IBM Security QRadar
Version 7.3.1

Guide d'identification et de résolution des problèmes et notifications système

Important
Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations figurant à la section «Remarques», à la page 49.

Ce document s'applique à IBM QRadar Security Intelligence Platform version 7.3.1 et à toutes les versions et modifications ultérieures sauf indication contraire dans les nouvelles éditions.

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- http://www.fr.ibm.com (serveur IBM en France)
- http://www.ibm.com/ca/fr (serveur IBM au Canada)
- http://www.ibm.com (serveur IBM aux Etats-Unis)

Compagnie IBM France
Direction Qualité
17, avenue de l'Europe
92275 Bois-Colombes Cedex

Table des matières

Avis aux lecteurs canadiens

Le présent document a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

Terminologie

La terminologie des titres IBM peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

IBM France	**IBM Canada**
ingénieur commercial	représentant
agence commerciale	succursale
ingénieur technico-commercial	informaticien
inspecteur	technicien du matériel

Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien de type QWERTY.

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

- les pages de codes 850 (multilingue) et 863 (français-canadien),
- le code pays 002,
- le code clavier CF.

Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

France	Canada	Etats-Unis
(Pos1)		Home
Fin	Fin	End
(PgAr)		PgUp
(PgAv)		PgDn
Inser	Inser	Ins
Suppr	Suppr	Del
Echap	Echap	Esc
Attn	Intrp	Break
Impr écran	ImpEc	PrtSc
Verr num	Num	Num Lock
Arrêt défil	Défil	Scroll Lock
(Verr maj)	FixMaj	Caps Lock
AltGr	AltCar	Alt (à droite)

Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.

A propos de ce guide

Le présent guide est destiné à l'utilisation avec IBM® Security QRadar. Il contient des informations de diagnostic et de résolution des notifications système et des erreurs fréquentes qui peuvent s'afficher lors de l'utilisation de QRadar SIEM.

IBM Security QRadar Troubleshooting and System Notifications Guide contient des informations sur l'identification et la résolution des notifications système qui s'affichent dans la console QRadar. Ces notifications peuvent s'appliquer à tout dispositif ou tout produit QRadar présent dans votre déploiement.

Sauf si vous remarquez autre chose, toutes les références à QRadar peuvent concerner les produits suivants :

- IBM Security QRadar SIEM
- IBM QRadar Log Manager

Utilisateurs concernés

Les administrateurs système chargés de l'identification et de la résolution des problèmes doivent disposer de droits d'accès d'administrateur sur IBM Security QRadar et sur votre périphérique réseau et vos pare-feux. L'administrateur système doit connaître les technologies de réseau d'entreprise et de mise en réseau.

Les administrateurs réseau chargés d'installer et de configurer les systèmes QRadar doivent être familiarisés avec les concepts de sécurité réseau et le système d'exploitation Linux.

Documentation technique

Pour rechercher la documentation produit IBM Security QRadar sur le Web, y compris toute la documentation traduite, accédez à IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome).

Pour savoir comment accéder à d'autres documents techniques dans la bibliothèque produit QRadar, voir la note technique Accessing IBM Security Documentation (en anglais) (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Contacter le service clients

Pour contacter le service clients, voir la note technique Support and Download (en anglais) (http://www.ibm.com/support/docview.wss?uid=swg21616144).

Instructions relatives aux bonnes pratiques de sécurité

La sécurité des systèmes informatiques implique la protection des systèmes et des informations par la prévention par la détection et la réponse aux accès non autorisés depuis l'intérieur ou l'extérieur de votre entreprise. L'accès incorrect peut engendrer la modification, la destruction, le détournement la mauvaise utilisation des informations ou peut engendrer l'endommagement ou la mauvaise utilisation des systèmes, en particulier pour l'utilisation dans les attaques ou autres. Aucun système informatique ou produit ne doit être considéré comme entièrement sécurisé et aucun produit unique, service ou aucune mesure de sécurité ne peut être entièrement efficace dans la prévention d'une utilisation ou d'un accès incorrect. Les systèmes, les produits et les services IBM sont conçus pour s'intégrer à une approche de sécurité complète, qui implique nécessairement des procédures opérationnelles supplémentaires, et

peuvent avoir besoin d'autres systèmes, produit ou services pour optimiser leur efficacité. IBM NE GARANTIT EN AUCUN CAS L'IMMUNITE DES SYSTEMES, PRODUITS OU SERVICES NI L'IMMUNITE DE VOTRE ENTREPRISE CONTRE LE COMPORTEMENT MALVEILLANT OU ILLEGAL DE L'UNE DES PARTIES.

Remarque/Commentaire :

L'utilisation de ce programme peut impliquer différents lois ou réglementations, concernant notamment la confidentialité, la protection des données, l'emploi, ainsi que les communications électroniques et le stockage. IBM Security QRadar peut être utilisé uniquement de façon réglementaire. Le client accepte d'utiliser ce programme conformément aux lois, réglementations et règles en vigueur et veille à s'y conformer. Le détenteur de licence déclare qu'il détiendra ou qu'il a obtenu les agréments, les autorisations ou les licences nécessaires pour une utilisation réglementaire d'IBM Security QRadar.

1 Techniques de traitement des problèmes

L'*identification et la résolution d'un problème* est une approche systématique de la résolution d'un problème. L'objectif du traitement des incidents est de déterminer pourquoi quelque chose ne fonctionne pas de la façon escomptée et comment résoudre le problème. Certaines techniques courantes peuvent faciliter la tâche d'identification et de résolution des problèmes.

La première étape de la procédure d'identification et de résolution des problèmes est de décrire complètement le problème. La description des problèmes vous permet, à vous et au représentant du support technique, de savoir où commencer à chercher la cause du problème. Cette étape implique de se poser des questions de base :

- Quels sont les symptômes du problème ?
- Où le problème se produit-il ?
- Quand le problème se produit-il ?
- Dans quelles conditions le problème se produit-il ?
- Le problème peut-il être reproduit ?

Les réponses à ces questions entraînent généralement une bonne description du problème, qui peut déboucher sur sa résolution.

Quels sont les symptômes du problème ?

Lorsque vous commencez à décrire un problème, la question la plus évidente est "Quel est le problème ?". Cette question peut sembler simple. Cependant,vous pouvez la diviser en différentes questions spécialisées, qui créent une image plus descriptive du problème. Ces questions peuvent inclure :

- Qui, ou quoi, signale le problème ?
- Quels sont les codes d'erreur et les messages ?
- Comment le système échoue-t-il ? Par exemple, le problème vient-il d'une boucle, d'un blocage, d'une panne, d'une dégradation des performances ou d'un résultat incorrect ?

Où le problème se produit-il ?

La détermination de la source du problème n'est pas toujours aisée, mais c'est l'une des étapes les plus importantes de la résolution d'un problème. Il peut y avoir de nombreuses couches de technologie entre les composants qui génèrent des rapports et les composants qui échouent. Les réseaux, les disques et les pilotes ne représentent que quelques-uns des composants à envisager lorsque vous étudiez des problèmes.

Les questions ci-dessous vous permettent d'isoler la couche qui pose problème :

- Le problème est-il spécifique à un seul dispositif ?
- L'environnement et la configuration actuels sont-ils pris en charge ?

Si une couche signale le problème, le problème ne vient pas forcément de cette couche. La compréhension de l'environnement dans lequel se produit le problème permet d'identifier en partie l'origine du problème. Prenez le temps de décrire complètement l'environnement du problème, dont le système d'exploitation et la version, tous les logiciels et les versions correspondants et le matériel. Confirmez que vous exécutez l'application dans un environnement pris en charge. De nombreux problèmes peuvent être dus à des niveaux de logiciel incompatibles, qui ne sont pas destinés à être exécutés ensemble ou qui n'ont pas été testés totalement ensemble.

Quand le problème se produit-il ?

Développez une chronologie détaillée des événements ayant entraîné un échec, en particulier pour les cas survenant une seule fois. Vous pouvez développer facilement une chronologie en travaillant de façon rétroactive : commencez à l'heure où une erreur a été signalée (aussi précisément que possible, à la milliseconde près) et revenez en arrière dans les journaux et les informations disponibles. En général, vous n'avez pas besoin de chercher plus loin que le premier événement suspicieux que vous détectez dans un journal de diagnostic.

Pour développer une chronologie détaillée des événements, répondez à ces questions :

- Le problème se produit-il seulement à une certaine heure du jour ou de la nuit ?
- A quelle fréquence le problème se produit-il ?
- Quelle séquence d'événements s'est enchaînée jusqu'à l'heure à laquelle le problème a été signalé ?
- Le problème se produit-il après une modification de l'environnement, comme une mise à niveau ou une installation du logiciel ou du matériel ?

Dans quelles conditions le problème se produit-il ?

Connaître les systèmes et les applications exécutés lorsqu'un problème se produit représente une partie importante de l'identification et de la résolution des problèmes. Ces questions concernant votre environnement peuvent vous aider à identifier la cause du problème :

- Le problème se produit-il toujours lorsque la même tâche est exécutée ?
- Une certaine séquence d'événements doit-elle être respectée pour que le problème se produise ?
- Y a-t-il d'autres applications qui échouent au même moment ?

La réponse à ces questions peut vous aider à expliquer l'environnement dans lequel le problème se produit et à corréler les dépendances éventuelles. N'oubliez pas, lorsque plusieurs problèmes se produisent en même temps, les problèmes ne sont pas forcément liés.

Le problème peut-il être reproduit ?

Les problèmes que vous pouvez reproduire sont souvent plus faciles à résoudre. Cependant, les problèmes que vous pouvez reproduire peuvent présenter un inconvénient. Si le problème a un impact professionnel significatif, vous ne souhaitez pas qu'il se reproduise. Si cela est possible, recréez le problème dans un environnement de test ou de développement, qui offre généralement plus de flexibilité et de contrôle lors de votre étude. Répondez aux questions suivantes :

- Le problème peut-il être recréé sur un système de test ?
- Y a-t-il plusieurs utilisateurs qui rencontrent le même type de problème ?
- Le problème peut-il être recréé en exécutant une commande unique ou un ensemble de commandes ?

2 Problèmes courants

Les informations qui suivent peuvent vous aider à identifier et résoudre les problèmes courants de votre déploiement IBM Security QRadar.

Erreur d'inaccessibilité du stockage sur disque

Chaque hôte de votre déploiement IBM Security QRadar surveille la disponibilité des partitions. La disponibilité du disque est testée toutes les minutes en ouvrant un fichier, en écrivant du contenu dessus et en le supprimant.

Si le test de disponibilité du disque prend plus des 5 secondes habituelles, le processus de contexte de l'hôte signale une erreur dans les journaux QRadar. Une erreur peut également se produire lorsque le système QRadar détecte que de grands volumes de données sont écrits, recherchés, purgés ou copiés sur un autre système.

L'erreur peut se présenter comme suit :

```
Jun 24 07:22:41 127.0.0.1 [hostcontext.hostcontext]
[5b3acf9a-aa8a-437a-b059-01da87333f43/SequentialEventDispatcher]
com.q1labs.hostcontext.ds.DiskSpaceSentinel: [ERROR]
[NOT:0150062100][172.16.77.116/- -]
[-/- -]The storage partition(s) /store/backup on qradarfc (172.16.77.116)
are not currently accessible. Manual intervention may be required to
restore normal operation.
```

Si le message s'affiche de façon répétée, vérifiez le problème. Pour plus d'informations, voir «Vérification d'un problème de stockage de partition».

Vérification d'un problème de stockage de partition

Vous vérifiez un problème de stockage de partition en créant un fichier temporaire sur la console IBM Security QRadar ou sur un hôte géré.

Avant de commencer

Vérifiez que le problème de stockage de partition n'est pas dû à un stockage externe lent ou indisponible.

Procédure

1. Utilisez SSH pour vous connecter à QRadar Console.
2. Créez un test en entrant les commandes suivantes :
   ```
   touch /store/backup/testfile
   ls -la /store/backup/testfile
   ```
3. Si l'un des deux messages ci-dessous s'affiche, augmentez la période d'expiration du test de partition.
   - `touch: cannot touch `/store/backup/testfile': Read-only file system`
   - `nfs server time out`
   a. Cliquez sur l'onglet **Admin**.
   b. Dans le menu **Configuration système**, sélectionnez **Paramètres système** > **Avancé**.
   c. Dans la zone de liste **Délai d'attente de testeur de partition (secondes)**, sélectionnez ou entrez `20`.
   d. Cliquez sur **Sauvegarder**.
4. Sélectionnez l'une des options suivantes :

- Si vous utilisez un système de fichiers réseau, comme iSCSI, Fibre Channel ou Network File System (NFS), contactez l'administrateur du stockage pour vérifier que les serveurs de fichiers sont accessibles et opérationnels.
- Si vous utilisez un système de fichiers local, vous pouvez rencontrer un problème de système de fichiers ou un échec au niveau du disque.

Résolution d'une erreur de source de journal après la mise à jour du protocole

Un message d'erreur peut s'afficher lorsque vous tentez de modifier une source de journal après avoir mis à niveau IBM Security QRadar, un module de prise en charge de périphérique, un protocole ou des composants de services d'information sur les vulnérabilités. Pour supprimer des fichiers mis en mémoire cache, redémarrez le service web QRadar et effacez les fichiers QRadar de votre mémoire cache de navigateur.

Avant de commencer

Vous devez disposer d'un accès SSH et de données d'identification de compte root.

Pourquoi et quand exécuter cette tâche

Le message ci-dessous indique que le serveur web n'a pas redémarré après la mise à jour de QRadar :

```
Une erreur s'est produite. Actualisez votre navigateur (appuyez sur la touche F5)
et réessayez l'action.
Si le problème persiste, contactez le service clients
pour obtenir une assistance.
```

Un fichier peut être mis en mémoire cache par le service web QRadar ou votre navigateur de bureau. Vous devez redémarrer le service web QRadar et supprimer les fichiers mis en mémoire cache sur votre bureau.

Procédure

1. Utilisez SSH pour vous connecter à QRadar.
2. Arrêtez le service web QRadar en entrant la commande suivante :

   ```
   service tomcat stop
   ```
3. Gardez une fenêtre de navigateur ouverte.
4. Pour effacer la mémoire cache du navigateur, accédez aux paramètres de préférences de votre navigateur web.
5. Redémarrez le navigateur.
6. Redémarrez le service web QRadar en entrant la commande suivante :

   ```
   service tomcat start
   ```

Vérification des niveaux d'utilisation du disque

La partition `/var/log` continue à fonctionner lorsque l'utilisation du disque atteint 100 %. Cependant, les données de journal peuvent ne pas être écrites sur le disque, ce qui peut affecter les processus et les composants au démarrage de IBM Security QRadar.

Procédure

1. Utilisez SSH pour vous connecter à QRadar ou à un hôte géré.
2. Pour examiner l'utilisation de la partition du disque, entrez la commande suivante :

   ```
   df -h
   ```

3. Examinez les partitions pour vérifier les niveaux d'utilisation du disque.

Que faire ensuite

Si l'une des partitions surveillées atteint 95 %, voir «Résolution des problèmes d'utilisation du disque».

Résolution des problèmes d'utilisation du disque

Les partitions du système de fichier atteignent 95 % lorsque les paramètres de période de conservation des données sont trop élevés ou si le stockage disponible ne suffit pas pour le taux auquel IBM Security QRadar reçoit les données. Si vous reconfigurez vos paramètres de conservation du stockage en compartiment, le stockage dans votre déploiement QRadar entier est affecté.

