NetWitness® Plate-forme

Version 12.4.0.0

Guide de mise à niveau

NETWITNESS

Platform

Informations de contact

NetWitness Community à l'adresse https://community.netwitness.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

Contrat de licence

Licences tierces

Remarque sur les technologies de chiffrement

Distribution

Divers

Mars 2024

Sommaire

Mettre à niveau NetWitness Platform

Ce document fournit des informations sur les avantages et le processus de mise à niveau de NetWitness Platform vers 12.4. Assurez-vous de respecter les conditions préalables et les tâches préalables à la mise à niveau avant de mettre à niveau NetWitness Platform. Vous pouvez mettre à niveau NetWitness Platform à l'aide de quatre options différentes en fonction de votre connectivité Internet. Après la mise à niveau, vous devez également effectuer certaines tâches post-mise à niveau et vérifications d'intégrité post-mise à niveau répertoriées dans ce guide pour finaliser le processus de mise à niveau avec succès. Les instructions fournies dans ce document s'appliquent aux hôtes physiques et virtuels (y compris AWS, le Cloud public Azure et Google Cloud Platform), sauf indication contraire.

IMPORTANT : Les versions 11.7.x, 12.0 et 12.1 ont atteint la fin de vie (EOL) le 31 décembre 2023. Pour plus d'informations, consultez https://community.netwitness.com/t5/product-life-cycle/product-version-life-cycle-for-rsa-netwitness-platform/ta-p/569875. Si vous souhaitez mettre à niveau les versions 11.7.x (packs de service) ou 11.7.x.x (correctifs) vers la version 12.4.0.0, vous devez d'abord effectuer une mise à niveau vers la version 12.2.0.0 ou 12.3.0.0 avant de passer à la version 12.4.

Remarque : NetWitness Platform prend désormais en charge l'installation de plusieurs serveurs UEBA dans votre environnement. Pour plus d'informations, voir le sujet **Configurer plusieurs serveurs UEBA** dans le *Guide de configuration NetWitness UEBA*.

Vous pouvez activer de nombreuses nouvelles fonctionnalités intéressantes après avoir effectué la mise à niveau vers la version 12.4. Pour obtenir une description complète des nouvelles fonctionnalités de version, consultez les *notes de mise à jour pour NetWitness Platform 12.4*. Accédez à la page Documents NetWitness toutes versions et recherchez les guides NetWitness Platform pour résoudre les problèmes. Pour plus d'informations sur les nouvelles fonctionnalités publiées dans les versions précédentes, consultez https://community.netwitness.com/t5/netwitness-platform-online/what-s-new-in-previous-releases-11-x-to-12-x/ta-p/695650.

Règles de mise à niveau prises en charge pour 12.4

Les stratégies de mise à niveau suivantes sont prises en charge par NetWitness 12.4 :

- NetWitness 12.3.1.0 vers 12.4
- NetWitness 12.3.0.0 vers 12.4
- NetWitness 12.2.0.1 vers 12.4
- NetWitness 12.2.0.0 vers 12.4

Exécution dans un environnement en mode mixte

NetWitness Platform prend en charge le mode mixte lors de la mise à niveau. Le mode Mixte se produit lorsque certains services sont mis à niveau vers la dernière version et que certains services fonctionnent toujours avec les versions plus anciennes.

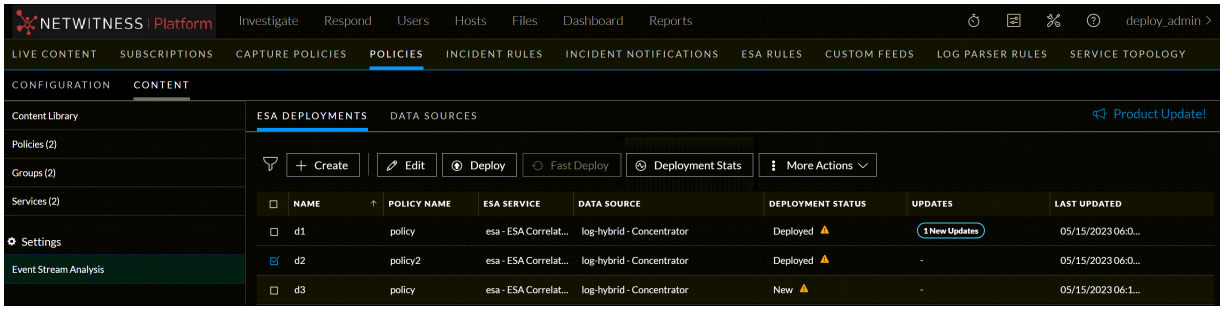
Pour plus d'informations, consultez **Exécution en mode mixte** dans le *guide de démarrage sur les hôtes et les services NetWitness*.

Remarque :
- Si la mise à niveau de tous les hôtes de votre environnement prend plus de temps, contactez l'assistance NetWitness pour éviter tout problème.
- Si vous exécutez Endpoint Log Hybrid en mode mixte, assurez-vous qu'Endpoint Broker exécute la même version que l'un des serveurs Endpoint.
- Le mode mixte n'est pas pris en charge pour les hôtes ESA dans NetWitness Platform.

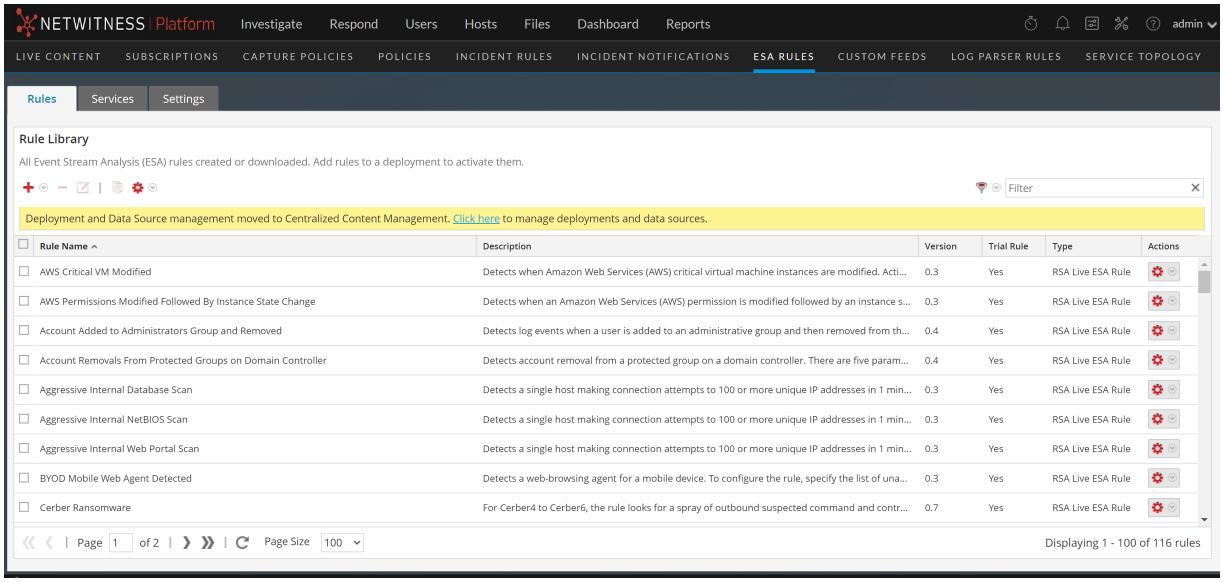
Considérations relatives à la mise à niveau pour les hôtes ESA

IMPORTANT : Le serveur NetWitness, l'hôte principal ESA et l'hôte secondaire ESA doivent tous exécuter la même version de NetWitness Platform.

- Vous pouvez gérer les déploiements ESA et les sources de données uniquement via la **gestion centralisée du contenu**. Accédez à la page **(CONFIGURER) > Règles > Contenu > Event Stream Analysis** pour gérer les déploiements ESA et les sources de données. Reportez-vous à la figure suivante.



- Vous ne pouvez gérer les règles ESA que sur la page **Règles ESA**. Reportez-vous à la figure suivante.



- Après avoir effectué la mise à niveau vers la version 12.4, tous les déploiements ESA seront migrés vers la page (**CONFIGURER**) > **Règles**. Chaque déploiement sera converti en une règle et un groupe et ne pourra être géré qu'après la mise à niveau des serveurs de corrélation vers la version 12.4. Veillez à planifier le processus de mise à niveau de manière à ce que les serveurs de corrélation soient mis à niveau immédiatement après la mise à niveau du serveur d'administration. Les déploiements ne seront pas accessibles tant que les serveurs de corrélation correspondants ne seront pas mis à niveau. Toutefois, les serveurs de corrélation continueront à traiter les alertes et les événements.
- Vous devez mettre à niveau les hôtes ESA immédiatement après la mise à niveau du serveur d'administration.

  Pour plus d'informations sur la **Gestion centralisée de contenu** et la gestion des déploiements, consultez le Guide de gestion centralisée de contenu pour NetWitness.

Mettre à jour ou installer la Collection Windows d'ancienne génération

Reportez-vous au Guide de collecte Windows d'ancienne génération pour NetWitness pour connaître les instructions de mise à niveau et d'installation de la collecte Windows d'ancienne génération.

Remarque : Après avoir mis à niveau ou installé la collecte Windows d'ancienne génération, redémarrez le système pour vous assurer que Log Collection fonctionne correctement.

Terminologies

Nom	Description
AVX	Extensions vectorielles avancées
VMX	Extension de machine virtuelle
NFS	Network File System
BTRFS	Système de fichiers B-Tree
DPDK	Kit de développement de Data plane

Vérifications préalables à la mise à niveau

Vous devez exécuter les vérifications préalables à la mise à niveau avant de procéder à la mise à niveau vers NetWitness Platform 12.4 pour identifier tout problème pouvant entraîner un échec de la mise à niveau.

Pour exécuter les vérifications préalables à la mise à niveau :

1. Connectez-vous en SSH au Serveur d'administration.
2. À l'aide de l'outil Vérification préalable à la mise à niveau, exécutez les commandes suivantes dans l'ordre indiqué :
   a. `nw-precheck-tool-standalone os-migration-checklist`: Cette commande permet à l'outil Vérification préalable à la mise à niveau d'effectuer des contrôles d'intégrité pour la liste des invites dans la Liste de contrôle de la migration du système d'exploitation.
   b. `nw-precheck-tool-standalone upgrade-checklist`: Cette commande permet à l'outil Vérification préalable à la mise à niveau d'effectuer des contrôles d'intégrité pour la liste des invites dans la Liste de contrôle Mise à niveau.
   c. `nw-precheck-tool-standalone network-checklist`: Cette commande permet à l'outil Vérification préalable à la mise à niveau d'effectuer des contrôles d'intégrité pour la liste des invites dans la Liste de contrôle du réseau.
   d. `nw-precheck-tool-standalone cert-checklist`: Cette commande permet à l'outil Vérification préalable à la mise à niveau d'effectuer des contrôles d'intégrité pour la liste des invites dans la Liste de contrôle du certificat.

Liste de contrôle de la migration du système d'exploitation

L'outil Vérification préalable à la mise à niveau effectue les contrôles d'intégrité pour la liste d'invites suivante dans la liste de contrôle de la migration du système d'exploitation :

- **Invite de vérification de version** : Vérifie si la version NetWitness du système est la version la plus récente de 12.2.0.0 ou non.
- **Invite AVX / VMX** : Vérifie si les indicateurs AVX/VMX sont activés ou non pour les nœuds qui les nécessitent.
- **Invite de montage NFS** : Vérifie si le point de montage de type NFS est actif sur l'un des nœuds.
- **Invite de package de développement multiple du noyau** : Vérifie si Decoder et PacketHybrid ont ou non plusieurs versions du package kernel-devel.
- **Invite de périphérique de capture PF Ring** : Vérifie le périphérique de capture PF_ring sur les décodeurs et génère un avertissement pour remplacer le périphérique de capture PF_ring par un périphérique de capture DPDK.
- **Invite de montage BTRFS** : Vérifiez si la partition BTRFS est montée.

  Remarque : Les systèmes d'exploitation LEAPP et Alma ne prennent pas en charge la partition BTRFS.

- **Vérification de l'espace disque** : Vérifie qu'il y a suffisamment de disque libre dans la partition / sur chaque nœud.
- **Vérification du mode Fips** : Vérifie que le mode Fips est désactivé (défini sur false) sur tous les nœuds.
- **Invite de vérification du montage** : Vérifie si toutes les partitions ou répertoires de fichiers sont montés correctement.

Liste de contrôle Mise à niveau

L'outil Vérification préalable à la mise à niveau effectue les contrôles d'intégrité pour la liste d'invites suivante dans la liste de contrôle de la mise à niveau :

- **Vérification des fichiers clients de sécurité** : Vérifie que le fichier `security-client-amqp.yml` n'est pas présent.
- **Vérification de l'état de l'ID de service NW du nœud 0** : Garantit que tous les identifiants de service sont intacts avec tous les différents services du nœud 0.
- **Vérification du fichier de lien symbolique Trustpeer du service Broker** : Garantit que le fichier Symlink Trustpeer du Broker Service `(/etc/netwitness/ng/broker/trustpeers/)` n'est pas endommagé.
- **Vérification de l'état des services NW du nœud 0** : Vérifie l'état de tous les services du nœud 0.
- **Vérification du référentiel externe Yum** : Garantit que les référentiels externes ne sont pas disponibles et ne sont pas activés.
- **Vérification de l'index de la base de données RPM du nœud 0** : Vérifie si la base de données RPM est corrompue ou non.
- **Vérification de la communication Salt Master** : Vérifie la communication salt du nœud 0 vers tous les nœuds.
- **Vérification des certificats du nœud 0** : Vérifie si des certificats sont manquants, expirés ou de type d'émetteur invalide.
- **Authentification Mongo** : Valide les `deploy_admin` informations d'identification extraites de `security-cli-client` à l'aide du client Mongo.
- **Authentification Rabbitmq** : Valide les `deploy_admin` informations d'identification extraites de `security-cli-client` à l'aide de RabbitMQ.
- **(Hôtes de composants) Vérification de l'état du service NW du nœud X** : Vérifie l'état des services (Actifs ou Inactifs) sur tous les nœuds X.
- **(Hôtes de composants) Vérification des certificats du nœud X** : Vérifie l'expiration du certificat, les certificats manquants, corrompus et la non-concordance des émetteurs dans toutes les catégories du nœud X.

- **Fournissez les informations sur la mémoire CPU des nœuds** : Fournit des détails sur le processeur et la mémoire de tous les nœuds ainsi que la mémoire disponible en temps réel.
- **(Serveur administrateur) Vérification de l'utilisation du système de fichiers du nœud 0** : Vérifie l'utilisation des partitions de disque de `/var/netwitness/mongo`, `/var/netwitness` et `root` sur le nœud 0.
- **(Hôtes de composants) Vérification de l'utilisation du système de fichiers du nœud X** : Vérifie l'utilisation des partitions de disque de `/var/netwitness/mongo`, `/var/netwitness` et `root` pour les services ESA primaire et Endpoint Log Hybrid sur le nœud X.
- **Vérification du mode d'autorisation du fichier Mongo (ESA primaire)** : Vérifie le nœud ESA primaire dans le système ou la pile et vérifie le mode d'autorisation du fichier Mongo.
- **Vérification du mode normal du serveur d'orchestration** : Vérifie si le service d'orchestration s'exécute en mode normal ou sans échec.
- **(Serveur d'administration) Vérification de l'état d'initialisation du nœud 0** : Vérifie s'il existe des problèmes qui pourraient faire échouer le processus d'initialisation.
- **Vérification du mode Fips** : Vérifie que le mode Fips est désactivé (défini sur false) avant et après la mise à niveau.
- **Vérification de l'index de la base de données RPM du nœud X** : Vérifie l'état de la base de données RPM sur le nœud X pour s'assurer qu'elle n'est pas corrompue.
- **Vérification du proxy Yum sur le nœud Z** : Vérifie l'existence du fichier yum.conf et la disponibilité du proxy dans le fichier sur Node -Z.
- **Vérification du proxy Yum sur le nœud X** : Vérifie l'existence du fichier yum.conf et la disponibilité du proxy dans le fichier sur Node -X.
- **Invite de vérification des informations sur l'hôte** : Vérifie si les champs d'informations obligatoires de tous les hôtes du système (IP de l'hôte, nom d'hôte, services installés et version brute) sont disponibles.
- **Invite de vérification du chiffrement sur le nœud Z** : Vérifie si les chiffrements requis sont disponibles à l'emplacement `/etc/rabbitmq/rabbitmq.config` sur le nœud 0.
- **Invite de vérification du chiffrement sur le nœud X** : Vérifie si les chiffrements requis sont disponibles à l'emplacement `/etc/rabbitmq/rabbitmq.config` sur tous les nœuds X.
- **Invite de vérification de la version matérielle sur le nœud X** : Vérifie la version matérielle de tous les nœuds X accessibles.
- **Invite de vérification de la version matérielle sur le nœud Z** : Vérifie la version matérielle du serveur d'administration.
- **Invite de vérification des certificats PuppetCA** : Vérifie si les certificats Puppet CA obsolètes sont présents à l'emplacement `/etc/pki/nw/trust/truststore.pem`.
- **Invite AdminCertCheck** : Vérifie si les certificats d'administrateur sur tous les nœuds sont les mêmes que les certificats d'administrateur sur le serveur d'administration.

