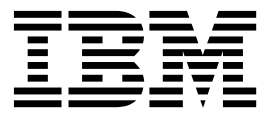


IBM Security QRadar
Version 7.3.0

Guide de mise à niveau



Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations figurant à la section «Remarques», à la page 21.

Ce document s'applique à IBM QRadar Security Intelligence Platform version 7.3.0 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*

© Copyright IBM France 2017. Tous droits réservés.

© **Copyright IBM Corporation 2012, 2017.**

Table des matières

Avis aux lecteurs canadiens	v
Introduction à la mise à niveau des logiciels QRadar.	vii
Chapitre 1. Nouveautés concernant la mise à niveau vers QRadar version 7.3.0.	1
Chapitre 2. Préparation de la mise à niveau	3
Mise à jour du microprogramme.	3
Configuration logicielle requise pour les mises à niveau	3
Mémoire et espace disque requis	3
Sauvegarde de données tierces	5
Ordre des mises à niveau dans les déploiements distribués	6
Mise à niveau des déploiements haute disponibilité	6
Précautions lors de la mise à niveau des dispositifs	6
Chapitre 3. Mise à niveau des dispositifs QRadar	9
Effacement du cache du navigateur Web après les mises à niveau	11
Chapitre 4. Mise à niveau des installations logicielles QRadar	13
Copie des fichiers nécessaires	13
Exigences et recommandations liées aux partitions	14
Installation de RHEL version 7.3 et configuration des partitions	16
Installation de QRadar.	18
Remarques	21
Marques	23
Dispositions relatives à la documentation du produit	23
Déclaration IBM de confidentialité en ligne.	24

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.

Introduction à la mise à niveau des logiciels QRadar

Les informations sur la mise à niveau d'IBM® Security QRadar s'appliquent aux produits IBM Security QRadar SIEM et IBM QRadar Log Manager.

Utilisateurs concernés

Les administrateurs système chargés de la mise à niveau des systèmes IBM Security QRadar doivent être familiarisés avec les concepts de sécurité réseau et les configurations des unités.

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).

Contactez 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'IMMUNITÉ DES SYSTÈMES, PRODUITS OU SERVICES NI L'IMMUNITÉ DE VOTRE ENTREPRISE CONTRE LE COMPORTEMENT MALVEILLANT OU ILLÉGAL 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.

Chapitre 1. Nouveautés concernant la mise à niveau vers QRadar version 7.3.0

IBM Security QRadar version 7.3.0 introduit un pool de licences partagé pour la gestion de la capacité EPS et du FPM, et utilise désormais Red Hat Enterprise Linux (RHEL) 7.3.

Pool de licences partagé

Vous pouvez ajuster votre système en fonction des modifications en répartissant la capacité d'événements par seconde (EPS) et le flux par minute (FPM) sur n'importe quel hôte du déploiement, quel que soit le dispositif auquel la licence a été accordée.

Vous disposez par exemple d'un déploiement distribué de QRadar version 7.2.8 comportant deux processeurs d'événements, l'un avec 7 500 EPS et l'autre avec 15 000 EPS. Lors d'une mise à niveau vers QRadar version 7.3.0, chaque processeur conserve les allocations EPS antérieures à la mise à niveau, mais l'ensemble des 22 500 EPS deviennent membres du pool de licences partagé. En cas de variation des volumes de données des processeurs d'événement ou lorsque vous ajoutez un hôte géré, vous pouvez répartir la capacité d'EPS.

Pour plus d'informations sur la gestion du pool de licences partagé, consultez le chapitre relatif à la gestion des licences dans *IBM Security QRadar Administration Guide*.

Avantages de RHEL 7.3

RHEL 7.3 rend QRadar plus sécurisé. RHEL 7.3 prend également en charge la gestion de volume logique, qui offre une fonctionnalité de partitionnement de disque avancée et flexible. Le gestionnaire de volume logique vous permet de créer des partitions, de les redimensionner et de regrouper de clusters de stockage.

Vous disposez, par exemple, d'un dispositif virtuel QRadar tout-en-un. Vous avez besoin de davantage d'espace disque local pour stocker les événements pendant plus longtemps. Vous pouvez étendre la partition `/store` en rajoutant un disque.

Chapitre 2. Préparation de la mise à niveau

Pour mettre à niveau correctement un système IBM Security QRadar, vérifiez votre mode de mise à niveau, en particulier si vous effectuez une mise à niveau à partir de versions anciennes nécessitant des étapes intermédiaires. Vous devez également consulter la configuration logicielle, matérielle et haute disponibilité requise.

Important : Lorsque vous mettez à niveau QRadar version 7.2.6 ou version ultérieure, les clés SSH sur chacun des hôtes gérés sont remplacées. Si vous vous connectez sur ou depuis un hôte géré QRadar et utilisez l'authentification par clé, veuillez ne pas retirer ni modifier les clés SSH. Le retrait ou la modification des clés peut interrompre la communication entre la console QRadar et les hôtes gérés, entraînant ainsi une perte de données.

Mise à jour du microprogramme

Mettez à jour le microprogramme sur les dispositifs IBM Security QRadar afin de pouvoir profiter des avantages des mises à jour et des fonctions supplémentaires pour les composants matériels internes.

