

# Notes de version de Sentinel 8.5

Août 2021

Sentinel 8.5 résout plusieurs problèmes des versions antérieures et ajoute quelques nouvelles fonctionnalités.

La plupart de ces améliorations ont été apportées en réponse directe aux suggestions de nos clients. Nous vous remercions du temps que vous avez pris pour nous écrire. Nous espérons que vous continuerez à nous aider pour que nos produits répondent à tous vos besoins. Vous pouvez publier vos commentaires sur le [forum Sentinel](#), notre communauté en ligne qui reprend aussi des informations sur le produit, des blogues et des liens vers des ressources utiles. Vous pouvez également partager vos idées pour améliorer le produit sur le [Portail des idées](#).

La documentation de ce produit est disponible aux formats HTML et PDF sur une page qui ne nécessite pas de connexion. Si vous avez des suggestions pour améliorer la documentation, cliquez sur l'icône de commentaire sur l'une des pages de la version HTML de la documentation publiée sur la page de [documentation de Sentinel](#). Pour télécharger ce produit, rendez-vous sur le site Web de [téléchargement de produits](#).

- ♦ « Nouveautés » page 1
- ♦ « Configuration système requise » page 4
- ♦ « Informations sur la licence et l'achat » page 4
- ♦ « Installation de Sentinel 8.5 » page 4
- ♦ « Mise à niveau vers Sentinel 8.5 » page 4
- ♦ « Problèmes connus » page 5
- ♦ « Contacter Micro Focus » page 12
- ♦ « Mentions légales » page 12

## Nouveautés

Les sections suivantes décrivent les principales fonctionnalités de cette version, ainsi que les problèmes résolus dans cette édition :

- ♦ « Intégration d'ArcSight Intelligence à Sentinel » page 2
- ♦ « MITRE ATT&CK » page 2
- ♦ « Mise à niveau du JDK » page 2
- ♦ « Stockage des événements bruts à partir du connecteur » page 3
- ♦ « Prise en charge de TLS » page 3
- ♦ « Versions du système d'exploitation (OS) » page 3
- ♦ « Correctifs logiciels » page 3

## Intégration d'ArcSight Intelligence à Sentinel

Avec cette version, Sentinel permet d'intégrer les technologies d'analyse intéressantes d'ArcSight Intelligence. Par conséquent, les utilisateurs de Sentinel peuvent obtenir un score de risque presque en temps réel et l'utiliser dans le cadre d'analyses approfondies dans leur propre règle de corrélation, etc. Sentinel est dès lors davantage orienté sur la recherche de menaces.

ArcSight Intelligence est une solution d'analyse du comportement des utilisateurs et des entités qui fait appel à la science des données et à des analyses avancées pour identifier les entités et les comportements les plus à risque au niveau de votre organisation. Intelligence établit tout d'abord le comportement normal de vos entités organisationnelles, utilise des analyses avancées pour identifier les comportements inhabituels des entités, puis fournit un score de risque approprié à chacune de ces entités.

Sentinel permet d'intégrer ArcSight Intelligence 6.3. Grâce à cette intégration, les utilisateurs de Sentinel peuvent envoyer leurs données à ArcSight Intelligence à des fins d'analyse et recevoir les détails du score de risque des entités d'Intelligence. Sentinel détecte ainsi tous les utilisateurs et entités les plus à risque de l'organisation qui pourraient compromettre l'ensemble du système et représenter une menace potentielle.

## MITRE ATT&CK

MITRE ATT&CK aide les équipes de cybersécurité à évaluer l'efficacité des processus de leur centre SOC (Security Operations Center), ainsi que les mesures de protection pour identifier les domaines à améliorer. MITRE ATT&CK est une base de connaissances sur les tactiques et techniques employées par les cybercriminels, basée sur des observations concrètes et accessible dans le monde entier. La base de connaissances MITRE ATT&CK sert de base pour développer des modèles de menace et des méthodologies spécifiques dans le secteur privé, dans l'administration publique et dans la communauté des produits et services de cybersécurité.