- **Invite NTP** : Vérifie tous les nœuds pour s'assurer qu'ils sont synchronisés avec le serveur NTP.
- **Invite de vérification StaleCerts** : Vérifie le mongo et avertit s'il contient des certificats obsolètes inutilisés.
- **Invite NodeCertIDCheck** : Vérifie le champ d'objet du certificat de nœud et s'assure qu'il est identique à l'ID de nœud de l'hôte.
- **Déployer l'invite de vérification de l'expiration du mot de passe administrateur** : Vérifie si le mot de passe deploy_admin a expiré sur le nœud-0.
- **Vérification des autorisations de fichiers/dossiers** : Cette invite vérifie si les fichiers/dossiers disposent des autorisations appropriées.

Liste de contrôle du réseau

L'outil Vérification préalable à la mise à niveau effectue les contrôles d'intégrité pour la liste d'invites suivante dans la liste de contrôle du réseau :

- **(Serveur Admin) Vérification des ports fermés sur le nœud 0** : Vérifie si les ports de service requis pour les services NetWitness sont ouverts et à l'écoute sur le nœud 0.
- **(Hôtes de composants) Vérification des ports fermés sur le nœud X** : Vérifie si les ports de service requis pour les services NetWitness sont ouverts et à l'écoute sur le nœud X.

Liste de contrôle du certificat

L'outil Vérification préalable à la mise à niveau effectue les contrôles d'intégrité pour la liste d'invites suivante dans la liste de contrôle du certificat :

- **Vérification de la validité des certificats de service du nœud 0** : Vérifie la validité des certificats de service à l'emplacement `/etc/pki/nw/service/` sur le nœud 0.
- **Vérification de la validité des certificats de service du nœud X** : Vérifie la validité des certificats de service à l'emplacement `/etc/pki/nw/service/` sur le nœud X.
- **Vérification de la validité des certificats sur le nœud 0** : Vérifie la validité des certificats de nœud à l'emplacement `/etc/pki/nw/service` sur le nœud 0.
- **Vérification de la validité des certificats d'autorité de certification racine** : Vérifie la validité des certificats d'autorité de certification racine à l'emplacement `/etc/pki/nw/ca`.

Préparez-vous à mettre à niveau NetWitness Platform

Effectuez les tâches suivantes pour préparer la mise à niveau vers NetWitness Platform 12.4.

Tâche 1. (Important) Préparez-vous à mettre à niveau le système d'exploitation AlmaLinux

Système de fichier non pris en charge

Démonter et supprimer BTRFS

BTRFS est un système de fichiers de copie sur écriture (CoW) pour Linux qui vise à implémenter des fonctionnalités avancées du système de fichiers tout en se concentrant sur la tolérance de panne, la réparation et la simplicité d'administration. Le système de fichiers BTRFS est obsolète dans Red Hat Enterprise Linux 8 et le système d'exploitation AlmaLinux ne prend pas en charge le système de fichiers BTRFS. NetWitness n'utilise pas BTRFS par défaut, mais dans certaines catégories comme le décodeur réseau, le réseau hybride, etc., le module BTRFS existe et est chargé. Si BTRFS est monté en tant que système de fichiers, effectuez les étapes ci-dessous pour démonter manuellement la partition BTRFS (si BTRFS n'est pas monté, ignorez les étapes ci-dessous) :

a. Déplacer les données.

b. Démontez la partition BTRFS à l'aide de la commande suivante.

c. umount <btrfs partition path>. Vous pouvez obtenir les informations sur la partition btrfs à partir des commandes `/etc/fstab or df -hT`.

d. Supprimez la partition BTRFS de `/etc/fstab`.

e. Vérifiez si le module du noyau est toujours chargé en utilisant `lsmod | grep btrfs`. Si le module du noyau est toujours chargé, utilisez `modprobe -r btrfs` pour décharger le module du noyau btrfs.

f. Déclencher/redéclencher la mise à niveau.

Pour plus d'informations, reportez-vous à l'article de la base de connaissances « Mise à niveau vers le système d'exploitation Alma lorsque le système de fichiers BTRFS est monté ».

Démonter NFS

Les systèmes de fichiers de type NFS actifs sur les nœuds entraînent l'échec de la mise à niveau pour les nœuds. Vous devez démonter manuellement ces points de montage à partir de l'interface de ligne de commande de chaque nœud où ils se trouvent. Pour démonter le NFS manuellement, procédez comme suit :

a. Connectez-vous en SSH aux nœuds où le point de montage NFS est détecté.

b. Dans chaque nœud, exécutez `mount | grep 'type nfs'` et récupérez le chemin du répertoire du point de montage NFS.

> **Remarque :** Avant de démonter NFS, vous devez arrêter les services NetWitness qui dépendent de NFS.
> Par exemple : Si les services Archiver et Warehouse Connector s'exécutent sur NFS, vous devez exécuter les commandes suivantes pour arrêter les services avant de démonter NFS.
> `systemctl stop nwarchiver`
> `systemctl stop nwwarehouseconnector`

c. Exécutez umount <dir_path> depuis le terminal, où <dir_path> est le chemin du répertoire de l'étape b.

d. Ouvrez le `/etc/fstab` fichier dans l'éditeur de votre choix et commentez les lignes relatives aux points de montage NFS.

e. Exécutez la mise à niveau de NetWitness.

f. Une fois la mise à niveau terminée avec succès, supprimez le commentaire de l'entrée correspondante de `/etc/fstab` et exécutez `mount -a` à partir du terminal pour rajouter les points de montage NFS.

Vérification du jeu d'instructions du processeur AVX/VMX

L'indicateur de processeur AVX/VMX doit être activé pour NetWitness Platform 12.4. Exécutez la commande
`salt '*' cmd.run "lscpu | grep -E 'avx|vmx'"` pour vérifier si le jeu d'instructions du processeur AVX/VMX est activé. Reportez-vous à l'article de la base de connaissances « Utiliser le jeu d'instructions AVX pour la prise en charge de MongoDB 5.0 Platform » pour plus d'informations.

> **Remarque :** Pour l'appliance matérielle NetWitness, le jeu d'instructions du processeur AVX/VMX est activé par défaut.

Prise en charge de la migration de PF_RING vers DPDK

La configuration de capture du décodeur ne sera pas valide pour les clients utilisant la capture PF_RING (CentOS) et effectuant une mise à niveau directe vers 12.4 (AlmaLinux). Ils doivent d'abord migrer les appareils PF_RING vers DPDK, puis mettre à niveau les appareils.

Reportez-vous à Migrer les appareils PF_RING vers DPDK pour obtenir des instructions de migration.

Tâche 2 (facultative). Supprimer les référentiels de packages hérités

Vous pouvez libérer de l'espace disque en supprimant les référentiels obsolètes des versions précédentes.

Pour supprimer les référentiels obsolètes :

1. Identifiez la version de l'hôte NetWitness Platform le plus ancien dans votre environnement à l'aide de l'outil Référentiel NetWitness. Effectuez ce qui suit :

- Connectez-vous en SSH au serveur d'administration en tant qu'utilisateur `root`.
- Exécutez la commande suivante :

  ```
  nw-repo-tool --list-obsolete
  ```

  Après avoir exécuté cette commande, vous obtiendrez une liste de tous les référentiels obsolètes.

2. Exécutez la commande suivante pour supprimer tous les référentiels obsolètes.

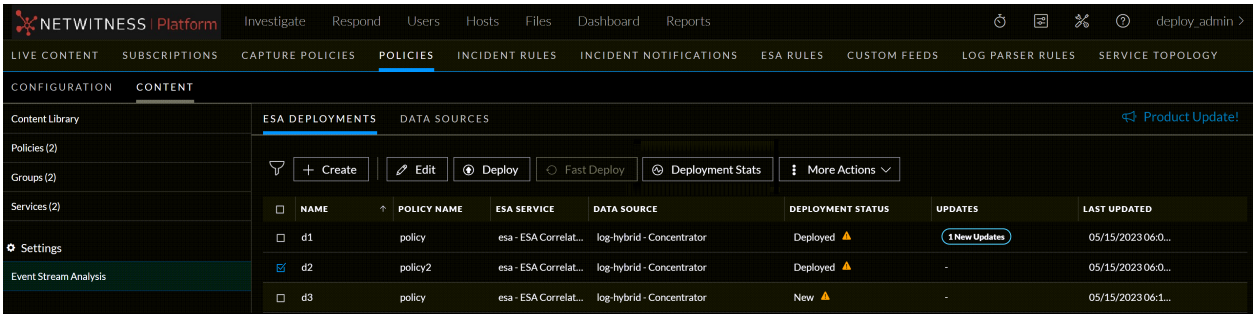
   ```
   nw-repo-tool --purge-obsolete
   ```

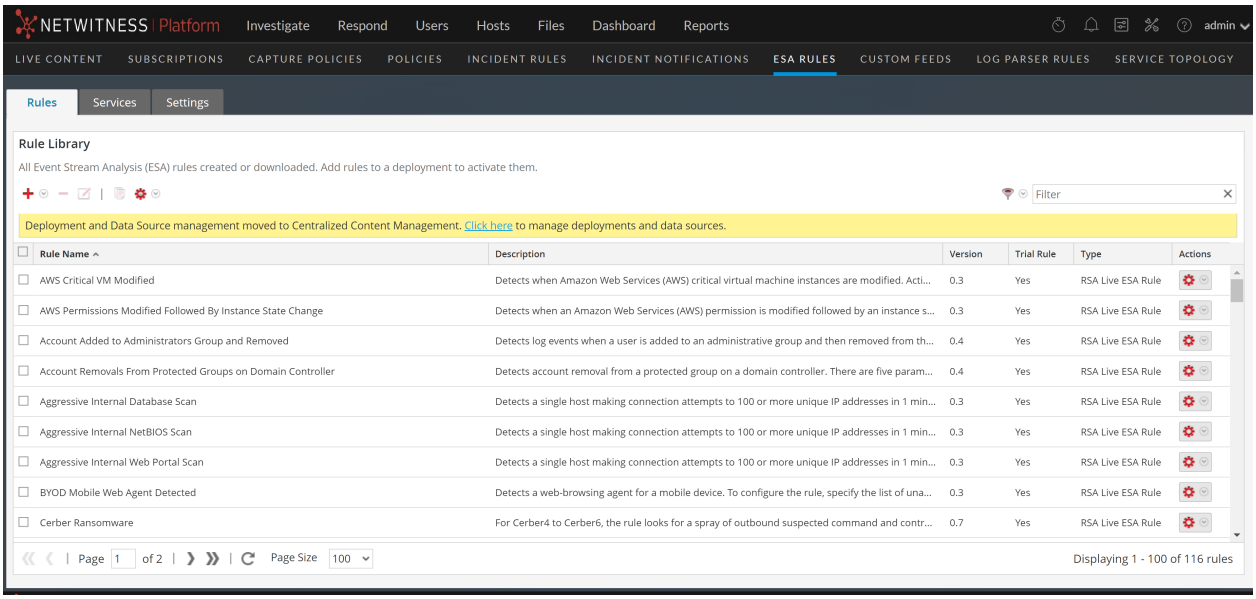
Tâche 3. Préparer les déploiements ESA pour la migration vers 12.4

Avant la mise à niveau vers 12.4, NetWitness recommande que tous les déploiements ESA maintiennent un état sans erreur. Vous devez supprimer tous les déploiements ESA inutilisés, car les déploiements ESA seront migrés vers des règles et des groupes après la mise à niveau vers 12.4. Chaque déploiement sera converti en une règle et un groupe et ne pourra être géré qu'après la mise à niveau des serveurs de corrélation vers la version 12.4.

Gérer les déploiements ESA et les sources de données

Vous pouvez gérer les déploiements ESA et les sources de données uniquement via la **gestion centralisée du contenu**. Accédez à la page (**CONFIGURER**) > **Règles** > **Contenu** > **Event Stream Analysis** pour gérer les déploiements ESA et les sources de données. Vous ne pouvez gérer les règles ESA que sur la page **Règles ESA**. Reportez-vous aux figures suivantes.





Veillez à planifier le processus de mise à niveau de manière à ce que les serveurs de corrélation soient mis à niveau immédiatement après la mise à niveau du serveur d'administration. Les déploiements ne seront pas accessibles tant que les serveurs de corrélation correspondants ne seront pas mis à niveau. Toutefois, les serveurs de corrélation continueront à traiter les alertes et les événements. Vous devez mettre à niveau les hôtes ESA immédiatement après la mise à niveau du serveur d'administration.

Pour plus d'informations sur la **Gestion centralisée de contenu** et la gestion des déploiements, consultez le Guide de gestion centralisée de contenu pour NetWitness.

IMPORTANT : S'il est nécessaire d'importer des règles et des enrichissements ESA, NetWitness recommande d'importer les règles et enrichissements manquants avant la mise à niveau.

Les états des déploiements avant et après la mise à niveau sont représentés dans le tableau suivant.

SlNo	État de déploiement avant la mise à niveau	État de déploiement après la mise à niveau		
		Crée une règle	Crée un groupe	La règle sera publiée
1	Déploiement sain	Oui	Oui	Oui
2	Déploiement avec erreurs	Oui	Oui	Oui
3	Déploiement avec des règles seulement	Oui	Non	Non
4	Déploiement sans règle	Non	Non	Non

Un déploiement sain ne contient aucune erreur et les ressources requises telles que le serveur ESA, la source de données et les règles ESA sont ajoutées.

Remarque : NetWitness recommande que tous les déploiements maintiennent un état sans erreur. Vous devez supprimer tous les déploiements ESA inutiles ou inutilisés.

Tâche 4. Authentification unique (SSO) : Activer la journalisation des réponses SAML dans Microsoft Azure ADFS

La configuration suivante s'applique uniquement aux cas où la réponse SAML de Microsoft Azure ADFS a été uniquement chiffrée mais n'a pas été signée. Si votre Microsoft Azure ADFS est déjà configuré pour signer et chiffrer les réponses SAML, vous pouvez ignorer cette configuration et poursuivre le processus de mise à niveau.

Si vous ne signez pas la réponse SAML, NetWitness vous recommande de configurer Microsoft Azure ADFS pour chiffrer et signer les réponses SAML avant de mettre à niveau votre NetWitness Platform vers la version 12.4 pour une connexion par authentification unique (SSO) réussie. Pour activer la journalisation des réponses dans Active Directory Federation Service (AD FS), exécutez la commande suivante dans ***powershell*** :

```
Set-AdfsRelyingPartyTrust -TargetName <<relying-party-name>> -
SamlResponseSignature MessageAndAssertion
```

IMPORTANT : Il est obligatoire de configurer Microsoft Azure ADFS pour signer les réponses SAML avant de passer à la version 12.4 de NetWitness Platform. Sans respecter ces exigences, vous ne pourrez peut-être pas vous connecter via SSO.

Tâche 5 (facultative). Désactiver les contrôles du noyau FIPS basés sur STIG

Si vous avez activé les contrôles du noyau FIPS basés sur STIG, vous devez les désactiver avant de lancer le processus de mise à niveau de NetWitness Platform pour éviter les erreurs de démarrage. Pour désactiver les contrôles de noyau FIPS basés sur STIG, exécutez les commandes suivantes :

```
manage-stig-controls --disable-control-groups 3 --host-all
```

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

Après avoir mis à niveau NetWitness Platform, assurez-vous d'activer les contrôles du noyau FIPS basés sur STIG.

Remarque : Les contrôles de noyau FIPS basés sur STIG qui nécessitent des modifications des options de démarrage du noyau ne sont pas activés par NetWitness en l'état.

Tâche 6 (facultative). Vérifiez la connexion au serveur Live

Remarque : Cette tâche facultative ne vous concerne que si vous mettez à niveau NetWitness Platform via Live.

Accédez à `admin/system/live services` et effectuez un test de connexion pour vérifier si vous pouvez vous connecter au serveur Live car cela est essentiel pour le serveur source à partir de 12.x. Il s'agit d'une étape facultative et applicable uniquement aux clients qui ont configuré Live.

Tâche 7. Synchroniser l'heure sur les hôtes de composants avec l'hôte du serveur NW

Avant de mettre à niveau les hôtes, assurez-vous que l'heure de chaque hôte est synchronisée avec l'heure de NetWitness Server.

Pour synchroniser l'heure, procédez comme suit :

1. Configurer le serveur NTP.

Pour en savoir plus, consultez **Configurer les serveurs NTP** dans le guide de configuration du système.

2. Procédez comme suit :

a. Connectez-vous en SSH à l'hôte du serveur Admin.

b. Exécutez les commandes suivantes :

```
salt \* service.stop ntpd
salt \* cmd.run 'ntpdate nw-node-zero'
salt \* service.start ntpd
```

Exécuter les tâches de mise à niveau

Les clients doivent d'abord télécharger le RPM autonome à l'aide de https://community.netwitness.com/t5/netwitness-platform-downloads/netwitness-platform-standalone-precheck-tool/ta-p/709096 et se référer au fichier Lisez-moi pour obtenir des instructions sur l'installation du RPM autonome, puis exécuter la vérification préalable. Reportez-vous à la section « Exécuter les vérifications préalables à la mise à niveau » pour en savoir plus.