Pour plus d'informations sur la mise à jour du microprogramme, voir Firmware update for QRadar (<http://www-01.ibm.com/support/docview.wss?uid=swg27047121>).

Configuration logicielle requise pour les mises à niveau

Pour vous assurer qu'IBM Security QRadar est mis à niveau sans erreurs, veillez à n'utiliser que les versions du logiciel QRadar prises en charge :

- Assurez-vous que QRadar version 7.2.8 (20161118202122 et versions ultérieures) est installé. Pour en savoir plus sur les versions de QRadar, consultez la page QRadar Master Software List.
- Vérifiez la version du logiciel dans le logiciel en sélectionnant **Aide > A propos**.

Important : Lors d'un déploiement, tous les dispositifs IBM Security QRadar doivent posséder un niveau de version et de correctif identique. Les déploiements qui utilisent différentes versions du logiciel QRadar ne sont pas pris en charge.

Important : Dans le cas d'un déploiement WinCollect géré, vous devez utiliser WinCollect version 7.2.5 ou ultérieure. Si vous utilisez une version antérieure de WinCollect, vous devez effectuer une mise à niveau vers WinCollect version 7.2.5 avant de pouvoir appliquer la mise à niveau de QRadar version 7.3.0. Pour plus d'informations sur la mise à niveau des agents WinCollect, voir <http://www.ibm.com/support/docview.wss?uid=swg21999193>. Les informations de la page WinCollect V7.2.5 Release Notes pourront aussi vous être utiles.

Mémoire et espace disque requis

Avant la mise à niveau, assurez-vous qu'IBM Security QRadar répond aux exigences de mémoire et d'espace disque minimales ou recommandées.

Mémoire requise pour QRadar

Le tableau ci-dessous décrit la mémoire requise minimale et recommandée pour les dispositifs QRadar. La mémoire requise minimale définit la quantité de mémoire requise par les fonctions du logiciel. La mémoire requise recommandée inclut la quantité de mémoire requise par les fonctions actuelles du logiciel et la mémoire supplémentaire pour les éventuelles fonctions futures. Les dispositifs disposant d'une mémoire inférieure à la mémoire recommandée peuvent rencontrer des problèmes de performances lors des périodes chargées en événements et en trafic de flux.

Tableau 1. Mémoire requise minimale et facultative pour les dispositifs QRadar

Dispositif	Mémoire requise minimale	Mémoire requise recommandée
QFlow Collector 1201	6 Go	6 Go
QFlow Collector 1202	6 Go	6 Go
QFlow Collector Virtual 1299 sans QRadar Vulnerability Scanner	2 Go	2 Go
QFlow Collector Virtual 1299 avec QRadar Vulnerability Scanner	6 Go	6 Go
QFlow Collector 1301	6 Go	6 Go
QFlow Collector 1310	6 Go	6 Go
QRadarEvent Collector 1501	12 Go	16 Go
QRadar Event Collector Virtual 1599	12 Go	16 Go
QRadar Event Processor 1601	12 Go	48 Go
QRadar Event Processor 1605	12 Go	48 Go
QRadar Event Processor 1624	64 Go	64 Go
QRadar Event Processor 1628	128 Go	128 Go
QRadar Event Processor Virtual 1699	12 Go	48 Go
QRadar Flow Processor 1701	12 Go	48 Go
QRadar Flow Processor 1705	12 Go	48 Go
QRadar Flow Processor 1724	64 Go	64 Go
QRadar Flow Processor 1728	128 Go	128 Go
QRadar Flow Processor Virtual 1799	12 Go	48 Go
QRadar Event et Flow Processor 1805	12 Go	48 Go
QRadar Event et Flow Processor 1824	64 Go	64 Go
QRadar Event et Flow Processor 1828	128 Go	128 Go
QRadar SIEM 2100	24 Go	24 Go
QRadar SIEM 2100 Light	24 Go	24 Go
QRadar SIEM 3100	24 Go	48 Go
QRadar SIEM 3105	24 Go	48 Go
QRadar SIEM 3124	64 Go	64 Go

Tableau 1. Mémoire requise minimale et facultative pour les dispositifs QRadar (suite)

Dispositif	Mémoire requise minimale	Mémoire requise recommandée
QRadar SIEM 3128	128 Go	128 Go
QRadar SIEM Virtual 3199	24 Go	48 Go
QRadar xx48	128 Go	128 Go
QRadar Network Packet Capture	128 Go	128 Go
QRadar Network Insights	128 Go	128 Go
QRadar xx48	128 Go	128 Go
QRadar Log Manager 1605	12 Go	48 Go
QRadar Log Manager 1624	64 Go	64 Go
QRadar Log Manager 1628	128 Go	128 Go
QRadar Log Manager 2100	24 Go	24 Go
QRadar Log Manager 3105	24 Go	48 Go
QRadar Log Manager 3124	64 Go	64 Go
QRadar Log Manager 3128	128 Go	128 Go
QRadar Log Manager 3199	24 Go	48 Go

Autres exigences de mémoire

Si les conditions ci-dessous ne sont pas remplies, des exigences de mémoire supplémentaires peuvent être nécessaires :

- Si vous envisagez d'activer l'indexation des contenus, votre système nécessite au moins 24 Go de mémoire. Cependant, une mémoire de 48 Go est recommandée.
- Si vous installez le logiciel QRadar sur votre propre matériel, votre système nécessite au moins 24 Go de mémoire.

