QRadar on Cloud

Guide d'initiation

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 45.

Ce document s'applique à IBM® QRadar Security Intelligence Platform version 7.2.6 et à toutes les versions et modifications ultérieures sauf indication contraire dans les nouvelles éditions.

Table des matières

Introduction à l'intégration de QRadar on Cloud..... v

Chapitre 1. Présentation de QRadar on Cloud..... 1
Prise en charge de la migration vers QRadar on Cloud..... 2
Intégration de QRadar on Cloud..... 2
Prérequis pour les passerelles de données..... 2
Configuration système requise pour les passerelles de données..... 3
Passerelles de données..... 4
Création de votre machine virtuelle..... 5
Installation d'une passerelle de données QRadar..... 6
Configuration de la règle de notification d'état de la passerelle de données..... 33
Connexion d'un dispositif QRadar Network Insights à QRadar on Cloud..... 33
Envoi de données syslog TLS à QRadar Console..... 33
Eléments de travail QRadar on Cloud nécessitant un ticket de demande de service..... 34

Chapitre 2. Application Self Serve..... 37
Configuration d'un mappage de proxy..... 37
Ajout d'un mappage de proxy..... 37
Edition d'un mappage de proxy..... 38
Suppression d'un mappage de proxy..... 38
Gestion des utilisateurs..... 38
Affichage des utilisateurs..... 38
Ajout d'un utilisateur..... 38
Modification des paramètres utilisateur..... 39
Désactivation d'un compte utilisateur..... 39
Gestion des accès à la console..... 39
Génération d'un nouveau marqueur pour une passerelle de données..... 40
Placement d'une adresse IP sur liste autorisée..... 40
Modification ou suppression d'une adresse IP placée sur liste autorisée..... 41
Marqueurs de service autorisés..... 41
Ajout d'un marqueur de service autorisé..... 41
Suppression d'un marqueur de service autorisé..... 42
Etat de la passerelle de données..... 42
Affichage de l'état de la passerelle de données..... 42
Demande d'un ensemble de journaux pour votre instance QRadar on Cloud..... 42

Remarques..... 45
Marques..... 46
Dispositions relatives à la documentation du produit..... 46
Déclaration IBM de confidentialité en ligne..... 47

Introduction à l'intégration de QRadar on Cloud

Utilisez IBM QRadar on Cloud pour surveiller votre réseau avec IBM QRadar dans un modèle d'abonnement.

Utilisateurs concernés

Les administrateurs de réseau qui sont responsables de l'installation et de la configuration des systèmes QRadar doivent avoir une bonne connaissance des concepts de sécurité réseau et du 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/SSKMKU/com.ibm.qradar.doc_cloud/c_hosted_inst.html).

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

Contacter le service clients

Pour contacter le service clients, voir QRadar Support – Assistance 101 (https://ibm.biz/qradarsupport).

Bonnes pratiques de sécurité

La sécurité des systèmes informatiques implique la protection des systèmes et des informations par la prévention, la détection et la réponse aux accès non autorisés au sein comme à l'extérieur de votre entreprise. Un accès non autorisé peut se traduire par la modification, la destruction, ou une utilisation inadéquate ou malveillante de vos systèmes, y compris l'utilisation de ces derniers pour attaquer d'autres systèmes. Aucun système ou produit informatique ne doit être considéré comme totalement sécurisé et aucun produit ou mesure de sécurité ne peut être à lui seul entièrement efficace pour empêcher un accès inapproprié. 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, DES PRODUITS ET DES SERVICES, NI CELLE DE VOTRE ENTREPRISE, CONTRE LES CONDUITES MALVEILLANTES OU ILLICITES DE TIERS.

Remarque :

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 ne peut être utilisé que conformément aux besoins réglementaires et de manière légale. Le client accepte d'utiliser ce programme conformément aux lois, réglementations et règles en vigueur et veille à s'y conformer. Le Détenteur de la Licence déclare qu'il obtiendra ou a obtenu tous les accords, droits ou licences nécessaires à l'utilisation légale d'IBM Security QRadar.

Chapitre 1. Présentation de QRadar on Cloud

Dans un environnement où les conditions de sécurité sont dynamiques, IBM QRadar on Cloud fournit le contrôle de sécurité dont vous avez besoin et la possibilité de modifier vos activités de surveillance selon vos besoins.