Procédure

1. Identifiez et supprimez les anciens fichiers de débogage ou de correctifs sur le système de fichiers `/`.
2. Réduisez l'utilisation du disque dans le système de fichiers `/store`.
3. Sélectionnez l'une des options suivantes :
   - Supprimez les anciennes données dans le système de fichiers `/store/ariel/events`.
   - Réduisez la période de conservation des données en ajustant les paramètres de conservation par défaut du stockage en compartiment. Pour plus d'informations, voir *IBM Security QRadar Administration Guide*.
   - Si le fichier `/store` est saturé, identifiez les sources de journal que vous pouvez conserver moins longtemps. Utilisez les compartiments de conservation pour gérer les sources de journal. Pour plus d'informations, voir *IBM Security QRadar Administration Guide*.
   - Envisagez d'utiliser une solution de stockage externe, comme iSCSI ou Fibre Channel. Pour plus d'informations, voir *Offboard Storage Guide*.
   - Si le système de fichiers `/var/log` atteint 100 % de sa capacité, QRadar ne se ferme pas. Vos fichiers journaux peuvent grossir plus vite que prévu en raison d'autres problèmes.

Performances du traitement des événements

Votre configuration IBM Security QRadar peut avoir un impact sur le pipeline de traitement des événements.

Le traitement des événements peut être affecté par les extensions du module de prise en charge de périphérique, les propriétés personnalisées, les tests de règle et les vues globales. L'analyse syntaxique des événements et le moteur de règles personnalisées détectent automatiquement les événements supprimés, exécutent des diagnostics d'auto-surveillance et signalent les extensions de DSM, les règles et les propriétés qui sont lentes.

Propriétés personnalisées non optimisées

Les propriétés personnalisées sont marquées comme étant optimisées lorsqu'elles sont utilisées régulièrement pour les règles QRadar ou pour la recherche et le filtrage.

Les propriétés personnalisées non optimisées sont analysées par le système, ce qui affecte les vitesses de recherche et le taux de chargement du navigateur web.

Tests de règle ayant un impact sur les performances

Les règles qui testent les expressions régulières dans le contenu d'un événement affectent les performances de QRadar, car elles cherchent le contenu complet.

Avant d'ajouter un test de contenu à une règle, utilisez les filtres de règle pour réduire le nombre d'événements. Par exemple, lorsque vous cherchez un message spécifique dans les journaux Active Directory, appliquez les filtres ci-dessous à la règle :

- Filtre de type de source de journal
- Filtre de groupe de sources de journal ou de source de journal spécifique
- Filtre d'adresses IP source facultatif

Le test **Hôte avec port ouvert** peut avoir un impact sur les performances, car il compare les ports passifs et les ports actifs aux événements et aux flux reçus par QRadar. Avant d'utiliser le test, effectuez une vérification bidirectionnelle pour vous assurer que l'hôte répond à la demande de communication.

Vues globales

Une recherche enregistrée groupée selon différentes zones génère une vue globale comportant de nombreuses entrées uniques. L'augmentation du volume de données peut avoir un impact sur l'utilisation du disque, les délais de traitement et les performances de recherche.

Pour empêcher le volume de données d'augmenter, n'agrégez que les recherches sur les zones nécessaires. Vous pouvez réduire l'impact sur l'accumulateur en ajoutant un filtre à vos critères de recherche.

Identification des problèmes liés au gestionnaire de services de données et aux propriétés personnalisées optimisées

Pour résoudre les problèmes entraînant une dégradation des performances, identifiez les problèmes liés à des extensions de gestionnaire de services de données récemment installées ou à une propriété personnalisée récemment activée.

Pourquoi et quand exécuter cette tâche

Une extension de gestionnaire de services de données crée des méthodes d'analyse syntaxique personnalisées en utilisant le modèle d'expression régulière correspondant pour extraire des données d'événements de sources de journal non prises en charge ou incomplètes. Les propriétés personnalisées optimisées utilisent des modèles d'expression régulière pour extraire des données des événements lors de leur analyse syntaxique.

Les modèles d'expression régulière utilisés dans votre extension de gestionnaire de services de données ou propriété personnalisée optimisée peuvent avoir un impact sur le traitement des événements dans IBM Security QRadar. Des expressions régulières inefficaces peuvent router des données de manière incorrecte vers le stockage, provoquer une dégradation des performances de QRadar, et avoir une incidence sur le traitement d'événement.

Les problèmes liés au gestionnaire de services de données et aux propriétés personnalisées optimisées peuvent entraîner la notification système suivante :

```
Une dégradation des performances a été détectée dans le pipeline d'événements.
Les événements ont été acheminés directement vers le stockage.
```

Procédure

1. Désactivez les extensions de gestionnaire de services de données ou les propriétés personnalisées installées ou activées dernièrement.
2. Sélectionnez l'une des options suivantes :
   - Si QRadar cesse de supprimer les événements et que vous recevez une notification système, examinez vos extensions de gestionnaire de services de données ou vos propriétés personnalisées pour identifier et améliorer les modèles d'expression régulière inefficaces.

- Si QRadar continue à supprimer des événements, plusieurs extensions de gestionnaire de services de données ou propriétés personnalisées peuvent entraîner un problème lié au pipeline d'événements.

3. Utilisez SSH pour vous connecter au processeur d'événements QRadar qui supprime des événements et entrez la commande suivante :

   ```
   /opt/qradar/support/threadTop.ssh –p 7777
   ```

   La commande affiche l'activité du moteur de traitement de données. Le tableau suivant décrit les colonnes figurant dans la sortie :

Tableau 1. Colonnes du moteur de traitement de données

Colonnes	Description
Serveur	Port ou processus.
ID	ID du processus.
MSecs	Temps UC.
Nom	Nom du processus.

4. Si les unités d'exécution d'analyseur syntaxique s'exécutent pendant plus de 1500 millisecondes, entrez la commande suivante afin de passer en revue les piles d'unité d'exécution Java :

   ```
   /opt/qradar/support/threadTop.sh -p 7777 -s -e ".*Event Parser.*" | less
   ```

Que faire ensuite

Si la pile d'unité d'exécution contient `java.util.regex.Pattern$Curly.match`, la dégradation des performances peut être due à vos extensions DSM ou propriétés personnalisées coûteuses. Pour en savoir plus, voir «Extensions DSM coûteuses détectées», à la page 44 ou «Détection de propriétés personnalisées coûteuses», à la page 43.

Si la pile d'unité d'exécution Java ne comporte pas d'expressions régulières coûteuses, vos extensions DSM ou propriétés personnalisées peuvent présenter des problèmes d'analyse syntaxique. Pour plus d'informations, consultez la rubrique relative aux problèmes d'analyse syntaxique dans le manuel *IBM Security QRadar Log Sources - Guide d'utilisation*.

Résultats de rapport incomplets

Une fois que vous avez configuré et exécuté les rapports IBM Security QRadar, vous pouvez découvrir des résultats inattendus. Un rapport peut sembler ne pas afficher toutes les données dont vous avez besoin.

Le cumul des données pour une recherche ne commence que lorsque la recherche est ajoutée à un rapport planifié. Par exemple, un rapport créé le mercredi, dont l'exécution est planifiée tous les lundis, n'affiche pas les données pour une semaine complète. En revanche, le rapport suivant contient les données d'une semaine complète.

Essayez l'une de ces solutions :

Réexécutez la recherche.
Utilisez l'onglet **Réseau**, **Activité** ou **Activité du journal** pour réexécuter la recherche. Vous pouvez comparer les résultats au rapport généré.

Examinez le message de notification sous l'onglet Rapports.
L'onglet **Rapports** affiche un message de notification lorsque vos données sont incomplètes.

Exécutez votre rapport sur des données brutes de la période initiale.

Assurez-vous d'avoir saisi toutes les données de rapport en exécutant votre rapport sur les donnés brutes de la période initiale. Pour plus d'informations, voir *IBM Security QRadar - Guide d'utilisation*.

Des rapports incomplets sont également générés lorsque le système ne peut pas cumuler des agrégations de données dans un intervalle de 60 secondes. Chaque minute, QRadar crée des agrégation de données pour chaque recherche agrégée. Si le nombre de recherches et les valeurs unique des recherches sont trop importants, le délai nécessaire au traitement des agrégations peut dépasser 60 secondes. Lorsque le cumul ne peut pas être terminé en 60 secondes, l'intervalle de cumul est supprimé. Des colonnes peuvent être manquantes dans les graphiques et les rapports de série temporelle pour la période à laquelle s'est produit le problème. Pour plus d'informations, voir «L'accumulateur ne peut pas lire la définition de vue pour les données agrégées», à la page 22.

Concepts associés:

«Retard dans l'accumulateur», à la page 20

38750099 - `L'accumulateur a été incapable d'agréger tous les événements / flux pour cet intervalle.`

Résolution d'un espace disque limité pour les partitions de sauvegarde

Une notification système s'affiche, car le système de fichiers de destination possède un espace disque limité. IBM Security QRadar ne peut pas terminer la sauvegarde en raison d'un espace disque insuffisant.

Vous risquez de recevoir la notification système suivante :

`Sauvegarde : Espace libre insuffisant pour effectuer la sauvegarde.`

Les notifications système concernant un espace disque limité sont générées lorsque l'espace libre de la partition `/store/backup/` est inférieur au double de la taille du dernier fichier de sauvegarde. Un espace disque limité est dû au volume de données et à vos paramètres de période de conservation de sauvegarde. Pour plus d'informations, consultez le document *IBM Security QRadar Administration Guide*.

La configuration des paramètres de conservation de stockage en compartiment a un impact général sur le stockage dans tout votre déploiement QRadar.

Des avertissements d'utilisation du disque peuvent se produire sur la console QRadar Console ou sur un hôte géré dans votre déploiement QRadar. Pour vérifier les niveaux d'utilisation du disque, examinez les partitions surveillées sur la console QRadar Console ou sur vos hôtes gérés.

Procédure

1. Vérifiez les niveaux du disque de partition de sauvegarde.
   a. Utilisez SSH pour vous connecter à QRadar Console ou à l'hôte géré.
   b. Entrez la commande suivante :
      ```
      df -PTh /store/backup
      ```
2. Examinez la partition de sauvegarde pour vérifier les niveaux d'utilisation du disque.
   a. Si la partition de sauvegarde est supérieure au double de la taille du fichier de sauvegarde, identifiez l'emplacement de votre sauvegarde.
      - Si votre sauvegarde se trouve sur le même système de fichiers que le répertoire `/store/ariel`, déplacez-la sur un autre système de stockage.
      - Si votre sauvegarde est externe, vérifiez votre utilisation et assurez-vous que la période de conservation de votre sauvegarde ne nécessite pas plus d'espace que ce dont vous disposez.
   b. Réduisez l'utilisation du disque dans le système de fichiers `/store`.

- Envisagez d'augmenter la taille de votre stockage externe en utilisant une solution de stockage externe, comme iSCSI ou Fibre Channel. Pour plus d'informations, consultez le document *Offboard Storage Guide*.
- Si votre partition de sauvegarde QRadar est montée sur un partage NFS, essayez de réduire la période de conservation de la sauvegarde. La période de conservation de sauvegarde par défaut est de deux jours. Pour plus d'informations sur la configuration des périodes de conservation de sauvegarde, voir *IBM Security QRadar Administration Guide*.

Notifications système des licences

La console IBM Security QRadar gère toutes les licences du déploiement. Des notifications système quotidiennes sont générées avant et après l'expiration des licences.

Le tableau ci-dessous affiche les composants QRadar qui dépendent des licences actives.

Tableau 2. Effets d'une licence QRadar arrivée à expiration

Type de licence arrivée à expiration	Résultats
Console	Lorsque la licence QRadar Console arrive à expiration, les sources d'événement ou les sources de flux transférées directement à la console ne sont pas traitées ou stockées. Les données existantes ne sont pas concernées. Tant que la licence de la console n'est pas renouvelée, dirigez les sources d'événements vers un hôte géré avec une licence valide dans le déploiement.
Hôte géré	Lorsqu'une licence d'hôte géré arrive à expiration dans votre déploiement, le contexte de l'hôte est désactivé sur cet hôte géré. Le dispositif arrivé à expiration ne traite pas les données d'événement ou de flux.
Fonction	Lorsqu'une licence de fonction arrive à expiration, comme X-Force, la fonction cesse de recevoir les mises à jour des données. La fonction s'appuie sur le dernier flux de données fourni par X-Force.

Suppression d'une licence pour empêcher les notifications système récurrentes

Lorsqu'un dispositif IBM Security QRadar arrive à expiration, il ne peut pas être utilisé tant que la licence associée n'a pas été mise à jour.

Pourquoi et quand exécuter cette tâche

Si une fonction, comme X-Force, est associée à une licence arrivée à expiration, supprimez la licence pour empêcher des notifications système récurrentes.

Si vous utilisez des dispositifs haute disponibilité, supprimez la licence de l'hôte haute disponibilité secondaire.

Procédure

1. Connectez-vous à QRadar Console.
2. Cliquez sur l'onglet **Admin**.
3. Dans le menu de navigation, cliquez sur **Configuration système**.
4. Cliquez sur l'icône **Gestion du système et de la licence**.

5. Dans la zone de liste **Afficher**, sélectionnez **Licences**.
6. Sélectionnez la licence arrivée à expiration. La zone **Messages d'information sur la licence** répertorie les licences arrivées à expiration.
7. Sélectionnez **Actions** > **Supprimer la licence**.
8. Cliquez sur **Confirmer**.

Que faire ensuite

Mettez à jour la licence arrivée à expiration. Pour plus d'informations, voir Transfert d'une clé de licence (http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/t_qradar_adm_upload_license_key.html).

Résolution des erreurs de connexion avec des comptes Active Directory

Si une erreur est générée lorsque vous vous connectez à IBM Security QRadar avec un compte Active Directory valide, vérifiez si vous rencontrez des problèmes de synchronisation de l'heure.

Pourquoi et quand exécuter cette tâche

Lorsqu'un compte Active Directory valide n'est pas synchronisé avec votre console QRadar Console, une erreur de connexion comme celle-ci peut se produire :

```
Le nom d'utilisateur et le mot de passe indiqués ne sont pas valides. Réessayez.
```

Vous pouvez synchroniser manuellement les données entre le serveur QRadar et le serveur d'authentification LDAP.

Si vous utilisez une autorisation basée sur des attributs ou des groupes d'utilisateurs, les informations des utilisateurs sont importées automatiquement du serveur LDAP sur la console QRadar.

Chaque groupe configuré sur le serveur LDAP doit comporter un rôle d'utilisateur ou un profil de sécurité configuré dans la console QRadar. Pour chaque groupe correspondant, les utilisateurs sont importés et des autorisations basées sur ce rôle d'utilisateur ou ce profil de sécurité leur sont affectées.

Par défaut, la synchronisation a lieu toutes les 24 heures. Le délai de synchronisation dépend de l'heure de la dernière exécution. Par exemple, si vous exécutez manuellement la synchronisation à 23 h 45 et que vous définissez l'intervalle de synchronisation sur 8 heures, la synchronisation suivante aura lieu à 7 h 45. Si les autorisations d'accès changent pour un utilisateur connecté lors de la synchronisation, la session n'est plus valide. L'utilisateur est redirigé vers l'écran de connexion pour la demande suivante.

Suivez cette procédure.

Procédure

1. Si votre serveur Active Directory n'a pas été configuré récemment, utilisez SSH pour vous connecter à QRadar en tant qu'utilisateur root.
2. Entrez la commande suivante :

   ```
   cat /opt/qradar/conf/login.conf
   ```
3. Vérifiez que le serveur est configuré pour l'authentification Active Directory. Par exemple, un serveur authentifié peut se présenter comme suit :

   ```
   LDAPServerURL=ldaps://<serveur>:<port>
   ```

   L'option <*serveur*> est le contrôleur de domaine Active Directory qui reçoit l'authentification QRadar. Le port 389 est le port LDAP Active Directory par défaut.
4. Copiez l'adresse IP du contrôleur de domaine Active Directory.