Espace disque requis

Avant d'effectuer la mise à niveau vers QRadar version 7.3.0, vérifiez que la taille totale du disque principal est d'au moins 130 gigaoctets (Go).

Le test préalable de mise à niveau détermine si une partition comporte suffisamment d'espace disponible pour effectuer une mise à niveau. Avant de pouvoir effectuer une mise à niveau, vous devez libérer suffisamment d'espace disque sur la partition définie dans le message d'erreur du test préalable.

Sauvegarde de données tierces

Avant de procéder à la mise à niveau, veillez à sauvegarder toutes les données tierces du système.

Toutes les données tierces du système sont supprimées lors de la mise à niveau du système d'exploitation, au cours de la mise à niveau de QRadar. Seules les données stockées dans la partition `/store` sont conservées. Il est conseillé de sauvegarder toutes les données avant d'effectuer la mise à niveau, telles que :

- les données et les comptes utilisateur tiers,
- les fichiers, scripts ou données situés dans `/root`.

Ordre des mises à niveau dans les déploiements distribués

Lorsque vous mettez à niveau des systèmes IBM Security QRadar, vous devez d'abord effectuer la procédure de mise à niveau de la console QRadar. Vous devez pouvoir accéder à l'interface utilisateur sur votre système de bureau avant de mettre à niveau la console QRadar secondaire et les hôtes gérés.

Mettez à niveau vos systèmes QRadar dans l'ordre suivant :

1. Console
2. Les systèmes QRadar suivants peuvent être mis à niveau simultanément :
 - Processeurs d'événement
 - QRadar Event Collectors
 - Processeurs de flux
 - Collecteurs QFlow

Mise à niveau des déploiements haute disponibilité

Avant de mettre à niveau IBM Security QRadar dans un déploiement haute disponibilité (HD), vérifiez que l'hôte principal est bien le système actif de votre déploiement. Vous devez mettre à niveau l'hôte principal avant de mettre à niveau manuellement l'hôte secondaire.

Avant de mettre à niveau l'hôte secondaire, copiez le fichier ci-dessous de l'hôte HA principal vers l'hôte HA secondaire pour que les interfaces de gestion des deux hôtes correspondent une fois la mise à niveau terminée :

```
scp /opt/qradar/conf/capabilities/map_localhost_interfaces.txt.bak  
root@<ip_secondaire>:/opt/qradar/ha/map_localhost_interfaces.txt
```

Si le cluster HD est déconnecté ou si vous souhaitez ajouter un nouvel hôte HD secondaire, vous devez réinstaller QRadar sur l'hôte HD secondaire. Pour plus d'informations sur la réinstallation du logiciel, consultez le *manuel d'installation* de votre système. Une fois que vous avez réinstallé l'hôte HD secondaire, connectez-vous à l'interface utilisateur pour vous reconnecter ou pour créer un autre cluster HD.

Avant de mettre à niveau un cluster HA déconnecté, copiez le fichier ci-dessous de l'hôte HA principal vers l'hôte HA secondaire pour que les interfaces de gestion des deux hôtes correspondent une fois la mise à niveau terminée :

```
scp /opt/qradar/conf/capabilities/map_localhost_interfaces.txt.bak  
root@<ip_secondaire>:/opt/qradar/ha/map_localhost_interfaces.txt
```

Important : La réplication du disque et la reprise sont désactivées tant que les hôtes principal et secondaire ne sont pas synchronisés et que le statut Mise à niveau nécessaire ou Echec n'a pas été effacé de l'hôte secondaire.

Après la mise à niveau de l'hôte secondaire, vous pouvez avoir besoin de restaurer la configuration de l'hôte secondaire. Pour plus d'informations sur la restauration d'un hôte en échec, consultez le *manuel d'administration* de votre produit.

Précautions lors de la mise à niveau des dispositifs

Prenez certaines précautions avant de mettre à niveau les dispositifs QRadar.

Veillez à prendre les précautions suivantes :