Avec QRadar on Cloud, vous pouvez protéger votre réseau et respecter les exigences de surveillance et de production de rapports avec un coût total de possession réduit. Hormis un dispositif de passerelle utilisé pour la connexion à QRadar, vous n'avez pas besoin d'installer de matériel supplémentaire sur votre site.

Vous profitez de toutes les capacités de QRadar sans avoir besoin d'investir dans les équipements et logiciels nécessaires dans un déploiement de QRadar sur site. Ce sont les professionnels de la sécurité IBM qui gèrent l'infrastructure, tandis que vos analystes de la sécurité s'occupent des tâches de gestion et de détection des menaces. Vous pouvez avoir jusqu'à six utilisateurs, et vous pouvez leur attribuer un accès d'administrateur de la sécurité.

Pour plus d'informations sur les capacités de QRadar on Cloud, consultez *"Fonctions de votre produit Security Intelligence"* dans le manuel *IBM QRadar SIEM Administration Guide*.

Dispositif de passerelle

Téléchargez et installez le logiciel d'activation sur votre dispositif de passerelle pour collecter les données de flux et d'événements à partir de toutes les sources de journal prises en charge dans votre déploiement sur site ou cloud.

Les données d'événements et de flux collectées sont transférées par le logiciel d'activation, via un tunnel VPN sécurisé, à l'instance QRadar fonctionnant dans le cloud IBM, où elles sont stockées et gérées.

Connectez-vous à la console QRadar à partir d'un navigateur web afin de gérer vos paramètres de sécurité et les tâches de gestion des menaces, comme vous le feriez avec QRadar déployé sur votre site.

L'image suivante montre les périphériques de votre réseau qui envoient des informations à votre dispositif de passerelle. Le dispositif de passerelle communique ensuite avec une instance de QRadar qui s'exécute dans le cloud IBM

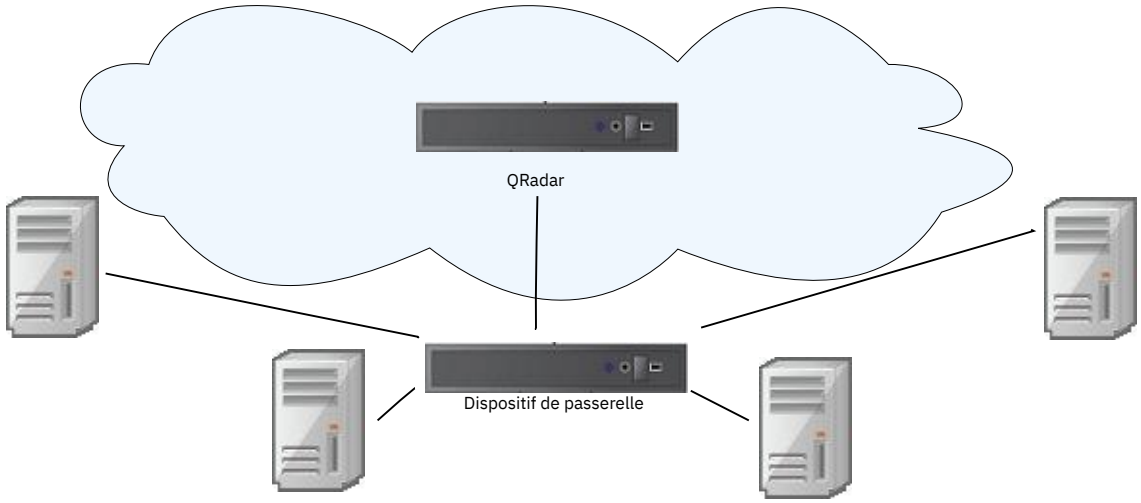


Figure 1. Exemple de déploiement QRadar on Cloud

Limites d'EPS et de FPM

Votre dispositif de passerelle peut collecter 20 000 événements par seconde (EPS) si vous ne collectez pas de données de flux. Le tableau suivant contient les limites d'événements par seconds (EPS) et de flux par minute (FPM) si des données de flux et des événements sont collectés.