5. Exécutez la commande ci-dessous et utilisez l'adresse IP du contrôleur de domaine Active Directory pour l'option *<serveur>* :

   ```
   ntpdate -q <serveur>
   ```

6. Vérifiez que le temps de décalage est supérieur à +/- 300 secondes. Le résultat peut se présenter comme suit :

   ```
   server 9.24.207.12, stratum 3, offset -10774.586000, delay 0.04221 19 Nov 13:59:16
   ntpdate[22011]: step time server 9.24.207.12 offset -10774.586000 sec
   ```

   Si le temps de décalage dépasse +/- 300 secondes, l'intervalle entre QRadar Console et le serveur Active Directory entraîne des problèmes d'authentification.

7. Redémarrez le service web QRadar en exécutant la commande suivante :

   ```
   service tomcat restart
   ```

   Le redémarrage du service web QRadar déconnecte tous les utilisateurs et interrompt les événements d'exportation et la génération des rapports. Vous aurez peut-être besoin de redémarrer manuellement certains rapports ou d'attendre une fenêtre de maintenance pour terminer cette procédure.

8. Si l'heure système de QRadar Console et l'heure système du serveur Active Directory diffèrent d'au moins 5 minutes, suivez cette procédure :
   a. Cliquez sur l'onglet **Admin**.
   b. Dans le menu de navigation, cliquez sur **Configuration système**.
   c. Cliquez sur **Authentification**.
   d. Dans la liste **Module d'authentification**, sélectionnez **LDAP**.
   e. Sélectionnez **Gérer la synchronisation** > **Exécuter une synchronisation maintenant**.

Vérification de la réception des événements syslog par QRadar

Pour vérifier que IBM Security QRadar reçoit des événements, examinez l'en-tête syslog complet pour les événements source syslog distants. Il peut arriver que QRadar ne reçoive pas des événements syslog, car un pare-feu a bloqué la communication ou le périphérique n'a pas envoyé les événements.

Avant de commencer

Examinez la source d'événement qui envoie des événements syslog et vérifiez son adresse IP.

Procédure

1. Utilisez SSH pour vous connecter à QRadar en tant qu'utilisateur root.
2. Si la destination syslog se trouve sur un autre dispositif, comme un collecteur d'événements, utilisez SSH pour vous connecter au collecteur d'événements.
3. Sélectionnez l'une des options suivantes.
   - Pour un protocole TCP syslog, entrez la commande suivante :

     ```
     tcpdump -s 0 -A host adresse_périphérique and port 514
     ```

   - Pour un protocole UDP syslog, entrez la commande suivante :

     ```
     tcpdump -s 0 -A host adresse_périphérique and port UDP 514
     ```

   adresse_périphérique doit être une adresse IPv4 ou un nom d'hôte. La commande **tcpdump** doit être exécutée sur le dispositif QRadar qui reçoit les événements de votre périphérique. Par défaut, les dispositifs QRadar sont configurés de manière à recevoir des événements syslog en utilisant le protocole TCP ou UDP et le port 514. Ne configurez pas le pare-feu QRadar.
4. Si la commande **tcpdump** n'affiche pas d'événements, les événements syslog ne sont pas envoyés à QRadar Console.
   a. Demandez à l'administrateur de pare-feu ou au groupe d'opérations de vérifier les pare-feux qui bloquent la communication entre le dispositif QRadar et le périphérique.
   b. Vérifiez qu'un port TCP est ouvert pour Telnet en entrant la commande ci-dessous dans QRadar :

```
telnet adresse_IP_périphérique 514
```

c. Examinez la configuration syslog du périphérique distant pour vous assurer que les événements sont envoyés au dispositif approprié.

Résolution des événements syslog non reçus

Si la commande **tcpdump** répertorie des événements, mais qu'aucun événement ne s'affiche dans l'activité des journaux, la console IBM Security QRadar ne reçoit pas les événements système.

Procédure

1. Consultez les notifications système.
2. Si les notifications système affichent l'adresse source incorrecte pour la source de journal, sélectionnez l'une des options suivantes :
   - Recréez manuellement la source de journal.
   - Mettez à jour la zone **Identificateur de la source de journal** en utilisant le nom d'hôte ou l'adresse IP approprié.
3. Vérifiez que le périphérique prend en charge la détection automatique de QRadar. L'annexe du document *IBM Security QRadar DSM Configuration Guide* répertorie les modules de service de périphérique qui prennent en charge la création automatique de source de journal.
4. Vérifiez que les sources de journal dans QRadar correspondent aux résultats de la commande tcpdump.
   a. Cherchez le nom d'hôte de la source de journal ou l'adresse IP du paquet dans les résultats de la commande tcpdump.
   b. Cliquez sur l'onglet **Admin**.
   c. Dans le menu de navigation, cliquez sur **Sources de données**.
   d. Dans le volet Evénements, cliquez sur **Sources de journal**.
   e. Cherchez le nom d'hôte de la source de journal ou l'adresse IP du paquet.

   Si le nom d'hôte de QRadar ou l'adresse IP du paquet ne correspond pas aux résultats de la commande tcpdump, la source de journal peut être créée avec une adresse incorrecte. Pour certains périphériques, des valeurs inattendues sont générées dans l'en-tête syslog lorsque la source d'événements gère les événements de différents périphériques. Votre périphérique peut conserver l'adresse IP de l'événement initial avant que l'événement syslog soit envoyé.
5. Cherchez une valeur de contenu unique dans QRadar.
   a. Examinez les contenus bruts de la commande tcpdump.
   b. Sélectionnez un identificateur unique pour votre source d'événements.
   c. Cliquez sur l'onglet **Activité du journal**.
   d. Dans la barre d'outils, cliquez sur **Ajouter un filtre**.
   e. Dans le menu **Paramètre**, sélectionnez **Le contenu contient**.
   f. Dans la zone **Valeur**, entrez votre identificateur unique.
   g. Examinez les résultats de la recherche.

Que faire ensuite

Si les résultats renvoient une autre source de journal, un faux positif est généré lors de la détection automatique. Supprimez la source de journal détectée par erreur.

Si la source de journal est détectée par erreur, vérifiez que QRadar Console est installé avec la dernière version du module de prise en charge de périphérique. Redétectez la source de journal.

3 Notifications système de QRadar

Utilisez les notifications système générées par IBM Security QRadar pour surveiller le statut et l'état de santé de votre système. Les outils et processus matériels et logiciels surveillent en continu les dispositifs QRadar et fournissent des messages d'information, d'avertissement et d'erreur aux utilisateurs et aux administrateurs.

Les notifications système s'affichent dans le tableau de bord QRadar ou dans la fenêtre de notification en cas de comportement système inattendu. Vous pouvez identifier et résoudre les problèmes liés aux notifications QRadar les plus fréquentes.

Notifications système d'utilisation du disque

La sentinelle de disque IBM Security QRadar surveille les partitions `/`, `/store`, `/storetmp`, `/transient` et `/var/log` avant qu'elles n'atteignent un seuil d'utilisation prédéfini.

Les rubriques qui suivent peuvent vous aider à identifier et résoudre les problèmes courants de votre déploiement IBM Security QRadar. Le tableau ci-dessous afficher les notifications système du contexte des hôtes qui dépend de l'utilisation du disque de chaque partition surveillée.

Tableau 3. Notification d'utilisation du disque

Notification	Description	Action suggérée
`Sentinelle de disque : L'utilisation du disque a dépassé le seuil d'avertissement.`	L'utilisation du disque est à 90 % pour une partition surveillée. QRadar n'est pas concerné lorsque la partition atteint ce seuil. Continuez à surveiller les niveaux de partition.	Voir «L'utilisation du disque a dépassé le seuil d'avertissement», à la page 34.
`Sentinelle de disque : L'utilisation du disque a dépassé le seuil maximal.`	L'utilisation du disque est à 95 % pour une partition surveillée. Les procédures de collecte et de recherche des données QRadar sont fermées pour protéger le système de fichiers d'atteindre 100 %.	Voir «L'utilisation du disque a dépassé le seuil maximal», à la page 14.
`Sentinelle de disque : L'utilisation du disque système est revenue à un niveau normal.`	Une fois que l'utilisation du disque atteint un seuil de 95 %, il doit revenir à 92 % avant que QRadar redémarre automatiquement les procédures de collecte et de recherche des données.	Pour réduire le seuil d'utilisation du disque, supprimez manuellement les données des partitions concernées. Voir «Retour à la normale de l'utilisation du disque», à la page 46.

Notifications d'erreurs pour les dispositifs QRadar

Les notifications d'erreurs dans les produits IBM Security QRadar nécessitent une réponse de l'utilisateur ou de l'administrateur.

Erreur de saturation de la mémoire

`38750004 - Mémoire insuffisante pour l'application`

Explication

Lorsque le système essaie d'utiliser une quantité de mémoire plus importante que celle allouée, l'application ou le service peut cesser de fonctionner. Les problèmes de saturation de mémoire sont

souvent causés par des requêtes et opérations provenant du logiciel ou définies par l'utilisateur, qui épuisent la mémoire disponible.

Intervention de l'utilisateur

Suivez les procédures de résolution suivantes :

- Examinez le message d'erreur consigné dans le fichier `/var/log/qradar.log` afin de déterminer le composant défaillant.
- Si le serveur proxy Ariel effectue une recherche sur de gros volumes de données ou s'il utilise une option de regroupement qui génère des valeurs uniques dans les résultats de la recherche, réduisez le nombre de valeurs uniques ou le délai de recherche.
- Si l'accumulateur génère un graphique de séries temporelles avec de nombreuses valeurs uniques agrégées, réduisez la taille de la requête.
- Si une source de journal basée sur un protocole a été récemment activée, diminuez la période d'interrogation afin de réduire le volume de données interrogées. Si plusieurs sources de journal basées sur un protocole s'exécutent en même temps, échelonnez les heures de début.
- Si la règle a été récemment modifiée pour un suivi des propriétés uniques sur de longues périodes, réduisez la durée de moitié ou réduisez le nombre d'événements correspondants en ajoutant un autre filtre.

L'utilisation du disque a dépassé le seuil maximal

38750038 - `Sentinelle de disque : L'utilisation du disque a dépassé le seuil maximal.`

Explication

Au moins un disque sur votre système est plein à 95 %.

Afin de prévenir l'altération des données, certains processus s'arrêtent. La collecte d'événements est interrompue jusqu'à ce que l'utilisation de disque passe au-dessous de 92 %.

Intervention de l'utilisateur

Identifiez la partition qui est saturée, par exemple / et les systèmes de fichiers `/store`. Libérez de l'espace disque en supprimant des fichiers qui ne sont pas nécessaires. Par exemple, la sortie de débogage et les fichiers correctifs peuvent être retirés du système de fichiers /. Si la système de fichiers `/store` approche sa pleine capacité, diminuez vos paramètres de conservation pour les événements et les flux.

Vous pouvez aussi supprimer d'anciennes données dans les répertoires `/store/ariel/`. Le système redémarre automatiquement les processus après que vous libérez suffisamment d'espace disque pour tomber en dessous d'un seuil de capacité de 92 %.

L'application de moniteur de processus n'est pas parvenue à démarrer à plusieurs reprises

38750043 - `Moniteur de processus : l'application n'est pas parvenue à démarrer à plusieurs reprises.`

Explication

Le système ne parvient pas à lancer une application ou un processus sur votre système.

Intervention de l'utilisateur

Passez en revue les composants défaillants. Par exemple, QFlow Collector ne peut pas démarrer lorsqu'aucune source de flux n'est affectée. Utilisez les actions de déploiement pour retirer ce composant QFlow.

Le moniteur de processus doit réduire l'utilisation du disque

38750045 - Moniteur de processus : l'utilisation du disque doit être réduite.

Explication

Le moniteur de processus ne parvient pas à lancer des processus en raison d'une pénurie de ressources système. La partition de stockage sur le système est probablement saturée à 95 % ou plus.

Intervention de l'utilisateur

Libérez de l'espace disque en supprimant manuellement des fichiers ou en modifiant vos politiques d'administration de conservation de données d'événements ou de flux. Le système redémarre automatiquement les processus système une fois que l'utilisation de l'espace disque passe au-dessous du seuil de 92 %.

Evénements supprimés par le pipeline d'événements

38750060 - Des événements/flux ont été supprimés par le pipeline d'événements.

Explication

En cas de problème avec le pipeline d'événements ou de dépassement des limites de la licence, il se peut qu'un événement ou un flux soit supprimé.

Les événements et les flux supprimés ne peuvent pas être restaurés.

Intervention de l'utilisateur

Vérifiez les options suivantes :

- Vérifiez les débits d'événements et de flux entrants sur votre système. Si la licence est dépassée et que le pipeline d'événements supprime des événements, étoffez votre licence pour gérer plus de données.
- Examinez les modifications récentes apportées à la politique d'administration ou aux propriétés personnalisées. Ces modifications peuvent entraîner des fluctuations de vos débits d'événements ou de flux et affecter les performances système.
- Déterminez si le problème est associé à des notifications SAR. Les notifications SAR peuvent indiquer que les événements et les flux mis en file d'attente résident dans le pipeline d'événements. Le système achemine habituellement les événements vers l'espace de stockage au lieu de les supprimer.
- Ajustez le système pour réduire le volume d'événements et de flux accédant au pipeline d'événements.

Abandon de connexions par le pipeline d'événements

38750061 - Des connexions ont été supprimées par le pipeline d'événements.

Explication

Un protocole TCP a supprimé une connexion établie avec le système.

Le nombre de connexions pouvant être établies par des protocoles TCP est limité pour garantir l'établissement des connexions et le réacheminement des événements. Le service de collecte d'événements (ECS) autorise un maximum de 15 000 descripteurs de fichier et chaque connexion TCP utilise trois de ces descripteurs.

Les protocoles TCP qui incluent des notifications d'abandon de connexion sont les suivants :

- Protocole TCP syslog
- Protocole TLS syslog
- Protocole TCP multiligne

Intervention de l'utilisateur

Vérifiez les options suivantes :

- Répartissez les événements vers d'autres dispositifs. Les connexions à d'autres processeurs d'événement et de flux distribuent la charge de travail de la console.
- Configurez les événements de source de journal TCP à faible priorité afin qu'ils utilisent le protocole réseau UDP.
- Ajustez le système pour réduire le volume d'événements et de flux accédant au pipeline d'événements.

Erreur lors de la mise à jour automatique

38750066 - L'installation des mises à jour automatiques n'a pas pu se terminer. Consultez le journal des mises à jour automatiques pour plus d'informations.

Explication

Le processus de mise à jour a rencontré une erreur et ne parvient pas à se connecter à un serveur de mise à jour. Le système n'a pas été mis à jour.

Intervention de l'utilisateur

Sélectionnez l'une des options suivantes :

- Vérifiez l'historique des mises à jour automatiques pour déterminer la cause de l'erreur à l'installation.
  Dans l'onglet **Admin**, cliquez sur l'icône **Mise à jour automatique** et sélectionnez **Afficher le journal**.
- Vérifiez que votre console peut se connecter au serveur de mise à jour.
  Dans la fenêtre Mises à jour, sélectionnez **Modifier les paramètres**, puis cliquez sur l'onglet **Avancé** pour visualiser votre configuration de mise à jour automatique. Vérifiez l'adresse dans la zone **Serveur Web** pour garantir que le serveur de mise à jour automatique soit accessible.

Mise à jour automatique installée avec des erreurs

38750067 - Les mises à jour automatiques ont été installées tout en rencontrant des erreurs. Consultez le journal des mises à jour automatiques pour plus d'informations.

Explication

La raison la plus fréquente d'échecs de mises à jour automatiques relève d'une dépendance logicielle manquante pour une mise à jour de DSM, de protocole ou de scanner.

Intervention de l'utilisateur

Sélectionnez l'une des options suivantes :

- Dans l'onglet **Admin**, cliquez sur l'icône **Mise à jour automatique** et sélectionnez **Afficher l'historique des mises à jour** afin de déterminer la cause de l'erreur d'installation. Vous pouvez afficher, sélectionner, puis réinstaller un RPM ayant échoué.
- S'il est impossible de réinstaller une mise à jour automatique via l'interface utilisateur, téléchargez et installez manuellement la dépendance manquante sur votre console. La console réplique le fichier installé sur tous les hôtes gérés.