- Sauvegardez vos données et confirmez que les sauvegardes sont terminées avant de commencer la mise à niveau.
Pour plus d'informations sur la sauvegarde et la récupération, consultez le *manuel d'administration* de votre produit.
- Vérifiez qu'une console QRadar est connectée à votre matériel ou que vous disposez d'une connexion à distance vers le port de gestion (souvent appelée configuration de gestion hors bande). Cette vérification est importante car si vous rencontrez un problème lors de la réinstallation de RHEL, vous devrez avoir accès au serveur via l'une de ces connexions.
- Vérifiez que votre dispositif est mis à jour avec la version de microprogramme BIOS ou UEFI la plus récente.
- Mettez à niveau tous les hôtes gérés avant de déployer les modifications.
- Pour éviter des erreurs d'accès dans votre fichier journal, fermez toutes les sessions QRadar.
- Vérifiez que votre dispositif respecte la configuration minimale requise pour QRadar. Pour plus d'informations sur la configuration système requise, voir «Mémoire et espace disque requis», à la page 3.
- Déconnectez tous les hôtes haute disponibilité (HA) avant la mise à niveau si le répertoire `/store` entier est monté sur un stockage externe. Pour plus d'informations sur la déconnexion d'un cluster HA, consultez le manuel *IBM Security QRadar High Availability Guide*.
- Assurez-vous que l'ordre des points de montage dans le fichier `/etc/fstab` correspond aux hôtes HA principal et secondaire :
 - `/store`
 - `/store/tmp`
 - `/store/transient`
 - Sous-répertoires `/store` si la partition est montée sur un stockage externe
 Redémarrez le système après les mises à jour du fichier `/etc/fstab`.
- Si le répertoire `/store` entier est monté sur un stockage externe, exécutez la commande ci-dessous pour préparer le système pour la mise à niveau :
`/media/cdrom/post/prepare_offboard_storage_upgrade.sh`
- Si vous n'êtes pas invité à remonter la solution de stockage externe pendant la mise à niveau, remontez le stockage à la fin de la mise à niveau.
Pour connaître la procédure de mise à niveau supplémentaire pour les solutions de stockage externe iSCSI et Fibre Channel et pour plus d'informations sur le remontage du stockage externe, consultez le manuel *Offboard Storage Guide*.
- Avant de réaliser une mise à niveau vers QRadar version 7.3.0, vérifiez qu'aucune licence QRadar Incident Forensics n'est allouée à QRadar Console. La mise à niveau d'une instance de QRadar Console associée à une licence QRadar Incident Forensics peut générer la surallocation du pool de licences partagé et vous empêcher d'utiliser certaines fonctions des onglets Activité du journal et Activité réseau. Pour éviter ce problème, retirez la licence QRadar Incident Forensics et réinstallez-la après la mise à niveau. Pour plus d'informations sur la gestion des licences, voir le manuel *IBM Security QRadar Administration Guide*.

Chapitre 3. Mise à niveau des dispositifs QRadar

Vous devez mettre à niveau tous les produits IBM Security QRadar dans votre déploiement vers la même version. Lors de la mise à niveau, la version de Red Hat Enterprise Linux est mise à niveau vers la 7.3.

Pourquoi et quand exécuter cette tâche

Important : Avant de pouvoir effectuer une mise à niveau vers QRadar version 7.3.0, vous devez avoir installé le groupe de correctifs QRadar v7.2.8 -QRFULL-20161118202122 et versions ultérieures. Sélectionnez **Aide > A propos** pour afficher la version de QRadar. Téléchargez le correctif logiciel (<https://www-945.ibm.com/support/fixcentral/swg/selectFixes?product=ibm%2FOther+software%2FIBM+Security+QRadar+Risk+Manager&fixids=7.2.8-QRADAR-QRSIEM-20161118202122&source=dblusearch&function=fixId&parent=IBM%20Security>).

Commencez par mettre la console QRadar à niveau, puis mettez chaque hôte géré à niveau. Dans les déploiements haute disponibilité (HA), mettez d'abord à niveau l'hôte HA principal, puis l'hôte HA secondaire.

Important : La mise à niveau de la console QRadar vers la version 7.3.0 prend environ 2 heures. La mise à niveau des hôtes gérés prend environ 1 heure et demie. Si ces mises à niveau prennent davantage de temps, contactez le support pour vérifier leur progression.

Procédure

1. Si la version 7.2.8.1 ou une version supérieure de QRadar n'est pas installée, effectuez les opérations de mise à jour suivantes pour atteindre le niveau de correctif minimal du logiciel QRadar requis pour la mise à niveau vers QRadar version 7.3.0. Sinon, passez à l'étape 2.

Remarque : Avant d'appliquer un correctif à un hôte géré ou à un dispositif secondaire, vérifiez que le correctif a d'abord été appliqué à la console.

- a. Téléchargez le fichier `<QRadar_patchupdate>.sfs` à partir de Fix Central (www.ibm.com/support/fixcentral).
- b. Utilisez SSH pour vous connecter à votre système comme utilisateur root.
- c. Copiez le fichier correctif dans le répertoire `/tmp` ou à un autre emplacement comportant suffisamment d'espace disque.

Important : Ne copiez pas le fichier dans un répertoire système existant de QRadar, tel que `/store` ou `/root`.

- d. Pour créer le répertoire `/media/updates`, entrez la commande suivante :
`mkdir -p /media/updates`
- e. Modifiez-le pour utiliser le répertoire dans lequel vous avez copié le fichier correctif.
- f. Pour monter le fichier correctif dans le répertoire `/media/updates`, entrez la commande suivante :
`mount -o loop -t squashfs <QRadar_patchupdate>.sfs /media/updates/`
- g. Pour exécuter le programme d'installation des correctifs, entrez la commande suivante : `/media/updates/installer`

Conseil : La première fois que vous exécutez le script du programme d'installation des correctifs, il peut y avoir un délai avant que le menu du programme d'installation du premier correctif s'affiche.

- h. Répondez aux questions préalables en fonction de votre déploiement QRadar.
- i. A l'aide du programme d'installation des correctifs, appliquez le correctif logiciel à tous les systèmes de votre déploiement.

