de l'utilisateur. La sélection par défaut est NetWitness, qui désigne un utilisateur interne. Les options pour les utilisateurs externes sont Active Directory et le PAM. Ce champ est désactivé lors de la modification d'un utilisateur.
Nom d'utilisateur	Nom d'utilisateur pour le compte utilisateur NetWitness Suite.
Nom complet	Nom de l'utilisateur.
Mot de passe	(Boîte de dialogue Ajouter un utilisateur uniquement) Mot de passe pour vous connecter à NetWitness Suite.
Confirmer le mot de passe	(Boîte de dialogue Ajouter un utilisateur uniquement) Confirmation du mot de passe pour l'ajout du mot de passe utilisateur.
E-mail	Adresse e-mail de l'utilisateur.
Description	(Facultatif) Description de l'utilisateur.
Forcer le changement du mot de passe à la prochaine connexion	Fait expirer le mot de passe de l'utilisateur avant la prochaine connexion de l'utilisateur à NetWitness Suite. Ce champ s'applique uniquement aux utilisateurs internes. Cela n'affecte pas les sessions utilisateur actives. L'icône ⏰ s'affiche dans la ligne de l'utilisateur pour montrer que le mot de passe de l'utilisateur a expiré. Une fois le mot de passe expiré, il est impossible de l'annuler. Cette case est décochée à la prochaine modification du compte d'utilisateur.
Réinitialiser le formulaire	Supprime toute modification en cours.

Onglet Rôles

Le tableau ci-dessous fournit les descriptions des options présentées sous l'onglet Rôles. L'onglet Rôles présente les rôles attribués à l'utilisateur.

Option	Description
	Ouvre la boîte de dialogue Ajouter un rôle qui répertorie les rôles pouvant être attribués à l'utilisateur.
	Annule l'attribution du rôle sélectionné à l'utilisateur.
	Affiche les autorisations pour le rôle sélectionné.
Nom	Répertorie chaque rôle attribué à l'utilisateur.

Onglet Rôles

Cette rubrique présente les fonctions de la vue Admin > Sécurité > onglet Rôles.

Des rôles sont attribués à tous les utilisateurs NetWitness Suite. Les utilisateurs reçoivent les autorisations que leur octroient les rôles. Sous l'onglet Rôles, vous pouvez créer, dupliquer, modifier et supprimer un rôle. Vous pouvez aussi afficher la liste de tous les rôles et leurs autorisations respectives.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Admin	Afficher les rôles préconfigurés	Étape 1. Passer en revue les rôles préconfigurés NetWitness
Admin	Créer un rôle	Étape 2. (Facultatif) Ajouter un rôle et attribuer des autorisations

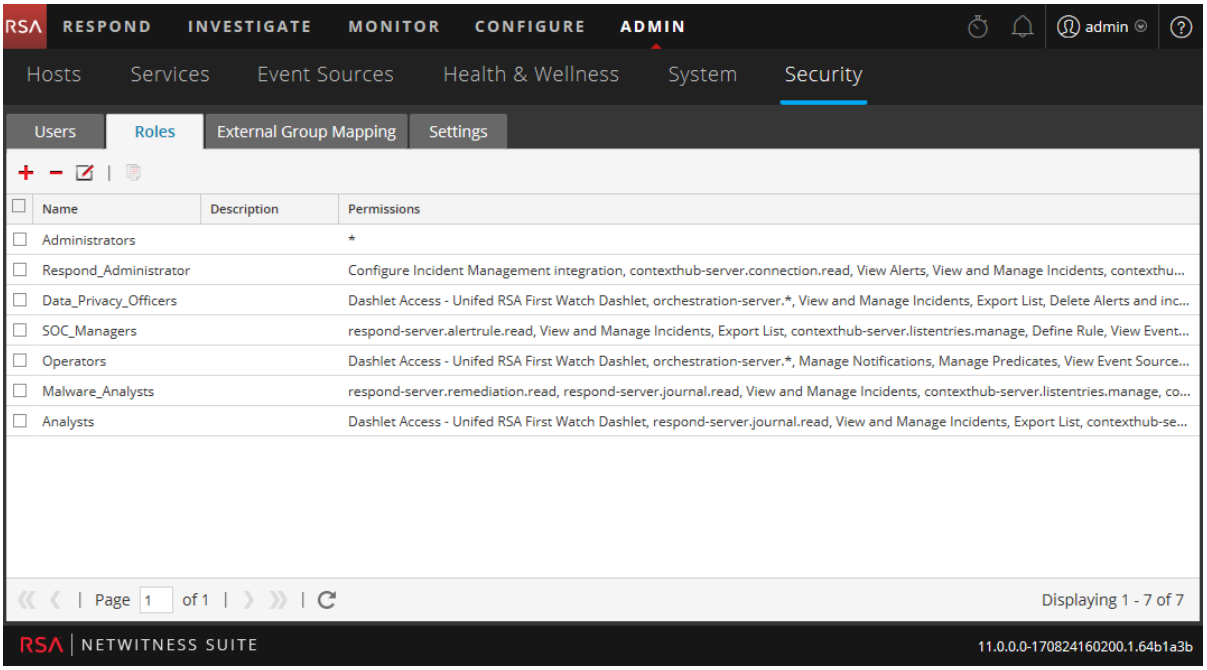
Rubriques connexes

- Boîte de dialogue Ajouter ou modifier un rôle

Pour accéder à cette vue :

1. Accédez à **ADMIN > Sécurité**.
   Par défaut, la vue Sécurité permet d'accéder à l'onglet **Utilisateurs**.

2. Cliquez sur l'onglet **Rôles**.



L'onglet Rôles se compose de la liste Rôles avec une barre d'outils en haut.