Echec du système de haute disponibilité (HA) de secours

38750080 - Echec du système de haute disponibilité de secours.

Explication

Le statut du dispositif secondaire passe à Echec et le système est dépourvu de protection de haute disponibilité.

Intervention de l'utilisateur

Suivez les procédures de résolution suivantes :

- Restaurez le système secondaire.

  Cliquez sur l'onglet **Admin**, sur **Gestion du système et de la licence**, puis sur **Restaurer le système**.
- Inspectez le dispositif à haute disponibilité secondaire pour vérifier s'il est hors tension ou a rencontré une panne matérielle.
- Utilisez la commande **ping** pour vérifier la communication entre le système principal et le système de secours.
- Vérifiez le commutateur qui relie le dispositif à haute disponibilité principal au dispositif secondaire.

  Vérifiez les IPtables sur le dispositif principal et secondaire.
- Examinez le fichier /var/log/qradar.log sur le dispositif de secours pour déterminer la cause de l'échec.

Echec du système de haute disponibilité (HA) actif

38750081 - Défaillance du système de haute disponibilité (HA) actif.

Explication

Le système actif ne peut pas communiquer avec le système de secours car le système actif ne répond pas ou est défaillant. Le système de secours prend le contrôle des opérations sur le système actif défaillant.

Intervention de l'utilisateur

Suivez les procédures de résolution suivantes :

- Inspectez le dispositif à haute disponibilité actif pour vérifier s'il est hors tension ou a rencontré une panne matérielle.
- Si le système actif est le système principal haute disponibilité, restaurez le système actif.

  Cliquez sur l'onglet **Admin**, puis sur **Gestion du système et de la licence**. Dans le menu **Haute disponibilité**, sélectionnez l'option **Restaurer le système**.
- Examinez le fichier /var/log/qradar.log sur le dispositif de secours pour déterminer la cause de l'échec.
- Utilisez la commande **ping** pour vérifier la communication entre le système actif et le système de secours.
- Vérifiez le commutateur qui relie le dispositif actif et le dispositif haute disponibilité principal de secours.

Vérifiez les IPtables sur le dispositif actif et de secours.

Echec de l'installation de la haute disponibilité

38750086 - Un problème est survenu lors de l'installation de la haute disponibilité sur le cluster.

Explication

Lorsque vous installez un dispositif à haute disponibilité (HA), le processus d'installation lie le dispositif principal et le dispositif secondaire. Le processus d'installation et de configuration contient un minuteur pour déterminer si une installation requiert votre attention. L'installation du dispositif de haute disponibilité a dépassé la limite fixée à 6 heures.

Aucune protection par haute disponibilité ne sera disponible tant que le problème n'aura pas été résolu.

Intervention de l'utilisateur

Contactez le service clients.

Echec de la désinstallation d'un dispositif à haute disponibilité

38750087 - Un problème est survenu lors du retrait de la fonctionnalité de haute disponibilité sur le cluster.

Explication

Lorsque vous retirez un dispositif à haute disponibilité (HA), le processus d'installation supprime les connexions et les processus de réplication de données entre le dispositif principal et le dispositif secondaire. Si le processus d'installation ne parvient pas à retirer correctement du cluster le dispositif à haute disponibilité, le système principal continue à fonctionner normalement.

Intervention de l'utilisateur

Essayez une nouvelle fois de retirer le dispositif à haute disponibilité.

Erreur à l'initialisation d'un scanner

38750089 - Un scanner n'est pas parvenu à s'initialiser.

Explication

Une analyse de vulnérabilités planifiée n'est pas parvenue à se connecter à un scanner externe pour lancer le processus d'importation d'analyse.

Les problèmes d'initialisation d'analyse sont généralement dus à des problèmes de données d'identification ou de connectivité au scanner distant. Les scanners dont l'initialisation échoue affichent des messages d'erreur détaillés dans l'infobulle d'une analyse planifiée avec un statut d'échec.

Intervention de l'utilisateur

Procédez comme suit :

1. Cliquez sur l'onglet **Admin**.
2. Dans le menu de navigation, cliquez sur **Sources de données**.
3. Cliquez sur l'icône **Planifier les scanners d'analyse des vulnérabilités**.

4. Dans la liste des scanners, positionnez le curseur au-dessus de la colonne **Statut** d'un scanner pour afficher un message de réussite ou d'échec détaillé.

Erreur d'échec d'analyse

38750090 - Une analyse a échoué.

Explication

Une analyse de vulnérabilité prévue n'a pas réussi à importer des données de vulnérabilité. Les échecs d'analyse résultent généralement de problèmes de configuration ou de performances qui résultent d'un grand volume de données à importer. Les échecs d'analyse peuvent également se produire quand un rapport d'analyse téléchargé par le système est dans un format illisible.

Intervention de l'utilisateur

Procédez comme suit :

1. Cliquez sur l'onglet **Admin**.
2. Dans le menu de navigation, cliquez sur **Sources de données**.
3. Cliquez sur **Planifier les scanners d'analyse des vulnérabilités**.
4. Dans la liste des scanners, positionnez le curseur au-dessus de la colonne **Statut** d'un scanner pour afficher un message de réussite ou d'échec détaillé.

Echec de l'initialisation du filtre

38750091 - Le filtre d'analyse du trafic n'est pas parvenu à s'initialiser.

Explication

Si une configuration n'a pas été sauvegardée correctement ou si un fichier de configuration est endommagé, l'initialisation du service de collecte d'événements (ECS) peut échouer. Si le processus d'analyse du trafic n'a pas démarré, les nouvelles sources de journal ne sont pas reconnues automatiquement.

Intervention de l'utilisateur

Sélectionnez l'une des options suivantes :

- Créer manuellement des sources de journal pour les nouveaux dispositifs ou sources d'événement jusqu'à ce que le processus d'analyse du trafic fonctionne.

  Toutes les nouvelles sources d'événements sont classées comme SIM générique jusqu'à ce qu'elles aient été mappées à une source de journal.
- Si vous rencontrez une erreur lors de la mise à jour automatique, examinez le journal pour déterminer si une erreur s'est produite lors de l'ajout d'un gestionnaire de service de données ou d'un protocole.

Stockage sur disque indisponible

38750092 - La sentinelle de disque a détecté qu'une ou plusieurs partitions de stockage ne sont pas accessibles.

Explication

La sentinelle disque n'a pas reçu de réponse dans les 30 secondes. Ceci peut être dû à un problème de partition ou le système peut connaître une charge lourde et ne pas pouvoir répondre dans les 30 secondes.

Intervention de l'utilisateur

Sélectionnez l'une des options suivantes :

- Vérifiez le statut de votre partition `/store` à l'aide de la commande **touch**.

Si le système répond à la commande **touch**, l'indisponibilité du stockage sur disque est probablement imputable à la charge système.

- Déterminez si la notification correspond à un abandon d'événements.

Le système supprime des événements s'il ne peut pas les écrire sur disque. Examinez le statut des partitions de stockage.

Concepts associés:

«Stockage sur disque disponible», à la page 46

38750093 - Une ou plusieurs partitions de stockage auparavant inaccessibles sont désormais accessibles.

Espace disque insuffisant pour exporter des données

38750096 - Espace disque insuffisant pour terminer la requête d'exportation de données.

Explication

Si le répertoire d'exportation ne dispose pas d'un espace suffisant, l'exportation des données d'événement, de flux et d'infractions est annulée.

Intervention de l'utilisateur

Sélectionnez l'une des options suivantes :

- Libérez de l'espace disque dans le répertoire `/store/exports`.
- Configurez la propriété **Répertoire d'exportation** dans la fenêtre Paramètres système de sorte à utiliser une partition disposant d'un espace disque suffisant.
- Configurez un périphérique de stockage externe.

Retard dans l'accumulateur

38750099 - L'accumulateur a été incapable d'agréger tous les événements / flux pour cet intervalle.

Explication

Ce message s'affiche lorsque le système ne parvient pas à accumuler des agrégations de données dans un intervalle de 60 secondes.

Chaque minute, le système crée des agrégation de données pour chaque recherche agrégée. Les agrégations de données sont utilisées dans les graphiques et rapports de série temporelle et elles doivent s'effectuer dans un intervalle de 60 secondes. Si le nombre de recherches et de valeurs uniques dans les recherches est trop élevé, le temps nécessaire au traitement des agrégations peut être supérieur à 60 secondes. Des colonnes peuvent être manquantes dans les graphiques et les rapports de série temporelle pour la période à laquelle s'est produit le problème.

Vous ne perdez pas de données lorsque ce problème survient. L'ensemble des données brutes, des événements et des flux sont toujours écrits sur le disque. Seules les accumulation, qui sont des ensembles de données générées à partir des données stockées, sont incomplètes.

Intervention de l'utilisateur

Les facteurs ci-après peuvent contribuer à une charge accrue susceptible d'entraîner un retard de l'accumulateur :

Fréquence des accumulations incomplètes
Si l'accumulation échoue uniquement une ou deux fois par jour, les suppressions peuvent être dues à une charge système accrue en raison de recherches, de cycles de compression de données ou de sauvegardes de données importants.

Les échecs non fréquents peuvent être ignorés. Si des échecs se produisent plusieurs fois par jour, à toute heure, vous devrez peut-être davantage investiguer.

Charge de système élevée
Si d'autres processus utilisent de nombreuses ressources système, la charge système accrue peut entraîner un ralentissement des agrégations. Recherchez la cause de la charge système accrue et remédiez-y si possible.

Par exemple, si les accumulations échouent lors d'une recherche de données importante qui dure longtemps, vous pouvez empêcher les suppressions d'accumulateur en réduisant la taille de la recherche sauvegardé.

Demandes d'accumulateur importantes
Si des intervalles d'accumulateur sont régulièrement supprimés, vous devrez peut-être réduire la charge de travail.

La charge de travail de l'accumulateur dépend du nombre d'agrégations et du nombre d'objets uniques dans ces agrégation. Le nombre d'objets uniques dans une agrégation dépend des paramètres group-by et des filtres qui sont appliqués à la recherche.

Par exemple, une recherche qui agrège des services, filtre les données à l'aide d'un élément de hiérarchie de réseau local, par exemple une zone DMZ. Le regroupement par adresse IP peut produire des résultats de recherche contenant jusqu'à 200 objets uniques. Si vous ajoutez des ports de destination à la recherche, et si chaque serveur héberge 5 à 10 services sur différents ports, le nouvel agrégat `destination.ip + destination.port` peut accroître le nombre d'objets uniques à 2000. Si vous ajoutez l'adresse IP source à l'agrégat, et si vous avez plusieurs milliers d'adresses IP distantes qui correspondent à chaque service, la vue agrégée peut avoir des centaines de milliers de valeurs uniques. Cette recherche crée une forte demande sur l'accumulateur.

Pour afficher les vues agrégées qui exercent la plus fore demande sur l'accumulateur :

1. Sous l'onglet **Admin**, cliquez sur **Gestion de données agrégées**.
2. Cliquez dans la colonne **Données écrites** afin de trier dans l'ordre croissant et afficher les vues les plus importantes.
3. Passez en revue l'étude de rentabilité pour chacune des agrégation les plus importantes afin de voir si elles sont encore nécessaires.

Concepts associés:

«Résultats de rapport incomplets», à la page 7
Une fois que vous avez configuré et exécuté les rapports IBM Security QRadar, vous pouvez découvrir des résultats inattendus. Un rapport peut sembler ne pas afficher toutes les données dont vous avez besoin.

Echec de la lecture de règles par le CRE

`38750107 - La dernière tentative de lecture des règles (due en général à une modification de règle) a échoué. Examinez les détails du message et le journal d'erreurs pour plus d'informations sur la résolution du problème.`

Explication

Le moteur de règles personnalisées (CRE) sur un processeur d'événement ne parvient pas à lire une règle pour corréler un événement entrant. La notification peut contenir l'un des messages suivants :

- Si le moteur de règles personnalisées n'est pas parvenu à lire une seule règle, dans la plupart des cas, ceci est dû à une modification récente de la règle. Le contenu du message de notification affiche la règle ou la règle de la chaîne de règles en cause.
- Dans de rares cas, des données endommagées peuvent induire un échec total de l'ensemble de règles. Une erreur d'application s'affiche et l'interface de l'éditeur de règles peut cesser de répondre ou générer des erreurs supplémentaires.

Intervention de l'utilisateur

Dans le cas d'une erreur de lecture d'une seule règle, envisagez les options suivantes :

- Pour identifier la règle à l'origine de la notification, désactivez temporairement la règle.
- Modifiez la règle pour annuler les dernières modifications.
- Supprimez et recréez la règle à l'origine de l'erreur.

En cas d'erreurs d'application où le CRE n'est pas parvenu à lire des règles, contactez le service clients.

L'accumulateur ne peut pas lire la définition de vue pour les données agrégées

38750108 - Accumulateur : impossible de lire la définition de vue de données agrégées pour éviter un problème de désynchronisation. Des vues de données agrégées ne peuvent plus être créées ou chargées. Les graphiques de série temporelle et les rapports ne fonctionneront pas eux non plus.

Explication

Un problème de synchronisation s'est produit. La configuration de la vue de données agrégées en mémoire a consigné des données erronées dans la base de données.

Pour éviter que les données ne soient endommagées, le système désactive les vues de données agrégées. Lorsque ces vues sont désactivées, les graphiques de séries temporelles, les recherches sauvegardées et les rapports planifiés affichent des graphiques vides.

Intervention de l'utilisateur

Contactez le service clients.

Une planification de stockage et retransmission n'a pas transmis tous les événements

38750109 - Une planification de stockage et retransmission s'est terminée alors qu'il restait des événements sur le disque. Ces événements seront stockés sur le collecteur d'événement local jusqu'à la prochaine session de retransmission.

Explication

Si la planification contient un début et de fin de courte ou de nombreux événements à retransmettre, l'appareil Collecteur d'événements pourrait ne pas avoir suffisamment de temps pour transférer les événements en file d'attente. Les événements sont stockés jusqu'à la prochaine possibilité de transférer des événements. Lorsque le prochain intervalle de stockage et retransmission se produit, les événements sont transmis au processeur d'événements.

Intervention de l'utilisateur

Augmentez le taux de transfert des événements à partir de votre appareil collecteur d'événements ou augmentez l'intervalle de temps qui est configuré pour transmettre les événements.

Panne disque

38750110 - Panne disque : le moniteur de matériel a déterminé qu'un disque est en état d'échec.

Explication

Les outils système embarqués ont détecté une panne disque. Le message de notification fournit des informations sur le disque en panne et sur l'emplacement ou la baie où s'est produite la panne.

Intervention de l'utilisateur

Si la notification persiste, contactez le service clients ou remplacez les composants en cause.

Panne disque anticipée

38750111 - Panne disque anticipée : le moniteur de matériel a anticipé un état d'échec pour un disque.

Explication

Le système surveille le statut du matériel sur une base horaire pour déterminer quand une intervention matérielle est requise sur le dispositif.

Les outils système embarqués ont détecté qu'un disque est sur le point de tomber en panne ou arrive en fin de vie. L'emplacement ou la baie concernés par la panne sont identifiés.

Intervention de l'utilisateur

Planifiez une maintenance pour le disque dont l'état d'échec est anticipé.

Echec de l'outil d'analyse

38750118 - Une analyse s'est arrêtée inopinément. Dans certains cas, ceci peut entraîner l'arrêt du scanner.

Explication

Le système ne parvient pas à initialiser une analyse de vulnérabilités et les résultats de l'analyse des actifs ne peuvent pas être importés de scanners externes. Si les outils d'analyse s'arrêtent de manière inattendue, le système ne peut pas communiquer avec un scanner externe. Le système tente à cinq reprises de se connecter au scanner externe à 30 secondes d'intervalle.

Dans de rares cas, les outils de reconnaissance détectent une configuration d'hôte ou de réseau non testée.