Mettez à niveau les systèmes de votre environnement dans l'ordre suivant :

1. Serveurs hôtes NW
2. Hôtes Analyste UI
3. Hôtes ESA primaire
4. Hôtes ESA secondaires
5. Hôtes Broker autonomes
6. Hôtes Concentrator
7. Hôtes Archiver
8. Hôtes Packet Decoder
9. Hôtes Log Decoder
10. Hôte Log Collector/VLC
11. Le reste des hôtes de composant

IMPORTANT : Le serveur NW, l'interface utilisateur de l'hôte analyste et les hôtes ESA primaires et secondaires doivent tous être mis à niveau le même jour. Les autres composants de vos hôtes peuvent être mis à niveau le même jour ou plus tard. Veillez à planifier le processus de mise à niveau de manière à ce que les serveurs de corrélation soient mis à niveau immédiatement après la mise à niveau du serveur d'administration. Pour plus d'informations, consultez « **Tâche 3. Préparer les déploiements ESA pour la migration vers la version 12.4** » dans la rubrique Préparez-vous à mettre à niveau NetWitness Platform. Le mode mixte n'est pas pris en charge pour les hôtes ESA dans NetWitness Platform. Le serveur NetWitness, l'hôte principal ESA et l'hôte secondaire ESA doivent tous exécuter la même version de NetWitness Platform.

Pour plus d'informations sur tous les types d'hôtes dans NetWitness, consultez le *Guide de démarrage des hôtes et services NetWitness*. Accédez à la page Documents NetWitness toutes versions et recherchez les guides NetWitness Platform pour résoudre les problèmes.

IMPORTANT : Après la mise à niveau du serveur NW principal (y compris le service Respond Server), le service Respond Server n'est automatiquement réactivé qu'après la mise à niveau de l'hôte ESA principal vers la même version. Les tâches Respond post-mise à niveau ne s'appliquent qu'une fois que le service Respond Server est mis à niveau et est dans l'état activé.

Remarque : Pour la version 12.4 avec Log Collector Windows d'ancienne génération, vous devez effectuer quelques tâches supplémentaires après la mise à niveau. Reportez-vous à la section Collection de logs Windows d'ancienne génération dans Exécuter les tâches postérieures à la mise à niveau pour connaître ces tâches post-mise à niveau supplémentaires.

Sélectionnez des options de mise à niveau

Vous pouvez choisir l'une des options de mise à niveau suivantes en fonction de votre connexion Internet. Elles sont répertoriées dans l'ordre recommandé par NetWitness Platform.

- Option 1 : Mettre à niveau NetWitness Platform à l'aide de Live Services
- Option 2 : Mettre à niveau NetWitness Platform hors ligne
- Option 3 : Mettre à niveau NetWitness Platform à l'aide de l'interface de ligne de commande (hors ligne)
- Option 4 (facultatif) : Référentiel de mise à niveau préalable en téléchargeant des packages

Les règles suivantes s'appliquent lorsque vous mettez à niveau des hôtes à l'aide de l'une des 4 méthodes de mise à niveau :

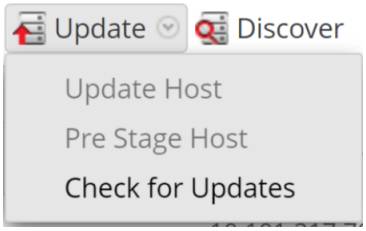
- Vous devez d'abord mettre à niveau l'hôte du serveur NW.
- Vous ne pouvez appliquer qu'une version compatible avec la version existante de l'hôte.
- Les hôtes de serveur NW, ESA primaire, ESA secondaire et d'interface utilisateur d'analyste doivent tous être sur la même version de NetWitness Platform.

Option 1 : Mettre à niveau NetWitness Platform à l'aide de Live Services

Vous pouvez utiliser cette méthode si l'hôte de serveur NW est connecté aux Services Live.

Attention : Vous devez passer en revue votre règle réseau avant de télécharger le package de mise à niveau qui fait environ 11,7 Go. Si vous avez configuré une règle interdisant le téléchargement de fichiers au-delà de 10 Go, le téléchargement du package de mise à niveau échoue.

Remarque : Vous pouvez préparer le référentiel de mise à niveau à l'aide de la fonctionnalité **Hôte de préclassement**. Reportez-vous à la figure suivante. Pour plus d'informations, voir Option 4 (facultatif) : Référentiel de mise à niveau préalable en téléchargeant des packages.



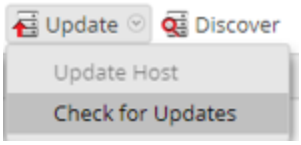
Conditions préalables

1. L'option **Télécharger automatiquement les informations sur les nouvelles mises à jour tous les jours** est sélectionnée et appliquée dans **(Admin) > Système > Mises à jour**.

2. Les mises à jour sont disponibles. Accédez à **(Admin) > Hôtes > Mise à jour > Rechercher des mises à jour** afin de rechercher des mises à jour. La vue Hôte affiche l'état **Mise à jour disponible**.
3. 12.4 est disponible dans la colonne **Mettre à jour la version**.

Pour mettre à niveau depuis 12.2.0.0, 12.2.0.1, 12.3.0.0, et 12.3.1.0 vers 12.4 :

1. Accédez à **(Admin) > Hôtes**.
2. Sélectionnez l'hôte du serveur NW (`nw-server`).
3. Vérifiez les dernières mises à jour.



Mise à jour disponible s'affiche dans la colonne **État** si vous disposez d'une version mise à jour dans le référentiel de mises à jour local pour l'hôte sélectionné.

4. Sélectionnez **12.4** dans la colonne **Mettre à jour la version**.

Remarque :
- Si vous souhaitez afficher une boîte de dialogue contenant les principales fonctionnalités de la mise à niveau et des informations sur les mises à jour, cliquez sur l'icône d'information ( ) à droite du numéro de version de la mise à niveau.

- Si vous ne trouvez pas la version dont vous avez besoin, sélectionnez **Mettre à jour > Rechercher des mises à jour** pour vérifier si des mises à jour sont disponibles dans le référentiel. Si une mise à jour est disponible, le message « Les nouvelles mises à jour sont disponibles » s'affiche et la colonne **État** se met automatiquement à jour pour afficher les mises à jour disponibles. Par défaut, seules les mises à jour prises en charge par l'hôte sélectionné sont affichées.

5. Cliquez sur **Mettre à jour** > **Mettre à jour l'hôte** dans la barre d'outils.
6. Cliquez sur **Commencer la mise à jour**.
7. Cliquez sur **Redémarrer l'hôte**.
8. Répétez les étapes 5 à 7 pour les autres hôtes.

Remarque : Vous pouvez sélectionner plusieurs hôtes à mettre à niveau simultanément, mais seulement après la mise à jour et le redémarrage de l'hôte du serveur NW. Tous les hôtes ESA, Endpoint et Malware Analysis doivent être mis à niveau vers la même version que celle de l'hôte du serveur NW.

Option 2 : Mettre à niveau NetWitness Platform hors ligne

Vous pouvez mettre à niveau manuellement NetWitness Platform en effectuant les tâches suivantes.

Tâche 1. Remplir le dossier intermédiaire (`/var/netwitness/common/update-stage/`) avec les fichiers de mise à niveau de version. Procédez comme suit :

1. Téléchargez le package de mise à niveau `netwitness-12.4.0.0.zip` depuis NetWitness Community (https://community.netwitness.com/) > **Téléchargements** > **NetWitness Platform** > **Version 12.4** vers un répertoire local :
   - Si vous effectuez une mise à niveau depuis 12.2.0.0, 12.2.0.1, 12.3.0.0, et 12.3.1.0, téléchargez `netwitness-12.4.0.0.zip`.
2. Ouvrez une session SSH sur l'hôte du serveur NW.
3. Téléchargez `netwitness-12.4.0.0.zip` vers `/var/netwitness/common/update-stage/` sur l'hôte du serveur NW.
   Par exemple :

   ```
   mv /var/netwitness/tmp/netwitness-12.4.0.0.zip
   /var/netwitness/common/update-stage/
   ```

Remarque : NetWitness Platform décompresse le fichier automatiquement.

Tâche 2. Appliquer les mises à niveau de la zone de stockage temporaire à chaque hôte. Procédez comme suit :

Attention : Vous devez mettre à niveau l'hôte de serveur NW avant de mettre à niveau tout hôte autre que ceux du serveur NW.

1. Connectez-vous à NetWitness.
2. Accédez à  **(Admin) > Hôtes**.

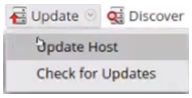
   Remarque : Si vous êtes déjà sur la page  **(Admin) > Hôtes** et sur l'option **Rechercher des mises à jour** (**Mise à jour** > **Rechercher des mises à jour**) est grisé, actualisez la page depuis le navigateur pour rechercher des mises à jour.
3. Recherchez des mises à jour et attendez que les paquets de mise à niveau soient copiés, validés et prêts à être initialisés.

   Le message « Prêt à initialiser les packages » s'affiche si :
   - NetWitness Platform peut accéder au package de mise à niveau.
   - Le paquet est complet et exempt d'erreur.

   Reportez-vous à Dépannage des installations et des mises à jour de versions pour obtenir des instructions sur le dépannage des erreurs (par exemple, « Erreur lors du déploiement de la version <numéro-version> » et « Packages de mise à jour suivants manquants » s'affichent dans la boîte de dialogue **Lancer le package de mise à jour pour RSA NetWitness Platform**.)
4. Cliquez sur **Initialiser la mise à jour**.

L'initialisation des packages prend un certain temps car les fichiers sont volumineux et doivent être décompressés. Le temps varie en fonction de la configuration de l'hôte.
Une fois l'initialisation réussie, la colonne **État** affiche Mise à jour disponible.

5. Cliquez sur **Mettre à jour** > **Mettre à jour les hôtes** dans la barre d'outils.



6. Cliquez sur **Démarrer la mise à jour** dans la boîte de dialogue **Mise à jour disponible**.
Une fois l'hôte mis à niveau, vous êtes invité(e) à le redémarrer.
7. Cliquez sur **Redémarrer l'hôte** à partir de la barre d'outils.

Option 3 : Mettre à niveau NetWitness Platform à l'aide de l'interface de ligne de commande (hors ligne)

Vous pouvez utiliser cette option si l'hôte de serveur NW n'est pas connecté aux Services Live.

Avant de commencer

Assurez-vous d'avoir téléchargé le fichier suivant depuis NetWitness Community (https://community.netwitness.com/) > **Produits > NetWitness Platform** > **Téléchargements** vers un répertoire local :

- Si vous effectuez une mise à niveau depuis 12.2.0.0, 12.2.0.1, 12.3.0.0 et 12.3.1.0 vers 12.4, téléchargez :

  `netwitness-12.4.0.0.zip`

- Si vous utilisez un référentiel externe, vous pouvez mettre à jour le référentiel externe avec le dernier contenu de la mise à niveau. Pour plus d'informations, voir Instructions relatives au référentiel externe pour la mise à niveau via l'interface de ligne de commande.

Pour mettre à niveau les hôtes du serveur NW et les serveurs de composants :

Remarque : Si vous copiez et collez les commandes à partir du PDF dans le terminal SSH Linux, les caractères ne fonctionnent pas. Cependant, vous pouvez copier les commandes de la page HTML https://community.netwitness.com/t5/netwitness-platform-online/upgrade-tasks-for-12-1-1/ta-p/695018#Option3 et collez-les sur le terminal SSH Linux.

1. Organisez les fichiers 12.4.0.0 pour les préparer à la mise à niveau. Imaginons les scénarios suivants.
   - **Option 1 (Manuel)** : Connectez-vous au Serveur NetWitness et créez le répertoire suivant :

     `/var/netwitness/tmp/upgrade/12.4.0.0/`
     Copiez ensuite le fichier zip du package dans le `/var/netwitness/tmp/` répertoire du serveur NW et extrayez les fichiers du package depuis `/var/netwitness/tmp/` vers le répertoire approprié à l'aide de la commande suivante :

`unzip netwitness-12.4.0.0.zip -d /var/netwitness/tmp/upgrade/12.4.0.0`
Assurez-vous de supprimer le fichier zip de mise à jour du répertoire intermédiaire après son extraction.

- **Option 2 (automatisée)** : Connectez-vous au Serveur NetWitness et créez le répertoire suivant : `/var/netwitness/tmp/upgrade/`
  Copiez ensuite les fichiers zip du package NetWitness 12.4.0.0 dans le `/var/netwitness/tmp/` répertoire sur le serveur NetWitness.
  Après cela, exécutez la commande ci-dessous pour extraire, valider et initialiser les fichiers zip 12.4.0.0 :
  ```
  [root@SA ~]# upgrade-cli-client --init --stage-dir /var/netwitness
  /tmp/upgrade --download-path /var/netwitness/tmp/ --version 12.4.0.0
  ```
  Une fois le message **(INFO), le téléchargement et l'extraction de tous les fichiers zip NetWitness nécessaires sont terminés** s'affiche dans la console du serveur d'administration, alors le processus d'initialisation commence.

Remarque : Si vous ne recevez pas le message **(INFO) Le téléchargement et l'extraction de tous les fichiers zip NetWitness nécessaires sont terminés**, exécutez à nouveau la commande précédente.

IMPORTANT : Après la préparation de 12.4.0.0 (à l'aide de l'option 2), si l'initialisation échoue, exécutez la commande `upgrade-cli-client --init --version 12.4.0.0 --stage-dir /var/netwitness/tmp/upgrade`. Si l'initialisation réussit, ignorez l'étape 2 Initialiser la mise à niveau ci-dessous et passez aux étapes 3 à 6 suivantes.

2. Initialisation de la mise à niveau à l'aide de la commande suivante :
   `upgrade-cli-client --init --version 12.4.0.0 --stage-dir /var/netwitness/tmp/upgrade`
3. Mettez à niveau l'hôte du serveur NW à l'aide de la commande suivante :
   `upgrade-cli-client --upgrade --version 12.4.0.0 --host-key <ID / display name / (hostname/ IP address)>`

Remarque : Une fois la mise à niveau déclenchée, le serveur NW redémarrera automatiquement environ 10 minutes après le début du processus de mise à niveau. Il démarrera dans le nouveau noyau (4.18 pour Alma Linux 8.9).

Attention : Il est conseillé aux utilisateurs d'attendre que l'interface utilisateur soit opérationnelle, ce qui peut prendre jusqu'à une heure. Après 20 à 30 minutes de migration, vous pouvez lancer SSH et vérifier si le système d'exploitation est migré. Une fois la migration du système d'exploitation terminée, l'affichage de l'interface utilisateur peut prendre au moins 30 minutes lorsque la mise à niveau NW s'exécute en arrière-plan.

Le processus de mise à niveau ci-dessus peut être suivi via une console virtuelle pour les machines virtuelles ou une console distante pour les serveurs dotés d'iDRAC.

Une fois le système d'exploitation migré et capable de se connecter en SSH au nœud d'administration, exécutez la commande suivante sur l'hôte pour confirmer la migration réussie du système d'exploitation :

- `cat /etc/redhat-release`
- `AlmaLinux release 8.9 (Midnight Oncilla)`

Attention : Après la migration du système d'exploitation, réinstallez tous les RPM tiers que vous avez précédemment installés.

4. Une fois le serveur d'orchestration opérationnel, il déclenchera automatiquement la mise à niveau NW via chef vers la version NW souhaitée. Pour vérifier la progression de cette opération, veuillez vous connecter en SSH au serveur d'administration et exécuter la commande suivante :
   - `orchestration-cli-client --check-admin-upgrade-status`

   Remarque : Exécutez la commande ci-dessus uniquement pour le serveur admin NW.
5. Lorsque la mise à niveau de l'hôte du serveur NW est réussie, redémarrez l'hôte à partir de l'interface utilisateur de NetWitness Platform dans la vue Hôtes.
6. (Conditionnel) Si le serveur de secours à chaud est déployé, répétez les étapes 1 à 5 sur l'hôte du serveur Warm Standby.
7. Répétez les étapes 3 et 5 pour chaque hôte de composant, modifiez l'adresse IP pour l'hôte du composant qui est en cours de mise à niveau.

Remarque : Vous pouvez vérifier les versions de tous les hôtes à l'aide de la commande `upgrade-cli-client --list` sur l'hôte du serveur NW. Si vous souhaitez afficher le contenu de l'aide de `upgrade-cli-client`, utilisez la commande `upgrade-cli-client --help`.

Instructions relatives au référentiel externe pour la mise à niveau via l'interface de ligne de commande

Pour plus d'informations sur la configuration d'un référentiel externe, consultez l'**Annexe A. Configurer un référentiel externe** dans *12.4Guide de mise à niveau pour NetWitness Platform*. Les instructions suivantes supposent que vous disposez déjà d'un référentiel externe configuré. Accédez à la page Documents NetWitness toutes versions et recherchez les guides NetWitness Platform pour résoudre les problèmes.