Le programme d'installation des correctifs répertorie les options suivantes.

- Console
- Tous

Si vous sélectionnez **Tous**, le correctif logiciel est appliqué d'abord à QRadar Console, puis à tous les hôtes gérés. Si vous sélectionnez **Console**, le correctif logiciel n'est appliqué qu'à QRadar Console. Une fois le correctif logiciel appliqué à QRadar Console, le menu répertorie les hôtes gérés restants et l'option **Tous**.

Si votre session SSH est déconnectée alors que l'application du correctif est en cours, l'application du correctif continue. Lorsque vous rouvrez votre session SSH et que vous réexécutez le programme d'installation, l'installation reprend.

- j. Une fois le correctif appliqué, démontez la mise à jour logicielle à l'aide de la commande suivante : `umount /media/updates`
 - k. Maintenant que vous avez installé le niveau de correctif minimal requis pour la version 7.2.8, suivez la procédure ci-dessous pour passer à QRadar version 7.3.0.
2. Pour effectuer la mise à niveau, téléchargez le fichier `<QRadar>.iso` à partir de Fix Central (www.ibm.com/support/fixcentral).
- a. Utilisez SSH pour vous connecter à votre système comme utilisateur root.
 - b. Copiez le fichier ISO dans le répertoire `/tmp` ou un autre emplacement disposant de suffisamment d'espace.

Important : Ne copiez pas le fichier dans un répertoire système QRadar existant, comme `/store` ou `/root`.

- c. Pour créer le répertoire `/media/cdrom`, exécutez la commande suivante :
`mkdir -p /media/cdrom`
- d. Modifiez le répertoire dans lequel vous avez copié le fichier ISO.
- e. Pour monter le fichier ISO dans le répertoire `/media/cdrom`, exécutez la commande suivante :
`mount -o loop <QRadar>.iso /media/cdrom/`
- f. Prétestez l'installation en exécutant la commande suivante :
`/media/cdrom/setup -t`
- g. Si le déploiement a échoué à l'un des prétests, vérifiez la sortie de prétest et exécutez l'une des actions suggérées.
- h. Pour exécuter le programme d'installation, exécutez la commande suivante :
`/media/cdrom/setup`

Important : La connexion SSH est interrompue pendant 20 minutes, car le système redémarre. Surveillez l'écran de la console pour vérifier le moment auquel SSH est disponible une fois que le système a redémarré.

- i. Si le déploiement inclut un stockage externe, consultez le manuel *IBM Security QRadar Offboard Storage Guide* pour connaître la procédure de reconnexion et de remontage des types de stockage externe.

Que faire ensuite

1. Effectuez une mise à jour automatique pour garantir que vos fichiers de configuration contiennent les informations de sécurité réseau les plus récentes. Pour plus d'informations, voir *IBM Security QRadar SIEM Administration Guide*.
2. Videz le cache du navigateur Web. Après la mise à niveau de QRadar, l'onglet **Vulnérabilités** risque de ne pas être affiché. Pour utiliser QRadar Vulnerability Manager après la mise à niveau, vous devez transférer et allouer une clé de licence valide. Pour plus d'informations, consultez le *manuel d'administration* de votre produit.

Effacement du cache du navigateur Web après les mises à niveau

Après la mise à niveau, effacez le cache du navigateur Web avant de vous connecter à IBM Security QRadar.

Procédure

1. Pour effacer le cache du navigateur Web, assurez-vous qu'une seule instance du navigateur Web est ouverte, puis effacez le cache.
2. Connectez-vous à QRadar en entrant l'adresse IP du système QRadar dans un navigateur Web :

`https://adresse IP`

Le nom d'utilisateur par défaut est admin.

Chapitre 4. Mise à niveau des installations logicielles QRadar

Effectuez une mise à niveau de la version 7.2.8 à la version 7.3.0 d'IBM Security QRadar sur votre propre dispositif avec une installation logicielle de QRadar. Une installation logicielle comprend des partitions Red Hat Enterprise Linux (RHEL) personnalisées déjà configurées.

Important : Avant de pouvoir effectuer une mise à niveau vers QRadar version 7.3.0, vous devez avoir installé le groupe de correctifs QRadar v7.2.8 -QRFULL-20161118202122 et versions ultérieures. Sélectionnez **Aide > A propos** pour afficher la version de QRadar. Téléchargez le correctif logiciel (<https://www-945.ibm.com/support/fixcentral/swg/selectFixes?product=ibm%2FOther+software%2FIBM+Security+QRadar+Risk+Manager&fixids=7.2.8-QRADAR-QRSIEM-20161118202122&source=dbluesearch&function=fixId&parent=IBM%20Security>).

Pour mettre QRadar à niveau avec les partitions RHEL personnalisées, vous devez effectuer les tâches suivantes :

1. Copiez les fichiers nécessaires sur votre dispositif et commencez la mise à niveau.
2. Installez RHEL 7.3 et configurez les partitions.
3. Suivez les instructions de l'assistant d'installation pour effectuer l'installation de QRadar.

Important : La mise à niveau de la console QRadar vers la version 7.3.0 prend environ 2 heures. La mise à niveau des hôtes gérés prend environ 1 heure et demie. Si ces mises à niveau prennent davantage de temps, contactez le support pour vérifier leur progression.