Intervention de l'utilisateur

Sélectionnez l'une des options suivantes :

- Examinez dans l'éditeur de déploiement la configuration des scanners externes pour vérifier que l'adresse IP de la passerelle est correcte.
- Assurez-vous que le scanner externe peut communiquer via l'adresse IP configurée.
- Assurez-vous que les règles de pare-feu de votre zone démilitarisée ne bloquent pas la communication entre votre dispositif et les actifs que vous désirez analyser.

Echec de passerelle d'analyse externe

38750119 - Une adresse IP de passerelle non valide ou inconnue a été soumise au scanner externe hébergé. L'analyse a été arrêtée.

Explication

Lors de l'ajout d'un scanner externe, une adresse IP de passerelle est requise. Si l'adresse configurée pour le scanner dans l'éditeur de déploiement est incorrecte, le scanner ne peut pas accéder à votre réseau externe.

Intervention de l'utilisateur

Sélectionnez l'une des options suivantes :

- Examinez la configuration des scanners externes configurés dans l'éditeur de déploiement pour vérifier que l'adresse IP de la passerelle est correcte.
- Assurez-vous que le scanner externe peut communiquer via l'adresse IP configurée.
- Assurez-vous que les règles de pare-feu de votre zone démilitarisée ne bloquent pas la communication entre votre dispositif et les actifs que vous désirez analyser.

L'authentification de l'utilisateur a échoué pour des mises à jour automatiques

38750127 - Les mises à jour automatiques d'authentification utilisateur ont échoué. Un ID IBM individuel est requis.

Explication

Des informations d'identification valides sont requises pour autoriser les téléchargements automatiques à partir du serveur de mise à jour.

Intervention de l'utilisateur

Sélectionnez l'une des options suivantes :

- Les administrateurs doivent s'inscrire à un compte sur le site Web de support IBM (http://www.ibm.com/support/).
- Pour afficher les paramètres de mise à jour automatique, sur l'onglet **Admin**, cliquez sur l'icône **Mise à jour automatique** et sélectionnez **Modifier les paramètres** > **Avancé**. Les administrateurs peuvent confirment que le nom d'utilisateur et le mot de passe dans la fenêtre Paramètres sont corrects.

La limite de données agrégées a été atteinte

38750130 - La vue de données agrégées n'a pas pu être créée en raison d'une limite d'agrégation.

Explication

Le processus de l'accumulateur compte et prépare les événements et les flux dans les accumulations de données afin d'aider aux recherches, à l'affichage de graphiques et de rapports de performance. Il regroupe les données dans un intervalle de temps prédéfini afin de créer des vues de données agrégées. Une *vue de données agrégées* est un ensemble de données qui est utilisé pour dessiner un graphique de série temporelle, créer des rapports planifiés ou déclencher des règles de détection des anomalies.

La console est limitée à 130 vues de données d'agrégation.

Les actions utilisateur suivantes permettent de créer une nouvelle vue de données d'agrégation :

- Nouvelles règles de détection des anomalies.

- Nouveaux rapports.
- Nouvelles recherches sauvegardées utilisant des données de séries temporelles.

Lorsque la limite de vue de données d'agrégation est atteinte, la notification est générée. Lorsque des utilisateurs essaient de créer des règles d'anomalie, des rapports ou des recherches sauvegardées, ils sont informés via l'interface utilisateur que le système a atteint la limite.

Intervention de l'utilisateur

Pour résoudre ce problème, les administrateurs peuvent passer en revue les vues de données d'agrégation actives sous l'onglet **Admin** dans la fenêtre **Gestion de données agrégées**. La fonction de gestion des données agrégées fournit des informations sur les rapports, les recherches et les règles de détection des anomalies en cours d'utilisation dans chaque vue de données d'agrégation. L'administrateur peut passer en revue la liste des vues de données d'agrégation afin de déterminer les données qui sont les plus importantes pour les utilisateurs. Les vues de données d'agrégation peuvent être désactivées afin de permettre aux utilisateurs de créer une règle, un rapport ou une recherche sauvegardée qui nécessite une vue de données d'agrégation.

Si l'administrateur décide de supprimer une vue de données d'agrégation, un récapitulatif fournit un aperçu des recherches, des règles ou des rapports affectés. Pour recréer une vue des données agrégées supprimée, l'administrateur doit uniquement réactiver ou recréer la recherche, la règle d'anomalie, ou le rapport. Le système crée automatiquement la vue de données d'agrégation d'après les données requises.

Le magistrat ne peut pas conserver les mises à jour d'infraction

38750147 - `Le magistrat a détecté des erreurs graves susceptibles d'empêcher la mise à jour des infractions.`

Explication

Le système a détecté une exception lors de l'écriture des mises à jour d'infraction dans la base de données.

Les événements sont traités et enregistrés, mais ils ne contribuent pas aux infractions.

Intervention de l'utilisateur

Procédez à un nettoyage léger du modèle de données SIM avec l'option **Désactiver toutes les infractions** désélectionnée.

1. Cliquez sur l'onglet **Admin**.
2. Dans la barre d'outils, cliquez sur **Avancé** > **Nettoyer le modèle SIM**.
3. Cliquez sur **Nettoyage léger** pour définir les infractions sur Inactif.
4. Assurez-vous que l'option **Désactiver toutes les infractions** n'est pas sélectionnée.
5. Sélectionnez la case **Voulez-vous vraiment réinitialiser le modèle de données ?** et cliquez sur **Continuer**.

Lorsque vous nettoyez le modèle SIM, toutes les infractions existantes sont clôturées. Le fait de nettoyer le modèle SIM n'affecte pas les événements et flux existants.

Notifications d'avertissements pour les dispositifs QRadar

Les notifications de santé du système IBM Security QRadar sont des messages proactifs relatifs à des incidents logiciels ou matériels réels ou imminents.

Nombre maximal de détecteurs surveillés

38750006 - L'analyse de trafic surveille déjà le nombre maximal de sources de journal.

Explication

Le système est sujet à une limite quant au nombre de sources de journal pouvant être mises en file d'attente pour reconnaissance automatique par l'analyse du trafic. Si le nombre maximal de sources de journal dans la file d'attente est atteint, de nouvelles sources de journal ne peuvent pas être ajoutées.

Les événements de la source de journal sont classifiés comme SIM générique avec le libellé Journal d'événements inconnu.

Intervention de l'utilisateur

Sélectionnez l'une des options suivantes :

- Examinez les sources de journal classifiées comme SIM générique dans l'onglet **Activité du journal** pour déterminer le type de dispositif depuis le contenu de l'événement.
- Vérifiez que les mises à jour automatiques peuvent télécharger les mises à jour DSM les plus récentes afin d'identifier et d'analyser correctement les événements de source de journal.
- Vérifiez si la source de journal est officiellement prise en charge.

  Si votre dispositif est pris en charge, créez manuellement une source de journal pour les événements qui n'ont pas été reconnus automatiquement.
- Si votre dispositif n'est pas pris en charge officiellement, créez un DSM universel pour identifier et classer vos événements.
- Attendez que le périphérique ait soumis 1000 événements.

  Si le système ne parvient pas à reconnaître automatiquement la source de journal après 1000 événements, celle-ci est supprimée de la file d'attente d'analyse du trafic. Ceci libère de l'espace pour la reconnaissance automatique d'une autre source de journal.

Impossible de déterminer la source de journal associée.

38750007 - Impossible de détecter automatiquement la source de journal associée à l'adresse IP <*adresse IP* >. Impossible de détecter automatiquement la source de journal associée à l'adresse IP.

Explication

Lorsque des événements sont envoyés depuis une unité non détectée ou non reconnue, le composant d'analyse du trafic a besoin d'au moins 25 événements pour identifier une source de journal.

Si la source de journal n'est toujours pas identifiée après 1000 événements, le système abandonne le processus de reconnaissance automatique et génère la notification système. Le système classifie ensuite la source de journal comme SIM générique et libelle les événements comme Journal d'événements inconnu.

Intervention de l'utilisateur

Vérifiez les options suivantes :

- Vérifiez l'adresse IP dans la notification système afin d'identifier la source de journal.
- Examinez l'onglet **Activité du journal** pour déterminer le type de dispositif à partir de l'adresse IP dans le message de notification, puis créez manuellement une source de journal.

  Assurez-vous que la zone **Identificateur de la source de journal** correspond au nom d'hôte dans l'en-tête syslog du contenu d'origine. Vérifiez que les événements apparaissent sur l'unité en déployant les modifications et en recherchant la source de journal créée manuellement.

- Examinez les sources de journal véhiculant à faible débit les événements. Les sources de journal avec des débits d'événements faibles sont généralement à l'origine de cette notification.
- Pour analyser correctement les événements pour votre système, vérifiez que la mise à jour automatique télécharge bien les gestionnaires de service de données les plus récents.
- Examinez toutes les sources de journal fournissant des événements via un serveur de journaux central. Les sources de journal issues d'un serveur de journaux central ou de consoles de gestion peuvent devoir être créées manuellement.
- Vérifiez si la source de journal est officiellement prise en charge. Si votre dispositif est pris en charge, créez manuellement une source de journal pour les événements et ajoutez une extension de source de journal.
- Si votre dispositif n'est pas pris en charge officiellement, créez un DSM universel pour identifier et classer vos événements.

Nombre maximal d'événements ou de flux atteint

38750008 - Au cours de la dernière heure, le dispositif a dépassé l'allocation EPS ou FPM.

Explication

Le pool de licences alloue à chaque dispositif un volume spécifique de données d'événement et de flux. Au cours de la dernière heure, le dispositif a dépassé l'allocation EPS ou FPM.

Le dépassement de la capacité allouée au dispositif risque de déclencher la mise en file d'attente les événements et des flux par le système, ou la suppression des données lorsque la file d'attente de sauvegarde arrive à saturation.

Intervention de l'utilisateur

- Réglez les allocations du pool de licence de manière à augmenter la capacité EPS et FPM du dispositif.
- Optimisez le système pour réduire le volume d'événements et de flux accédant au pipeline d'événements.

Le collecteur de flux ne parvient pas établir la synchronisation d'horloge initiale

38750009 - Le collecteur de flux n'est pas parvenu à établir la synchronisation d'horloge initiale.

Explication

Le processeur QFlow Collector comporte une fonction avancée pour configurer une adresse IP de serveur pour synchronisation d'horloge. Dans la plupart des cas, vous n'avez pas besoin de configurer une valeur. Si celle-ci est configurée, le processus QFlow tente toutes les heures de synchroniser l'heure avec le serveur d'horloge de l'adresse IP.

Intervention de l'utilisateur

Dans les actions de déploiement, sélectionnez le processus QFlow. Cliquez sur **Actions** > **Configurer**, puis sur **Avancé**. Effacez la valeur de la zone **Adresse IP du serveur de synchronisation d'horloge**, puis cliquez sur **Sauvegarder**.

Impossible d'exécuter une demande de sauvegarde

38750033 - Sauvegarde : Espace libre insuffisant pour effectuer la sauvegarde.

Explication

La sentinelle de disque est responsable du suivi des problèmes de disque et de stockage système. Avant le début de la sauvegarde, la sentinelle disque vérifie l'espace disque disponible afin de déterminer si la sauvegarde peut aboutir. Si l'espace disque disponible est inférieur à deux fois la taille de la dernière sauvegarde, la sauvegarde est annulée. Par défaut, les sauvegardes sont stockées dans `/store/backup`.

Intervention de l'utilisateur

Pour résoudre ce problème, sélectionnez l'une des options suivantes :

- Libérez de l'espace disque sur votre dispositif pour allouer suffisamment d'espace pour la réalisation d'une sauvegarde dans `/store/backup`.
- Configurez vos sauvegardes existantes pour utiliser une partition avec l'espace disque disponible.
- Configurez davantage de stockage pour votre dispositif. Pour plus d'informations, consultez le manuel *Offboard Storage Guide*.

Impossible d'exécuter une demande de sauvegarde

38750035 - `Sauvegarde : impossible d'exécuter une demande de sauvegarde.`

Explication

Une sauvegarde ne peut pas démarrer ou ne peut pas être effectuée pour l'une des raisons suivantes :

- Le système ne parvient pas à nettoyer la table de synchronisation de réplication de sauvegarde.
- Le système est incapable d'exécuter une demande de suppression.
- Le système ne peut pas synchroniser la sauvegarde avec les fichiers qui sont sur le disque.
- Le répertoire de sauvegarde monté NFS n'est pas disponible ou comporte des options d'exportation NFS incorrectes (`no_root_squash`).
- Le système ne peut pas initialiser la sauvegarde à la demande.
- Le système ne peut pas récupérer la configuration pour le type de sauvegarde sélectionné.
- Impossible d'initialiser une sauvegarde planifiée.

Intervention de l'utilisateur

Lancez une sauvegarde manuellement pour déterminer où survient l'échec. Si plusieurs sauvegardes ne parviennent pas à démarrer, contactez le Support client.

La licence du moniteur de processus a expiré ou n'est pas valide

38750044 - `Moniteur de processus : Impossible de démarrer le processus : la licence a expiré ou n'est pas valide.`

Explication

La licence est arrivée à expiration pour un hôte géré. Tous les processus de collecte de données s'arrêtent sur le dispositif.

Intervention de l'utilisateur

Contactez votre ingénieur commercial pour renouveler votre licence.

Détection d'un processus non géré entraînant une transaction longue

38750048 - `Sentinelle de transaction : détection d'un processus non géré entraînant une transaction anormalement longue affectant négativement la stabilité du système.`

Explication

La sentinelle de transaction a déterminé qu'un processus externe (tel qu'un problème de réplication de base de données, un script de maintenance, une mise à jour automatique) ou un processus de ligne de commande ou une transaction a provoqué un verrou de base de données. La plupart des processus ne peuvent pas s'exécuter pendant plus d'une heure. Des occurrences répétées du même processus doit faire l'objet d'une investigation.

Intervention de l'utilisateur

Sélectionnez l'une des options suivantes :

- Recherchez dans le fichier `/var/log/qradar.log` le mot `TxSentry` pour déterminer l'identificateur du processus à l'origine de vos problèmes de transaction.
- Attendez de voir si le processus achève la transaction et libère le verrou de base de données.
- Libérez manuellement le verrou de base de données en redémarrant l'identificateur de processus.

Restauration de la santé du système par l'annulation de transactions bloquées

38750049 - `Sentinelle de transaction : restauration de la santé du système par l'annulation de transactions bloquées ou de verrous.`

Explication

La sentinelle de transaction a restauré un état de santé normal du système en annulant des transactions de base de données suspendues ou en supprimant des verrous de base de données. Pour déterminer le processus à l'origine de l'erreur, recherchez dans le fichier `qradar.log` le mot `TxSentry`.

Intervention de l'utilisateur

Aucune action n'est requise.

Nombre maximal d'infractions actives atteint

38750050 - `MPC: Impossible de créer une nouvelle infraction. Le nombre maximal d'infractions actives a été atteint.`

Explication

Le système ne parvient pas à créer des infractions ou à changer en active le statut d'une infraction en sommeil. Le nombre par défaut d'infractions actives pouvant être ouvertes sur votre système est limité à 2500. Par infraction active, on entend une infraction qui a continué à recevoir des mises à jour du nombre d'événements les cinq derniers jours, ou moins.

Intervention de l'utilisateur

Sélectionnez l'une des options suivantes :

- Faites passer les infractions de sécurité mineures de l'état ouvertes ou actives à fermées, ou à fermées et protégées.
- Ajustez votre système en réduisant le nombre d'événements générant des infractions.

  Pour empêcher la suppression d'une infraction fermée par votre politique d'administration de conservation des données, définissez cette infraction comme 'protégée'.

Nombre maximal d'infractions atteint

38750051 - MPC: Impossible de traiter l'infraction. Le nombre maximal d'infractions a été atteint.

Explication

Par défaut, la limite de traitement est fixée à 2500 infractions actives et à 100 000 infractions au total.