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

Fonctionnalité	Description
+	Affiche la boîte de dialogue Ajouter un rôle.
✎	Affiche la boîte de dialogue Modifier le rôle.
−	Affiche un message d'avertissement et vous invite à confirmer que vous voulez supprimer un rôle.
⧉	Duplique un rôle à enregistrer sous un nom différent.

Le tableau suivant décrit les fonctionnalités de la liste des rôles.

Colonne	Description
Nom	Affiche le nom d'un rôle qui peut être attribué à un utilisateur.
Description	Affiche une description du rôle.
Autorisations	Affiche les autorisations attribuées au rôle.

Boîte de dialogue Ajouter ou modifier un rôle

Cette rubrique présente les boîtes de dialogue Ajouter un rôle et Modifier un rôle, accessibles à partir de la vue Admin > Sécurité > onglet Rôles.

Les boîtes de dialogue Ajouter un rôle et Modifier le rôle vous permettent d'ajouter ou de modifier un rôle, ainsi que les autorisations qui lui sont attribuées. Vous pouvez également spécifier les attributs de gestion de requêtes pour permettre aux membres du rôle de verrouiller les informations qu'ils peuvent récupérer. Ces deux boîtes de dialogue ont la même structure. La seule différence est que vous pouvez ajouter un nouveau rôle ou modifier un rôle existant.

Lorsque vous modifiez les autorisations d'un rôle, les modifications sont immédiatement appliquées aux utilisateurs qui se voient affecter le rôle spécifique après l'enregistrement du rôle.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur	Afficher les rôles préconfigurés	Étape 1. Passer en revue les rôles préconfigurés NetWitness
Administrateur	Créer un rôle	Étape 2. (Facultatif) Ajouter un rôle et attribuer des autorisations
Administrateur	Modifier un rôle	Étape 2. (Facultatif) Ajouter un rôle et attribuer des autorisations
Administrateur	Supprimer un rôle	Étape 2. (Facultatif) Ajouter un rôle et attribuer des autorisations

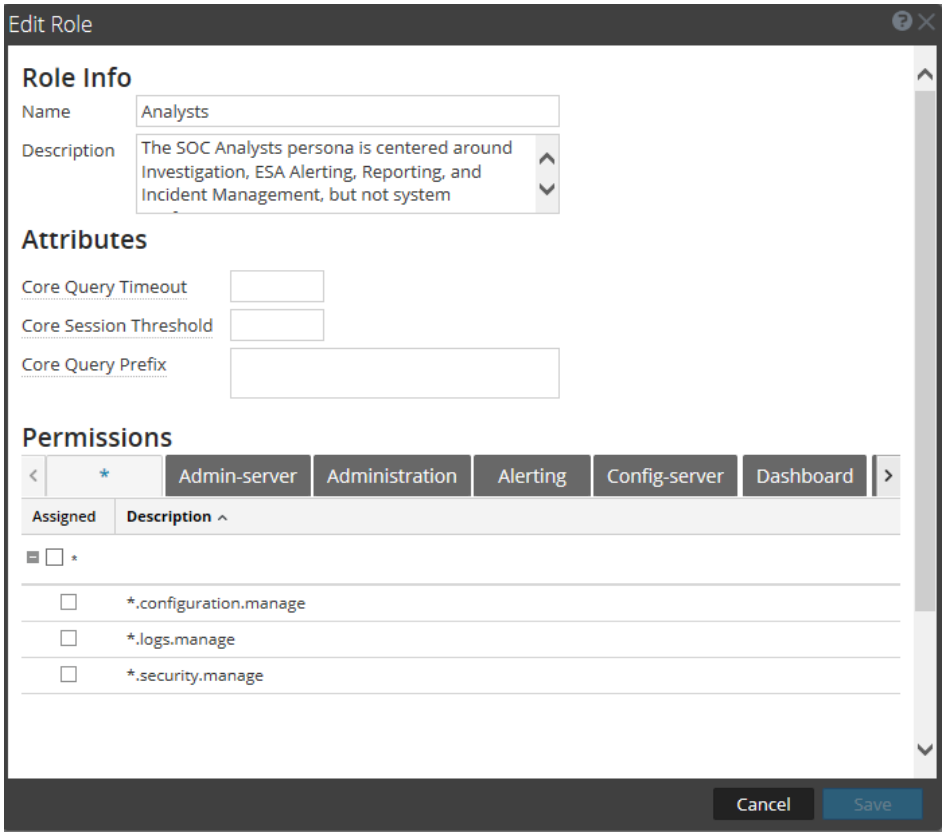
Pour accéder à cette vue :

1. Dans NetWitness Suite, accédez à **ADMIN > Sécurité**.
   Par défaut, la vue Sécurité permet d'accéder à l'onglet **Utilisateurs**.