À partir de cette version de Sentinel, les administrateurs peuvent assigner des règles de corrélation à un ID MITRE ATT&CK. La matrice MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) est un langage commun des tactiques et techniques employées par les cybercriminels, basé sur des observations réelles.

Les administrateurs Sentinel peuvent désormais assigner leur propre règle de corrélation prédéfinie ou personnalisée directement à l'ID MITRE ATT&CK. Par conséquent, ils disposent de nombreuses analyses de données, ce qui leur permet de savoir quelles sont les règles qui sont déclenchées ou quelles sont les tactiques et techniques MITRE exploitées par leurs clients. Sentinel leur fournit un ensemble d'outils leur permettant d'obtenir immédiatement une vue d'ensemble de leur réseau et des attaques les plus importantes qu'ils doivent empêcher.

Si une règle de corrélation assignée à un ID MITRE ATT&CK est déclenchée, les événements déclenchés auront un ID et un nom MITRE ATT&CK. Ces événements sont analysés via un widget disponible dans un tableau de bord d'état de santé de sécurité par défaut. Les dix premiers noms MITRE ATT&CK apparaissent dans ce tableau de bord pour une période de 1 jour et un intervalle d'affichage de 1 heure.

## Mise à niveau du JDK

Afin d'éviter les failles de sécurité (CVE-2021-2161, CVE-2021-2163, CVE-2021-2341, CVE-2021-2432, CVE-2021-2369, CVE-2021-2388) et pour utiliser les fonctions de sécurité des nouvelles normes JDK, JDK est mis à niveau de la version 1.8.0\_update242 vers la version 1.8.0\_update302.

## Stockage des événements bruts à partir du connecteur

À partir de la version 2021.1r1, le connecteur Sentinel Syslog autorise le stockage des événements bruts provenant des connecteurs ArcSight SmartConnector. Il s'agit des événements non traités qui sont directement générés par le périphérique final. Ce paramètre peut être activé en cochant l'option **Preserve Raw Event** (Conserver l'événement brut) dans le connecteur SmartConnector correspondant.

## Prise en charge de TLS

La prise en charge de TLS 1.0 et de TLS 1.1 a été supprimée.

## Versions du système d'exploitation (OS)

**Installation traditionnelle** : Sentinel est désormais certifié sur la nouvelle plate-forme suivante :

- ♦ Red Hat Enterprise Linux (RHEL) 8.3

**Systèmes d'exploitation obsolètes** : les systèmes d'exploitation suivants sont désormais obsolètes depuis que RHEL et SLES ont supprimé leur prise en charge :

- ♦ RHEL 7.6 et 7.7
- ♦ SLES 15 SP1

## Correctifs logiciels

Sentinel 8.5 inclut des correctifs logiciels qui résolvent les problèmes suivants :

- ♦ [« La conversion au format FIPS sur le serveur Sentinel remplace le protocole TLS 1.2 par TLS 1.1 » page 3](#)
- ♦ [« Échec des appels REST Sentinel après la mise à niveau du client Java Sentinel » page 3](#)
- ♦ [« Erreur lors de la génération d'un nouveau rapport » page 4](#)

### La conversion au format FIPS sur le serveur Sentinel remplace le protocole TLS 1.2 par TLS 1.1

**Problème** : lors de la conversion au format FIPS sur le serveur Sentinel, le protocole passe de TLS 1.2 à TLS 1.1, ce qui interrompt la connexion entre le SAM et le serveur Sentinel. Toutefois, le client doit utiliser TLS 1.2.

**Correction** : désormais, lors de la conversion au format FIPS, la version 1.2 de TLS n'est pas remplacée par la version 1.1.

### Échec des appels REST Sentinel après la mise à niveau du client Java Sentinel

**Problème** : après la mise à niveau du client Java Sentinel de la version 8.1 vers la version 8.2, les appels REST échouent.

**Correction** : désormais, après la mise à niveau du client Java Sentinel de la version 8.1 vers la version 8.2, les appels REST n'échouent plus.