Si une infraction active ne reçoit pas de mise à jour d'événement dans les 30 minutes, son statut passe à En sommeil. Si une mise à jour d'événement survient, une infraction en sommeil peut passer à l'état Active. Au bout de cinq jours, les infractions en sommeil n'ayant pas reçu de mise à jour d'événement passent à l'état Inactive.

Intervention de l'utilisateur

Sélectionnez l'une des options suivantes :

- Ajustez votre système en réduisant le nombre d'événements générant des infractions.
- Appliquez à la politique d'administration de conservation des infractions un délai au terme duquel elle pourra éliminer les infractions inactives.

  Pour empêcher la suppression d'une infraction fermée par votre politique d'administration de conservation des données, définissez cette infraction comme 'protégée'.
- Pour libérer de l'espace disque pour les infractions actives importantes, modifiez le statut d'infractions actives à En sommeil.

Arrêt des rapports à exécution longue

38750054 - Un rapport dont l'exécution se prolonge au delà du seuil maximal configuré a été arrêté.

Explication

Le système annule le rapport dont l'exécution a dépassé le délai imparti. Les rapports dont l'exécution dépasse les délais par défaut suivants sont annulés.

Tableau 4. Délais limites d'exécution par fréquence de rapport

Fréquence du rapport	Délai limite d'exécution (en heures)
Horaire	2
Quotidienne	12
Manuel	12
Hebdomadaire	24
Mensuelle	24

Intervention de l'utilisateur

Sélectionnez l'une des options suivantes :

- Réduisez la couverture de votre rapport, mais planifiez celui-ci pour s'exécuter plus fréquemment.
- Editez les rapports manuels pour leur exécution d'après un calendrier.

  Un rapport manuel peut reposer sur des données brutes mais ne peut pas avoir accès aux données cumulées. Modifiez votre rapport manuel de sorte à utiliser un planning horaire, quotidien, hebdomadaire ou mensuel.

Erreur liée à une saturation de la mémoire et redémarrage de l'application en erreur

38750055 - Saturation de la mémoire : système restauré. Application en erreur redémarrée.

Explication

Une application ou un service ne dispose pas d'assez de mémoire et a été redémarré. Les problèmes de saturation mémoire sont généralement provoqués par des problèmes logiciels ou des requêtes définies par l'utilisateur.

Intervention de l'utilisateur

Suivez les procédures de résolution suivantes :

- Examinez le message d'erreur consigné dans le fichier /var/log/qradar.log afin de déterminer le composant défaillant.
- Si le serveur proxy Ariel effectue une recherche sur de gros volumes de données ou s'il utilise une option de regroupement qui génère des valeurs uniques dans les résultats de la recherche, réduisez le nombre de valeurs uniques ou le délai de recherche.
- Si l'accumulateur génère un graphique de séries temporelles avec de nombreuses valeurs uniques agrégées, réduisez la taille de la requête.
- Si une source de journal basée sur un protocole a été récemment activée, diminuez la période d'interrogation afin de réduire le volume de données interrogées. Si plusieurs sources de journal basées sur un protocole s'exécutent en même temps, échelonnez les heures de début.
- Si la règle a été récemment modifiée pour un suivi des propriétés uniques sur de longues périodes, réduisez la durée de moitié ou réduisez le nombre d'événements correspondants en ajoutant un autre filtre.

Transactions longues pour un processus géré

38750056 - Sentinelle de transaction : détection d'un processus géré entraînant une transaction anormalement longue affectant négativement la stabilité du système.

Explication

La sentinelle de transaction détermine qu'un processus géré, tel que Tomcat ou un service de collecte d'événements (ECS), est la cause d'un verrou de base de données.

Un processus géré est forcé de redémarrer.

Intervention de l'utilisateur

Pour déterminer le processus à l'origine de l'erreur, recherchez dans le fichier qradar.log le mot TxSentry.

Configuration incorrecte de la source du protocole

38750057 - Une configuration de source de protocole peut empêcher la collecte d'événements.

Explication

Le système a détecté une configuration de protocole incorrecte pour une source de journal. Les sources de journal qui utilisent des protocoles pour extraire des événements depuis de sources distante peuvent générer une erreur d'initialisation lorsqu'un problème de configuration est détecté dans le protocole.

Intervention de l'utilisateur

Corrigez les problèmes de configuration de protocole en procédant comme suit :

- Examinez la source de journal pour vérifier que la configuration du protocole est correcte.

  Vérifiez les zones d'authentification, les chemins de fichier, les noms de base de données JDBC, et assurez-vous que le système peut communiquer avec les serveurs distants. Survolez une source de journal avec le pointeur de la souris pour afficher des informations d'erreur supplémentaires.
- Examinez le journal `/var/log/qradar.log` pour plus d'informations sur l'erreur de configuration du protocole.

MPC : le processus n' pas été arrêté correctement

38750058 - `MPC : le serveur n'a pas été arrêté correctement. Les infractions sont en train d'être fermées dans l'ordre pour pouvoir effectuer une resynchronisation et assurer la stabilité du système.`

Explication

Le processus de magistrat a rencontré une erreur. Les infractions actives se ferment, les services redémarrent et les tables de base de données sont vérifiées et recréées si nécessaire.

Le système procède à une synchronisation pour éviter que des données ne soient endommagées. Si le composant magistrat détecte un état endommagé, les tables de base de données et les fichiers seront régénérés.

Intervention de l'utilisateur

Le composant magistrat s'auto-répare. Si l'erreur persiste, contactez le service clients.

La dernière sauvegarde a dépassé le délai d'exécution imparti

38750059 - `Sauvegarde : La dernière sauvegarde planifiée dépasse le seuil d'exécution.`

Explication

Le délai d'exécution imparti est déterminé par la priorité de sauvegarde affectée lors de la configuration.

Intervention de l'utilisateur

Sélectionnez l'une des options suivantes :

- Modifiez la configuration de sauvegarde en prolongeant la durée maximale configurée pour son exécution. N'étendez pas la durée d'exécution au-delà de 24 heures.
- Modifiez la sauvegarde ayant échoué en lui attribuant un niveau de priorité plus élevé. Des niveaux de priorité plus élevés allouent plus de ressources système à l'exécution de la sauvegarde.

Déploiement d'une mise à jour automatique

38750069 - `L'installation des mises à jour automatiques a abouti. Dans l'onglet Admin, cliquez sur Déployer les changements.`

Explication

Une mise à jour automatique (par exemple, une mise à jour RPM) a été téléchargée et nécessite de déployer ses modifications pour terminer la procédure d'installation.

Intervention de l'utilisateur

Dans l'onglet **Admin**, cliquez sur **Déployer les changements**.

Source de journal créée à l'état désactivée

38750071 - Une source de journal a été créée à l'état désactivé en raison de limites de licence.

Explication

L'analyse de trafic est un processus qui identifie et crée automatiquement des sources de journal à partir d'événements. Si vous avez atteint la limite de licence actuelle des sources de journal, le processus d'analyse du trafic peut créer la source de journal à l'état désactivé. Les sources de journal désactivées ne collectent pas d'événements et ne sont pas comptabilisées dans la limite des sources de journal.

Intervention de l'utilisateur

Vérifiez les options suivantes :

- Dans l'onglet **Admin**, cliquez sur l'icône **Sources de journal** et désactivez ou supprimez les sources de journal à faible priorité. Les sources de journal désactivées ne sont pas comptabilisées dans votre utilisation de licence de source de journal.
- Vérifiez que les sources de journal supprimées ne font pas l'objet d'une nouvelle reconnaissance automatique. Vous pouvez désactiver la source de journal pour empêcher sa reconnaissance automatique.
- Vérifiez que vous ne dépassez pas la limite imposée par votre licence lorsque vous ajoutez de nouvelles sources de journal en bloc.
- Si vous avez besoin d'une licence étendue pour inclure des sources de journal supplémentaires, contactez votre ingénieur commercial.

Seuil de sentinelle SAR franchi

38750073 - Sentinelle SAR : seuil franchi.

Explication

L'utilitaire SAR (System Activity Reporter) a détecté que votre charge système est au-dessus du seuil fixé. Votre système peut rencontrer une réduction des performances.

Intervention de l'utilisateur

Vérifiez les options suivantes :

- Dans la plupart des cas, aucune résolution n'est nécessaire.

  Par exemple, quand l'utilisation de l'unité centrale dépasse 90 %, le système tente automatiquement de revenir à une opération normale.
- Si cette notification est récurrente, augmentez la valeur par défaut de la sentinelle SAR.

  Cliquez sur l'onglet **Admin**, puis sur **Notifications système globales**. Augmentez le seuil de notification.
- Pour les notifications de charge système, réduisez le nombre de processus pouvant s'exécuter simultanément.

  Echelonnez l'heure de début des rapports, des analyses de vulnérabilités ou des importations de données pour vos sources de journal. Planifiez des sauvegardes et des processus système déclenchés à des heures différentes pour réduire la charge système.

L'utilisateur n'existe pas ou n'est pas défini

38750075 - L'utilisateur n'existe pas ou son rôle n'a pas été défini.

Explication

Le système a tenté de mettre à jour un compte utilisateur avec des autorisations supplémentaires, mais le compte utilisateur ou le rôle utilisateur n'existe pas.

Intervention de l'utilisateur

Dans l'onglet **Admin**, cliquez sur **Déployer les changements**. Les mises à jour de comptes ou de rôles utilisateur nécessitent de déployer les changements.

L'utilisation du disque a dépassé le seuil d'avertissement

38750076 - Sentinelle disque : L'utilisation du disque a dépassé le seuil d'avertissement.

Explication

La sentinelle disque a détecté que l'utilisation du disque sur votre système dépasse 90 %.

Afin de prévenir l'altération de données, le système désactive des processus lorsque l'espace disque sur votre système atteint 95 % d'utilisation. Les processus de collecte d'événements font partie des processus désactivés.

Intervention de l'utilisateur

Vous devez libérer de l'espace disque en supprimant des fichiers ou en modifiant vos politiques d'administration de conservation des données. Le système peut redémarrer automatiquement des processus une fois que l'utilisation de l'espace disque passe au-dessous du seuil de 92 %.

Le composant d'infrastructure est endommagé ou n'a pas démarré

38750083 - Composant d'infrastructure endommagé.

Explication

Lorsque le service de message (IMQ) ou la base de données PostgreSQL ne peut pas démarrer ou être régénérée, l'hôte géré ne peut pas opérer correctement ou communiquer avec la console.

Intervention de l'utilisateur

Contactez le service clients.

Difficulté de réplication des données

38750085 - La réplication de données rencontre des problèmes.

Explication

La réplication des données garantit que les hôtes gérés peuvent continuer à recueillir des données si la console est indisponible.

Un hôte géré a eu des difficultés lors du téléchargement de données. Si un hôte géré échoue à plusieurs reprises pour télécharger des données, le système peut rencontrer des problèmes de performance ou de communication.

Intervention de l'utilisateur

Si un hôte géré ne résout pas le problème de réplication par ses propres moyens, contactez le support client.

Evénements acheminés directement vers l'espace de stockage

38750088 - Une dégradation des performances a été détectée dans le pipeline d'événements. Des événements ont été acheminés directement vers l'espace de stockage.

Explication

Pour empêcher la saturation des files d'attente et la suppression d'événements par le système, le système de collecte d'événements (ECS) achemine des données vers l'espace de stockage. Les événements et les flux entrants ne sont pas classés par catégorie. Toutefois, les données d'événements bruts et de flux sont collectées et consultables.

Intervention de l'utilisateur

Vérifiez les options suivantes :

- Vérifiez les débits d'événements et de flux entrants. Si le pipeline d'événements place les événements en file d'attente, étoffez votre licence pour héberger plus de données.
- Examinez les modifications récentes apportées à la politique d'administration ou aux propriétés personnalisées. Ces modifications peuvent entraîner des fluctuations soudaines de vos débits d'événements ou de flux. Ces modifications peuvent affecter les performances du système ou entraîner le routage d'événements vers un espace de stockage.
- Des problèmes d'analyse DSM peuvent entraîner le routage des données d'événements vers un espace de stockage. Vérifiez si la source de journal est officiellement prise en charge.
- Les notifications SAR peuvent indiquer que les événements et les flux mis en file d'attente résident dans le pipeline d'événements.
- Ajustez le système pour réduire le volume d'événements et de flux accédant au pipeline d'événements.

Propriété personnalisée désactivée

38750097 - Une propriété personnalisée a été désactivée.

Explication

Une propriété personnalisée a été désactivée en raison de problèmes lors de son traitement. Les règles, rapports ou recherches utilisant la propriété personnalisée désactivée ne fonctionneront pas correctement.

Intervention de l'utilisateur

Sélectionnez l'une des options suivantes :

- Examinez la propriété personnalisée désactivée afin de corriger vos structures d'expression régulière. Ne réactivez pas de propriétés personnalisées désactivées avant d'avoir examiné et optimisé la structure ou le calcul de l'expression régulière.
- Si la propriété personnalisée est utilisée pour des règles ou rapports personnalisés, prenez soin de cocher la case **Optimiser l'analyse syntaxique pour les règles, rapports et recherches**.

Echec de la sauvegarde de l'unité

38750098 - Une défaillance s'est produite lors de la tentative de sauvegarde d'une unité ou la sauvegarde a été annulée.

Explication

L'erreur est généralement due à des erreurs de configuration dans CSM (Configuration Source Management) ou à l'annulation d'une sauvegarde par l'utilisateur.

Intervention de l'utilisateur

Sélectionnez l'une des options suivantes :

- Examinez les données d'identification et les jeux d'adresses dans CSM pour vérifier que le dispositif peut se connecter.
- Vérifiez que le protocole configuré pour se connecter à votre périphérique réseau est valide.
- Vérifiez que votre périphérique réseau et sa version sont pris en charge.
- Vérifiez que votre périphérique réseau se connecte au dispositif.
- Vérifiez que les adaptateurs installés sont les plus récents.

Données d'événement ou de flux non indexées

38750101 - `Les données d'événement/de flux ne sont pas indexées pour l'intervalle.`

Explication

Si des index trop nombreux sont activés ou que la charge système est trop lourde, le système peut supprimer l'événement ou le flux de la portion index.

Intervention de l'utilisateur

Sélectionnez l'une des options suivantes :

- Si la fréquence de suppression de l'index survient avec des notifications de la sentinelle SAR, le problème est probablement imputable à la charge système ou à un espace disque faible.
- Pour désactiver temporairement certains index afin de réduire la charge du système, sur l'onglet **Admin**, cliquez sur l'icône **Gestion de l'index**.

Seuil atteint pour actions de réponse

38750102 - `Action de réponse : seuil atteint.`

Explication

Le moteur de règles personnalisées (CRE) ne peut pas répondre à une règle car le seuil de réponse est saturé.

Des règles génériques ou un système optimisé peuvent générer plusieurs actions de réponse, en particulier les systèmes pour lesquels l'option **IF-MAP** est activée. Les actions de réponse sont placées en file d'attente. Des actions de réponse peuvent être supprimées si la file d'attente dépasse 2000 éléments dans le système de collecte d'événements (ECS) ou 1000 actions de réponse dans Tomcat.

Intervention de l'utilisateur

- Si l'option **IF-MAP** est activée, vérifiez que la connexion au serveur **IF-MAP** existe et qu'un problème de bande passante ne provoque pas une réponse de règle à la file d'attente dans Tomcat.
- Ajustez votre système en réduisant le nombre de règles déclenchées.

Retard dans la réplication de disque

38750103 - `Sentinelle du dispositif de bloc répliqué distribué : La réplication de disque prend du retard. Reportez-vous au journal pour plus d'informations.`

Explication

Si la file d'attente de réplication se remplit sur le dispositif principal, la charge système augmente sur ce système. Les problèmes de réplication sont généralement dus à des problèmes de performance sur le système principal, à des problèmes de stockage sur le système secondaire ou à des problèmes de bande passante entre les dispositifs.