Tableau 1. Limites d'EPS et de FPM du dispositif de passerelle de données d'QRadar on Cloud	
Evénements par seconde	**Flux par minute**
0	600 000
1000	540 000
2000	480 000
3000	420 000
4000	360 000
5000	300 000
6000	240 000
7000	180 000
8000	120 000
9000	60 000
10 000 à 20 000	0

Prise en charge de la migration vers QRadar on Cloud

La migration depuis un déploiement QRadar sur site vers QRadar on Cloud n'est pas couverte par le support IBM ; contactez les consultants Security Expert Labs (www.ibm.com/security/security-expert-labs) ou sel@us.ibm.com pour obtenir de l'aide concernant les actions suivantes :

- Migration de configurations
- Migration de données
- Intégration de sources de journaux

Intégration de QRadar on Cloud

Lorsque vous achetez IBM QRadar on Cloud, IBM vous envoie les informations nécessaires à l'utilisation de QRadar on Cloud.

Prérequis pour les passerelles de données

Certains prérequis doivent être satisfaits pour que vous puissiez utiliser le dispositif de passerelle QRadar on Cloud.

- Vous devez disposer du nom d'hôte public de la console à laquelle vous vous connectez via le dispositif de passerelle. IBM vous indique le nom d'hôte public.
- Vérifiez que l'adresse IP publique du dispositif de passerelle de données figure sur la liste autorisée dans QRadar on Cloud. Indiquez le dispositif de passerelle de données dans la liste autorisée avant de demander le jeton. Pour plus d'informations, voir «Placement d'une adresse IP sur liste autorisée», à la page 40.
- Vous devez disposer de votre jeton QRadar on Cloud. Vous avez besoin d'un jeton pour chaque dispositif de passerelle que vous souhaitez utiliser pour la connexion à QRadar on Cloud sur le cloud IBM. Accédez à **Admin** > **Hosted QRadar** dans QRadar pour extraire votre jeton. Si vous n'avez pas de jeton, voir «Génération d'un nouveau marqueur pour une passerelle de données», à la page 40.
- Vous devez avoir un lien de téléchargement vers l'ISO IBM QRadar du dispositif de passerelle. Ce lien de téléchargement se trouve dans **Admin** > **Hosted QRadar** dans QRadar.
- Vous devez disposer d'une adresse IP statique pour vous connecter à QRadar on Cloud via le dispositif de passerelle. N'utilisez pas d'adresse IP dans la plage 192.168.0.0/16.

L'adresse IP statique doit être comprise dans l'une des plages CIDR du réseau dans le tableau suivant.

Tableau 2. Plage d'adresses IP pour les routages CIDR du réseau

Routage CIDR du réseau	Plage d'adresses IP
10/8	10.0.0.0 - 10.255.255.255
172.16/12	172.16.0.0 - 172.31.255.255

- Vos serveurs DNS doivent indiquer l'adresse IP appropriée du nom d'hôte de la console.
- Votre dispositif de passerelle doit être derrière un pare-feu NAT.
- Si le trafic de votre passerelle est routé à travers un serveur proxy, celui-ci doit être transparent ou en ligne afin de ne pas exiger d'authentification.
- Vous devez disposer de la largeur de bande suffisante pour envoyer des données de sécurité à QRadar on Cloud. En moyenne, 0,72 mégabit par seconde est requis pour 1 000 événements par seconde (EPS), 7,2 mégabits par secondes pour 10 000 EPS. Utilisez la formule suivante pour déterminer vos exigences en matière de bande passante :

  EPS * ((taille moyenne des événements + 200) octets x 8) / (1000 x 1000 x 10) = valeur en Mbit/s.

  Exemple : 1000 * ((700 + 200) x 8) / (1000 x 1000 x 10) = 0,7 Mbit/s

  Un minimum de 5 Mbit/s est requis, quel que soit le débit d'événements.
- Votre dispositif de passerelle doit respecter la configuration système requise.
- Vous devez autoriser les connexions à l'adresse IP publique de la QRadar Console et du serveur VPN sur le port 443.
- Vous devez autoriser le trafic existant et connexe pour les connexions sur le port 443.
- Vous devez autoriser le trafic HTTPS et OpenVPN pour les connexions sur le port 443.

Configuration système requise pour les passerelles de données

Le dispositif de passerelle que vous installez sur votre site communique avec QRadar on Cloud et doit répondre à des spécifications précises.

La limite matérielle du dispositif physique repose sur le nombre d'UC dans votre déploiement.

Conseil : Pour vous assurer que votre passerelle de données respecte les exigences, voir «Prérequis pour les passerelles de données», à la page 2.