2. Cliquez sur l'onglet **Rôles**.
3. Exécutez l'une des opérations suivantes :
   - Dans la barre d'action, cliquez sur  .

     La boîte de dialogue **Ajouter un rôle** s'affiche.
   - Sélectionnez un rôle dans la barre d'action, cliquez sur  .

     La boîte de dialogue **Modifier un rôle** apparaît.



Les boîtes de dialogue Ajouter un rôle et Modifier un rôle contiennent trois sections : **Info rôle**, **Attributs** et **Autorisations**.

Infos sur les rôles

Il s'agit des informations de la section **Infos sur les rôles**.

Fonctionnalité	Description
Nom	Nom du rôle d'utilisateur.
Description	Description facultative du rôle d'utilisateur.

Attributs

Ce sont les informations contenues dans la section **Attributs**. Une valeur en italique indique une valeur par défaut, par exemple, *5*. Une valeur qui n'est pas en italique indique un changement de la valeur par défaut, par exemple `1200`. Étape 3. Vérifier les attributs Requête (Query) et Session par rôle fournit plus d'informations.

Fonctionnalité	Description
Expiration du délai de requête de base	(Facultatif) Spécifie le nombre maximal de minutes durant lesquelles un utilisateur peut exécuter une requête. La valeur par défaut est 5 minutes. Ce délai s'applique uniquement aux requêtes exécutées dans Investigation. Si cette valeur est définie, elle doit être égale à zéro (0) ou supérieure. Une valeur zéro signifie qu'il n'y a aucun délai. Lors de la migration vers NetWitness Suite 10.5 et versions ultérieures, s'il n'y a aucune valeur définie pour les rôles, 5 minutes est la valeur définie par défaut. **Remarque :** Les services de base de NetWitness Suite 10.5 et toute version ultérieure utilisent ce champ.
Seuil de session de base	Contrôle la façon dont le service analyse les valeurs méta pour déterminer le nombre de sessions. Cette valeur doit être égale à zéro (0) ou supérieure. Si cette valeur est supérieure à zéro, une optimisation de requête extrapole le nombre total de sessions qui dépasse ce seuil. Si la valeur des métadonnées renvoyée par la requête atteint le seuil, le système : • Arrête la détermination du nombre de sessions • Affiche le seuil et le pourcentage du temps de requête utilisé pour atteindre le seuil La valeur par défaut est `100000`. La limite que vous renseignez ici remplace la valeur du **Nb max exports de session** définie dans les paramètres de la vue ENQUÊTER.

Fonctionnalité	Description
Préfixe de requête de base	(Facultatif) Filtre les résultats de requête pour limiter les éléments que voient les membres du rôle. Par défaut, ce champ est vide. Par exemple, le préfixe de requête `'service' = 80` précède les requêtes exécutées par l'utilisateur et l'utilisateur peut accéder uniquement aux métadonnées des sessions HTTP.

Autorisations

Il s'agit des informations de la section **Autorisations**. La section Autorisations du rôle décrit les autorisations.

Fonctionnalité	Description
Onglets **Module**	Il y a huit onglets, un pour chaque module : Administration, Alertes, Incidents, Procédure d'enquête, Live, Malware, Rapports et Tableau de bord. Chaque onglet affiche les autorisations d'un module.
Colonne **Description**	Affiche toutes les autorisations relatives au module.
Colonne **Attribué**	Case indiquant si une autorisation de module est attribuée au rôle.
Enregistrer	Enregistre le rôle avec les autorisations sélectionnées qui lui sont attribuées.
Annuler	Annule une tâche et ferme la boîte de dialogue.

Onglet Mappage de groupe externe

Si vous configurez l'authentification de l'utilisateur externe, vous pouvez mapper les rôles d'utilisateur NetWitness Suite à un groupe externe. L'onglet Mappage de groupe externe fournit des informations sur chaque groupe externe auquel vous avez mappé des rôles.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Administrateur	Mapper un rôle à un groupe externe	Étape 5. (Facultatif) Mapper des rôles d'utilisateur aux groupes externes
Administrateur	Rechercher un groupe externe	Rechercher les groupes externes