## Erreur lors de la génération d'un nouveau rapport

**Problème** : erreur lors de la génération d'un nouveau rapport. La principale cause est l'altération du keystore ou un mot de passe incorrect.

**Correction** : pas d'erreur lors de la génération d'un nouveau rapport.

## Configuration système requise

Pour obtenir des informations sur la configuration matérielle requise, ainsi que sur les systèmes d'exploitation et les navigateurs pris en charge, reportez-vous à la [configuration système requise pour Sentinel](#).

## Informations sur la licence et l'achat

Pour acquérir une licence d'entreprise ou mettre à niveau votre licence existante, appelez le 1-800-529-3400, envoyez un message électronique à l'adresse [info@microfocus.com](mailto:info@microfocus.com) ou rendez-vous sur <https://www.microfocus.com/fr-fr/products/netiq-sentinel/contact>.

## Installation de Sentinel 8.5

Pour plus d'informations sur l'installation de Sentinel 8.5, reportez-vous au [guide d'installation et de configuration de Sentinel](#).

---

**REMARQUE** : tous les hôtes utilisés pour le serveur Sentinel et ses composants doivent être créés dans un environnement à résolution DNS bidirectionnel (nom d'hôte vers IP et IP vers nom d'hôte).

---

## Mise à niveau vers Sentinel 8.5

Vous pouvez effectuer une mise à niveau vers Sentinel 8.5 à partir de n'importe quelle version antérieure de Sentinel (version 8.2 ou ultérieure).

---

**IMPORTANT** : en raison de la dernière mise à niveau du JDK, pour configurer LDAPS et SDK, l'utilisateur doit utiliser un nom d'hôte (qui doit pouvoir être résolu) au lieu d'une adresse IP.

---

---

**IMPORTANT** : la procédure de mise à niveau de l'installation traditionnelle et de l'appliquatif a changé. Suivez la procédure décrite à la section [Paramètres de communication de grappe sécurisée dans Elasticsearch](#). Cette procédure ne s'applique que si vous effectuez une mise à niveau de Sentinel 8.3.1 ou version antérieure vers la dernière version.

---

---

**IMPORTANT** : vous pouvez effectuer une mise à jour hors ligne en téléchargeant l'image ISO de correctif hors ligne pour chaque applicatif. Pour plus d'informations, reportez-vous à la section [Mise à jour hors ligne](#).

---

---

**AVERTISSEMENT** : si vous effectuez une mise à niveau à partir d'une version antérieure à Sentinel 8.3, vous devez assigner manuellement l'autorisation [Envoyer des événements et des pièces jointes](#) aux utilisateurs qui ne sont pas administrateurs et qui envoient des événements ou des pièces jointes à Sentinel. Si vous n'assignez pas cette autorisation, Sentinel ne recevra plus les événements et les pièces jointes de Change Guardian et de Secure Configuration Manager.

---

Pour une installation traditionnelle, reportez-vous à la section [Mise à niveau du système d'exploitation du Guide d'installation et de configuration de Sentinel](#).

## Problèmes connus

Micro Focus s'efforce de garantir que ses produits offrent des solutions de qualité qui répondent aux besoins logiciels de votre entreprise. Les problèmes connus suivants font actuellement l'objet de recherches visant à trouver des solutions. Si vous avez besoin d'aide pour résoudre un problème, contactez le [support technique](#).

La mise à jour de Java 8 incluse dans Sentinel peut avoir des répercussions sur les plug-ins suivants :

- ◆ Cisco SDEE Connector
- ◆ Connecteur SAP (XAL)
- ◆ Remedy Integrator

Nous réglerons tout problème avec ces plug-ins conformément aux procédures standard de traitement des défauts et dans l'ordre prévu par celles-ci. Pour plus d'informations sur les stratégies de support, reportez-vous aux [Stratégies de support](#).