Copie des fichiers nécessaires

Copiez les fichiers sur l'hôte sur lequel vous souhaitez mettre à niveau IBM Security QRadar et commencez la procédure de configuration.

Avant de commencer

- Téléchargez le fichier ISO de l'édition QRadar à partir de Fix Central (<https://www-945.ibm.com/support/fixcentral>).
- Obtenez le fichier ISO de Red Hat Enterprise Linux 7.3.
- Vérifiez que votre dispositif respecte la configuration minimale requise pour QRadar. Pour plus d'informations sur la configuration système requise, voir «Mémoire et espace disque requis», à la page 3.
- Mettez à niveau tous les hôtes gérés avant de déployer les modifications.
- Déconnectez tous les hôtes haute disponibilité (HA) avant la mise à niveau si le répertoire `/store` entier est monté sur un stockage externe. Pour plus d'informations sur la déconnexion d'un cluster HA, consultez le manuel *IBM Security QRadar High Availability Guide*.
- Assurez-vous que l'ordre des points de montage dans le fichier `/etc/fstab` correspond aux hôtes HA principal et secondaire :
 - `/store`
 - `/store/tmp`
 - `/store/transient`

- Sous-répertoires /store si la partition est montée sur un stockage externe Redémarrez le système après les mises à jour du fichier /etc/fstab.
 - Si le répertoire /store entier est monté sur un stockage externe, exécutez la commande ci-dessous pour préparer le système pour la mise à niveau :
/media/cdrom/post/prepare_offboard_storage_upgrade.sh
 - Si vous n'êtes pas invité à remonter la solution de stockage externe pendant la mise à niveau, remontez le stockage à la fin de la mise à niveau.
- Pour connaître la procédure de mise à niveau supplémentaire pour les solutions de stockage externe iSCSI et Fibre Channel et pour plus d'informations sur le remontage du stockage externe, consultez le manuel *Offboard Storage Guide*.

Procédure

1. Copiez le fichier ISO du DVD du système d'exploitation Red Hat Enterprise Linux sur l'une des unités de stockage amovible :
 - DVD (Digital Versatile Disk)
 - Clé USB flash amorçable
2. A l'aide d'un programme SFTP (Secure File Transfer Protocol), comme WinSCP, copiez le fichier ISO de QRadar sur l'hôte sur lequel vous souhaitez installer QRadar.
3. Utilisez SSH pour vous connecter au système en tant qu'utilisateur root.
4. Créez le répertoire d'installation en exécutant la commande suivante :
mkdir -p /media/cdrom
5. Montez le fichier ISO de QRadar en exécutant la commande suivante :
mount -o loop <fichier_ISO_QRadar> /media/cdrom
6. Commencez à configurer QRadar en exécutant la commande suivante :
/media/cdrom/setup

Exigences et recommandations liées aux partitions

Lors du processus de mise à niveau, des exigences et des recommandations liées aux partitions sont générées. Si ces instructions ne fonctionnent pas, vous pouvez configurer la partition manuellement.

Les partitions suivantes doivent être conservées et ne doivent pas être reformatées :

Tableau 2. Exigences (conservez et ne reformatez pas ces partitions)

Partition	Description
/store	Stocke les fichiers de données.
/storetmp	Stocke les fichiers de configuration.
/transient	Stocke les recherches sauvegardées.

Tableau 3. Exigences (tailles de partition minimales pour la mise à niveau vers Red Hat version 7.3 & QRadar version 7.3.0)

Partition	Taille(Mio)	Type d'unité	Groupe de volumes	Type de système de fichiers
/boot	100 Mio Remarque : La taille conseillée est d'au moins 200 Mio. La taille idéale est de 1024 Mio.	Partition standard	N/A	XFS
/	5000 Mio (normalement 1000 Mio, mais /store requiert 4000 Mio.) Remarque : /store doit être démontée lors de l'installation de QRadar version 7.3.0 en vue de la mise à niveau, donc l'exigence revient à /.	Gestionnaire de volume logique	rootrhel	XFS
/opt	6000 Mio	Gestionnaire de volume logique	rootrhel	XFS
/var	500 Mio	Gestionnaire de volume logique	rootrhel	XFS
/home	1 Mio	Gestionnaire de volume logique	rootrhel	XFS
/tmp	500 Mio	Gestionnaire de volume logique	rootrhel	XFS
/var/log	1000 Mio	Gestionnaire de volume logique	varlogrhel	XFS
/var/log/audit	1000 Mio	Gestionnaire de volume logique	varlogrhel	XFS

Recommandations :

- Conservez et reformatiez la partition /boot/efi si elle existe dans l'agencement de partition existant. Sinon, il n'est pas nécessaire de la créer.
- Supprimez et recréez /boot avec une taille de 1024 Mio en prenant l'espace à partir de swap ou de / si possible. Sinon, recréez /boot avec sa taille initiale.

Remarque : S'il n'existe aucune partition /boot/efi, prenez 1 Mio de /boot et créez le point de montage biosboot avec une taille de 1 Mio.