Tableau 3. Configuration système requise de la passerelle pour les dispositifs physiques

Spécification	Valeur requise
Processeur	2,6 GHz, 16 coeurs, 15 Mo de cache
RAM	16 Go
Disque dur	500 Go minimum (recommandation : 2 To) 300 IOPS Vitesse de transfert des données : 300 Mo/s

Tableau 4. Configuration système requise de la passerelle pour les dispositifs virtuels	
Spécification	**Valeur requise**
Processeur	4 coeurs pour 1000 événements par seconde (EPS) ou moins 8 coeurs pour 7 000 EPS maximum 16 coeurs pour 7 500 à 17 000 EPS 16 coeurs pour les déploiements avec QRadar Vulnerability Manager 16 coeurs pour toute passerelle de données recueillant aussi des données de flux.
RAM	16 Go 32 Go pour les déploiements avec QRadar Vulnerability Manager
Disque dur	500 Go minimum (recommandation : 2 To) 300 IOPS Vitesse de transfert des données : 300 Mo/s

Port 443 sortant

Assurez-vous que le port 443 soit ouvert dans votre pare-feu pour les deux adresses IP HTTPS et de VPN qui vous sont fournies pour votre déploiement. IBM vous fournit deux adresses IP pour votre déploiement de QRadar on Cloud. L'une est l'adresse HTTPS pour la console, l'autre est pour le VPN. Ces adresses figurent dans le mail de bienvenue qui vous a été envoyé. Le port 443 doit être ouvert dans votre pare-feu pour ces deux adresses.

Network Time Protocol (NTP)

IBM QRadar on Cloud utilise un système de localisation GPS doté d'un récepteur dans chaque centre de données pour synchroniser les systèmes selon le protocole de synchronisation NTP (Network Time Protocol). L'heure obtenue est susceptible de différer légèrement de celle des clients qui utilisent le pool NIST pour NTP dans leurs propres systèmes.

Passerelles de données

Vous vous connectez à IBM QRadar on Cloud via une passerelle de données. Celle-ci peut être installée sur un dispositif physique ou sur une machine virtuelle, soit sur votre propre serveur dans Microsoft Azure, soit dans AWS.

La version de la passerelle de données que vous installez doit être identique à celle de la console QRadar on Cloud que vous utilisez.

Logiciels tiers sur des passerelles de données

IBM QRadar est un dispositif de sécurité basé sur Linux, et conçu pour résister aux attaques. QRadar n'est pas destiné à faire office de serveur multi-utilisateurs et polyvalent. Il est spécialement conçu et développé pour la prise en charge des fonctions prévues. Le système d'exploitation et les services sont prévus pour un fonctionnement sécurisé. QRadar comprend un pare-feu intégré. Il autorise un accès administrateur uniquement via une connexion sécurisée qui exige un accès chiffré et authentifié et garantit des mises à niveau et des mises à niveau contrôlées. Les passerelles de données QRadar ne requièrent pas et ne prennent pas en charge les agents traditionnels antivirus ou de protection contre les logiciels malveillants. Elles ne prennent pas non plus en charge l'installation de modules ou de programmes tiers.

Prérequis et configuration système requise

Pour connaître les prérequis et la configuration système requise lors de l'installation d'une passerelle de données, voir «Intégration de QRadar on Cloud», à la page 2.

Création de votre machine virtuelle

Créez une machine virtuelle sur laquelle vous pouvez installer IBM Security QRadar si vous ne souhaitez pas l'installer sur un dispositif physique.

Avant de commencer

Pour installer un dispositif virtuel, vous devez utiliser VMware vSphere Client 5.1 ou version ultérieure afin de créer une machine virtuelle.

Important : Si vous installez QRadar sur un système UEFI (Unified Extensible Firmware Interface), l'amorçage sécurisé doit être désactivé.

Pourquoi et quand exécuter cette tâche

Construisez votre machine virtuelle en fonction des spécifications recommandées pour IBM QRadar on Cloud. Pour plus d'informations, voir «Intégration de QRadar on Cloud», à la page 2.

Procédure

1. A partir de VMware vSphere Client, cliquez sur **File** > **New** > **Virtual Machine**.
2. Choisissez les options comme indiqué ci-après :
   a) Dans le panneau **Configuration** de la fenêtre **Create New Virtual Machine**, sélectionnez **Custom**.
   b) Dans le panneau **Virtual Machine Version**, sélectionnez la version 13 du matériel de machine virtuelle.