- ◆ « Impossible d'afficher le graphique Prévission de la capacité du stockage » page 6
- ◆ « Erreur lors du lancement d'un tableau de bord Kibana après la mise à niveau de Sentinel » page 6
- ◆ « Impossible de copier les liens d'alerte de toutes les alertes dans une vue d'alerte dans Mozilla Firefox et Microsoft Edge » page 6
- ◆ « L'installation de Sentinel, de Collector Manager et de Correlation Engine en tant qu'image d'applicatif OVF n'affiche pas l'écran de connexion » page 7
- ◆ « L'applicatif Sentinel 8.2 dans Microsoft Hyper-V Server 2016 ne démarre pas quand vous redémarrez » page 7
- ◆ « Erreur lors de la mise à niveau vers l'applicatif Sentinel 8.2 HA » page 7
- ◆ « L'installation des applicatifs Collector Manager et Correlation Engine échoue dans toutes les langues sauf l'anglais dans le mode MFA » page 7
- ◆ « Problèmes d'utilisation dans les écrans d'installation de l'applicatif » page 8
- ◆ « Collector Manager manque de mémoire si la synchronisation horaire est activée dans open-vm-tools » page 8
- ◆ « Authentification SQL requise par Agent Manager en cas d'activation du mode FIPS 140-2 » page 8
- ◆ « Affichage d'une erreur lorsque l'installation de Sentinel en haute disponibilité n'utilise pas le mode FIPS 140-2 » page 8
- ◆ « La commande keytool affiche un message d'avertissement » page 9
- ◆ « Sentinel ne traite pas les flux de renseignements sur les menaces en mode FIPS » page 9
- ◆ « La déconnexion de Sentinel Main n'entraîne pas la déconnexion des tableaux de bord, et inversement, en mode d'authentification multi-critères » page 9
- ◆ « Le tableau de bord personnalisé Kibana ne s'affiche pas après la mise à niveau vers Sentinel 8.3.1 » page 9
- ◆ « Un message d'erreur de conflit s'affiche au lancement de Kibana » page 10
- ◆ « Au redémarrage du système d'exploitation Redhat 8.1 ou 8.2, Sentinel ne démarre pas automatiquement » page 10
- ◆ « Un message d'erreur s'affiche à l'ouverture de la console de gestion de l'applicatif Sentinel » page 10

- ♦ « Les utilisateurs qui disposent de l'autorisation de visualisation Masquer la gestion peuvent toujours voir l'onglet Gestion sur la page Kibana » page 10
- ♦ « Lorsque l'administrateur modifie le rôle utilisateur d'alertes, les modifications ne sont pas immédiatement mises à jour sur la page Kibana » page 10
- ♦ « Un message d'erreur s'affiche au lancement du tableau de bord de visualisation en tant qu'utilisateur locataire » page 10
- ♦ « Sous RHEL, RCM et RCE ne se connectent pas au serveur lorsque la fonction CRL est activée » page 11
- ♦ « RCM ne transfère pas les événements au serveur Sentinel lorsque les fonctions Visualisation des événements, FIPS et CRL sont activées » page 11
- ♦ « Les rapports d'incident échouent avec des exceptions après la mise à niveau du système d'exploitation d'une version antérieure vers la dernière version » page 11
- ♦ « Une exception est consignée lors de la première tentative de réindexation » page 11
- ♦ « Erreur lors de l'exécution de `convert_to_fips.sh` dans la build d'applicatif RCM/RCE Sentinel 8.5 » page 11

## Impossible d'afficher le graphique Prévision de la capacité du stockage

**Problème :** Dans **Sentinel Main** (Sentinel - Principal) > **Stockage** > **Santé**, le graphique **Prévision de la capacité du stockage** n'est pas disponible, car Zulu OpenJDK n'inclut pas les polices nécessaires.