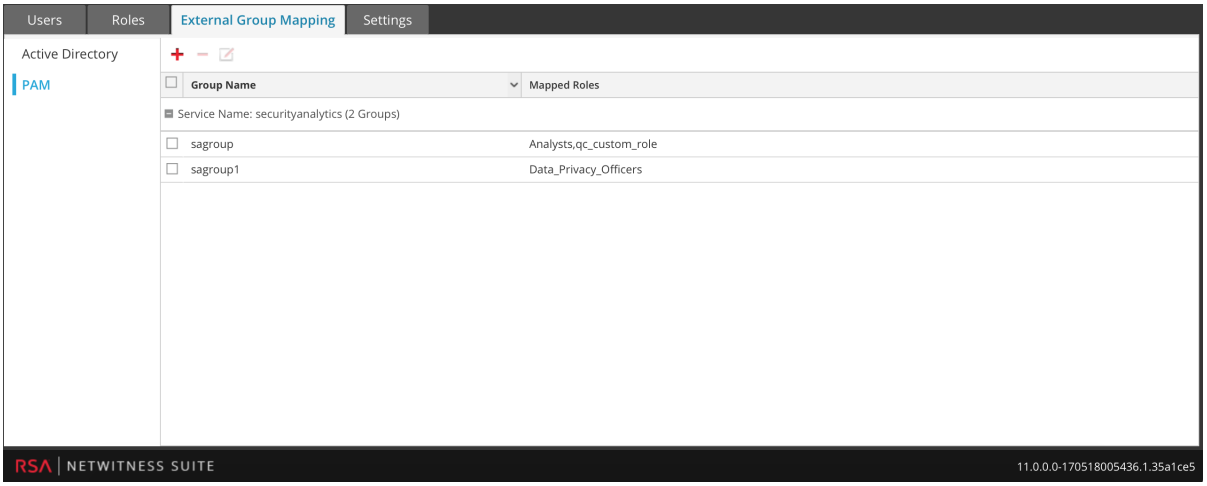
Rubriques connexes

- Boîte de dialogue Ajouter un mappage de rôle
- Boîte de dialogue Rechercher les groupes externes

Pour accéder à cette vue :

1. Dans NetWitness Suite, accédez à **ADMIN > Sécurité**.
   La vue Sécurité s'affiche avec l'onglet **Utilisateurs** ouvert.

2. Cliquez sur l'onglet **Mappage de groupe externe**.



L'onglet Mappage de groupe externe comprend une barre d'outils et une liste.

La liste contient les fonctionnalités ci-dessous.

Fonctionnalité	Description
Type de groupe	Dans la colonne de gauche, cliquez sur **Active Directory** ou **PAM** pour afficher les groupes correspondant au type sélectionné.
Zone de sélection	Sur une ligne, déplace la sélection d'un nom de groupe. Dans la barre de titre, déplace la sélection de tous les noms de groupe.
Nom de groupe	Affiche le nom du groupe externe qui a accès à NetWitness Suite.
Rôles mappés	Affiche les rôles NetWitness Suite mappés au groupe externe.

La **barre d'outils** contient les fonctionnalités ci-dessous.

Fonctionnalité	Description
+	Affiche la boîte de dialogue Ajouter un mappage de rôles, qui permet de sélectionner un groupe externe et de le mapper à un rôle NetWitness Suite.
−	Affiche un message d'avertissement et invite à confirmer la suppression de tous les rôles NetWitness Suite mappés au groupe externe.

Fonctionnalité	Description
	Affiche la boîte de dialogue Modifier le mappage de rôles, qui permet d'ajouter ou de supprimer des rôles NetWitness Suite dans le groupe externe.

Boîte de dialogue Ajouter un mappage de rôle

Cette rubrique présente les fonctions de la vue Admin > Sécurité > onglet Mappage de groupe externe > Boîte de dialogue Ajouter un mappage de rôles.

Dans NetWitness Suite, chaque rôle utilisateur possède son propre ensemble d'autorisations. Vous pouvez mapper un ou plusieurs rôles NetWitness Suite à un groupe externe pour octroyer à ce dernier le même ensemble d'autorisations que celles du rôle.

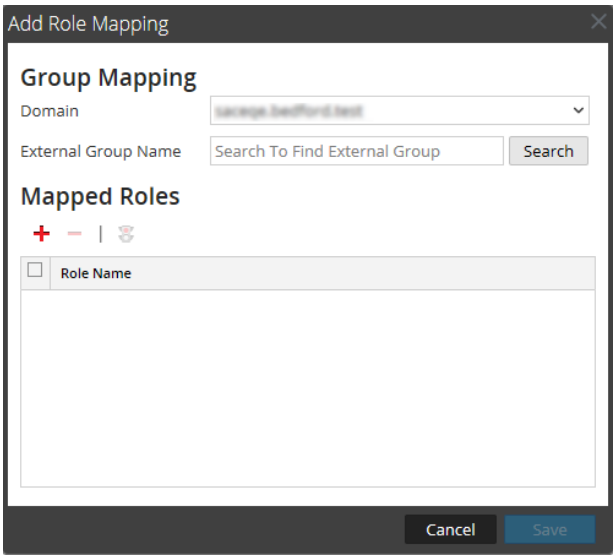
Que voulez-vous faire ?

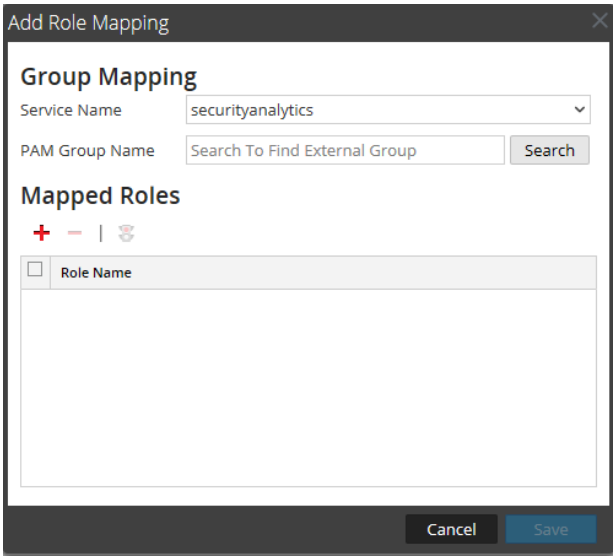
Rôle	Je souhaite...	Me montrer comment
Administrateur	Mapper un rôle à un groupe externe	Étape 5. (Facultatif) Mapper des rôles d'utilisateur aux groupes externes
Administrateur	Rechercher un groupe externe	Rechercher les groupes externes

Pour accéder à cette boîte de dialogue :

1. Dans NetWitness Suite, accédez à **ADMIN > Sécurité**.
2. Cliquez sur l'onglet **Mappage de groupe externe**.
3. Dans la barre d'outils cliquez sur +.