1. Organisez les fichiers 12.4.0.0 pour les préparer à la mise à niveau. Imaginons les scénarios suivants.
   - **Si vous effectuez une mise à niveau depuis 12.2.0.0**, **12.2.0.1**, **12.3.0.0** et **12.3.1.0**, il vous suffit de préparer 12.4.0.0.
     - **Option 1 (Manuel)** : Connectez-vous au Serveur NetWitness et créez le répertoire suivant :

       `/var/netwitness/tmp/upgrade/12.4.0.0/`
       Copiez ensuite le fichier zip du package dans le `/var/netwitness/tmp/` répertoire du serveur NW et extrayez les fichiers du package depuis `/var/netwitness/tmp/` vers le répertoire approprié à l'aide de la commande suivante :

       `unzip netwitness-12.4.0.0.zip -d /var/netwitness/tmp/upgrade/12.4.0.0`
       Assurez-vous de supprimer le fichier zip de mise à jour du répertoire intermédiaire après son extraction.

- **Option 2 (automatisée)** : Connectez-vous au Serveur NetWitness et créez le répertoire suivant :
  `/var/netwitness/tmp/upgrade/`
  Copiez ensuite les fichiers zip du package NetWitness 12.4.0.0 dans le `/var/netwitness/tmp/` répertoire sur le serveur NetWitness.
  Après cela, exécutez la commande ci-dessous pour extraire, valider et initialiser les fichiers zip 12.4.0.0 :
  ```
  [root@SA ~]# upgrade-cli-client --init --stage-dir /var/netwitness
  /tmp/upgrade --download-path /var/netwitness/tmp/ --version 12.4.0.0
  ```
  Une fois le message **(INFO), le téléchargement et l'extraction de tous les fichiers zip NetWitness nécessaires sont terminés** s'affiche dans la console du serveur d'administration, alors le processus d'initialisation commence.

Remarque : Si vous ne recevez pas le message **(INFO) Le téléchargement et l'extraction de tous les fichiers zip NetWitness nécessaires sont terminés**, exécutez à nouveau la commande précédente.

IMPORTANT : Après la préparation de 12.4.0.0 (à l'aide de l'option 2), si l'initialisation échoue, exécutez la commande `upgrade-cli-client --init --version 12.4.0.0 --stage-dir /var/netwitness/tmp/upgrade`. Si l'initialisation réussit, ignorez l'étape 2 Initialiser la mise à niveau ci-dessous et passez aux étapes 3 à 6 suivantes.

2. Initialisation de la mise à niveau à l'aide de la commande suivante :
   ```
   upgrade-cli-client --init --version 12.4.0.0 --stage-dir
   /var/netwitness/tmp/upgrade
   ```

3. Mettez à niveau l'hôte du serveur NW à l'aide de la commande suivante :
   ```
   upgrade-cli-client --upgrade --version 12.4.0.0 --host-key <ID / display
   name / (hostname/ IP address)>
   ```

Remarque : Une fois la mise à niveau déclenchée, le serveur NW redémarrera automatiquement environ 10 minutes après le début du processus de mise à niveau. Il démarrera dans le nouveau noyau (4.18 pour Alma Linux 8.9).

Attention : Il est conseillé aux utilisateurs d'attendre que l'interface utilisateur soit opérationnelle, ce qui peut prendre jusqu'à une heure. Après 20 à 30 minutes de migration, vous pouvez lancer SSH et vérifier si le système d'exploitation est migré. Une fois la migration du système d'exploitation terminée, l'affichage de l'interface utilisateur peut prendre au moins 30 minutes lorsque la mise à niveau NW s'exécute en arrière-plan.

Le processus de mise à niveau ci-dessus peut être suivi via une console virtuelle pour les machines virtuelles ou une console distante pour les serveurs dotés d'iDRAC.

Une fois le système d'exploitation migré et capable de se connecter en SSH au nœud d'administration, exécutez la commande suivante sur l'hôte pour confirmer la migration réussie du système d'exploitation :

- `cat /etc/redhat-release`
- `AlmaLinux release 8.9 (Midnight Oncilla)`

Attention : Après la migration du système d'exploitation, réinstallez tous les RPM tiers que vous avez précédemment installés.

4. Une fois le serveur d'orchestration opérationnel, il déclenchera automatiquement la mise à niveau NW via chef vers la version NW souhaitée. Pour vérifier la progression de cette opération, veuillez vous connecter en SSH au serveur d'administration et exécuter la commande suivante :
   - `orchestration-cli-client --check-admin-upgrade-status`

   Remarque : Exécutez la commande ci-dessus uniquement pour le serveur admin NW.
5. Lorsque la mise à niveau de l'hôte du serveur NW est réussie, redémarrez l'hôte à partir de l'interface utilisateur de NetWitness Platform dans la vue Hôtes.
6. (Conditionnel) Si le serveur de secours à chaud est déployé, répétez les étapes 1 à 5 sur l'hôte du serveur Warm Standby.
7. Répétez les étapes 3 et 5 pour chaque hôte de composant, modifiez l'adresse IP pour l'hôte du composant qui est en cours de mise à niveau.

Remarque : Vous pouvez vérifier les versions de tous les hôtes à l'aide de la commande `upgrade-cli-client --list` sur l'hôte du serveur NW. Si vous souhaitez afficher le contenu de l'aide de `upgrade-cli-client`, utilisez la commande `upgrade-cli-client --help`.

Option 4 (facultatif) : Référentiel de mise à niveau préalable en téléchargeant des packages

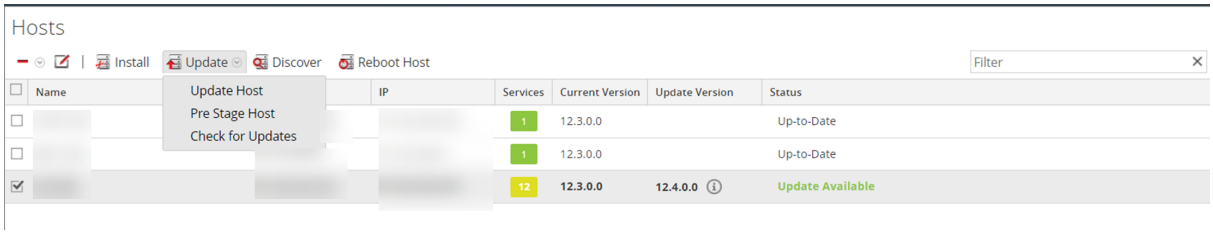
Vous pouvez préparer le référentiel de mise à niveau en téléchargeant les packages requis (.zip) sans affecter le système. Cela minimise le temps d'arrêt de la mise à niveau et garantit que la mise à niveau est terminée dans les délais prévus.

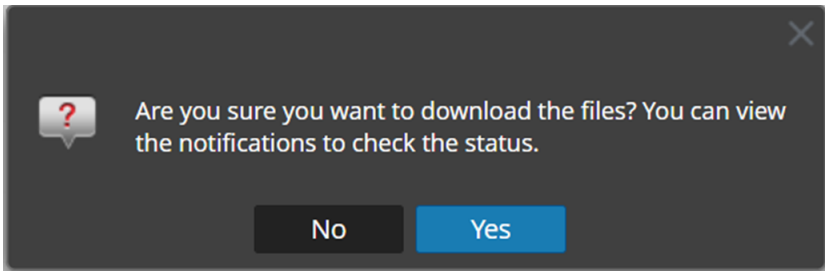
Pour préparer le référentiel de mise à niveau et mettre à jour les hôtes :

1. Accédez à  **(Admin) > Hôtes**.
2. Cliquez sur **Mettre à jour > Rechercher des mises à jour** dans la barre d'outils.

   Toutes les versions de mise à jour possibles seront affichées dans la liste déroulante Versions.
3. Cliquez sur **Mettre à jour** > **Hôte de préclassement** et sélectionnez la version dans la colonne de version de mise à jour.

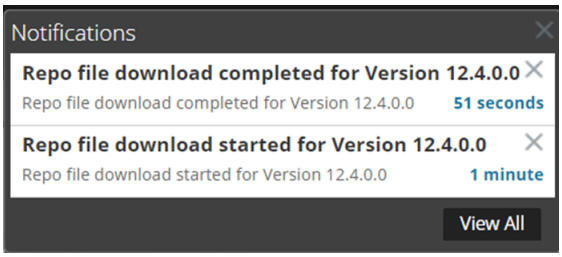
   Un message de confirmation du téléchargement des fichiers s'affiche.





4. Cliquez sur **Oui** pour télécharger les packages de mise à niveau vers le référentiel.
5. Vérifiez l'état du téléchargement dans la zone de notification, comme indiqué ci-dessous.

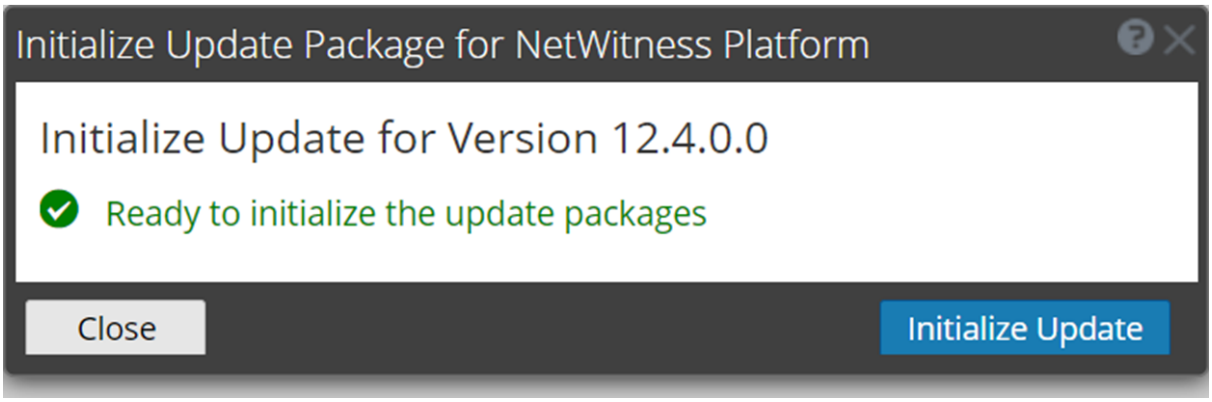
   L'**hôte de préclassement** et **l'hôte de mise à niveau** seront désactivés jusqu'à la fin du préclassement.



Remarque : La version actuelle et la version de la mise à jour dans l'interface utilisateur seront les mêmes pendant la phase préliminaire, car il ne s'agit pas de la mise à jour proprement dite. En effet, seuls les fichiers du référentiel sont téléchargés et aucune mise à niveau réelle n'est effectuée. La version ne sera modifiée qu'après la mise à niveau.

6. Si le téléchargement réussit, **Recherchez des mises à jour** pour lancer l'initialisation.
7. Cliquez sur **Initialiser la mise à jour**.

   L'initialisation du package prendra un certain temps car les fichiers sont volumineux et devront être décompressés.



IMPORTANT : Les étapes 1 à 4 de la préparation du référentiel de préclassement peuvent être effectuées à tout moment. Cependant, des étapes 5 à 8, le processus de mise à niveau commence et vous ne devez PAS redémarrer l'hôte ou redémarrer le serveur jetty pendant cette période car cela corromprait les fichiers .ZIP.

8. Vérifiez l’état de l’initialisation dans la zone de notification.
9. Une fois l’initialisation terminée avec succès, cliquez sur **Mettre à jour** > **Mettre à jour l’hôte**.
   Une fois l’hôte mis à jour, vous serez invité à le redémarrer.
10. Configurez l’hôte, puis redémarrez-le.

Exécuter les tâches postérieures à la mise à niveau

Cette rubrique répertorie les tâches que vous devez effectuer après la mise à niveau de NetWitness Platform. Effectuez les tâches qui s'appliquent aux hôtes de votre environnement.

Général

Vous devez configurer Jetty, restaurer le contenu des services principaux et également démarrer la capture réseau, la capture des journaux et l'agrégation après la mise à niveau de NetWitness Platform.

Configurer Jetty

Pour connaître la configuration de Jetty et les informations associées, consultez la rubrique **Gérer les entrées d'hôte personnalisées** dans le Guide de maintenance du système.

Assurez-vous que les services ont redémarré et qu'ils capturent et agrègent les données

Assurez-vous que les services ont redémarré et capturent les données (cela dépend si le démarrage automatique est activé ou non).

Si nécessaire, redémarrez la capture et l'agrégation des données pour les services suivants :

- Decoder
- Log Decoder
- Broker
- Concentrator
- Archiver

Démarrer la capture réseau :

1. Dans le menu NetWitness Platform, accédez à  (Admin) > **Services**.
   La vue **Services** s'affiche.
2. Sélectionnez chaque service **Décodeur**.

3. Sous  (actions), sélectionnez **Vue** > **Système**.
4. Dans la barre d'outils, cliquez sur 

Pour démarrer la capture des logs :

1. Dans le menu NetWitness Platform, accédez à  (Admin) > **Services**.
   La vue **Services** s'affiche.
2. Sélectionnez chaque service **Log Decoder**.
3. Sous  (actions), sélectionnez **Vue** > **Système**.
4. Dans la barre d'outils, cliquez sur 

Pour démarrer l'agrégation :

1. Dans le menu NetWitness Platform, accédez à  (Admin) > **Services**.
   La vue **Services** s'affiche.
2. Pour chaque service **Concentrator**, **Broker** et **Archiver** :
   a. Sélectionnez le service.
   b. Sous  (actions), sélectionnez **Afficher** > **Config**.
   c. Dans la barre d'outils, cliquez sur 

3. For Event Stream Analysis (ESA) :

   Remarque : Le mode mixte n'est pas pris en charge pour les hôtes ESA dans NetWitness Platform version 11.6 et ultérieures. Le serveur NetWitness, l'hôte principal ESA et l'hôte secondaire ESA doivent tous exécuter la même version de NetWitness Platform.

   Aucune tâche post-mise à niveau n'est requise pour ESA. Pour le dépannage ESA, consultez Informations sur le dépannage ESA.

   Si vous souhaitez ajouter la prise en charge des règles de contenu Endpoint, UEBA et Live, vous devez mettre à jour les clés méta `multi-valued` et `single-valued` de paramètres sur le service de corrélation ESA pour inclure toutes les clés méta requises. Il n'est pas nécessaire d'effectuer ces ajustements lors de la mise à niveau ; vous pourrez effectuer les ajustements plus tard, à un moment opportun. Pour obtenir des informations et des instructions détaillées, consultez **Mettre à jour vos règles ESA pour les clés méta à valeurs multiples et à valeur unique requises** dans le Guide de configuration ESA.

Restaurer le contenu des services de base

Une fois la mise à niveau vers la version 12.4 effectuée, le contenu des services de base tels que les fichiers de configuration (.cfg), les flux, les analyseurs et les périphériques de journalisation est copié à l'emplacement **.tar** des composants respectifs, tels que Decoder, Log Hybrid, Network Hybrid et Log Decoder.

Le tableau suivant répertorie les chemins du contenu des services de base et l'emplacement **.tar** des composants respectifs où le contenu des services de base est copié.

Chemins de contenu des services de base	Composants	Emplacement .tar des composants
/etc/netwitness/ng/feeds (Flux)	Decoder	/var/netwitness/decoder/decoder_backupcontent_ccm.tar
/etc/netwitness/ng/parsers (analyseurs)	Log Hybrid	/var/netwitness/logdecoder/logdecoder_backupcontent_ccm.tar
/etc/netwitness/ng/envision/etc/devices (périphériques de journalisation)	Réseau hybride	/var/netwitness/decoder/decoder_backupcontent_ccm.tar
/etc/netwitness/ng/NwDecoder.cfg (Fichiers de configuration (.cfg))	Log Decoder	/var/netwitness/logdecoder/logdecoder_backupcontent_ccm.tar

L'option CCM est désactivée par défaut. Après la mise à niveau vers 12.4, si vous activez CCM et rencontrez la perte du contenu des services de base, vous pouvez utiliser les fichiers tar de sauvegarde pour récupérer les données perdues. Pour plus d'informations, consultez https://community.netwitness.com/t5/netwitness-knowledge-base/automatic-backup-of-core-service-content-after-upgrading-core/ta-p/694527.

Event Stream Analysis (ESA)

Après avoir effectué la mise à niveau vers la version 12.4, tous les déploiements ESA seront migrés vers la page (**CONFIGURER**) > **Règles**. Chaque déploiement sera converti en une règle et un groupe et ne pourra être géré qu'après la mise à niveau des serveurs de corrélation vers la version 12.4. Veillez à planifier le processus de mise à niveau de manière à ce que les serveurs de corrélation soient mis à niveau immédiatement après la mise à niveau du serveur d'administration. Les déploiements ne seront pas accessibles tant que les serveurs de corrélation correspondants ne seront pas mis à niveau. Toutefois, les serveurs de corrélation continueront à traiter les alertes et les événements. Vérifiez si tous les déploiements ESA sont dans un état sain. Pour plus d'informations, consultez la rubrique **Afficher un déploiement** dans le *Guide de gestion des services Live*.