**Solution :** utilisez les commandes suivantes pour installer les polices :

- ♦ `yum install fontconfig`
- ♦ `yum install dejavu`

## Erreur lors du lancement d'un tableau de bord Kibana après la mise à niveau de Sentinel

**Problème :** lors du lancement d'un tableau de bord Kibana, le message suivant s'affiche : `No default index pattern. You must select or create one to continue.`

**Solution :** pour définir un modèle d'index Kibana comme modèle d'index par défaut, procédez comme suit :

1. Sélectionnez l'un des modèles suivants :
  - ♦ `alerts.alerts`
  - ♦ `security.events.normalized_*`
2. Cliquez sur **Set as Default** (Définir par défaut).

## Impossible de copier les liens d'alerte de toutes les alertes dans une vue d'alerte dans Mozilla Firefox et Microsoft Edge

**Problème :** l'option **Sélectionner les <nombre d'alertes> alertes > Copier le lien d'alerte** ne fonctionne pas dans Firefox ni dans Edge.

**Solution :** effectuez la procédure suivante.

1. Sélectionnez manuellement toutes les alertes de chaque page de la vue d'alerte en activant la case à cocher qui permet de sélectionner toutes les alertes.

2. Cliquez sur **Copier le lien d'alerte**.
3. Collez-le dans l'application de votre choix.

## L'installation de Sentinel, de Collector Manager et de Correlation Engine en tant qu'image d'applcatif OVF n'affiche pas l'écran de connexion

**Problème** : le programme d'installation s'arrête à l'écran d'installation en cours et n'affiche pas l'écran de connexion, même si l'installation est terminée.

**Solution** : redémarrez la machine virtuelle et lancez Sentinel, Collector Manager ou Correlation Engine.

## L'applcatif Sentinel 8.2 dans Microsoft Hyper-V Server 2016 ne démarre pas quand vous redémarrez

**Problème** : Dans Hyper-V Server 2016, l'applcatif Sentinel ne démarre pas lorsque vous le redémarrez et il affiche le message suivant :

```
A start job is running for dev-disk-by\..
```

Ce problème se produit parce que le système d'exploitation modifie l'UUID du disque lors de l'installation. Par conséquent, lors du redémarrage, il ne trouve pas le disque.

**Solution** : Modifiez manuellement le disque UUID. Pour plus d'informations, reportez-vous à [l'article 7023143 de la base de connaissances](#).

## Erreur lors de la mise à niveau vers l'applcatif Sentinel 8.2 HA

**Problème** : Lorsque vous effectuez une mise à niveau vers l'applcatif Sentinel 8.2 HA, Sentinel affiche l'erreur suivante :

```
Installation of novell-SentinelSI-db-8.2.0.0-<version> failed:  
with --nodeps --force) Error: Subprocess failed. Error: RPM failed: Command exited  
with status 1.  
Abort, retry, ignore? [a/r/i] (a):
```

**Solution** : Avant de répondre à l'invite ci-dessus, procédez comme suit :

- 1 Démarrez une autre session à l'aide de PuTTY ou de logiciels similaires sur l'hôte sur lequel vous effectuez la mise à niveau.
- 2 Ajoutez l'entrée suivante dans le fichier `/etc/csync2/csync2.cfg` :  
`/etc/opt/novell/sentinel/config/configuration.properties`
- 3 Supprimez le dossier `sentinel` de `/var/opt/novell` :  
`rm -rf /var/opt/novell/sentinel`
- 4 Revenez à la session à partir de laquelle vous avez démarré la mise à niveau et entrez `r` pour la poursuivre.

## L'installation des applicatifs Collector Manager et Correlation Engine échoue dans toutes les langues sauf l'anglais dans le mode MFA

**Problème** : l'installation des applicatifs Collector Manager et Correlation Engin échoue en mode MFA si la langue du système d'exploitation n'est pas l'anglais.

**Solution** : installez les applicatifs Collector Manager et Correlation Engine en anglais. À la fin de l'installation, modifiez la langue si nécessaire.