   La boîte de dialogue **Ajouter un mappage de rôle** pour la méthode d'authentification externe que vous avez configurée s'affiche.





Les boîtes de dialogue Ajouter un mappage de rôles et Modifier le mappage de rôles sont pratiquement identiques. La seule différence repose sur le fait que vous ne pouvez pas effectuer de recherches dans la boîte de dialogue Modifier le mappage de rôles.

Mappage de groupes

La section **Mappage de groupes** est dotée des fonctionnalités suivantes :

Fonctionnalité	Description
Domaine	Affiché si vous avez configuré Active Directory pour l'authentification des utilisateurs externes. Nom de domaine du groupe AD externe auquel les rôles sont mappés.

Fonctionnalité	Description
Nom du groupe externe	Affiché si vous avez configuré Active Directory pour l'authentification des utilisateurs externes. Groupe externe auquel les rôles sont mappés.
Nom du groupe PAM	Affiché si vous avez configuré PAM pour l'authentification des utilisateurs externes. Nom du groupe externe auquel les rôles sont mappés.
Rechercher	Affiche une boîte de dialogue dans laquelle vous pouvez rechercher des groupes externes. Aucune recherche n'est possible dans la boîte de dialogue Modifier le mappage de rôles.

Rôles mappés

La section **Rôles mappés** est dotée des fonctionnalités suivantes :

Fonctionnalité	Description
+	Ouvre la boîte de dialogue Ajouter un rôle qui répertorie les rôles d'utilisateur NetWitness Suite configurés à ajouter.
−	Supprime les rôles sélectionnés de la grille Rôles mappés.
Name	Affiche le nom du rôle d'utilisateur NetWitness Suite.
Autorisations	Affiche les autorisations associées au rôle d'utilisateur NetWitness Suite.
Annuler	Annule le nouveau mappage de groupe ou celui qui a été modifié, et ferme la boîte de dialogue.
Enregistrer	Enregistre le nouveau mappage de groupe ou celui qui a été modifié, et ferme la boîte de dialogue.

Boîte de dialogue Rechercher les groupes externes

Cette rubrique décrit les fonctions de la vue Admin > Sécurité > boîte de dialogue Rechercher les groupes externes.

Si vous configurez l'authentification d'utilisateur externe, vous pouvez mapper les rôles d'utilisateur externe NetWitness Suite aux groupes externes. Vous recherchez des groupes externes pour sélectionner les groupes auxquels vous souhaitez mapper des rôles NetWitness Suite.

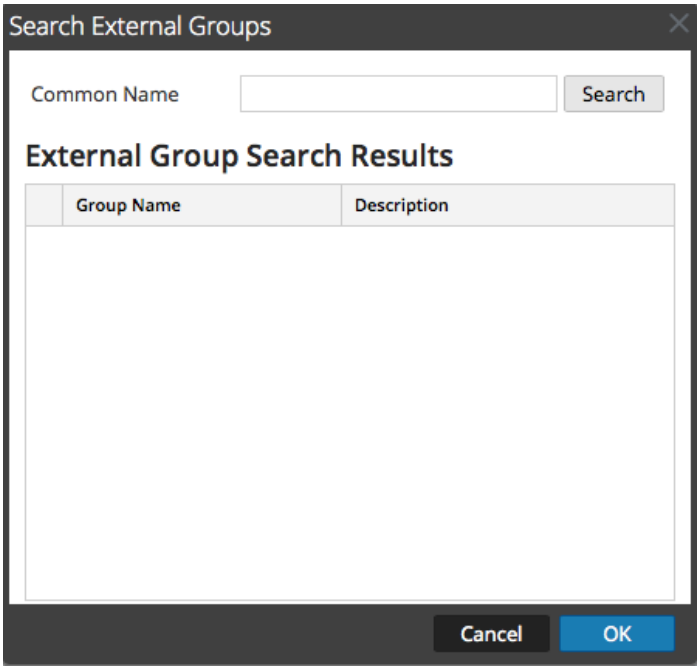
Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Admin	Mapper un rôle à un groupe externe	Étape 5. (Facultatif) Mapper des rôles d'utilisateur aux groupes externes
Admin	Afficher les mappages de groupes externes	Onglet Mappage de groupe externe
Admin	Rechercher les groupes externes	Rechercher les groupes externes

Pour accéder à cette boîte de dialogue :

1. Accédez à **ADMIN > Sécurité**.
   La vue Sécurité s'affiche avec l'onglet **Utilisateurs** ouvert.
2. Cliquez sur l'onglet **Mappage de groupe externe**.
3. Dans la barre d'outils cliquez sur +.
   La boîte de dialogue Ajouter un mappage de rôle pour la méthode d'authentification externe que vous avez configurée s'affiche.
4. Dans la section Mappage de groupes, sélectionnez un **domaine**.

5. Dans la section Mappage de groupes, cliquez sur **Rechercher**.
   La boîte de dialogue **Rechercher les groupes externes** s'affiche.