Intervention de l'utilisateur

Sélectionnez l'une des options suivantes :

- Examinez l'activité de bande passante en chargeant une recherche sauvegardée **MGMT : Gestionnaire de bande passante** depuis l'onglet **Activité du journal**. Cette recherche affiche l'activité de bande passante entre la console et les hôtes.
- Si des notifications de sentinelle SAR sont récurrentes sur le dispositif principal, les files d'attente du dispositif de bloc répliqué distribué risquent d'être saturées sur le système principal.
- Utilisez SSH et la commande `cat /proc/drbd` pour surveiller le statut du dispositif de bloc répliqué distribué de l'hôte principal ou secondaire.

Annulation de la modification d'actifs

38750106 - Abandon de la modification d'actifs.

Explication

Une modification d'actif a dépassé le plafond de modification et le gestionnaire de profil d'actifs ignore la demande de modification d'actif.

Le gestionnaire de profil d'actif inclut un processus de persistance d'actifs qui met à jour les informations de profil d'actifs. Le processus collecte de nouvelles données d'actif, puis place en file d'attente les informations avant que le modèle d'actif ne soit mis à jour. Lorsqu'un utilisateur tente d'ajouter ou de modifier un actif, les données sont stockées en stockage temporaire et ajoutées à la fin de la file d'attente des modifications. Si la file d'attente de modifications est importante, la modification des actifs peut dépasser le délai imparti et le stockage temporaire est alors supprimé.

Intervention de l'utilisateur

Sélectionnez l'une des options suivantes :

- Ajoutez ou éditez l'actif à nouveau.
- Ajustez ou échelonnez l'heure de début de vos analyses de vulnérabilités ou réduisez la taille de vos analyses.

Saturation du disque de file d'attente de persistance d'actifs

38750113 - Saturation du disque de file d'attente de persistance d'actifs.

Explication

Le système a détecté que l'espace disque de débordement affecté à la file d'attente de persistance d'actifs est saturé. Les mises à jour de persistance d'actifs sont bloquées jusqu'à ce qu'un espace disque suffisant soit disponible. Les informations ne sont pas supprimées.

Intervention de l'utilisateur

Réduisez la taille de votre analyse. La réduction de la taille de votre analyse peut éviter le débordement de vos files d'attente de persistance d'actifs.

Saturation du disque de la file d'attente de résolution de mise à jour d'actifs

38750115 - Saturation du disque de la file d'attente de résolution de mise à jour d'actif.

Explication

Le système a détecté que l'espace disque de débordement affecté à la file d'attente de résolution s'actif est saturé.

Le système écrit en continu les données sur le disque pour éviter toute perte de données. Toutefois, si le système est à court d'espace disque, il supprime des données d'analyse. Le système ne peut pas traiter les données d'analyse d'actif entrantes tant qu'un espace disque suffisant n'est pas disponible.

Intervention de l'utilisateur

Vérifiez les options suivantes :

- Vérifiez que votre système dispose d'un espace disque disponible suffisant. La notification peut accompagner des notifications de la sentinelle SAR pour vous aviser de problèmes potentiels d'espace disque.
- Réduisez la taille de vos analyses.
- Diminuez la fréquence d'analyse.

Disque saturé pour la file d'attente de modification d'actifs

38750117 - File d'attente du programme d'écoute de modification d'actifs saturé.

Explication

Le gestionnaire de profil d'actif inclut un processus, à savoir un programme d'écoute des modifications, qui calcule des statistiques pour mettre à jour le score CVSS d'un actif. Le système consigne les données sur disque pour éviter la perte de données de statistiques d'actif en attente. Cependant, si l'espace disque est saturé, le système supprime les données d'analyse.

Le système ne peut pas traiter les données d'analyse d'actif entrantes tant qu'un espace disque suffisant n'est pas disponible.

Intervention de l'utilisateur

Sélectionnez l'une des options suivantes :

- Vérifiez que votre système dispose d'un espace disque disponible suffisant.
- Réduisez la taille de vos analyses.
- Diminuez la fréquence d'analyse.

Détection d'une règle personnalisée onéreuse

38750120 - Des règles personnalisées onéreuses ont été identifiées dans le moteur de règles personnalisées. Une dégradation des performances a été constatée dans le pipeline d'événements. Des règles personnalisées onéreuses ont été identifiées dans le moteur de règles personnalisées.

Explication

Le moteur de règles personnalisées (CRE) est un processus qui vérifie si un événement correspond à un ensemble de règles, puis déclenche des alertes, des infractions ou des notifications.

Un utilisateur peut créer une règle personnalisée dont la portée est étendue, qui utilise un canevas d'expression régulière qui n'est pas efficace, qui inclut des tests **Le contenu contient** ou associe la règle à des expressions régulières. Lorsque cette règle personnalisée est utilisée, elle a un impact négatif sur les performances, ce qui peut causer des erreurs lors de l'acheminement direct des événements vers l'espace de stockage. Les événements sont indexés et normalisés mais ils ne déclenchent pas d'alertes ou d'infractions.

Lorsque plusieurs tests de règles onéreuses ou inefficaces sont utilisés, le débit d'événement maximum peut être réduit, ce qui entraîne un retard des événements passant par le moteur de règles. es événements peuvent être acheminés directement vers le stockage et cet avertissement s'affiche.

Intervention de l'utilisateur

Effectuez les vérifications suivantes :

- Vérifiez le contenu de la notification afin de déterminer la règle onéreuse du pipeline qui a une incidence sur les performances.

  Par exemple, le contenu suivant signale le test : Règle "Vérification de contenu" dans le pipeline et débit EPS signalé de 787 événements par seconde, ce qui peut réduire le débit maximum du moteur de règles.

  ```
  Feb 23 15:56:58 ::ffff:10.1.2.4 [ecs-ep]
  [Timer-27]com.q1labs.semsources.cre.CRE:
  [WARN] [NOT:0040004101][10.1.2.4/-  -]
  [-/--]Expensive Custom Rules Based On Average Throughput in the last 60 seconds:
  Test: Payload Verification=787.98045190917eps,
  Monitoring: Suspect IPs seen with successful logins=899.02679830748eps
  ```

- Dans l'onglet **Infractions**, cliquez sur **Règles** et utilisez la fenêtre de recherche pour identifier et modifier ou désactiver la règle onéreuse. Si vous éditez la règle, vous pouvez réduire la quantité de donnés qui passe par le règle, en appliquant un filtre de source de journal ou de plage d'adresses IP. Les tests onéreux, comme "Le contenu contient", peuvent aussi être réduits ou retirés, s'ils ne sont pas nécessaires. Les tests de l'ensemble de références doivent être passés en revue afin de vérifier qu'ils n'interrogent pas un grand ensemble de référence.
- Utilisez SSH pour vous connecter au processeur d'événements et vérifiez que les unités d'exécution d'analyseur syntaxique s'exécutent pendant plus de 1500 millisecondes pour les charges EPS à l'aide de la commande suivante :

  ```
  /opt/qradar/support/threadTop.ssh –p 7799
  ```

  Recherchez la pile d'unité d'exécution Java pour `regex.Pattern.Curly`, `referenceSet`, `assets`, `host profile` et `port profile` à l'aide de la commande suivante :

  ```
  /opt/qradar/support/threadTop.sh -p 7799 -s -e ".*CRE Processor.*"
  ```

  – Si la sortie contient `regex.Pattern.Curly`, cela indique peut-être des problèmes au niveau des tests **Le contenu contient**.
  – Si la sortie contient `referenceSet`, des problèmes peuvent survenir pour des tests avec de grands ensembles de références.
  – Si la sortie contient `assets`, `host profile` et `port profile`, des problèmes peuvent survenir au niveau des tests **Hôte avec port ouvert** ou des tests d'actif.

Les règles ne sont peut-être pas à l'origine du problème

Cette notification peut se déclencher lorsque des événements sont routés vers l'espace de stockage du moteur de règles. Lorsque vous examinez cette remarque, si le taux "EPS" dans la notification est supérieur à ~20 000 EPS, cela peut indiquer que le problème est ailleurs. Une règle qui peut traiter des événements au-delà de 20 000 EPS est correctement optimisée. La situation qui a déclenché les 'événements routés vers l'espace de stockage' n'est peut-être pas une règle, il doit s'agir d'autre chose. Les autres éléments à considérer sont présentés ci-dessous.

- Le système est-il soumis à une plus forte charge pour d'autres raisons, par exemple une recherche de données de longue durée ?
- Le niveau d'utilisation des disque est-il égal ou supérieur à 85% "on/store", et une compression de données peut-elle éventuellement avoir une incidence sur les performances de stockage ?
- Si la haute disponibilité est utilisée, et que les débits d'événements sont supérieurs à 10 000 EPS, assurez-vous qu'il y a suffisamment de bande passante entre les deux noeuds à haute disponibilité. Par exemple, une simple connexion à 1Gbit/s, même dans un croisement dédié, peut limiter les performances de stockage.
- Existe-t-il une partition "/transient/" distincte ? Si ce n'est pas le cas, il est possible que la décompression de données temporaires utilise également des ressources de stockage et contribue à des demandes de stockage élevées.

L'accumulation est désactivée pour le moteur de détection des anomalies

38750121 - L'accumulation est désactivée pour le moteur de détection des anomalie.

Explication

La vue de données agrégées est désactivée ou indisponible ou une nouvelle règle requiert des données qui sont indisponibles.

Une accumulation abandonnée n'indique pas que des données d'anomalie ont été perdues. Les données d'anomalie d'origine sont conservées vu que les accumulations sont des ensembles de données générés à partir des données stockées. La notification fournit plus de détails sur la fréquence d'accumulation abandonnée.

Le moteur de détection d'anomalies ne peut pas examiner cette fréquence des données d'anomalie pour l'accumulation.

Intervention de l'utilisateur

Mettez à jour les règles de détection d'anomalies afin d'utiliser un plus petit ensemble de données.

Si la notification correspond à une erreur de sentinelle SAR récurrente, les performances du système peuvent être à l'origine du problème.

Le processus dépasse le délai d'exécution imparti

38750122 - L'exécution du processus prend trop de temps. Sa durée maximale par défaut est de 3600 secondes.

Explication

La limite par défaut d'une heure pour l'achèvement d'un processus donné est dépassée.

Intervention de l'utilisateur

Examinez le processus en cours d'exécution pour déterminer si la tâche correspond à un processus pouvant se poursuivre ou si elle doit être arrêtée.

Licence expirée

38750123 - Une licence allouée a expiré et n'est plus valide.

Explication

Lorsqu'une licence expire sur la console, une nouvelle licence doit être appliquée. Lorsqu'une licence arrive à expiration sur un hôte géré, le dispositif continue de traiter les événements et les flux jusqu'au niveau alloué par le pool de licences partagé.

Lorsque la licence participe à la capacité EPS et FPM du pool de licences partagé, son expiration peut entraîner un déficit pour le pool, qui n'a plus la capacité suffisante pour répondre aux besoins du déploiement. Dans une telle situation, les fonctionnalités des onglets **Activité réseau** et **Activité du journal** sont bloquées.

Intervention de l'utilisateur

1. Identifiez le dispositif dont la licence est arrivée à expiration.
   a. Sur l'onglet **Admin**, cliquez sur **Gestion du système et de la licence**.
   b. Dans la zone **Afficher**, sélectionnez **Licences**.
      Les licences arrivées à expiration figurent à la section **Messages d'information sur la licence**.
2. Si la licence expirée est sur la console, remplacez-la.
3. Si elle est sur un hôte géré, vérifiez que le pool de licences partagé dispose d'une capacité EPS et FPM suffisante.
   a. En cas de surallocation du pool de licences partagé, remplacez la licence expirée par une nouvelle licence dont la capacité EPS et FPM est à même de répondre aux besoins du système.
   b. Si la capacité du pool de licences est suffisante, supprimez la licence expirée. Dans la table **Licence**, sélectionnez la ligne de la licence expirée (sous la ligne récapitulative de l'hôte géré), puis sélectionnez **Actions** > **Supprimer la licence**.

Analyse externe d'adresse IP ou de plage non autorisée

38750126 - L'exécution d'une analyse externe a tenté d'analyser une adresse IP ou une plage d'adresses non autorisée.

Explication

Lorsqu'un profil d'analyse inclut une plage CIDR ou une adresse IP hors de la liste d'actifs définie, l'analyse se poursuit. Cependant, les plages CIDR ou les adresses IP d'actifs non visibles depuis votre liste de scanners externes sont ignorées.

Intervention de l'utilisateur

Mettez à jour la liste de plages CIDR ou d'adresses IP autorisées pour les actifs analysés par votre scanner externe. Examinez vos profils d'analyse pour vérifier que l'analyse est configurée pour les actifs inclus dans la liste réseau externe.

Echec de la synchronisation d'horloge

38750129 - La synchronisation d'horloge avec le système principal ou la console a échoué.

Explication

L'hôte géré ne peut pas se synchroniser avec la console ou le dispositif de haute disponibilité de secours ne peut pas se synchroniser avec le dispositif principal.

Les administrateurs doivent autoriser la communication **ntpdate** sur le port 123. Lorsque l'horloge est désynchronisée, il se peut que les données ne soient pas signalées correctement à la console. Plus longtemps les systèmes ne sont pas synchronisés et plus grand est le risque qu'une recherche de données, de rapport ou d'infraction renvoie un résultat erroné. La synchronisation d'horloge est cruciale pour

l'aboutissement des demandes auprès des hôtes gérés et des unités.

Intervention de l'utilisateur

Contactez le service clients.

Chaîne de dépendance cyclique de règle personnalisée détectée

38750131 - Une chaîne de dépendance cyclique de règles personnalisées a été détectée.

Explication

Une règle unique se réfère à elle-même directement ou via une série d'autres règles ou de blocs de construction. L'erreur se produit lorsque vous déployez une configuration complète. L'ensemble de règles n'est pas chargé.

Intervention de l'utilisateur

Modifiez les règles ayant créé la dépendance cyclique. La chaîne de règle peut être interrompue afin d'éviter une notification système récurrente. Une fois la chaîne de règles corrigée, un enregistrement recharge automatiquement les règles et résout le problème.

Notification de liste noire

38750136 - Les règles d'exclusion de rapprochement des actifs ont ajouté de nouvelles données d'actif aux listes noires d'actif.

Explication

Une donnée d'actif, comme une adresse IP, un nom d'hôte, ou une adresse MAC, montre un comportement qui est compatible avec les écarts de croissance d'actifs.

Une *liste noire d'actifs* est une collecte de données d'actifs qui est considérée comme peu fiable par les règles de moteur personnalisées d'exclusion de rapprochement d'actifs. Les règles surveillent la cohérence et l'intégrité des données d'actifs. Si une donnée d'actif présente un comportement suspect au moins deux fois dans les 2 heures, cette donnée est ajoutée aux listes noires d'actifs. Les mises à jour ultérieures qui contiennent les données d'actifs en liste noire ne sont pas appliquées à la base de données d'actifs.

Intervention de l'utilisateur

- Dans la description de notification, cliquez sur **Règles d'exclusion de rapprochement d'actifs** pour afficher les règles qui sont utilisées pour surveiller les données d'actifs.
- Dans la description de notification, cliquez sur **Ecarts d'actifs par source de journal** pour afficher les rapports d'écarts d'actifs qui se sont produits dans les dernières 24 heures.
- Si vos listes noires se remplissent de façon trop rapide, vous pouvez affiner les règles d'exclusion de rapprochement d'actifs qui les remplissent.
- Si vous voulez que les données d'actifs soient ajoutées à la base de données d'actifs, supprimez les données d'actifs de la liste noire et ajoutez-les à la liste blanche d'actifs correspondante. L'ajout de données d'actifs à la liste blanche les empêche de réapparaître par inadvertance sur la liste noire.
- Consultez Mises à jour des données d'actifs (http://www.ibm.com/support/knowledgecenter/SS42VS_7.3.1/com.ibm.qradar.doc/c_qradar_ug_asset_reconciliation.html).