## Problèmes d'utilisation dans les écrans d'installation de l'applicatif

**Problème** : Dans certains cas, les boutons **Suivant** et **Précédent** ne s'affichent pas ou sont désactivés dans les écrans d'installation de l'applicatif, par exemple :

- ◆ Lorsque vous cliquez sur **Précédent** dans l'écran de vérification préalable de Sentinel pour modifier ou passer en revue les informations contenues dans l'écran des paramètres réseau de l'applicatif de serveur Sentinel, aucun bouton **Suivant** n'est disponible pour poursuivre l'installation. Le bouton **Configurer** permet uniquement de modifier les informations spécifiées.
- ◆ Si vous avez spécifié des paramètres réseau incorrects, l'écran de vérification préalable de Sentinel indique que vous ne pouvez pas poursuivre l'installation, car les informations réseau sont incorrectes. Aucun bouton **Précédent** n'est disponible pour revenir à l'écran précédent afin de modifier les paramètres réseau.

**Solution** : Redémarrez l'installation de l'applicatif.

## Collector Manager manque de mémoire si la synchronisation horaire est activée dans open-vm-tools

**Problème** : Si vous installez et activez manuellement la synchronisation horaire dans open-vm-tools, ils synchronisent régulièrement l'heure entre l'applicatif Sentinel (invité) et le serveur VMware ESX (hôte). Ces synchronisations horaires peuvent avoir pour conséquence que l'horloge de l'invité soit en retard ou en avance par rapport à l'heure du serveur ESX. Jusqu'à ce que l'heure soit synchronisée entre l'applicatif Sentinel (invité) et le serveur ESX (hôte), Sentinel ne traite pas les événements. Par conséquent, un nombre élevé d'événements sont placés en attente dans le gestionnaire Collector Manager, qui peut finir par abandonner des événements dès qu'il a atteint son seuil. Pour éviter ce problème, Sentinel désactive la synchronisation horaire par défaut dans la version des outils open-vm-tools disponible dans Sentinel.

**Solution** : Désactivez la synchronisation horaire. Pour plus d'informations sur la désactivation de la synchronisation horaire, reportez-vous à la section [Disabling Time Synchronization \(Désactivation de la synchronisation horaire\)](#).

## Authentification SQL requise par Agent Manager en cas d'activation du mode FIPS 140-2

**Problème** : lorsque le mode FIPS 140-2 est activé dans Sentinel, l'utilisation de l'authentification Windows pour Agent Manager entraîne l'échec de la synchronisation avec la base de données Agent Manager.

**Solution** : Utilisez l'authentification SQL pour Agent Manager.

## Affichage d'une erreur lors de l'installation de Sentinel en haute disponibilité n'utilise pas le mode FIPS 140-2

**Problème** : l'installation de Sentinel en haute disponibilité (HA) en mode non FIPS 140-2 s'effectue correctement, mais le message d'erreur suivant s'affiche à deux reprises :

```
/opt/novell/sentinel/setup/configure.sh: line 1045: [: too many arguments
```



**Solution** : ce message d'erreur est normal et vous pouvez l'ignorer en toute sécurité. Même si le programme d'installation affiche ce message d'erreur, la configuration de Sentinel en haute disponibilité fonctionne en mode non-FIPS 140-2.

## La commande keytool affiche un message d'avertissement

**Problème** : lorsque vous utilisez la commande Keytool, l'avertissement suivant s'affiche :

```
The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12which is an industry standard format using "keytool -importkeystore -srckeystore /<sentinel_installation_path>/etc/opt/novell/sentinel/config/.webserverkeystore.jks -destkeystore /<sentinel_installation_path>/etc/opt/novell/sentinel/config/.webserverkeystore.jks -deststoretype pkcs12".
```

**Solution** : cet avertissement est normal et vous pouvez l'ignorer en toute sécurité. Bien que le message d'avertissement s'affiche, la commande Keytool fonctionne comme prévu.

## Sentinel ne traite pas les flux de renseignements sur les menaces en mode FIPS

**Problème** : En mode FIPS, lors du traitement des flux de renseignements sur les menaces prêts à l'emploi à partir d'URL, Sentinel affiche l'erreur suivante : `Received fatal alert: protocol_version` (Alerte fatale reçue : `version_protocole`). Ce problème se produit parce que les flux de menaces prêts à l'emploi prennent désormais en charge uniquement TLS 1.2, qui ne fonctionne pas en mode FIPS.