Le tableau suivant décrit les fonctions de la boîte de dialogue Rechercher les groupes externes.

Fonctionnalité	Description
Nom commun	Nom du groupe que vous recherchez. Peut correspondre au nom ou peut contenir le caractère générique (*) qui remplace un caractère.
Nom du groupe	Groupe externe auquel vous pouvez mapper des rôles.
Description	Texte facultatif relatif au groupe.
OK	Affiche la boîte de dialogue Ajouter un mappage de rôles, qui contient le groupe externe que vous avez sélectionné.
Annuler	Ferme la boîte de dialogue.

Onglet Paramètres

Cette rubrique explique la vue Admin > Sécurité > onglet Paramètres. Dans l'onglet Paramètres, configurez la complexité du mot de passe pour les utilisateurs NetWitness Suite internes et les paramètres de sécurité de l'ensemble du système.

Pour plus d'informations sur la configuration de la sécurité NetWitness Suite, reportez-vous à Configurer la sécurité du système.

Les exigences en matière de complexité des mots de passe s'appliquent uniquement aux utilisateurs internes et ne sont pas obligatoires pour les utilisateurs externes. Les utilisateurs externes comptent sur leurs propres méthodes et systèmes pour faire respecter les exigences de complexité des mots de passe.

Que voulez-vous faire ?

Rôle	Je souhaite...	Me montrer comment
Admin	Configurer la complexité des mots de passe	Étape 1. Configurer la complexité des mots de passe
Admin	Configurer les paramètres de sécurité au niveau du système	Étape 3. Configurer les paramètres de sécurité au niveau du système
Admin	(Facultatif) Configurer l'authentification externe	Étape 4. (Facultatif) Configurer l'authentification externe

Rubriques connexes

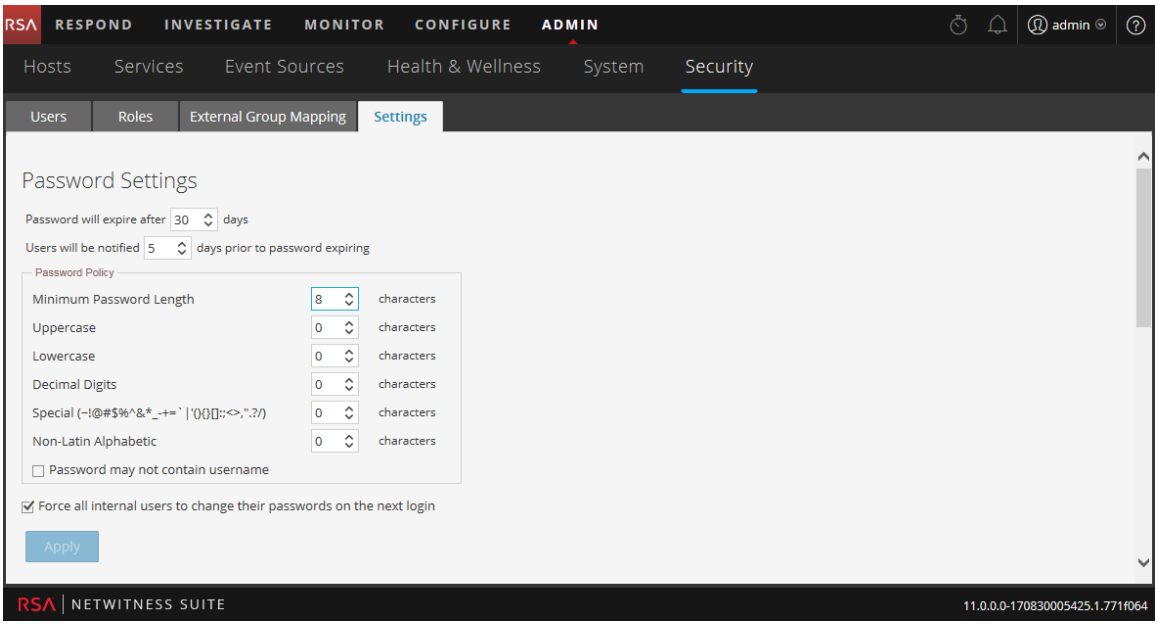
- Configurer la sécurité du système

Vue Admin > Sécurité - Onglet Paramètres

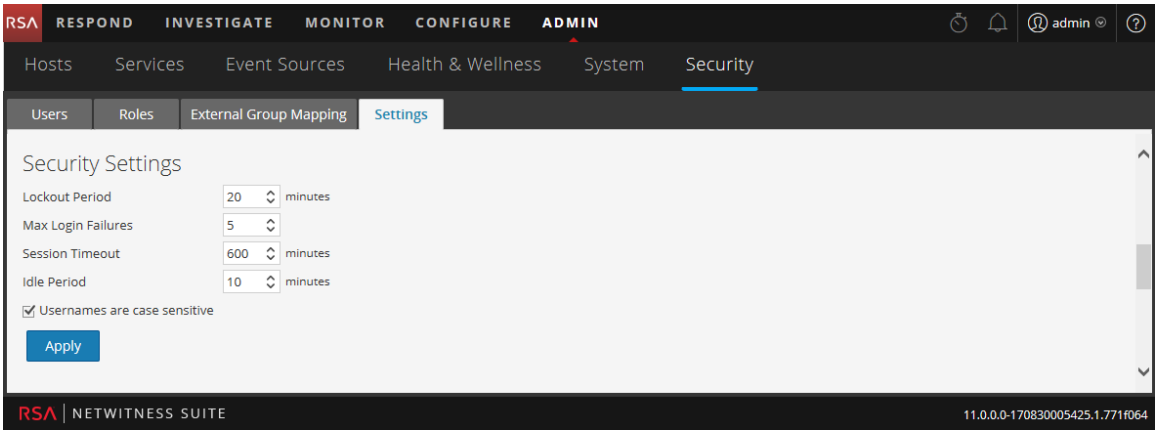
Pour accéder à l'onglet Paramètres :