Remarque : Les analystes doivent disposer des autorisations appropriées pour afficher les règles ESA sous les pages (**CONFIGURER**) > **Règles ESA** et (**CONFIGURER**) > **Règles**. Pour en savoir plus, consultez la section **Serveur source** dans la rubrique **Autorisations du rôle** du *Guide de la sécurité du système et de la gestion des utilisateurs*.

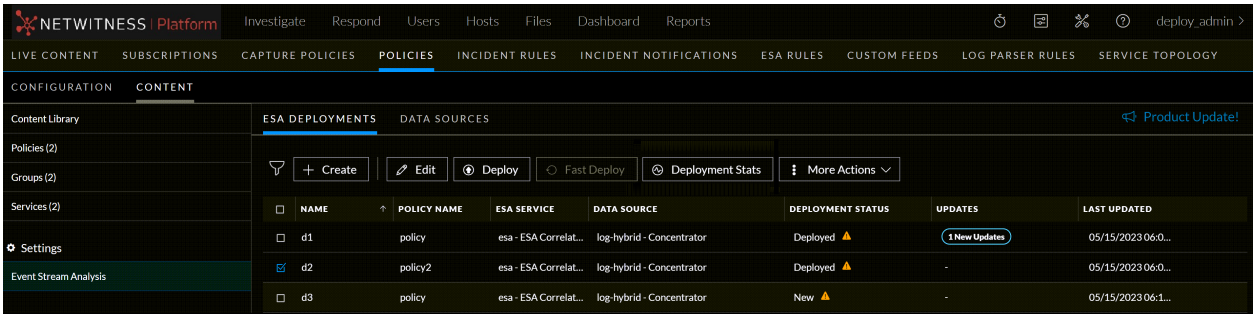
Les états des déploiements avant et après la mise à niveau sont représentés dans le tableau suivant.

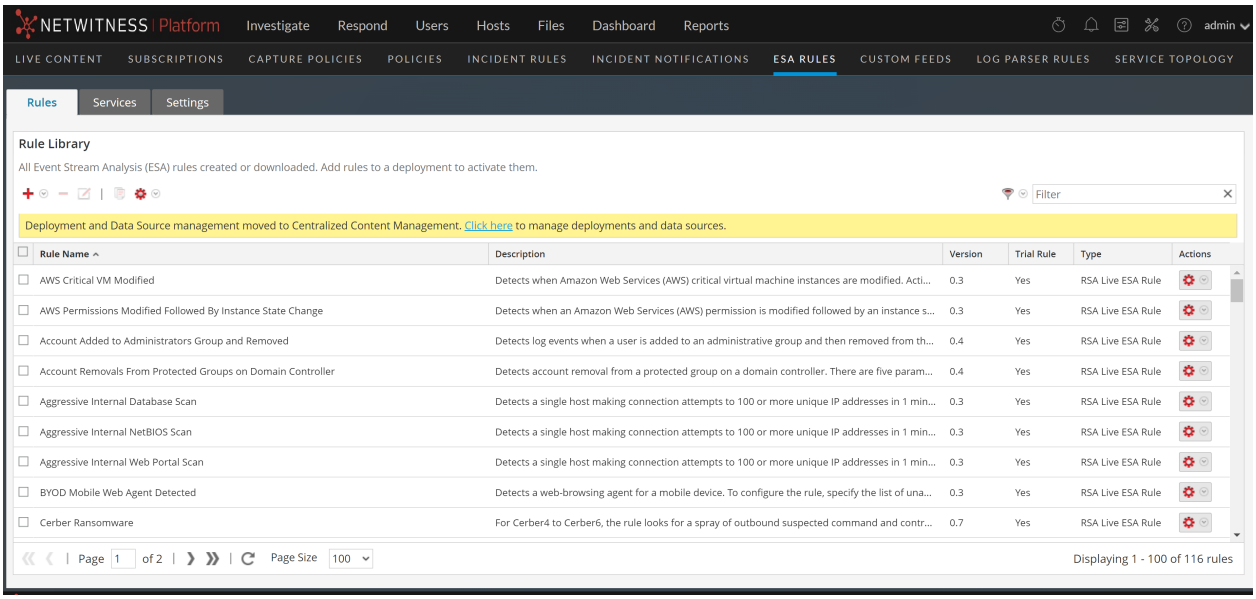
SINo	État de déploiement avant la mise à niveau	État de déploiement après la mise à niveau		
		Crée une règle	Crée un groupe	La règle sera publiée
1	Déploiement sain	Oui	Oui	Oui
2	Déploiement avec erreurs	Oui	Oui	Oui
3	Déploiement avec des règles seulement	Oui	Non	Non
4	Déploiement sans règle	Non	Non	Non

(Facultatif) À l'aide du bouton **Fusionner la règle**, vous pouvez fusionner une règle comportant du contenu ESA avec une règle sans contenu ESA. Pour plus d'informations, consultez la rubrique **Fusionner la règle avec le contenu ESA** dans le *Guide de gestion des services Live*.

Gérer les déploiements ESA et les sources de données

Vous pouvez gérer les déploiements ESA et les sources de données uniquement via la **gestion centralisée du contenu**. Accédez à la page (**CONFIGURER**) > **Règles** > **Contenu** > **Event Stream Analysis** pour gérer les déploiements ESA et les sources de données. Vous ne pouvez gérer les règles ESA que sur la page **Règles ESA**. Reportez-vous aux figures suivantes.





Vous devez mettre à niveau les hôtes ESA immédiatement après la mise à niveau du serveur d'administration.

Pour plus d'informations sur la **Gestion centralisée de contenu** et la gestion des déploiements, consultez le Guide de gestion centralisée de contenu pour NetWitness.

Respond

Le serveur ESA principal doit être mis à niveau vers 12.4 avant de pouvoir effectuer la tâche suivante.

Remarque : Après la mise à niveau du serveur NW principal (y compris le service Respond Server), le service Respond Server n'est automatiquement réactivé qu'après la mise à niveau de l'hôte ESA principal vers la version 12.4. Les tâches Respond post-mise à niveau ne s'appliquent qu'une fois que le service Respond Server est mis à niveau et est dans l'état activé.

(Conditionnel) Restaurer toutes les clés personnalisées du service de réponse dans custom_normalize_alerts.js et prendre en charge la nouvelle source de données

Remarque : Si vous n'avez pas personnalisé manuellement custom_normalize_alerts.js, vous pouvez ignorer cette tâche. Nous essayons de migrer automatiquement les clés personnalisées. Cependant, en cas d'échec, effectuez cette étape pour vérifier l'intégrité des données personnalisées.

Si vous avez ajouté des clés personnalisées dans le fichier `/var/netwitness/respond-server/scripts/custom_normalize_alerts.js` à utiliser dans la normalisation personnalisée, modifiez le fichier `/var/netwitness/respond-server/scripts/custom_normalize_alerts.js` et ajoutez les clés normalisées personnalisées à partir du fichier de sauvegarde automatique. Le fichier de sauvegarde se trouve dans `/var/netwitness/respond-server/scripts` et il est au format suivant :

```
custom_normalize_alerts.js.bak-<time of the backup>
```

En cas d'échec de la mise à jour automatique du script, ajoutez la prise en charge de Netwitness Core et NetWitness Insight en mettant à jour le fichier `custom_normalize_alerts.js` manuellement pour prendre en charge ces nouvelles sources dans la réponse.

Analytique comportementale des utilisateurs et des entités

Effectuez les opérations suivantes après avoir effectué la mise à niveau d'UEBA vers 12.4.

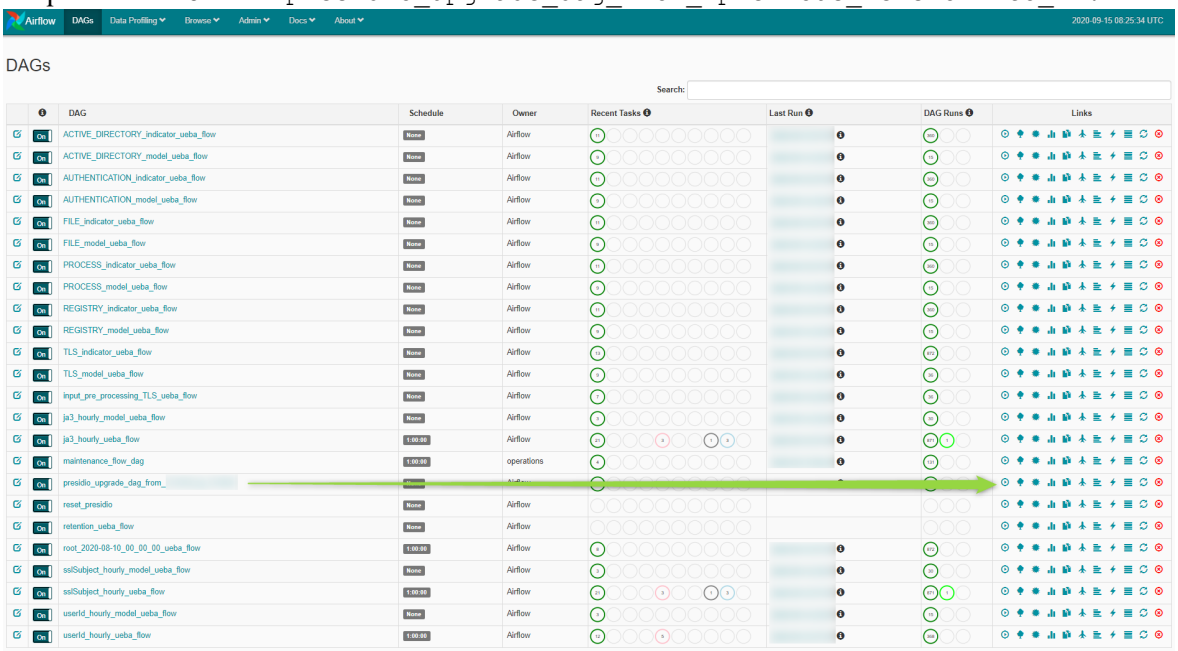
IMPORTANT : Avant la mise à niveau, si vous avez rencontré et résolu les problèmes d'échec des tâches, après la mise à niveau, vous devez remplacer le fichier `authentication.json` avant d'exécuter les tâches post-mise à niveau. Les problèmes d'échec des tâches dans Airflow et leurs solutions sont décrits dans la rubrique « Dépannage » du *Guide de configuration de l'UEBA*.

1. Mettez à jour la configuration UEBA à l'aide de la commande suivante depuis la machine UEBA.
   - `source /etc/sysconfig/airflow`
   - `source $AIRFLOW_VENV/bin/activate`
   - `python /var/netwitness/presidio/airflow/venv39/lib/python3.9/site-packages/presidio_workflows-1.0-py3.9.egg/presidio/resources/rerun_ueba_server_config.py`
   - `deactivate`
2. (Facultatif) Mettez à jour le schéma de traitement UEBA, si nécessaire.

   NetWitness recommande que la date de début de l'UEBA soit définie à 28 jours avant la date actuelle. Pour les systèmes UEBA qui ont l'intention de traiter des données TLS, vous devez vous assurer que la date de début est définie au plus tard 14 jours avant la date actuelle.

   Pour plus d'informations, consultez la section « reset-presidio script » dans le *Guide de configuration d'UEBA*.
3. Exécutez la mise à niveau Airflow DAG.
   - Accédez à la page principale Airflow `https://<UEBA-host-name>/admin`
   - Saisissez le nom et le mot de passe d'administrateur.

- Cliquez sur **Lire** dans `presidio_upgrade_dag_from_<previous_version> to_12.4`.



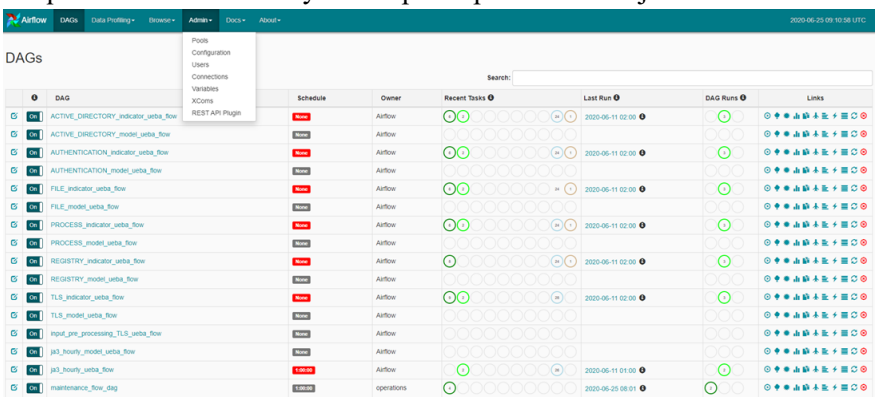
> **Remarque :** Un cercle vert clair apparaîtra en regard de la ligne de la mise à niveau DAG pendant la mise à niveau. Si le processus de mise à niveau s'achève avec succès, le cercle vert clair devient vert. En cas d'échec de la mise à niveau, le cercle vert clair devient rouge.

4. Définissez les emplacements « Boot Jar Pools » appropriés :

   - **Appliance physique** : Mettez à jour la `spring_boot_jar_pool` valeur de l'emplacement sur 18.
   - **Appliance virtuelle** : Mettez à jour la `spring_boot_jar_pool` valeur de l'emplacement sur 22.
     Pour mettre à jour les emplacements **Spring Boot Jar Pools**, accédez à la page principale d'Airflow, appuyez sur l'onglet **Admin** dans la barre supérieure, puis sur **Pools**.

   a. Pour accéder à l'interface utilisateur d'Airflow, accédez à `https://<UEBA_host>/admin` et saisissez les informations d'identification.
      Utilisateur : admin
      Mot de passe : Le mot de passe d'administrateur du déploiement de l'environnement.

b. Cliquez sur le trait de crayon des pools pour mettre à jour les valeurs des emplacements.



5. Modifiez le `spring_boot_jar_pool` et mettez à jour le nombre d'emplacements sur 22.

Log Collector Windows d'ancienne génération

Actualiser les certificats Log Collector Windows d'ancienne génération avec les certificats SA mis à jour

Étapes post-mise à niveau :

1. Exécutez la commande suivante dans SA :

   a. `wlc-cli-client --host-display-name` **`hostDisplayName`** `--service-display-name` **`serviceDisplayName`** `--host` **`WLChostIPAddress`** `--port 50101 --use-ssl false`

   Saisissez les informations suivantes :

   i. **Nom d'utilisateur REST de Log Collector Windows d'ancienne génération et mot de passe REST de Log Collector Windows d'ancienne génération** : Saisissez les informations d'identification de l'administrateur pour Log Collector Windows d'ancienne génération.

   ii. **Nom d'utilisateur du serveur de sécurité et mot de passe du serveur de sécurité** : Saisissez les informations d'identification administrateur pour NetWitness.

2. Redémarrez le système.

Effectuer des contrôles d'intégrité après la mise à niveau

Vous devez effectuer les vérifications d'intégrité suivantes après la mise à niveau vers NetWitness 12.4.

1. Accédez à la vue (Admin) > **Services** pour vérifier que tous les services sont actifs (en vert) après la mise à niveau.
2. Vérifiez que les services sont mis à niveau pour correspondre à la version de l'hôte. La version du service dans la vue (Admin) > **Services** doit correspondre à la version de l'hôte dans la vue (Admin) > **Hôtes** après la mise à niveau.
3. Dans la vue (Admin) > **Services**, procédez comme suit.
   - Sélectionnez un service Log Collector et accédez à la vue (actions) > **Afficher** > **Système** pour vérifier si la collecte de journaux requise est démarrée. Vous devez cliquer sur l'option déroulante Collection et accéder au bon protocole de collecte pour vérifier si la collecte des journaux est démarrée. Si la collecte requise n'est pas démarrée, sélectionnez Start à côté du protocole de collecte requis dans la liste pour démarrer la collecte.
   - Sélectionnez un service Log Decoder et accédez à la vue (actions) > **Afficher** > **Système** pour vérifier si Log Decoder capture correctement les journaux.
   - Sélectionnez un service Packet Decoder et accédez à la vue (actions) > **Afficher** > **Config** pour vérifier si l'interface de capture est configurée dans la section **Configuration de Decoder**. Si l'interface de capture n'est pas configurée, vous devez sélectionner l'interface de capture requise dans la liste déroulante pour la configurer. Si l'interface de capture est déjà configurée, accédez à la vue (actions) > **Vue** > **Système** de Packet Decoder et vérifiez si la capture est démarrée. Si la capture n'est pas démarrée, cliquez sur Start Capture pour démarrer la capture du package.
4. Accédez à la vue (Admin) > **Services** > sélectionnez un service Log Decoder ou Packet Decoder > (actions) > **Afficher** > **Statistiques** > **Général** pour analyser le taux de capture actuel.
5. Vérifiez que les Concentrators, Archivers et Brokers regroupent les données. Assurez-vous que vous pouvez enquêter sur chaque Concentrators, Archivers et Brokers pour valider qu'il est opérationnel.
6. Accédez à la vue **Respond** > **Alertes** pour vérifier si les alertes se déclenchent à partir de différentes sources.
7. Accédez à la vue (Admin) > **Intégrité** > **Alarmes** et vérifiez si le serveur SMS est opérationnel.
8. Accédez à la vue (Admin) > **Sources d'événements** > **Règles de surveillance** et vérifiez si les règles configurées avant la mise à niveau apparaissent.