**Solution** : Effectuez les opérations suivantes :

1. Cliquez sur **Sentinel Main** (Sentinel - Principal) > **Intégration** > **Sources de renseignements sur les menaces**.
2. Éditez chaque URL pour remplacer le protocole `http` par `https`.

## La déconnexion de Sentinel Main n'entraîne pas la déconnexion des tableaux de bord, et inversement, en mode d'authentification multi-critères

**Problème** : En mode d'authentification multi-critères, si vous vous déconnectez de **Sentinel Main** (Sentinel - Principal), vous n'êtes pas déconnecté des tableaux de bord Sentinel, et inversement, en raison d'un problème lié à Advanced Authentication Framework.

**Solution** : Jusqu'à ce qu'un correctif soit disponible dans Advanced Authentication Framework, rafraîchissez l'écran pour afficher l'écran de connexion.

## Le tableau de bord personnalisé Kibana ne s'affiche pas après la mise à niveau vers Sentinel 8.3.1

**Problème** : le tableau de bord personnalisé Kibana ne s'affiche pas lorsque vous effectuez une mise à niveau de Sentinel 8.3 ou version antérieure vers Sentinel 8.3.1.

**Solution** : veillez à recréer le tableau de bord personnalisé après la mise à niveau de Sentinel.

## Un message d'erreur de conflit s'affiche au lancement de Kibana

**Problème** : après l'installation ou la mise à niveau de Sentinel, le message d'erreur de conflit s'affiche au premier lancement de Kibana.

**Solution** : ignorez le message d'erreur de conflit, car il n'y a pas d'impact sur les fonctionnalités.

## Au redémarrage du système d'exploitation Redhat 8.1 ou 8.2, Sentinel ne démarre pas automatiquement

**Problème** : après l'installation de Sentinel sur le système d'exploitation Redhat 8.1 ou 8.2, Sentinel (Server, RCM ou RCE) ne démarre pas automatiquement après le redémarrage.

**Solution** : remplacez la valeur de SELINUX par **SELINUX=disabled** dans le fichier `/etc/selinux/config`.

## Un message d'erreur s'affiche à l'ouverture de la console de gestion de l'applicatif Sentinel

**Problème** : après la mise à niveau vers Sentinel 8.3, lorsque vous essayez d'ouvrir la console de gestion de l'applicatif Sentinel de Correlation Engine (CE) ou de Collector Manager (CM) des serveurs HA (High Availability), un message d'erreur `Erreur 404 - Introuvable` s'affiche.

**Solution** : pour plus d'informations, reportez-vous au [document de la base de connaissances Micro Focus](#).

## Les utilisateurs qui disposent de l'autorisation de visualisation Masquer la gestion peuvent toujours voir l'onglet Gestion sur la page Kibana

**Problème** : après la mise à niveau vers Sentinel 8.4, les utilisateurs qui disposent de l'autorisation de visualisation Masquer la gestion peuvent toujours voir l'onglet Management (Gestion) de la page Kibana, mais ne peuvent pas accéder aux fonctions de cet onglet.

## Lorsque l'administrateur modifie le rôle utilisateur d'alertes, les modifications ne sont pas immédiatement mises à jour sur la page Kibana

**Problème** : les utilisateurs existants ne peuvent pas voir immédiatement les alertes sur la page Kibana, même si l'administrateur met à jour l'autorisation d'affichage de ces alertes.

**Solution** : vous devez vous déconnecter puis vous reconnecter lorsque l'autorisation utilisateur est mise à jour.

## Un message d'erreur s'affiche au lancement du tableau de bord de visualisation en tant qu'utilisateur locataire

**Problème** : lorsqu'un utilisateur locataire autre que celui par défaut lance le tableau de bord de visualisation, un message d'erreur **Interdit** s'affiche. Ce message d'erreur s'affiche chaque fois que le tableau de bord est lancé par l'utilisateur locataire autre que celui par défaut qui dispose de l'autorisation **View-only** (Affichage uniquement) pour l'option **Gestion** et qu'aucun utilisateur ne dispose de l'autorisation **Edit** (Éditer) pour l'option **Gestion** sous ce locataire.