Écarts de croissance d'actifs détectés

38750137 - Le système a détecté des profils d'actifs qui dépassent le seuil de taille normale.

Explication

Le système a détecté un ou plusieurs profils d'actifs dans la base de données d'actifs qui montrent un écart ou une croissance anormale. L'écart de croissance se produit lorsqu'un seul actif accumule plusieurs adresses IP, noms d'hôte DNS, noms NetBIOS, ou adresses MAC que les seuils du système permettent. Lorsque des écarts de croissance sont détectés, le système suspend toutes les mises à jour ultérieures entrantes de ces profils d'actifs.

Intervention de l'utilisateur

Déterminer la cause des écarts de croissance d'actifs :

- Passez votre souris sur la description de notification pour examiner le contenu de la notification. Le contenu affiche une liste des cinq principaux actifs le plus fréquemment soumis aux écarts. Il fournit également des informations sur la raison pour laquelle le système a marqué chaque actif comme un écart de croissance et le nombre de fois que l'actif a tenté de dépasser le seuil de taille d'actif.
- Dans la description de notification, cliquez sur **Consulter un rapport sur ces actifs** pour voir un rapport complet des écarts de croissance d'actifs au cours des dernières 24 heures.
- Consultez Mises à jour des données d'actifs (http://www.ibm.com/support/knowledgecenter/SS42VS_7.3.1/com.ibm.qradar.doc/c_qradar_ug_asset_reconciliation.html).

Détection de propriétés personnalisées coûteuses

38750138 - Une dégradation des performances a été détectée dans le pipeline d'événements. Des règles personnalisées coûteuses ont été détectées.

Explication

Lors du traitement normal, les propriétés d'événement personnalisées et les propriétés de flux personnalisées, marquées comme optimisées sont extraites dans le pipeline. Les valeurs sont utilisées dans Custom Rules Engine (CRE) et dans les index de recherche.

Les instructions à base d'expression régulière, qui sont des expressions régulières mal formées, peuvent causer des erreurs lors de l'acheminement direct des événements vers l'espace de stockage.

Intervention de l'utilisateur

Sélectionnez l'une des options suivantes :

- Désactivez une propriété personnalisée qui a été récemment installée.
- Vérifiez le contenu de la notification. Si possible, clarifiez au maximum les instructions d'expression régulière associées à la propriété personnalisée.

  Par exemple, le contenu suivant indique le modèle d'expression régulière :

  ```
  Feb 23 11:44:43 ::ffff:10.1.12.12 [ecs-ec]
  [Timer-60] com.q1labs.semsources.filters.normalize.DSMFilter:
  [WARN] [NOT:0080004105][10.130.126.12/- -]
  [-/- -]Expensive Custom  Properties Based On Average
  Throughput in the last 60 seconds (most to  least expensive)
  - (\w+) /\S+=1136.0eps
  ```
- Modifiez la définition de la propriété personnalisée afin de réduire la portée des catégories que la propriété tente de mettre en corrélation.
- Spécifiez un nom d'événement unique dans la définition de la propriété personnalisée afin d'éviter des tentatives d'analyse d'événement superflues.
- Ordonnez les analyseurs syntaxiques de source de journal, en commençant par les événements les plus envoyés, puis désactivez les analyseurs syntaxiques inutilisés.

Problème de configuration de contrôleur Raid

38750140 - Problème de configuration de contrôleur Raid : Le moniteur de matériel a déterminé qu'une unité virtuelle est configurée de manière incorrecte.

Explication

Pour des performances maximum, il est nécessaire de configurer le cache et l'unité BBU des contrôleurs RAID pour l'utilisation de règles de cache d'écriture différée. Lorsque des règles de cache d'écriture différée sont utilisées, les performances de stockage se dégradent et peuvent causer une instabilité du système.

Intervention de l'utilisateur

Vérifiez l'état de l'unité de batterie de secours. Si l'unité de batterie de secours fonctionne correctement, modifiez la règle de cache en différé.

Une erreur s'est produite lors de la collecte des fichiers journaux

38750141 - Erreurs rencontrées lors de la collecte des journaux de prendre en charge requis. Voir System and License Manager.

Explication

Des erreurs ont été détectées lors de la collecte des fichiers journaux. La collecte des fichiers journaux a échoué.

Intervention de l'utilisateur

Pour afficher des informations concernant la cause de cet échec, procédez comme suit :

1. Cliquez sur **System and License Manager** dans le message de notification.
2. Développez **Messages d'activité de support du système**.
3. Affichez les informations supplémentaires sur la raison de l'échec de la collecte de fichiers journaux.

Extensions DSM coûteuses détectées

38750143 - Une dégradation des performances a été détectée dans le pipeline d'événements. Extensions DSM coûteuses détectées.

Explication

Une extension de source de journal est un fichier XML qui inclut toutes les structures d'expressions régulières requises pour identifier et classer les événements à partir de leur contenu. Les extensions de source de journal pourraient être appelées *extensions de périphériques* dans les journaux d'erreurs et certaines notifications système.

Pendant le traitement normal, les extensions de source de journal sont exécutées dans le pipeline d'événements. Les valeurs sont immédiatement disponibles pour le moteur de règles personnalisé (CRE) et sont stockées sur le disque.

Des expressions régulières mal formées (regex) peuvent provoquer l'acheminement direct des événements vers le stockage.

Intervention de l'utilisateur

Sélectionnez l'une des options suivantes :

- Désactivez une extension DSM qui a été récemment installée.
- Vérifiez le contenu de la notification afin de déterminer l'extension DSM onéreuse du pipeline qui a une incidence sur les performances. Si possible, améliorez les instructions regex associées à l'extension de périphérique.

  Par exemple, le contenu suivant indique que le pipeline est bloqué par le gestionnaire de service de données (DSM) de point de contrôle :

  ```
  Oct 23 12:32:53 ::ffff:10.1.2.4 [ecs-ec]
  [Timer-57] com.q1labs.semsources.filters.normalize.DSMFilter: [WARN]
  [NOT:0080014100][10.1.2.4/- -][-/- -]Expensive Log Source or Log Source
  Extensions Based On Average Throughput in the last 60 seconds
  (most to least expensive) - Checkpoint=0.0eps, CatOS=86.0eps, Apache=2500.0eps,
  Endpointprotection=2905.0eps
  ```

- Assurez-vous que l'extension de source de journal est appliquée uniquement aux sources de journal correctes.

  Dans l'onglet **Admin**, cliquez sur **Configuration du système** > **Sources de données** > **Sources journal**. Sélectionnez chaque source de journal et cliquez sur **Editer** pour vérifier les détails de la source du journal.
- Si vous travaillez avec des sources de journal basées sur un protocole, réduisez le régulateur d'événements pour garantir que les événements ne sont pas en mémoire tampon sur le disque. Les paramètres de régulateur d'événements font partie de la configuration du protocole pour la source de journal.
- Ordonnez les analyseurs syntaxiques de source de journal, en commençant par les événements les plus envoyés, puis désactivez les analyseurs syntaxiques inutilisés.
- Vérifiez que votre console est installée avec les dernières versions du gestionnaire de service de données.
- Si des sources de journal sont créées pour des unités qui ne font pas partie de votre environnement, retirez ces sources de journal à l'aide de la commande suivante :

  ```
  /opt/qradar/bin/tatoggle.pl
  ```

  Si vous avez plusieurs processeurs d'événement, copiez le fichier `/opt/qradar/conf/TrafficAnalysisConfig.xml` dans le répertoire `/store/configservices/staging/globalconfig/`. Sous l'onglet **Admin**, cliquez sur **Déployer la configuration entière** pour tous les hôtes gérés afin d'obtenir le fichier de configuration.

Notifications d'informations pour les dispositifs QRadar

IBM Security QRadar fournit des messages d'information sur l'état ou le résultat d'un processus ou d'une action

Le téléchargement des mises à jour automatiques a abouti

38750068 - `Le téléchargement des mises à jour automatiques a abouti. Consultez le journal des mises à jour automatiques pour plus d'informations.`

Explication

Des mises à jour automatiques ont été téléchargées.

Intervention de l'utilisateur

Cliquez sur le lien dans la notification pour déterminer si des mises à jour téléchargées requièrent une installation.

Réussite de la mise à jour automatique

38750070 - Mises à jour automatiques terminées.

Explication

Le téléchargement et l'installation des mises à jour logicielles automatiques a abouti.

Intervention de l'utilisateur

Aucune action n'est requise.

Sentinelle SAR : restauration des opérations

38750072 - Sentinelle SAR : opération normale restaurée.

Explication

L'utilitaire SAR (System Activity Reporter) a détecté que votre charge système est revenue à des niveaux acceptables.

Intervention de l'utilisateur

Aucune action n'est requise.

Retour à la normale de l'utilisation du disque

38750077 - Sentinelle disque : Retour à un niveau normal de l'utilisation du disque.

Explication

La sentinelle disque a détecté que l'utilisation de la capacité globale du disque est en-dessous de 90 %.

Intervention de l'utilisateur

Aucune action n'est requise.

Un composant d'infrastructure a été réparé

38750084 - Un composant d'infrastructure endommagé a été réparé.

Explication

Un composant endommagé qui est chargé des services hébergés sur un hôte géré a été réparé.

Intervention de l'utilisateur

Aucune action n'est requise.

Stockage sur disque disponible

38750093 - Une ou plusieurs partitions de stockage auparavant inaccessibles sont désormais accessibles.

Explication

La sentinelle disque a détecté que la partition de stockage est disponible après l'apparition de la notification de «Stockage sur disque indisponible», à la page 19. L'indisponibilité de disque a été résolue.

Intervention de l'utilisateur

Aucune action n'est requise.

Concepts associés:

«Stockage sur disque indisponible», à la page 19

38750092 - La sentinelle de disque a détecté qu'une ou plusieurs partitions de stockage ne sont pas accessibles.

Licence proche de son expiration

38750124 - Une licence est proche de sa date d'expiration. Elle devra bientôt être remplacée.

Explication

Le système a détecté que la licence pour un dispositif arrivera à expiration d'ici 35 jours.

Intervention de l'utilisateur

Aucune action n'est requise.

Les fichiers journaux ont été collectés avec succès

38750142 - Les journaux de prise en charge nécessaires ont été collectés avec succès. Voir System and License Manager.

Explication

Les fichiers journaux ont été collectés avec succès.

Intervention de l'utilisateur

Pour téléchargement la collecte de fichiers journaux, procédez comme suit :

1. Cliquez sur **System and License Manager** dans le message de notification.
2. Développez **Messages d'activité de support du système**.
3. Cliquez sur **cliquez ici pour télécharger le fichier**.

Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM. Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations
IBM Canada Ltd.
3600 Steeles Avenue East
Markham, Ontario
L3R 9Z7
Canada

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues par écrit à l'adresse suivante :

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

LE PRESENT DOCUMENT EST LIVRE "EN L'ETAT" SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFACON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE. Certaines juridictions n'autorisent pas l'exclusion des garanties tacites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut, à tout moment et sans préavis, modifier les produits et logiciels décrits dans ce document.

Toute référence à ces informations sur des sites web non-IBM est fournie par souci de commodité uniquement et ne constitue en aucun cas une adhésion au contenu de ces sites web. Les documents sur ces sites web ne font pas partie des documents de ce produit IBM et l'utilisation de ces sites web se fait à vos propres risques.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
U.S.A.

Ces informations peuvent être soumises à des conditions particulières, prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux dispositions de l'ICA, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performance et les exemples client ne sont présentés qu'à des fins d'illustration. Les résultats des performances réelles peuvent varier en fonction des configurations et des conditions de fonctionnement spécifiques.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Les instructions relatives aux intentions d'IBM pour ses opérations à venir sont susceptibles d'être modifiées ou annulées sans préavis, et doivent être considérées uniquement comme un objectif.

Tous les tarifs indiqués sont les prix de vente actuels suggérés par IBM et sont susceptibles d'être modifiés sans préavis. Les tarifs appliqués peuvent varier selon les revendeurs.

Le présent document peut contenir des exemples de données et de rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Tous ces noms sont fictifs, et toute ressemblance avec des noms de personnes ou de sociétés réelles serait purement fortuite.

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corp. dans de nombreux pays. Les autres noms de produits et de service peuvent être des marques d'IBM ou d'autres sociétés. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web "Copyright and trademark information" à l'adresse www.ibm.com/legal/copytrade.shtml.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

Dispositions relatives à la documentation du produit

Les droits d'utilisation relatifs à ces publications sont soumis aux dispositions suivantes.

Applicabilité

Ces dispositions viennent s'ajouter à toute autre condition d'utilisation applicable au site web IBM.

Utilisation personnelle

Vous pouvez reproduire ces publications pour votre usage personnel, non commercial, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez pas distribuer ou publier tout ou partie de ces publications ou en produire des oeuvres dérivées sans le consentement exprès d'IBM.

Utilisation commerciale

Vous pouvez reproduire, distribuer et afficher ces publications uniquement au sein de votre entreprise, sous réserve que toutes les mentions de propriété soient conservées. Vous ne pouvez pas reproduire, distribuer ou afficher tout ou partie de ces publications en dehors de votre entreprise ou en tirer des oeuvres dérivées, sans le consentement exprès d'IBM.

Droits

Exception faite des droits d'utilisation expressément accordés dans ce document, aucun autre droit, licence ou autorisation, tacite ou explicite, n'est accordé pour ces publications ou autres informations, données, logiciels ou droits de propriété intellectuelle contenus dans ces publications.

IBM se réserve le droit de retirer les autorisations accordées ici si, à sa discrétion, l'utilisation des publications s'avère préjudiciable à ses intérêts ou que, selon son appréciation, les instructions susmentionnées n'ont pas été respectées.

Vous ne pouvez télécharger, exporter ou réexporter ces informations qu'en total accord avec toutes les lois et règlements applicables dans votre pays, y compris les lois et règlements américains relatifs à l'exportation.

IBM N'OCTROIE AUCUNE GARANTIE SUR LE CONTENU DE CES PUBLICATIONS. LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU TACITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES PUBLICATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Déclaration IBM de confidentialité en ligne

Les Logiciels IBM, y compris les Logiciels sous forme de services ("Offres Logiciels"), peuvent utiliser des cookies ou d'autres technologies pour collecter des informations sur l'utilisation des produits, améliorer l'acquis utilisateur, personnaliser les interactions avec celui-ci, ou dans d'autres buts. Bien souvent, aucune information personnelle identifiable n'est collectée par les Offres Logiciels. Certaines Offres Logiciels vous permettent cependant de le faire. Si la présente Offre Logiciels utilise des cookies pour collecter des informations personnelles identifiables, des informations spécifiques sur cette utilisation sont fournies ci-dessous.

Selon la configuration déployée, la présente Offre Logiciels peut utiliser des cookies de session et des cookies persistants destinés à collecter le nom et le mot de passe des utilisateurs pour les fonctions de gestion des session et d'authentification. Ces cookies peuvent être désactivés, mais leur désactivation empêchera l'utilisation de la fonctionnalité qui leur est associée.

Si les configurations déployées de cette Offre Logiciels vous permettent, en tant que client, de collecter des informations permettant d'identifier les utilisateurs par l'intermédiaire de cookies ou par d'autres techniques, vous devez solliciter un avis juridique sur la réglementation applicable à ce type de collecte, notamment en termes d'information et de consentement.

Pour plus d'informations sur l'utilisation à ces fins des différentes technologies, y compris celle des cookies, consultez les Points principaux de la Déclaration IBM de confidentialité sur Internet (http://www.ibm.com/privacy/fr/fr) et la section "Cookies, pixels espions et autres technologies" de la Déclaration IBM de confidentialité sur Internet sur le site http://www.ibm.com/privacy/details/fr/fr, ainsi que la section "IBM Software Products and Software-as-a-Service Privacy Statement" sur le site http://www.ibm.com/software/info/product-privacy (en anglais).

Index