9. Accédez à la vue  (Admin) > **Intégrité** > **Nouvelle intégrité** > **Pivoter vers le tableau de bord** > **Élastique** > **Tableau de bord** et vérifiez les points suivants.
   - Les visualisations que vous avez créées avant la mise à niveau existent toujours.
   - Le serveur de métrique est fonctionnel.
   - Les alertes sont générées correctement pour les moniteurs que vous avez configurés avant la mise à niveau.

Installez le serveur relais 12.4

IMPORTANT : Après la mise à niveau d'EPLH des versions 12.2.xx et 12.3.xx vers 12.4, vous devez réinstaller le serveur relais sur le boîtier EL 8 (Alma Linux) car le serveur relais est un serveur autonome.

Avant de commencer

- Assurez-vous d'avoir le boîtier EL 8.
- Effectuez les tâches suivantes avant d'installer le serveur relais 12.4 :
  1. Mettre à niveau NetWitness Platform XDR.
  2. Une fois l'EPLH mis à niveau, téléchargez le packager de relais.
  3. Copiez le packager dans le boîtier EL 8.
  4. Éteignez le serveur relais existant.
  5. Configurez l'adresse IP de l'EL 8 en réutilisant l'adresse IP du serveur relais existant.

     Une fois que vous avez configuré l'adresse IP de l'EL 8, installez le serveur relais. Pour plus d'informations, consultez la section **(Facultatif) Installation et configuration du serveur relais** dans le Guide de configuration Endpoint. Accédez à la page Documents NetWitness toutes versions et recherchez les guides NetWitness Platform pour résoudre les problèmes.

Remarque : Vous devez maintenir les correctifs de sécurité à jour sur le serveur relais.

Mettre à niveau les agents Endpoint

Voir **Agents de mise à niveau** dans le Guide d'installation de l'agent Endpoint pour NetWitness Platform pour obtenir des instructions sur la façon de mettre à niveau les agents.

Résoudre les problèmes de mise à niveau

Cette section décrit les messages d'erreur affichés dans la vue Hôtes en cas de problèmes de mise à jour des versions de l'hôte et d'installation des services sur les hôtes dans la vue Hôtes. Si vous ne parvenez pas à résoudre un problème de mise à niveau ou d'installation, contactez le support client.

Les instructions de dépannage pour les erreurs suivantes, qui peuvent survenir lors de la mise à niveau, sont décrites dans cette section.

- Informations de dépannage du système d'exploitation AlmaLinux
- Erreur Mot de passe expiré deploy_admin
- Erreur de téléchargement
- Erreur lors du déploiement de la version <numéro de version> avec des paquets de mise à jour manquants
- Erreur d'échec de la mise à niveau
- Erreur de mise à jour du référentiel externe
- Erreur d'échec de la mise à jour de l'hôte
- Erreur Packages de mise à jour manquants
- Erreur de mise à jour du correctif vers un serveur non NW
- Erreur Redémarrer l'hôte après la mise à jour à partir d'une ligne de commande
- Reporting Engine redémarre après une mise à niveau

Des instructions de dépannage sont également fournies pour les erreurs des hôtes et services suivants qui peuvent survenir pendant ou après une mise à niveau.

- Service Log Collector
- Serveur NW
- Orchestration
- Reporting Engine
- Event Stream Analysis
- Log Collector Windows d'ancienne génération

Problème	Impossible de démarrer l'appliance après la mise à niveau
Solution de contournement	1. Modifiez manuellement la ligne de démarrage GRUB vers `FIPS=0` pour le faire démarrer. 2. Ici, désactivez FIPS à l'aide de la commande suivante : `manage-stig-controls --disable-control-groups 3 --host-all` 3. Vérifiez que la ligne `FIPS=1` soit supprimée de `/boot/grub2/grub.cfg`

- Dans le cas contraire, exécutez la commande suivante :

  ```
  grub2-mkconfig -o /boot/grub2/grub.cfg
  ```

4. Redémarrez.
5. Exécutez la commande suivante pour activer FIPS :

   ```
   manage-stig-controls --enable-control-groups 3 --host-all
   ```

6. Redémarrez à nouveau.

Informations de dépannage du système d'exploitation AlmaLinux

Pour une meilleure compréhension, la mise à niveau du système d'exploitation AlmaLinux peut être divisée en 4 parties :

1. Exécution de l'utilitaire de prévérification pour garantir la santé du système et détecter tout problème de mise à niveau. Cela peut être fait à tout moment avant la mise à niveau à l'aide de l'outil de pré-vérification autonome RPM. (uniquement obligatoire sur le serveur NW)

   Les journaux sont enregistrés ici - `/var/log/netwitness/precheck-tool/checklist.log`

2. Phase d'initialisation ou init (cela se produit uniquement sur le serveur NW)

   Pour tout problème pendant la phase d'initialisation, consultez ces journaux.

   - journaux salt minion - `/var/log/salt/minion`
   - journaux deployment-upgrade - `/var/log/netwitness/deployment-upgrade/chef-solo.log`

   Remarque : Veuillez effectuer l'initialisation uniquement lorsque vous envisagez d'effectuer la mise à niveau réelle. Il n'est pas recommandé d'effectuer une initialisation sans mettre à niveau le système dans la même fenêtre de modification.

3. Mise à niveau du système d'exploitation de CentOS vers AlmaLinux

   En tant que première étape de la mise à niveau du système d'exploitation, Salt est mis à niveau. Vous pouvez exécuter la commande ci-dessous pour voir que Salt est mis à niveau vers la version 3006 :

   ```
   cat /var/log/yum.log | grep salt
   ```

   Vous pouvez afficher une mise à jour similaire à la mise à jour ci-dessous, où xxx représente l'horodatage actuel :

   ```
   xxx Updated: salt-master-3006.2-0.x86_64
   xxx Updated: salt-api-3006.2-0.x86_64
   xxx Updated: salt-minion-3006.2-0.x86_64
   ```

   Pour tout problème lié à la mise à niveau de sel, veuillez vérifier :

- /var/log/netwitness/node-infra-server/node-infra-server.log
- /var/log/salt/master
- /var/log/salt/minion

Une fois salt mis à niveau, le processus Leapp démarre.

Les journaux peuvent être consultés dans `/var/log/salt/minion` :

```
xxx [salt.loaded.ext.module.nw_platform:445 ][INFO ][139407] [1/5]
Searching for leapp config for version: 12.4.0.0

xxx [salt.loaded.ext.module.nw_platform:453 ][INFO ][139407] [2/5]
Retrieving leapp config for version: 12.4.0.0

xxx [salt.fileclient :1333][INFO ][139407] Fetching file from saltenv
'base', ** done ** 'config/12.4.0.0-pre-upgrade.repo'

xxx [salt.loaded.ext.module.nw_platform:467 ][INFO ][139407] [3/5] Running
pre-requisites required to perform leapp upgrade

xxx [salt.fileclient :1333][INFO ][139407] Fetching file from saltenv
'base', ** done ** 'leapp/netwitnessmigrate/actor.py'

xxx [salt.fileclient :1333][INFO ][139407] Fetching file from saltenv
'base', ** done ** 'leapp/netwitnessmigrate/libraries/netwitnessmigrate.py'

xxx [salt.fileclient :1333][INFO ][139407] Fetching file from saltenv
'base', ** done ** 'leapp/netwitnessmigrate.py'

xxx [salt.fileclient :1333][INFO ][139407] Fetching file from saltenv
'base', ** done ** 'leapp/addupgradebootentry.py'

xxx [salt.loaded.ext.module.nw_platform:500 ][INFO ][139407] [4/5] Running
leapp pre-upgrade

xxx [salt.loaded.ext.module.nw_platform:503 ][INFO ][139407] [5/5] Running
leapp upgrade
```

Pour tout problème rencontré lors de la mise à niveau du système d'exploitation, les journaux ci-dessous seront utiles pour le dépannage.

- `/var/log/salt/minion`
- Si la pré-mise à niveau échoue - `/var/log/leapp/leapp-preupgrade.log`
- Si la mise à niveau de Leapp échoue - `/var/log/leapp/leapp-upgrade.log`

Si leapp échoue, `/var/log/leapp/leapp-report.txt` vous fournira des détails sur les inhibiteurs.

Quelques minutes après ce journal « Exécution de la mise à niveau leapp » dans /var/log/salt/minion, le système redémarrera et le retour peut prendre 20 à 30 minutes.

Une fois installé, vous pouvez confirmer le système d'exploitation à l'aide de la commande cat `/etc/almalinux-release`. S'il n'affiche pas la version d'Alma Linux, veuillez appeler le support client avant de prendre toute mesure.

De plus, si vous avez déclenché la mise à niveau via l'interface utilisateur et voyez l'état « `Performing OS Migration` » sur n'importe quel NodeX pendant plus d'une heure, veuillez vérifier les journaux leapp et contacter le support client.

4. Mise à niveau du logiciel NW vers la version 12.4

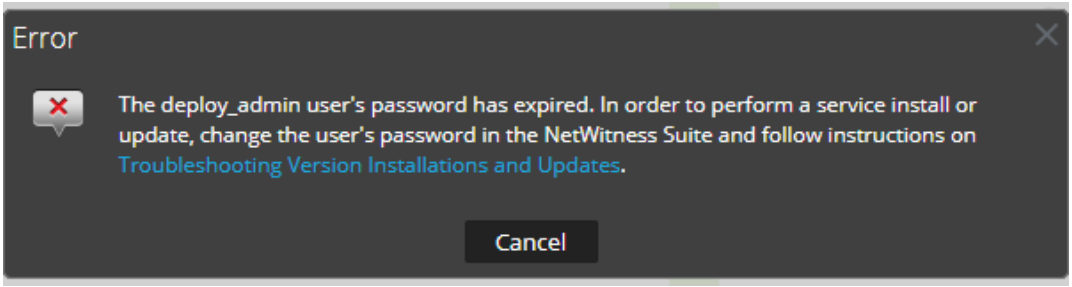
   Une fois la migration du système d'exploitation terminée, la mise à niveau du logiciel NW commence et prend jusqu'à 30 minutes avant que l'interface utilisateur ne soit fonctionnelle.

   Vous pouvez voir ces journaux `/var/log/salt/minion` lorsque la mise à niveau du logiciel NW démarre :

   ```
   xxx [salt.loaded.ext.module.nw_platform:276 ][INFO ][14035] Preparing node for upgrade to 12.4.0.0
   xxx [salt.loaded.ext.module.nw_platform:280 ][INFO ][14035] [1/2] Searching for yum config for version: 12.4.0.0
   xxx [salt.loaded.ext.module.nw_platform:287 ][INFO ][14035] [2/2] Retrieving yum config for version: 12.4.0.0
   xxx [salt.fileclient :1333][INFO ][14035] Fetching file from saltenv 'base', ** done ** 'config/12.4.0.0-pre-upgrade.repo'
   xxx [salt.loaded.ext.module.nw_platform:300][INFO ][14035] Upgrading chef package
   xxx [salt.loaded.ext.module.nw_platform:300][INFO ][14035] Upgrading rsa-nw-config-management package
   ```

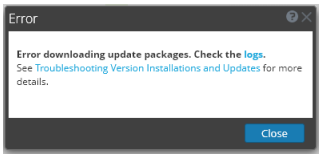
   Vous pouvez également vous référer aux journaux de gestion de la configuration sur `/var/log/netwitness/config-management/chef-solo.log` ou aux journaux de l'interface utilisateur `/var/netwitness/uax/logs/sa.log`

deploy_admin Erreur Mot de passe utilisateur expiré

Message d'erreur	
Cause	Le mot de passe de l'utilisateur `deploy_admin` a expiré.

Solution	Réinitialisez votre mot de passe `deploy_admin`. Procédez comme suit :
	1. Sur le serveur NW uniquement, exécutez la commande suivante.
	`nw-manage --update-deploy-admin-pw`
	`Please enter the new deploy_admin account password: <new-deploy-admin-password>`
	`Please confirm the new deploy_admin account password: <new-deploy-admin-password>`
	2. Examinez le résultat de la commande `nw-manage --update-deploy-admin-pw` pour vérifier que le mot de passe `deploy_admin` a été mis à jour avec succès sur tous les hôtes. Si un hôte NW est en panne ou échoue pour une raison quelconque, comme indiqué par le résultat de la commande `nw-manage --update-deploy-admin-pw`, exécutez `nw-manage --sync-deploy-admin-pw --host-key <host-identifier>` pour synchroniser le mot de passe entre le serveur NW et l'hôte en échec une fois que l'échec de la communication est résolu.
	3. Sur l'hôte dont l'installation ou l'orchestration a échoué, exécutez la commande `nwsetup-tui` et utilisez le nouveau mot de passe **deploy_admin** en réponse à l'invite **Mot de passe de déploiement**.

Erreur de téléchargement

Message d'erreur	
Problème	Lorsque vous sélectionnez une version de mise à jour, puis cliquez sur **Mettre à jour** >**Mettre à jour l'hôte**, le téléchargement démarre, mais ne parvient pas à terminer.
Cause	Les fichiers de téléchargement de version peuvent être volumineux et prendre beaucoup de temps à télécharger. S'il existe des problèmes de communication pendant le téléchargement, celui-ci échoue.
Solution	1. Essayez à nouveau de mettre à jour. 2. S'il échoue à nouveau avec la même erreur, essayez de mettre à jour à l'aide des méthodes hors ligne comme décrit dans « Méthode hors ligne à partir de la vue Hôtes » ou « Méthode hors ligne à l'aide de l'interface de ligne de commande » dans le *Guide de mise à niveau pour NetWitness Platform*. Accédez à la page Documents NetWitness toutes versions et recherchez les guides NetWitness Platform pour résoudre les problèmes. 3. Si vous ne parvenez toujours pas à effectuer la mise à jour, contactez le support client.

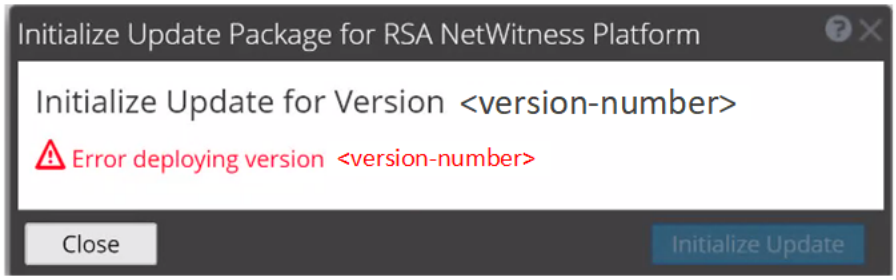
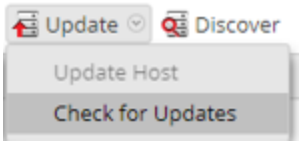
Message d'erreur	Si vous effectuez une mise à niveau de NetWitness Platform 11.x.x.x vers 11.6.x.x ou version ultérieure, la mise à niveau de l'interface utilisateur hors ligne échoue avec le message Erreur de téléchargement.

Solution	1. Dans l'interface de ligne de commande (CLI), procédez comme suit :
	a. Connectez-vous en SSH au serveur NW.
	b. Exécutez la commande suivante :
	`upgrade-cli-client --upgrade --host-key <ID, IP address, hostname or display name of host> --version <version number>`
	`For example:`
	`upgrade-cli-client --upgrade --host-key <ID, IP address, hostname or display name of host> --version 11.6.0.0`
	2. Une fois le serveur NW mis à jour avec succès, connectez-vous à l'interface utilisateur du serveur NW et accédez à **(Admin) > Hôtes**, où vous êtes invité à redémarrer l'hôte.
	3. Cliquez sur **Redémarrer l'hôte** à partir de la barre d'outils.
	Pour mettre à niveau tous les autres hôtes directement depuis l'interface utilisateur :
	1. Cliquez sur **Démarrer la mise à jour** dans la boîte de dialogue **Mise à jour disponible**.

Une fois l’hôte mis à niveau, vous êtes invité(e) à le redémarrer.

2. Cliquez sur **Redémarrer l'hôte** à partir de la barre d'outils.

Erreur lors du déploiement de la version <numéro de version> avec des paquets de mise à jour manquants

Message d'erreur	
Problème	L'erreur lors du déploiement de la version <numéro de version> s'affiche dans la boîte de dialogue **Initialiser le package de mise à jour pour NetWitness Platform** après avoir cliqué sur**Initialiser la mise à jour** si le package de mise à jour est corrompu.
Solution	1. Cliquez sur **Fermer** pour fermer la boîte de dialogue. 2. Retirez le dossier de version du dossier temporaire. 3. Assurez-vous que le service salt-master est en cours d'exécution. 4. Recopiez le fichier compressé du pack de mise à jour sur le dossier temporaire. 5. Dans la barre d'outils d'affichage **Hôtes**, sélectionnez **Vérifier les mises à jour** à nouveau.  6. Cliquez sur **Initialiser la mise à jour**. 7. Cliquez sur **Mettre à jour** > **Mettre à jour les hôtes** dans la barre d'outils. 8. Cliquez sur **Commencer la mise à jour** dans la boîte de dialogue **Mise à jour disponible**. Une fois l'hôte mis à jour, vous êtes invité à le redémarrer. 9. Cliquez sur **Redémarrer** à partir de la barre d'outils.