1. Accédez à **ADMIN > Sécurité**.
   La vue Sécurité s'affiche avec l'onglet **Utilisateurs** ouvert.
2. Cliquez sur l'onglet **Paramètres**.

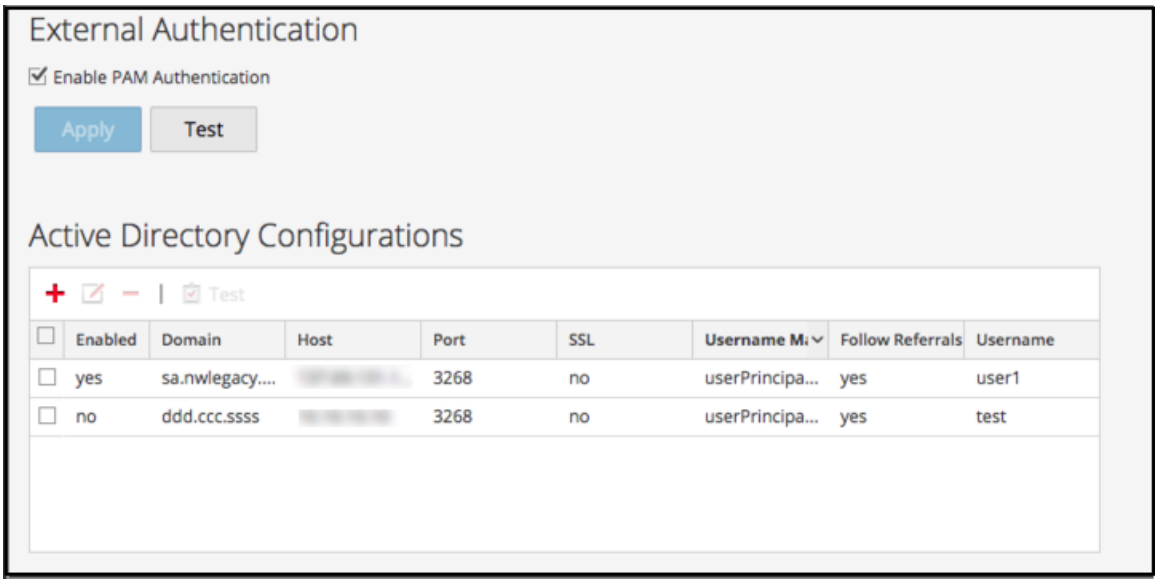
La figure suivante illustre la section Paramètres de mots de passe liée à l'onglet Paramètres.



La figure suivante illustre la section Paramètres de sécurité liée à l'onglet Paramètres.



La figure suivante illustre les sections Authentification PAM et Configurations Active Directory liées à l'onglet Paramètres.



Paramètres de mot de passe

La section Stratégie de mots de passe vous permet de configurer les conditions requises en matière de complexité des mots de passe pour les utilisateurs NetWitness Suite internes lorsqu'ils définissent leurs mots de passe.

Option	Description
Le mot de passe expirera après <n> jour (s)	Nombre de jours par défaut avant lequel un mot de passe expire pour tous les utilisateurs NetWitness Suite internes. La valeur zéro (0) désactive l'expiration du mot de passe. Pour les nouvelles installations, la valeur par défaut est 30. Concernant les mises à niveau, la valeur précédente migre automatiquement lors de l'installation de mises à niveau.
Les utilisateurs seront notifiés <n> jour(s) avant l'expiration du mot de passe	Nombre de jours avant la date d'expiration du mot de passe, pour avertir un utilisateur que son mot de passe est sur le point d'expiration. Les utilisateurs reçoivent un seul rappel par e-mail à la date spécifiée avant l'expiration de leur mot de passe. Ils peuvent également afficher la boîte de dialogue Message d'expiration de mot de passe lorsqu'ils se connectent à NetWitness Suite. La valeur minimale est 1 jour.