      Pour plus d'informations sur VMWare ESXi et les versions du matériel, voir ESXi/ESX hosts and compatible virtual machine hardware versions list (https://kb.vmware.com/s/article/2007240).
   c) Pour l'option **Operating System (OS)**, sélectionnez **Linux** et **Red Hat Enterprise Linux 7.3 (64-bit)**.
   d) Sur la page **CPUs**, configurez le nombre de processeurs virtuels que vous souhaitez sur la machine virtuelle :
      - Pour moins de 1000 événements par seconde (EPS), sélectionnez 4 coeurs.
      - Pour 1 000 EPS ou plus ou pour un déploiement avec QRadar Vulnerability Manager, sélectionnez 8 coeurs.
   e) Dans la zone **Memory Size**, sélectionnez 16 ou une valeur supérieure.
   f) Utilisez le tableau ci-dessous pour configurer les connexions réseau.

Tableau 5. Description des paramètres de configuration réseau

Paramètre	Description
Nombre de cartes d'interface réseau à connecter	Vous devez ajouter au moins une carte d'interface réseau.
Adaptateur	VMXNET3

   g) Dans le volet **SCSI controller**, sélectionnez **VMware Paravirtual**.
   h) Dans le volet **Disk**, sélectionnez **Create a new virtual disk** et utilisez le tableau ci-dessous pour configurer les paramètres du disque virtuel.

Tableau 6. Paramètres de taille de disque virtuel et paramètres de règles de mise à disposition	
Propriété	**Option**
Capacité	500 Go minimum 2 To ou plus (recommandation)
Mise à disposition des disques	Mise à disposition standard
Options avancées	Ne pas configurer

3. Sur la page **Ready to Complete**, vérifiez les paramètres puis cliquez sur **Finish**.

Installation d'une passerelle de données QRadar

Vous vous connectez à IBM QRadar on Cloud via une passerelle de données. Installez celle-ci sur un dispositif physique ou sur une machine virtuelle.

Avant de commencer

Vérifiez que votre dispositif respecte la configuration système requise de la passerelle de données. Voir «Configuration système requise pour les passerelles de données», à la page 3.

Programmez une fenêtre de maintenance pour cette tâche et assurez-vous que les utilisateurs ne déploient pas de changements pendant que la passerelle de données est ajoutée à votre déploiement.

Vérifiez que vous disposez des informations suivantes :

- jeton pour QRadar on Cloud,
- nom d'hôte complet de la console à laquelle vous vous connectez par le biais de votre dispositif de passerelle.

Pourquoi et quand exécuter cette tâche

Remarques :

- Les passerelles de données doivent être installées l'une après l'autre. Si vous installez plusieurs passerelles de données, attendez que l'installation en cours soit terminée avant d'effectuer la suivante.
- Vous définissez un mot de passe root lors du processus d'installation. Vous ne pouvez pas changer ce mot de passe une fois l'installation terminée. Le mot de passe root est aussi celui de l'hôte de la passerelle.

Procédure

1. Choisissez votre méthode d'installation.
   - Si vous installez votre passerelle de données sur un dispositif physique, commencez l'installation en procédant comme suit.
     a. Dans l'onglet **Admin** de QRadar, cliquez sur **Hosted QRadar** pour télécharger le fichier ISO.
     b. Créez une clé USB ou un DVD amorçable.
     c. Sélectionnez l'option d'amorçage de l'emplacement ISO de QRadar : DVD ou USB.
   - Si vous installez votre passerelle de données sur une machine virtuelle, commencez l'installation en procédant comme suit.
     a. Dans l'onglet **Admin** de QRadar, cliquez sur **Hosted QRadar** pour télécharger le fichier ISO.
     b. Pointez vers le fichier ISO sur l'unité de DVD.
     c. Configurez le menu d'amorçage de la machine virtuelle de manière qu'elle démarre sur l'unité de DVD à la mise sous tension du dispositif.

- Si vous installez votre passerelle de données dans Microsoft Azure, suivez les instructions dans «Installation d'une passerelle de données QRadar sur Microsoft Azure», à la page 8.
- Si vous installez votre passerelle de données dans Amazon Web Services (AWS), suivez les instructions dans «Installation d'une passerelle de données QRadar sur Amazon Web Services à partir de l'image de la place de marché», à la page 21.
- Si vous installez votre passerelle de données sur Google Cloud Platform, suivez les instructions de la rubrique «Installation d'une passerelle de données QRadar sur Google Cloud Platform», à la page 29.