- Supprimez la partition pré-existante / et recréez-la en tant que gestionnaire de volume logique. Veillez à utiliser rootrhel comme nom du groupe de volumes. Le type de système de fichiers doit être XFS, et le type d'unité Gestionnaire de volume logique.
- Effectuez la répartition comme suit :
Si l'espace a été pris à partir de /boot, supprimez cette quantité ici.

4 Mio pour les métadonnées du gestionnaire de volume logique

- Effectuez la répartition du reste en respectant les pourcentages ci-après. Vous pouvez utiliser la formule suivante pour calculer la taille des partitions.

Type de système de fichiers : XFS

Type d'unité : gestionnaire de volume logique

/ 36 %

/opt 36 %

/var 14 %

/home 2 %

/tmp 8 %

- Formule de calcul de taille des partitions :

La partition pré-existante / est de 20000 Mio, et la taille de /boot est prise à partir de /. Donc, $20000 - 4 - 1024 = 18972$.

$/ = 18972 * 36 / 100 = 6829,92$. Arrondissez à 6829.

$/opt = 18972 * 36 / 100 = 6829,92$. Arrondissez à 6829.

$/var = 18972 * 14 / 100 = 2656,08$. Arrondissez à 2656.

$/home = 18972 * 2 / 100 = 379,44$. Arrondissez à 379.

$/tmp = 18972 * 8 / 100 = 1517,76$. Arrondissez à 1517.

- Supprimez la partition /var/log pré-existante et recréez-la en tant que gestionnaire de volume logique. Veillez à utiliser rootrhel comme nom du groupe de volumes. Le type de système de fichiers doit être XFS, et le type d'unité Gestionnaire de volume logique.
- Effectuez la répartition comme suit :
4 Mio pour les métadonnées du gestionnaire de volume logique
- Effectuez la répartition du reste en respectant les pourcentages ci-après. Vous pouvez utiliser la formule suivante pour répartir la partition existante en gestionnaire de volume logique :
 $/var/log$ 83 %
 $/var/log/audit$ 17 %
- Formule de répartition de la partition existante en gestionnaire de volume logique avec de nouveaux volumes :
(taille totale de la partition pré-existante - 4 Mio pour les métadonnées du gestionnaire de volume logique - taille de /boot) * pourcentage / 100

Installation de RHEL version 7.3 et configuration des partitions

Lorsque vous lancez une mise à niveau d'IBM Security QRadar sur un hôte sur lequel des partitions RHEL personnalisées sont configurées, un message indiquant qu'il existe une installation du logiciel RHEL s'affiche. Copiez les recommandations de dimensionnement de vos partitions existantes pour RHEL 7.3 pour les utiliser par la suite lors de la procédure.

Procédure

1. Insérez l'unité de stockage amovible dans votre appareil et redémarrez l'appareil.
2. Dans le menu de démarrage, sélectionnez l'une des options suivantes :
 - Sélectionnez l'option d'amorçage Lecteur USB ou DVD.
 - Pour effectuer une installation sur un système qui prend en charge Extensible Firmware Interface (EFI), vous devez démarrer le système en mode legacy.

3. Suivez les instructions de l'assistant d'installation pour commencer l'installation :
 - a. Sélectionnez votre langue.
 - b. Cliquez sur **Date et heure** et définissez l'heure du déploiement.
 - c. Cliquez sur **Cible d'installation** et sélectionnez l'option **Je vais configurer le partitionnement**, puis cliquez sur **Terminé**.
4. Ajustez la taille des partitions en fonction des recommandations pour votre déploiement, figurant dans la fenêtre d'installation.

Exemple : La procédure ci-dessous est un exemple d'ajustement de la taille des partitions pour mettre à niveau un déploiement avec une partition /root qui représente 20 000 Mo.

Dans la section **Red Hat Enterprise Linux Server Linux V6.8 for x86_64**, modifiez les partitions suivantes :

- a. Sélectionnez **Permuter**, puis l'option **Reformater**.
- b. Sélectionnez **/store** et entrez **/store** dans la zone **Point de montage**.

Important : Cette option n'est disponible que dans les déploiements haute disponibilité (HA).

- c. Sélectionnez **/store/tmp** et entrez **/store/tmp** dans la zone **Point de montage**.
- d. Sélectionnez **/transient** et entrez **/transient** dans la zone **Point de montage**.
- e. Sélectionnez **/boot** et entrez la nouvelle valeur de **/bootold** dans la zone **Point de montage**.
- f. Supprimez **/**.

Dans la section **Nouvelle installation Red Hat Linux Enterprise V7.X**, cliquez sur **+** pour créer les partitions RHEL 7.3 :

Important : Après avoir créé chaque partition, cliquez sur **Mettre à jour les paramètres**.