Erreur d'échec de la mise à niveau

Message d'erreur	Vous recevrez une erreur semblable à celle-ci dans le journal des erreurs lors de la tentative de mise à jour vers la version 11.6 ou ultérieure : `FATAL: Chef::Exceptions::Package: yum_package[rsa-protobufs-rt] (rsa-audit::packages line 11) had an error: Chef::Exceptions::Package: No version specified, and no candidate version available for rsa-protobufs-rt`

Cause	Des builds/rpms personnalisés sont installés pour certains composants installés sur les hôtes, comme dans le cas de l'installation de correctifs.

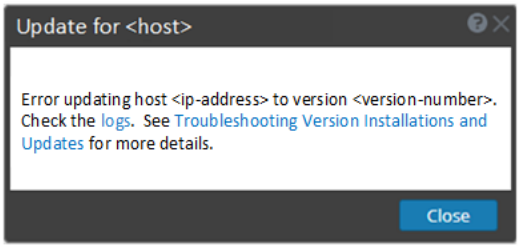
Solution	**Pour résoudre le problème :**
	1. Connectez-vous en SSH au Serveur d'administration.
	2. Localisez le fichier de descripteur de composant en exécutant la commande suivante.
	`cd /etc/netwitness/component-descriptor/`
	3. Ouvrez le fichier de descripteur de composant en exécutant la commande suivante.
	`vi nw-component-descriptor. json`
	4. Recherchez la section « packages » pour le composant pour lequel vous avez un build/rpm personnalisé. Par exemple, ci-dessous sont présentés les détails du package pour l'hôte « concentrateur » doté d'un build/rpm personnalisé.
	`"concentrator": {`
	`"cookbook_name": "rsa-concentrator",`
	`"service_names": ["rsa-nw-concentrator"],`
	`"family": "launch",`
	`"default_port": xxxx, "description": "Concentrator",`
	`"packages":[{ "name": "rsa-nw-concentrator",`
	`"version" : "11.6.0.0-2003001075220.5.cecf24b.e.17.centos"`
	`},`
	5. Supprimez les détails complets de la version, y compris le caractère (,) dans la section Packages. Par exemple, après avoir supprimé les détails de la version, elle devrait ressembler à l'illustration ci-dessous.
	`"packages": [{`
	`"name": "rsa-nw-concentrator"`
	`},`
	Remarque : Vous devez supprimer les détails de version de tous les hôtes dotés de builds/rpms personnalisés dans le descripteur de composant du serveur d'administration.
	6. Exécutez à nouveau le processus de mise à niveau.

Erreur de mise à jour du référentiel externe

Message d'erreur	Vous recevrez une erreur similaire à l'erreur suivante lors d'une tentative de mise à jour vers une nouvelle version à partir de : `.Repository 'nw-rsa-base': Error parsing config: Error parsing "baseurl = 'https://nw-node-zero/nwrpmrepo /<version-number>/RSA'": URL must be http, ftp, file or https not ""`
Cause	Chemin spécifié incorrect.
Solution	Vérifiez que : • l'URL existe sur l'hôte du serveur NW.

	• vous avez utilisé le chemin d'accès correct et supprimé les espaces qu'il contient.

Erreur d’échec de la mise à jour de l’hôte

Message d’erreur	
Problème	Lorsque vous sélectionnez une version de mise à jour, puis cliquez sur **Mettre à jour** > **Mettre à jour l’hôte**, le processus de téléchargement réussit, mais le processus de mise à jour échoue.

Solution	1. Essayez d’appliquer à nouveau la mise à jour de version à l’hôte. Souvent, c’est tout ce que vous avez à faire.
	2. Si vous ne parvenez toujours pas à appliquer la nouvelle mise à jour : Surveillez les journaux suivants sur le serveur NW au fur et à mesure de sa progression (par exemple, exécutez la commande `tail -f` à partir de la ligne de commande) :
	`/var/netwitness/uax/logs/sa.log`
	`/var/log/netwitness/orchestration-server/orchestration-server.log`
	`/var/log/netwitness/deployment-upgrade/chef-solo.log`
	`/var/log/netwitness/config-management/chef-solo.log`
	`/var/lib/netwitness/config-management/cache/chef-stacktrace.out`
	L’erreur apparaît dans un ou plusieurs de ces journaux.
	3. Si vous ne parvenez toujours pas à appliquer la mise à jour, rassemblez les journaux de **étape 2** ci-dessus et contactez le support client.

Message d’erreur	
Problème	Lorsque vous sélectionnez une version de mise à jour et cliquez sur **Mettre à jour** > **Rechercher les mises à jour**, le message d’erreur **Non autorisé** s’affiche. Par conséquent, la connexion au service en direct échoue.
Solution	1. Assurez-vous que le test de la connexion Live réussit. 2. Mettez à jour https://update.netwitness.com/RSA-netwitness dans **(Admin)** > **Système** > **Mises à jour**. 3. Connectez-vous en SSH au serveur d’administration et sauvegardez `/etc/default/jetty`.

	4. Mettez à jour l'entrée suivante à la fin de JAVA_OPTIONS dans le `/etc/default/jetty`.
	`JAVA_OPTIONS="${JAVA_OPTIONS} -Drsa.nw.legacy.web.server.system.update.repo.url=https://update.netwitness.com/RSA-netwitness/ -Drsa.nw.legacy.system.update.auth.url=https://update.netwitness.com/authenticate "`
	5. Redémarrez le service jetty. Exécutez la commande suivante :
	`service jetty restart`

Erreur Packages de mise à jour manquants

Message d'erreur	**Initialiser la mise à jour pour la version xx.x.x.x** Les packages de mise à jour suivants sont manquants Télécharger les packages depuis NetWitness Link
Problème	Les packages de mise à jour suivants manquants s'affiche dans la boîte de dialogue **Initialiser le package de mise à jour pour NetWitness Platform** lorsque vous mettez à jour un hôte à partir de la vue **Hôtes** hors ligne et des packages sont manquants dans le dossier temporaire.
Solution	1. Cliquez sur Télécharger les packages depuis NetWitness Community dans la boîte de dialogue **Initialiser le package de mise à jour pour NetWitness Platform**. La page NetWitness Community contenant les fichiers de mise à jour pour la version sélectionnée s'affiche. 2. Sélectionnez les packages manquants à partir du dossier temporaire. La boîte de dialogue **Initialiser le package de mise à jour pour NetWitness Platform** s'affiche pour vous indiquer que le système est prêt à initialiser les packages de mise à jour.

Erreur de mise à jour du correctif vers un serveur non NW

Message d'erreur	Le `/var/log/netwitness/orchestration-server/orchestration-server.log` présente une erreur similaire au message d'erreur suivant : **`API|Failure /rsa/orchestration/task/update-config-management [counter=10 reason=IllegalArgumentException::Version '11.x.x.n' is not supported`**
Problème	Après avoir mis à jour l'hôte du serveur NW vers une version, vous devez mettre à jour tous les hôtes de serveur non NW vers la même version. Par exemple, si vous mettez à jour le serveur NW de 11.4.0.0 vers 11.6.0.0 ou version ultérieure, le seul chemin de mise à jour pour les hôtes de serveur non NW est la même version (c'est-à-dire 11.6.0.0). Si vous essayez de mettre à jour un hôte qui n'est pas un serveur NW vers une version différente (par exemple, de 11.4.0.0 à 11.4.x.x), vous obtiendrez cette erreur.
Solution	Effectuez l'une des opérations suivantes :

	• Effectuez une mise à jour de l'hôte serveur autre que NW vers la version 11.6.0.0 ou version ultérieure, ou • Ne mettez pas à jour l'hôte serveur autre que NW (conservez sa version actuelle)

Erreur Redémarrer l'hôte après la mise à jour à partir d'une ligne de commande

Message d'erreur	Vous recevrez un message dans l'interface utilisateur vous invitant à redémarrer l'hôte après la mise à jour et le redémarrage de l'hôte hors connexion. 
Cause	L'erreur ci-dessus se produit lorsque vous utilisez l'interface de ligne de commande pour redémarrer l'hôte. Vous devez utiliser l'interface utilisateur pour redémarrer l'hôte.
Solution	Redémarrez l'hôte dans la vue **Hôte** dans l'interface utilisateur.

Reporting Engine redémarre après une mise à niveau

Problème	Dans certains cas, après une mise à niveau vers la version 11.6 ou une version ultérieure de la version 11.x, telle que la version 11.4, le service Reporting Engine tente de redémarrer en permanence, sans succès.
Cause	Les fichiers de base de données pour les graphiques en direct, l'état des alertes ou l'état des rapports peuvent ne pas être chargés avec succès car les fichiers peuvent être corrompus.
Solution	**Pour résoudre le problème :** 1. Vérifiez quels fichiers de base de données sont corrompus : Accédez au fichier situé à l'adresse `/var/netwitness/reserver/rsa/soc/reporting-engine/logs/reporting-engine.log` et vérifiez les blocs suivants : • Si le fichier de la base de données des graphiques en direct est corrompu, les journaux suivants s'affichent : Attempt Failed!!! Clearing pending acquires. While trying to acquire a needed new resource, we failed to succeed more than the maximum number of allowed acquisition attempts (30). Last acquisition attempt exception: org.h2.jdbc.JdbcSQLException: File corrupted while reading record: null. Possible solution: use the recovery tool [90030-196] at org.h2.message.DbException.getJdbcSQLException(DbException.java:345) at org.h2.message.DbException.get(DbException.java:168) org.springframework.beans.factory.BeanCreationException: Error creating bean with name 'chartSummaryDAOImpl': Invocation of init method failed; nested exception is com.rsa.soc.re.exception.ReportingException: java.sql.SQLException: Connections could not be acquired from the underlying database! • Si le fichier de la base de données des statuts des alertes est corrompu, les

journaux suivants s'affichent :

```
Attempt Failed!!! Clearing pending acquires. While trying to acquire a needed new resource, we failed to succeed more than the maximum number of allowed acquisition attempts (30). Last acquisition attempt exception:

org.h2.jdbc.JdbcSQLException: File corrupted while reading record: null. Possible solution: use the recovery tool [90030-196]

    at org.h2.message.DbException.getJdbcSQLException(DbException.java:345)

    at org.h2.message.DbException.get(DbException.java:168)

org.springframework.beans.factory.UnsatisfiedDependencyException: Error creating bean with name 'alertStatusHandler': Unsatisfied dependency expressed through field 'alertExecutionStatsDAO'; nested exception is org.springframework.beans.factory.UnsatisfiedDependencyException: Error creating bean with name 'alertExecutionStatsDAOImpl': Unsatisfied dependency expressed through field 'persistedAlertExecutionStatsDAO'; nested exception is org.springframework.beans.factory.BeanCreationException: Error creating bean with name 'persistedAlertExecutionStatsDAOImpl'
```

- Si le fichier de la base de données des statuts des rapports est corrompu, les journaux suivants s'affichent :

```
org.h2.jdbc.JdbcSQLException: File corrupted while reading record: null. Possible solution: use the recovery tool [90030-196]
```

2. Pour résoudre la corruption du fichier de base de données des graphiques en direct, procédez comme suit :
   a. Arrêtez le service Reporting Engine.
   b. Déplacez le fichier `livechart.mv.db` depuis le dossier `/var/netwitness/reserver/rsa/soc/reporting-engine/livecharts` vers un emplacement temporaire.
   c. Redémarrez le service Reporting Engine.

   Remarque : Certaines données de graphiques en direct peuvent être perdues lors de l'exécution des étapes ci-dessus.
3. Pour résoudre le problème de corruption du fichier de la base de données de l'état d'alerte ou de l'état du rapport, procédez comme suit :
   a. Arrêtez le service Reporting Engine.
   b. Remplacez le fichier de base de données corrompu par le dernier fichier `alertstatusmanager.mv.db` ou `reportstatusmanager.mv.db` du dossier `/var/netwitness/reserver/rsa/soc/reporting-engine/archives`.
   c. Redémarrez le service Reporting Engine.

Pour plus d'informations, consultez l'article de la base de connaissances Redémarrage de Reporting Engine après la mise à niveau vers NetWitness Platform 11.4.

Problème	Après une mise à niveau vers la version 11.6 ou une version ultérieure, le service Reporting Engine ne redémarre pas.
Cause	Le service Reporting Engine peut ne pas démarrer pour l'une des raisons suivantes. - workspace.xml n'est pas mis à jour. - L'heure n'est pas convertie correctement dans la base de données livechart h2.

Solution	- JCR (référentiel Jackrabbit) est corrompu avec une violation de clé primaire.

	Pour résoudre le problème, exécutez l'outil de récupération de migration Reporting Engine (`rsa-nw-re-migration-recovery.sh`) sur le serveur d'administration sur lequel le service Reporting Engine est installé.
	Remarque : Vous pouvez trouver l'outil de récupération de migration Reporting Engine à l'emplacement ci-dessous.
	`/opt/rsa/soc/reporting-engine-<version number>-<Tag>/nwtools`
	Par exemple :
	`/opt/rsa/soc/reporting-engine-11.6.0.0-<Tag>/nwtools`
	1. Connectez-vous en SSH au Serveur d'administration.
	2. Décompressez l'outil RE (Reporting Engine), exécutez la commande suivante.
	`tar -xvf rsa-nw-re-recovery-tool-bundle.tar`
	3. (Facultatif) Si vous souhaitez décompresser le fichier de l'outil RE dans un autre répertoire, vous pouvez créer un répertoire et décompresser l'outil RE. Exécutez les commandes suivantes :
	`mkdir <NAME OF THE DIRECTORY>`
	`tar -xvf rsa-nw-re-recovery-tool-bundle.tar --directory <PATH OF THE DIRECTORY>`
	4. Exécutez le script à l'aide de la commande suivante.
	`./<PATH OF THE DIRECTORY>/rsa-nw-re-recovery-tool.sh`
	Pour plus d'informations, consultez l'article de la base de connaissances **Outil de récupération de migration de Reporting Engine**.

Service Log Collector (`nwlogcollector`)

Les journaux d'installation Log Collector publiés sur `/var/log/install/nwlogcollector_install.log` sur l'hôte exécutant le service `nwlogcollector`.

Message d'erreur	`<timestamp>.NwLogCollector_PostInstall: Lockbox Status : Failed to open lockbox: The lockbox stable value threshold was not met because the system fingerprint has changed. To reset the system fingerprint, open the lockbox using the passphrase.`
Cause	Le Lockbox du Log Collector ne s'est pas ouvert après la mise à jour.
Solution	Connectez-vous à NetWitness et réinitialisez l'empreinte digitale du système en réinitialisant le mot de passe de la valeur stable du système pour le Lockbox comme décrit dans la rubrique **Réinitialiser la valeur stable du système** sous la rubrique **Configurer les paramètres de sécurité du Lockbox** dans le *Guide de configuration de Log Collection*.

Message d'erreur	`<timestamp> NwLogCollector_PostInstall: Lockbox Status : Not Found`
Cause	Le Lockbox du Log Collector n'a pas été configuré après la mise à jour.

Solution	Si vous utilisez le Lockbox de Log Collector, connectez-vous à NetWitness et configurez le Lockbox, comme décrit dans la rubrique **Configurer les paramètres de sécurité Lockbox** du *Guide de configuration de Log Collection*.

Message d'erreur	`<timestamp>: NwLogCollector_PostInstall: Lockbox Status : Lockbox maintenance required: The lockbox stable value threshold requires resetting. To reset the system fingerprint, select Reset Stable System Value on the settings page of the Log Collector.`
Cause	Vous devez réinitialiser le champ du seuil de valeur stable pour le Lockbox du Log Collector.
Solution	Connectez-vous à NetWitness et redéfinissez le mot de passe de la valeur du système stable pour le Lockbox, comme décrit dans la section **Réinitialiser la valeur du système stable** de la rubrique **Configurer des paramètres de sécurité Lockbox** du *Guide de configuration de Log Collection*.

Message d'erreur	Decoder tente de démarrer la capture des événements mais échoue. `Aug 27 01:44:41 nwdecoder NwDecoder[8052]: [Decoder] [failure] The PF_RING driver is not installed.`
Cause	La configuration de capture du décodeur ne sera pas valide pour les clients utilisant la capture PF_RING (CentOS) et effectuant une mise à niveau directe vers 12.4 (AlmaLinux). Ils doivent d'abord migrer les appareils PF_RING vers DPDK, puis mettre à niveau les appareils.
Solution	**Pour résoudre le problème :** Reportez-vous à Migrer les appareils PF_RING vers DPDK pour obtenir des instructions de migration.

Serveur NW

Ces logs sont publiés dans `/var/netwitness/uax/logs/sa.log` sur l'hôte de serveur NW.