2. Mettez le dispositif sous tension.
3. Acceptez le **contrat de licence d'utilisateur final** (EULA) qui apparaît.

   Conseil : Appuyez sur la barre d'espacement pour faire défiler le document.
4. Suivez les instructions de l'assistant d'installation.
   a) Dans la fenêtre d'installation de dispositif, sélectionnez l'option permettant d'installer le dispositif.
   b) Dans la fenêtre d'affectation d'un dispositif non logiciel, sélectionnez **Event Collector Gateway 7000**.
   c) Dans la fenêtre de configuration des informations réseau, n'utilisez pas d'adresse IP dans la plage 192.168.0.0/16. Vous devez utiliser une adresse IP statique. Ne changez pas cette adresse IP. Laissez la zone **IP publique** vide. Attribuez à chaque passerelle un nom d'hôte unique. Le nom d'hôte de la passerelle ne peut pas être identique au nom d'hôte de la console et ne peut pas être "qradar".
   d) Dans la fenêtre **Configuration du déploiement**, entrez le nom de domaine complet de la console et le jeton pour QRadar on Cloud.
   e) Dans la fenêtre d'accès Internet, sélectionnez l'option correspondant à une connexion directe.

   Une fois les paramètres d'installation configurés, plusieurs messages d'installation s'affichent. La procédure d'installation peut prendre quelques minutes.
5. Utilisez l'application QRadar on Cloud Self Serve afin de générer un jeton pour votre passerelle de données et inclure l'adresse IP de la passerelle de données dans la liste autorisée. Pour plus d'informations, voir «Gestion des accès à la console», à la page 39.
6. Une fois le marqueur reçu :
   a) Le dispositif ayant été redémarré après l'étape précédente, ouvrez à nouveau le shell du superutilisateur en entrant la commande suivante :

   ```
   sudo su -
   ```

   b) Pour terminer la configuration initiale de la passerelle de données, entrez la commande suivante :

   ```
   /opt/qradar/bin/setup_qradar_host.py mh_setup interactive -p
   ```
7. Mettez à jour le fichier de licence pour traiter le problème décrit dans l'APAR IJ30161 (https://www.ibm.com/support/pages/apar/IJ30161) en entrant la commande suivante :

   ```
   echo -n "QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" | tee /opt/
   qradar/ecs/license.txt /opt/ibm/si/services/ecs-ec-ingress/current/eventgnosis/
   license.txt /opt/ibm/si/services/ecs-ep/current/eventgnosis/license.txt /opt/ibm/si/services/
   ecs-ec/current/eventgnosis/license.txt /usr/eventgnosis/ecs/license.txt /opt/qradar/conf/
   templates/ecs_license.txt
   ```
8. Quittez le shell superutilisateur en entrant la commande suivante :

   ```
   exit
   ```

Installation d'une passerelle de données QRadar sur Microsoft Azure

Vous vous connectez à IBM QRadar on Cloud via une passerelle de données. Cette passerelle de données peut être installée dans Microsoft Azure.

Avant de commencer

Vérifiez que votre dispositif respecte la configuration système requise de la passerelle de données. Voir «Configuration système requise pour les passerelles de données», à la page 3.

Programmez une fenêtre de maintenance pour cette tâche et assurez-vous que les utilisateurs ne déploient pas de changements pendant que la passerelle de données est ajoutée à votre déploiement.

Vous devez connaître le nom d'hôte complet de la console à laquelle vous vous connectez à travers votre dispositif de passerelle.

Pourquoi et quand exécuter cette tâche

Pour tout problème lié au logiciel QRadar, contactez le support IBM. Si des problèmes liés à l'infrastructure Microsoft Azure surviennent, consultez la documentation du support Microsoft Azure. Si le support IBM détermine que le problème est provoqué par l'infrastructure Microsoft Azure, vous devez contacter Microsoft pour obtenir de l'aide concernant la résolution de ce problème.

Vous devez utiliser des adresses IP statiques privées et publiques.

Les passerelles de données doivent être installées l'une après l'autre. Si vous installez plusieurs passerelles de données, attendez que l'installation en cours soit terminée avant d'effectuer la suivante.

N'effectuez pas de changement de configuration, tel que l'ajout d'entrées DNS supplémentaires, tant que l'installation n'est pas terminée.

Procédure

1. Accédez à Microsoft Azure Marketplace (https://azuremarketplace.microsoft.com/fr-fr/marketplace/apps/ibm.qradar733?tab=Overview).