**Solution** : ignorez le message d'erreur, car il n'y a pas d'impact sur les fonctionnalités.

## Sous RHEL, RCM et RCE ne se connectent pas au serveur lorsque la fonction CRL est activée

**Problème** : Remote Collector Manager (RCM) et Remote Correlation Engine (RCE) ne peuvent pas se connecter au serveur lorsque la fonction CRL est activée dans RHEL.

**Solution** : mettez à niveau la **version cURL** sur la machine vers la version 7.60 ou une version ultérieure.

## RCM ne transfère pas les événements au serveur Sentinel lorsque les fonctions Visualisation des événements, FIPS et CRL sont activées

**Problème** : dans le cas d'une nouvelle installation en mode distribué, après l'activation des services Visualisation des événements, FIPS et CRL, Remote Collector Manager (RCM) ne transfère pas les événements au serveur Sentinel.

**Solution** : si les fonctions Visualisation des événements et FIPS ou Visualisation des événements et CRL sont activées, RCM transfère les événements au serveur Sentinel.

## Les rapports d'incident échouent avec des exceptions après la mise à niveau du système d'exploitation d'une version antérieure vers la dernière version

**Problème** : lors de la mise à niveau du système d'exploitation d'une version antérieure vers la dernière version, les rapports d'incident échouent avec des exceptions.

## Une exception est consignée lors de la première tentative de réindexation

**Problème** : une exception est consignée lors de la première exécution de l'opération de réindexation.

## Erreur lors de l'exécution de `convert_to_fips.sh` dans la build d'applicatif RCM/RCE Sentinel 8.5

**Problème** : lorsque l'administrateur système exécute `convert_to_fips.sh` dans la build d'applicatif RCM/RCE Sentinel 8.5, après avoir fourni les informations d'identification correctes des utilisateurs en boucle continue, le message d'erreur ci-dessous s'affiche :

```
ERROR: Failed to connect to <Sentinel server IP>:  
Failed to retrieve token for communication channel.
```

**Solution** : effectuez la procédure suivante.

1. Quittez l'exécution du script.
2. Accédez à `<installation Sentinel RCM/RCE>/etc/opt/novell/sentinel/config/configuration.properties`.
3. Définissez la valeur de `rest.endpoint.port` sur le port correspondant du serveur Web.  
Par exemple : `rest.endpoint.port=8443`.
4. Réexécutez `convert_to_fips.sh`.

## Contacter Micro Focus

En cas de problème spécifique du produit, contactez le support Micro Focus via le site Web <https://www.microfocus.com/support-and-services/>.

Vous trouverez des informations ou des conseils techniques à partir de plusieurs sources :

- ♦ Documentation produit, articles de la base de connaissances et vidéos : <https://www.microfocus.com/support-and-services/>
- ♦ Pages de la communauté Micro Focus : <https://www.microfocus.com/communities/>

## Mentions légales

**© Copyright 2001 - 2021 Micro Focus ou l'une de ses filiales.**

Les seules garanties pour les produits et services de Micro Focus et de ses filiales et concédants de licence (« Micro Focus ») sont énoncées dans les déclarations de garantie expresses accompagnant ces produits et services. Aucun élément du présent document ne doit être interprété comme constituant une garantie supplémentaire. Micro Focus ne pourra pas être tenu responsable des erreurs techniques ou éditoriales ou des omissions contenues dans le présent document. Les informations contenues dans le présent document sont susceptibles d'être modifiées sans préavis.

Pour plus d'informations, comme les mentions liées à la certification et les marques, consultez le site <http://www.microfocus.com/about/legal/> (<http://www.microfocus.com/about/legal/>).