Problème	Après la mise à niveau, vous remarquerez l'un des éléments suivants : • Les journaux d'audit ne sont pas transmis à la configuration d'audit globale configurée. • le message suivant s'affiche dans le `sa.log`. `Syslog Configuration migration failed. Restart jetty service to fix this issue`
Cause	La migration de l'installation d'audit global du serveur NW n'a pas réussi à migrer à partir de 11.4.x.x ou 11.5.x.x. à 11.6.0.0 ou version ultérieure.
Solution	1. Ouvrez une session SSH sur le serveur NW. 2. Exécutez la commande suivante : `orchestration-cli-client --update-admin-node`

Orchestration

Ces logs du serveur d'orchestration sont publiés dans `/var/log/netwitness/orchestration-server/orchestration-server.log` sur l'hôte de serveur NW.

Problème	1. Échec de la tentative de mise à niveau d'un hôte de serveur non NW. 2. Nouvelle tentative échouée de mise à niveau pour cet hôte. Le message suivant s'affiche dans le `orchestration-server.log`. `"'file' _virtual_ returned False: cannot import name HASHES""`
Cause	Salt Minion a peut-être été mis à niveau et n'a jamais redémarré sur un hôte de serveur non NW

Solution	1. SSH vers l'hôte de serveur non NW dont la mise à niveau a échoué.
	2. Exécutez les commandes suivantes.
	`systemctl unmask salt-minion`
	`systemctl restart salt-minion`
	3. Réessayez la mise à niveau de l'hôte de serveur non NW.

Problème	Lorsque vous installez et orchestrez un nouveau noyau Nœud X 12.4 sur le serveur d'administration (Nœud 0) mis à niveau de 12.0 ou de versions antérieures vers 12.4, les services de base tels que Concentrator, Log Decoder, Log Collector, Archiver, Decoder, Appliance, Workbench, Warehouse Connector et Broker apparaissent inactifs dans la colonne **Services** de la vue **Admin** > **Hôtes**. Par conséquent, vous ne pouvez pas accéder aux services de base de l'interface utilisateur. Cela ne s'applique pas si vous orchestrez un nouveau noyau Nœud X 12.4 sur le serveur d'administration 12.4 fraîchement installé (non mis à niveau de la version 12.0 ou antérieure vers la version 12.4).
Cause	Le Nœud X principal 12.4 utilise un certificat de serveur SA dédié au lieu du certificat de Nœud 0 commun sous ses homologues de confiance s'il est orchestré directement sur un hôte du serveur d'administration 12.4 mis à niveau.

Solution	Avant de démarrer et d'orchestrer l'hôte Nœud X principal 12.4, exécutez les commandes suivantes.
	1.
	`mkdir -p /etc/netwitness/platform`
	`touch /etc/netwitness/platform/nw-upgrade-mode`
	N'effectuez ce contournement que si vous avez ignoré le contournement précédent (contournement 1). Avant de démarrer et d'orchestrer l'hôte Nœud X principal 12.4, exécutez les commandes suivantes.
	2.
	`touch /etc/netwitness/platform/nw-upgrade-mode`
	`nw-manage --refresh-host --host-key <core-node-x-salt-minion-uuid>`

	`systemctl restart <core-service-name>` **Remarque :** - Référez le fichier `/etc/salt/minion` pour trouver `<core-node-x-salt-minion-uuid>`. - Vous devez saisir le nom de service de base tel que **nwarchiver** (Archiver), **nwdecoder** (Decoder), **nwlogcollector** (Log Collector), **nwappliance** (Appliance), **nwconcentrator** (Concentrator), **nwlogdecoder** (Log Decoder), **nwbroker** (Broker), **nwworkbench** (Workbench) et **nwwarehouseconnector** (Warehouse Connector) dans `<core-service-name>`.

Service Reporting Engine

Les logs de mise à jour du Reporting Engine sont publiés dans le fichier `/var/log/re_install.log` sur l'hôte exécutant le service Reporting Engine.

Message d'erreur	`<timestamp> : Available free space in /var/netwitness/re-server/rsa/soc/reporting-engine [ ><existing-GB ] is less than the required space [ <required-GB> ]`
Cause	Échec de la mise à jour du Reporting Engine car vous ne disposez pas de suffisamment d'espace disque.
Solution	Libérez de l'espace disque pour disposer de l'espace requis mentionné dans le message log. Consultez la rubrique **Ajouter de l'espace supplémentaire pour les rapports volumineux** dans le *Guide de configuration de Reporting Engine* pour obtenir des instructions sur la façon de libérer de l'espace disque.

Event Stream Analysis

Problème	Après la mise à niveau vers la version 12.4 ou ultérieure, le serveur de corrélation ESA ne regroupe pas les événements des sources de données configurées.
Message d'erreur	`Invalid username or password at com.rsa.netwitness.streams.base.RecordSourceSubscription.run (RecordSourceSubscription.java:173)`
Solution	**Pour résoudre le problème :** Dans l'interface utilisateur NetWitness, 1. Accédez à (**CONFIGURER**) > **Règles** > **Contenu** > **Event Stream Analysis** > **Sources de données**. Le panneau **Sources de données** s'affiche. 2. Sélectionnez la source de données et cliquez sur **Modifier la source de données** dans la barre d'outils. La boîte de dialogue **Modifier la source de données** s'affiche.

	3. Dans la boîte de dialogue **Modifier la source de données**, effectuez l'une des opérations suivantes : • Sélectionnez **Authentification approuvée**. • Sélectionnez **Utiliser les informations d'identification** et saisissez le nom d'utilisateur et le mot de passe. 4. Cliquez sur **Tester la connexion** pour vous assurer qu'il peut communiquer avec le service ESA, puis cliquez sur **OK**. **Remarque :** Effectuez la procédure ci-dessus pour toutes les sources de données configurées. 5. Déployez tous les déploiements associés aux sources de données modifiées dans le panneau **Sources de données** une fois que vous avez terminé d'apporter des modifications aux sources de données.

Log Collector Windows d'ancienne génération

Problème	• Le Log Collector Windows d'ancienne génération apparaît comme inactif après la mise à niveau de SA vers la version 12.4 et de Log Collector Windows d'ancienne génération vers les versions 11.6.x ou 11.7.x. • Log Collector Windows d'ancienne génération apparaît comme inactif lorsque la pile est mise à niveau vers 12.4.
Cause	La mise à jour du certificat dans le nœud SA.
Solution	Reportez-vous à la section Log Collector Windows d'ancienne génération dans Exécuter les tâches postérieures à la mise à niveau.

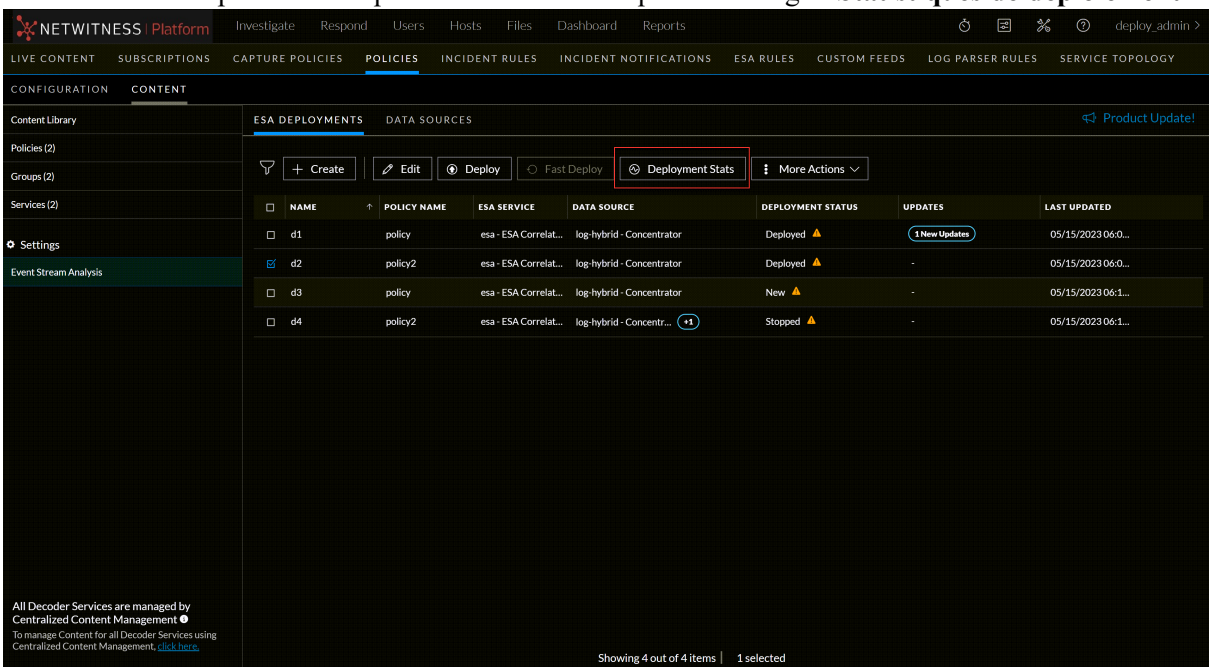
Informations de dépannage ESA

Les règles ESA ne créent pas d'alertes

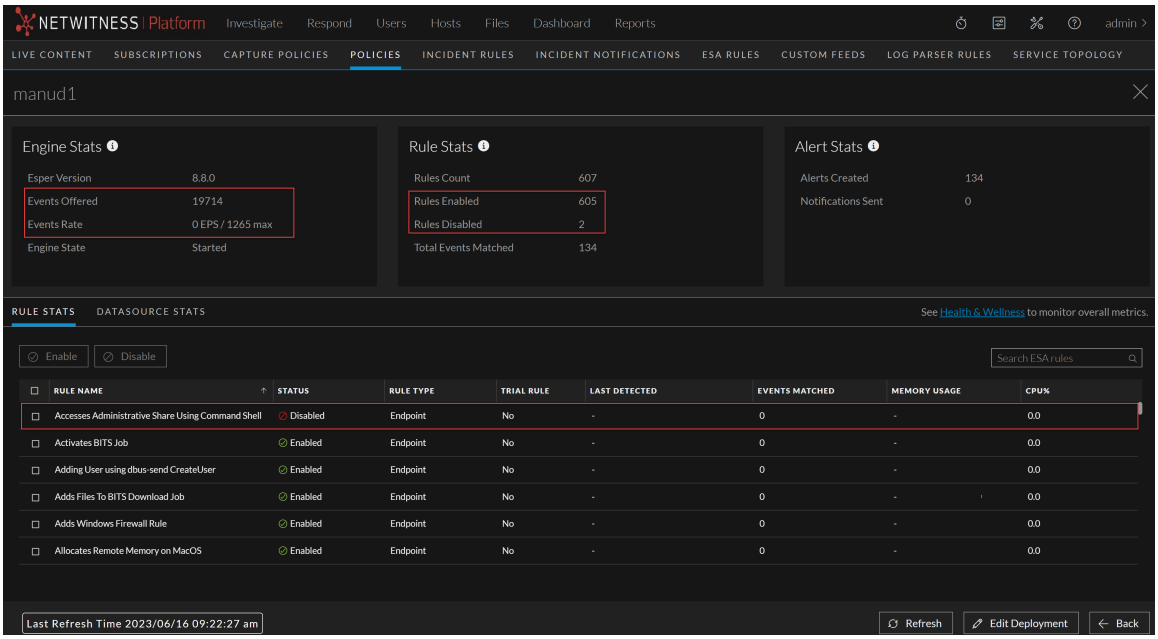
Si vous ne voyez aucune alerte, vérifiez l'état des déploiements de règles ESA.

1. Accédez à (**CONFIGURER**) > **Règles** > **Contenu** > **Event Stream Analysis** > **Déploiements ESA**.
   Le panneau **Déploiement ESA** s'affiche.

2. Sélectionnez le déploiement requis dans la liste et cliquez sur l'onglet **Statistiques de déploiement**.



3. La page Statistiques de déploiement s'affiche, indiquant l'état de vos services et déploiements ESA.
4. Pour chaque déploiement de règle ESA :
   a. Dans la section **Stat. Engine**, consultez **Événements proposés** et le **Taux fourni**. Cela confirme que les données sont agrégées et analysées correctement. Si vous voyez 0 pour Événements proposés, rien n'arrive pour le déploiement.
   b. Dans la section **Statistiques des règles**, examinez les **Règles activées** et les **Règles désactivées**. Si des règles sont désactivées, consultez la section **Statistiques des règles déployées** ci-dessous pour afficher les détails des règles désactivées. Les règles désactivées sont repérées par un cercle blanc. Les règles activées sont repérées par un cercle vert.



5. Si vous remarquez que des règles désactivées devraient être activées, procédez comme suit :

   a. Accédez à l'onglet  **(Configurer) > Règles ESA > Règles** et redéployez les déploiements de règles ESA qui contiennent des règles désactivées.

   b. Revenez à l'onglet **Services** et vérifiez si les règles sont toujours désactivées. Si les règles sont toujours désactivées, vérifiez les fichiers journaux du service de corrélation ESA, qui se trouvent à l'adresse `/var/log/netwitness/correlation-server/correlation-server.log`.

Remarque : Pour éviter une surcharge de traitement inutile, l'option Ignorer la casse a été supprimée de la boîte de dialogue Générateur de règle ESA - Créer une instruction pour les clés méta qui ne contiennent pas de valeurs de données textuelles. Lors de la mise à niveau vers la version 11.4 ou ultérieure, NetWitness Platform ne modifie pas les règles existantes pour l'option Ignorer la casse. Si l'option Ignorer la casse est sélectionnée pour une clé méta qui ne dispose plus de cette option dans une règle existante du Générateur de règles, une erreur se produit si vous essayez de modifier l'instruction et de l'enregistrer à nouveau sans désactiver la case à cocher.

Exemple de message d'avertissement du serveur de corrélation ESA pour les clés méta manquantes

Si vous voyez un message d'avertissement dans les journaux d'erreurs du serveur de corrélation ESA, cela signifie qu'il existe une différence entre le paramètre `default-multi-valued` et que les `multi-valued parameter` valeurs de la clé méta, le nouvel Endpoint, l'UEBA et les règles du contenu Live ne fonctionneront pas. Suivre la procédure **Mettre à jour les clés méta de paramètres à valeurs multiples et à valeurs uniques pour les dernières règles de contenu Endpoint, UEBA et RSA Live** dans le *guide de configuration ESA* devrait résoudre le problème.

Exemple de message d'avertissement à valeurs multiples

```
2019-08-23 08:55:07,602 [ deployment-0] WARN Stream|[alert, alert_id,
browserprint, cert_thumbprint, checksum, checksum_all, checksum_dst, checksum_
src, client_all, content, context, context_all, context_dst, context_src, dir_
path, dir_path_dst, dir_path_src, directory, directory_all, directory_dst,
directory_src, email_dst, email_src, feed_category, feed_desc, feed_name,
file_cat, file_cat_dst, file_cat_src, filename_dst, filename_src, filter,
function, host_all, host_dst, host_orig, host_src, host_state, ip_orig, ipv6_
orig, OS, param, param_dst, param_src, registry_key, registry_value, risk,
risk_info, risk_suspicious, risk_warning, threat_category, threat_desc,
threat_source, user_agent] are still MISSING from multi-valued
```

Exemple de message d'avertissement à valeur unique

```
2019-08-23 08:55:07,602 [ deployment-0] WARN Stream|[accesses, context_target,
file_attributes, logon_type_desc, packets] are still MISSING from single-
valued
```

Utiliser le portail de la communauté NetWitness pour obtenir de l'aide

Vous pouvez utiliser le portail communautaire NetWitness pour rechercher des documents spécifiques, trouver des informations relatives à la fin de vie des appliances et lire des blogs.

Ressources d'assistance en libre-service

Il existe plusieurs options qui vous fournissent de l'aide lorsque vous en avez besoin pour l'installation et l'utilisation de NetWitness :

- Consultez la documentation pour tous les aspects de NetWitness ici : https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation
- Utilisez les champs **Recherche** et **Créer une publication** du portail NetWitness Community pour trouver des informations spécifiques ici : https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions
- Voir la base de connaissances NetWitness : https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base
- Reportez-vous à la section Dépannage dans les guides.
- Voir également Articles de blog sur NetWitness® Platform.
- Si vous avez besoin d'une aide supplémentaire, contactez le support NetWitness.

Contactez le support NetWitness

Si vous contactez le support NetWitness, vous devrez vous trouver devant votre ordinateur. Soyez prêt à fournir les informations suivantes :

- Le numéro de version du produit ou de l'application NetWitness Platform que vous utilisez.
- Le type de matériel que vous utilisez.

Utilisez les informations de contact suivantes si vous avez des questions ou si vous avez besoin d'aide.

Portail NetWitness Community	https://community.netwitness.com Dans le menu principal, cliquez sur **Support > Portail de demandes > Afficher mes demandes**.
Contacts internationaux (contacter le support NetWitness)	https://community.netwitness.com/t5/support/ct-p/support
Communauté	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions
Mise à jour NW	https://update.netwitness.com

Interface utilisateur Live	https://live.netwitness.com

Réactions sur la documentation du produit

Vous pouvez envoyer un e-mail à l'adresse nwdocsfeedback@netwitness.com pour faire part de vos réactions sur la documentation RSA NetWitness Platform.