- a. Créez un point de montage **/boot** représentant 1 024 Mo, avec le système de fichiers **XFS** et le type d'unité **Partition standard**.
- b. Créez un point de montage **/** représentant 6 672 Mo, avec le système de fichiers **XFS** et le type d'unité **LVM**.
- c. La partition **/** étant toujours sélectionnée, cliquez sur **Modifier** sous le bouton **Groupe de volume** pour créer un groupe de volume **rootrhel** et sélectionnez **Règle de taille > Aussi grande que possible**.
- d. Créez un point de montage **/var** représentant 2 594 Mo, avec le système de fichiers **XFS** et le type d'unité **LVM**. Assurez-vous que **rootrhel** est sélectionné pour le **groupe de volume**.
- e. Créez un point de montage **/opt** représentant 6 672 Mo, avec le système de fichiers **XFS** et le type d'unité **LVM**. Assurez-vous que **rootrhel** est sélectionné pour le **groupe de volume**.
- f. Créez un point de montage **/tmp** représentant 1 482 Mo, avec le système de fichiers **XFS** et le type d'unité **LVM**. Assurez-vous que **rootrhel** est sélectionné pour le **groupe de volume**.
- g. Créez un point de montage **/home** représentant 370 Mo, avec le système de fichiers **XFS** et le type d'unité **LVM**. Assurez-vous que **rootrhel** est sélectionné pour le **groupe de volume**.

- h. Supprimez la partition /var/log dans la section **Red Hat Enterprise Linux Server Linux V6.8 for x86_64**.

Remarque : Ne sélectionnez pas l'option **Supprimer également tous les autres systèmes de fichiers dans le répertoire principal Red Hat Enterprise Linux Server Linux V6.8 for x86_64**.
 - i. Créez un point de montage /var/log représentant 8 063 Mo, avec le système de fichiers XFS et le type d'unité LVM.
 - j. La partition var/log étant toujours sélectionnée, cliquez sur **Modifier** sous le bouton **Groupe de volume** pour créer le groupe de volume **varlogrhel** et sélectionnez **Règle de taille > Aussi grand que possible**.
 - k. Créez un point de montage /var/log/audit représentant 1 651 Mo, avec le système de fichiers XFS et le type d'unité LVM. Assurez-vous que **varlogrhel** est sélectionné pour le **groupe de volume**.
 - l. Supprimez la partition /bootold dans la section **Red Hat Enterprise Linux Server Linux V6.8 for x86_64**. Seules trois partitions sont maintenant répertoriées pour RHEL V6.8 : /store, /storetmp et /transient.
 - m. Créez un point de montage biosboot et acceptez les paramètres par défaut.
5. Cliquez sur **Terminé** dans la fenêtre **Partitionnement manuel**.
 6. Suivez les instructions de l'assistant pour effectuer l'installation :
 - a. Cliquez sur **Réseau et nom d'hôte**.
 - b. Entrez le nom d'hôte de votre dispositif.
 - c. Sélectionnez l'interface dans la liste, placez le commutateur sur la position **Activé** et cliquez sur **Configurer**.
 - d. Sous l'onglet **Général**, sélectionnez l'option **Se connecter automatiquement à ce réseau lorsqu'il est disponible**.
 - e. Sous l'onglet **Paramètres IPv4**, dans la liste **Méthode**, sélectionnez **Manuelle**.
 - f. Cliquez sur **Ajouter** pour entrer l'adresse IP, le masque de sous-réseau et la passerelle pour le dispositif dans la zone **Adresses**.
 - g. Ajoutez deux serveurs DNS.
 - h. Cliquez sur **Sauvegarder**, cliquez sur **Terminé**, puis cliquez sur **Commencer l'installation**.
 7. Définissez le mot de passe root, puis cliquez sur **Terminer la configuration**.
 8. Redémarrez l'hôte une fois l'installation de RHEL 7.3 terminée.

Installation de QRadar

Après avoir configuré RHEL 7.3, effectuez l'installation d'IBM Security QRadar en préparant l'assistant d'installation de QRadar.

Procédure

1. Utilisez SSH pour vous connecter au système en tant qu'utilisateur root.
2. Modifiez la valeur SELINUX dans le fichier /etc/sysconfig/selinux sur SELINUX=disabled et redémarrez l'hôte.
3. Utilisez SSH pour vous reconnecter au système en tant qu'utilisateur root.
4. Vérifiez que la partition /store n'est pas montée en exécutant la commande suivante :

```
mount
```

Si la partition /store est montée, démontez-la à l'aide de la commande suivante :

```
umount /store
```

5. Vérifiez que la partition /storetmp est montée en exécutant la commande suivante :

```
mount /storetmp
```

6. Créez le répertoire /media/cdrom en exécutant la commande suivante :

```
mkdir -p /media/cdrom
```

7. Montez le fichier ISO de QRadar en exécutant la commande suivante :

```
mount /storetmp/730/<nom_fichier_ISO_QRadars> /media/cdrom
```

8. Exécutez la commande ci-dessous pour commencer la mise à niveau de QRadar :

```
/media/cdrom/setup
```

9. Une fois l'installation terminée, videz le cache du navigateur. Pour plus d'informations, voir «Effacement du cache du navigateur Web après les mises à niveau», à la page 11.

Conseil : QRadar version 7.3.0 utilise une technologie de synchronisation de l'heure différente de celle employée dans les versions précédentes. Après la mise à niveau de la console QRadar vers la version 7.3.0, vous pouvez recevoir des messages système signalant l'échec de la synchronisation de l'heure jusqu'à ce que tous les hôtes gérés exécutent la version 7.3.0.

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 CONTREFAÇON AINSI QU'EN CAS DE DEF AUT 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 services 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.



Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation 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 sessions 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).