Option	Description
Longueur minimale du mot de passe	Spécifie les exigences requises en matière de longueur du mot de passe des utilisateurs NetWitness Suite. La longueur minimale du mot de passe empêche les utilisateurs d'utiliser des mots de passe courts qui sont faciles à deviner.
en majuscules ;	Indique le nombre minimum de caractères en majuscules contenus dans le mot de passe. Ceci inclut les caractères des langues européennes de A à Z, comprenant des signes diacritiques, des caractères grecs et des caractères cyrilliques. Par exemple : • Lettre majuscule cyrillique : Д Ц • Lettre majuscule grecque : Π Λ
en minuscules ;	Indique le nombre minimum de caractères en minuscules contenus dans le mot de passe. Ceci inclut les caractères des langues européennes de a à z, comprenant des signes diacritiques, des caractères grecs et des caractères cyrilliques. Par exemple : • Lettre minuscule cyrillique : д ц • Lettre minuscule grecque : π λ
Chiffres décimaux	Indique le nombre minimum de caractères décimaux (compris entre 0 et 9) contenus dans le mot de passe.
Caractères spéciaux (~!@#$%^&*_-+=`|'(){}[]:;<>,".?/)	Indique le nombre minimum de caractères spéciaux contenus dans le mot de passe : `~!@#$%^&*_-+=`|'(){}[]:;<>,".?/`
Caractères alphabétiques non latins.	Spécifie le nombre minimum de caractères alphabétiques Unicode autres que les lettres majuscules et minuscules. Cela inclut les caractères Unicode des langues asiatiques. Par exemple : • Kanji (japonais) : 頁 (feuille) 枒 (arbre)

Option	Description
Le mot de passe ne peut pas contenir le nom d'utilisateur	Indique qu'un mot de passe ne peut pas contenir le nom d'utilisateur non sensible à la casse.
Forcer tous les utilisateurs internes à modifier leur mot de passe à la prochaine connexion	Force tous les utilisateurs internes à modifier leurs mots de passe la prochaine fois qu'ils se connectent à NetWitness Suite plutôt que lorsqu'ils créent ou modifient leurs mots de passe. Notez que ce paramètre est activé par défaut.
Appliquer	Les paramètres de niveau de sécurité du mot de passe prennent effet lorsque les utilisateurs NetWitness Suite créent ou modifient leurs mots de passe. Si **forcer tous les utilisateurs internes à modifier leur mot de passe à la prochaine connexion** est sélectionnée, tous les utilisateurs internes doivent modifier leur mot de passe la prochaine fois qu'ils se connectent à NetWitness Suite.

Paramètres de sécurité

La section Paramètres de sécurité vous permet de configurer les paramètres de sécurité globaux pour les utilisateurs de NetWitness Suite.

Option	Description
Période de blocage	Nombre de minutes durant lesquelles un utilisateur de NetWitness Suite est bloqué si le nombre configuré de tentatives de connexion est dépassé. La valeur par défaut est 20 minutes.

Option	Description
Nombre maximal d'échecs de la connexion	Nombre maximal d'échecs de la connexion avant le blocage d'un utilisateur. La valeur par défaut est 5
Expiration de la session	Durée maximale d'une session utilisateur avant expiration, en minutes. La valeur par défaut est 600. Si la valeur correspond à 0, il n'y aura pas de temps de session maximal. Si la valeur est un nombre entier positif, la session expirera lorsque le temps configuré se sera écoulé. L'utilisateur doit se reconnecter.
Période d'inactivité	Nombre de minutes d'inactivité avant l'expiration d'une session. La valeur par défaut est 10. Si la valeur définie est 0, la session ne va pas expirer.
Les noms d'utilisateur sont sensibles à la casse.	Sélectionnez cette option si vous souhaitez que le champ Nom d'utilisateur soit sensible à la casse sur l'écran de connexion NetWitness Suite . Par exemple, si les noms d'utilisateur sont sensibles à la casse, vous pouvez utiliser admin pour vous connecter à NetWitness Suite, mais vous ne pouvez pas utiliser Admin.
Appliquer	Permet aux paramètres de prendre effet immédiatement.

Authentification PAM

La section Authentification PAM vous permet de configurer NetWitness Suite pour utiliser Active Directory ou les modules PAM (Pluggable Authentification Modules) en vue d'authentifier et de tester les connexions des utilisateurs externes.

Option	Description
Activer l'authentification PAM	Permet à NetWitness Suite d'utiliser les modules PAM (Pluggable Authentication Modules) pour authentifier les connexions des utilisateurs externes.
Appliquer	Permet de rendre les paramètres de configuration PAM effectifs lors de la prochaine connexion.

Option	Description
Tester	Invite à fournir un nom d'utilisateur et un mot de passe, puis à tester la méthode d'authentification PAM en cours d'activation.

Configurations Active Directory

La section Configurations Active Directory vous permet de configurer NetWitness Suite pour utiliser Active Directory en vue d'authentifier les utilisateurs externes.

Option	Description
Activé	Active l'authentification Active Directory pour les utilisateurs NetWitness Suite.
Domaine	Nom du domaine où se trouve le service Active Directory.
Hôte	Nom d'hôte ou adresse IP où se trouve le service Active Directory.
Port	Port sur l'hôte qui est utilisé pour l'authentification du service Active Directory.
SSL	Indique si le service Active Directory utilise SSL.
Mappage du nom d'utilisateur	Désigne le champ de recherche Active Directory à utiliser pour le mappage du nom d'utilisateur. Vous pouvez spécifier userPrincipalName (UPN) ou sAMAccountName.
Suivre les références	Indique si NetWitness Suite suivra les références LDAP créées par Active Directory.
Nom d'utilisateur	Si le nom d'utilisateur est fourni ici, il est associé au service Active Directory lors de la recherche des groupes Active Directory. Ces informations d'identification ne sont pas utilisées à d'autres fins.