   L'onglet **Abonnements + tarification** peut vous servir à estimer le coût de certaines tailles de machine virtuelle, mais ce n'est pas sur cet écran que vous choisissez votre taille de machine virtuelle. Pour estimer ce coût, référez-vous aux colonnes **Coeurs** et **RAM**. Ignorez la colonne **Espace disque**, car toutes les images de QRadar proposées sur les places de marché incluent un disque pour le système d'exploitation et un disque de 1 To pour le stockage.
2. Cliquez sur **Obtenir**.
3. Sélectionnez **QRadar SIEM MH 7.3.3** dans la liste de menus **Abonnement logiciel** puis cliquez sur **Continuer**.
4. Cliquez sur **Créer** pour créer une instance pour la passerelle de données.
5. Configurez les paramètres de la machine virtuelle.
   a) Sélectionnez un groupe de ressources existant ou créez-en un nouveau.
   b) Entrez un nom de machine virtuelle.

      Remarque : Le nom de la machine virtuelle ne doit pas dépasser dix caractères.
   c) Sélectionnez une région.
   d) Cliquez sur **Change size** et vérifiez que votre machine virtuelle remplit les conditions minimales requises.

      Pour plus d'informations, voir «Intégration de QRadar on Cloud», à la page 2.
   e) Entrez un nom d'utilisateur pour le compte administrateur.
   f) Choisissez un élément dans la zone **SSH public key** ou **Password**.

      Pour plus d'informations sur la création et l'utilisation d'une paire de clés privée/publique SSH pour les machines virtuelles Linux dans Microsoft Azure, voir la documentation Microsoft.

g) Sélectionnez **Allow selected ports** pour l'option **Public inbound ports**.

h) Sélectionnez **SSH (22)** et **HTTPS (443)** pour l'option **Select inbound ports**.

6. Cliquez sur **Review + Create**.
7. Cliquez sur **Create** pour déployer l'instance.
8. Une fois votre machine virtuelle déployée dans Azure, définissez les adresses IP publique et privée comme statiques :
   a) Cliquez sur **Go to resource**.
   b) Cliquez sur l'adresse IP publique.
   c) Sélectionnez **Static** pour **Assignment**.
   d) Cliquez sur **Save**.
   e) Cliquez sur **Overview**.
   f) Cliquez sur le lien **Associated to**.
   g) Cliquez sur **IP configurations**.
   h) Dans la liste des configurations IP, cliquez sur la ligne de configuration dans laquelle l'option Primary est sélectionnée pour **Type**.
   i) Sélectionnez **Static** pour l'affectation d'adresse IP privée.
   j) Cliquez sur **Save**.
9. Créez ou sélectionnez un groupe de sécurité autorisant uniquement les connexions aux ports 22 et 443 depuis des adresses IP de confiance afin de créer une liste autorisée d'adresses IP pouvant accéder à votre déploiement QRadar.
   a) Cliquez sur **Virtual Machines** > **<nom_machine_virtuelle>**.
   b) Cliquez sur **Networking**.
   c) Cliquez sur la règle SSH associée au port 22.
   d) Dans le panneau d'édition, sélectionnez **IP Addresses** dans la liste **Source**.
   e) Dans la zone **Source IP addresses/CIDR ranges**, entrez la plage d'adresses autorisées à accéder à la machine virtuelle.
   f) Cliquez sur **Save**.
   g) Cliquez sur la règle HTTPS associée au port 443.
   h) Dans le panneau d'édition, sélectionnez **IP Addresses** dans la liste **Source**.
   i) Dans la zone **Source IP addresses/CIDR ranges**, entrez la plage d'adresses autorisées à accéder à la machine virtuelle.
   j) Cliquez sur **Save**.
10. Pour afficher les informations de connexion SSH pour l'adresse IP publique du dispositif virtuel, procédez comme suit :
    a) Cliquez sur **Virtual Machines** > **<nom_machine_virtuelle>**.
    b) Cliquez sur **Connect**.
11. Connectez-vous à votre machine virtuelle.
    - Pour vous connecter en utilisant SSH et votre paire de clés, entrez la commande suivante :

      ```
      ssh -i <key.pem> user@<public_IP_address>
      ```

    - Pour vous connecter en utilisant SSH et votre mot de passe, entrez la commande suivante :

      ```
      ssh user@<public_IP_address>
      ```

12. Pour vérifier la longueur de votre nom de domaine complet, entrez la commande suivante :

    ```
    hostname -f | wc -c
    ```

Si la commande renvoie une valeur supérieure à 63, l'installation échoue. Redémarrez cette procédure en utilisant un nom de machine virtuelle plus court.

Que faire ensuite

Si vous devez augmenter le stockage du système de fichiers au-delà de la taille de 1 To par défaut, suivez les étapes présentées dans «Augmentation du stockage du système de fichiers pour un nouvel hôte géré en recréant le disque de données avec une taille supérieure», à la page 10. Si possible, augmentez le stockage du système de fichiers avant de procéder à l'installation car il est plus risqué d'augmenter le stockage du système de fichiers sur un système en cours d'exécution qu'avant de procéder à l'installation.

Si vous n'avez pas besoin de plus d'1 To de stockage, passez à la section «Installation de la passerelle de données», à la page 16.

Information associée

Augmentation du stockage du système de fichiers pour un nouvel hôte géré en recréant le disque de données avec une taille supérieure

Augmentez la taille du système de fichiers sur l'hôte géré en recréant le disque de données existant avec une taille supérieure et en utilisant le gestionnaire de volume logique (LVM) de Red Hat.

Avant de commencer

Servez-vous du document QRadar: Storage Performance Requirements (www.ibm.com/support/docview.wss?uid=swg21993402) et de la feuille de calcul disponible dans la section *Calculating Event Storage Requirements* de la page Event FAQ (https://developer.ibm.com/qradar/2017/08/22/1775/) pour déterminer vos besoins en stockage.

Pour plus d'informations sur l'augmentation de la taille d'un disque, voir la documentation Microsoft.

Pourquoi et quand exécuter cette tâche

Avertissement : Cette procédure est valable pour les nouvelles installations uniquement et doit être effectuée avant les étapes présentées dans «Installation de la passerelle de données», à la page 16. Si vous suivez ces étapes une fois l'installation terminée, des erreurs seront générées et vous perdrez des données.

Procédure

1. Arrêtez votre machine virtuelle.
2. Cliquez sur **Disks**.

   Pour augmenter le stockage sous la barre des 4095 Gio :

   a) Cliquez sur le lien du disque de données.

   b) Cliquez sur **Size + performance**.

   c) Choisissez une option dans la liste ou entrez la nouvelle taille de disque en gibioctets.

   d) Cliquez sur **Save**.

   Pour augmenter le stockage au-dessus de la barre des 4095 Gio :

   a) Cliquez sur **Edit**.

   b) Cliquez sur **X** à côté du disque de données afin de déconnecter le disque.

   c) Cliquez sur **Save**.

   d) Cliquez sur **Home**.

   e) Cliquez sur **Disks**.

   f) Cliquez sur le disque associé à la machine virtuelle que vous éditez.

g) Cliquez sur **Size + performance**.

h) Entrez la nouvelle taille de disque en gibioctets.

i) Cliquez sur **Save**.

j) Accédez à l'écran d'accueil et cliquez sur **Virtual machines**.

k) Cliquez sur le nom de votre machine virtuelle.

l) Cliquez sur **Disks**.

m) Cliquez sur **+ Add data disk**.

n) Sélectionnez le disque que vous avez modifié.

o) Cliquez sur **Save**.

3. Une fois le disque de données développé, redémarrez votre machine virtuelle.
4. Connectez-vous à votre machine virtuelle avec **ssh**.
5. Déterminez le nom d'unité et le numéro de partition pour les systèmes de fichiers `/store` et `/transient` en entrant la commande suivante :

```
lsblk
```

Dans l'exemple de sortie de **`lsblk`**, pour les systèmes de fichiers `/store` et `/transient`, le nom d'unité est sdc, le numéro de partition est 1 et le groupe de volumes est data.

```
NAME                    MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
fd0                       2:0    1     4K  0 disk
sda                       8:0    0    98G  0 disk
├─sda1                    8:1    0     1G  0 part /boot
├─sda2                    8:2    0    20G  0 part /
├─sda3                    8:3    0   200M  0 part /boot/efi
├─sda4                    8:4    0     1K  0 part
└─sda5                    8:5    0  76.8G  0 part
  ├─rhel-var            253:0    0     8G  0 lvm  /var
  ├─rhel-var_log        253:1    0    18G  0 lvm  /var/log
  ├─rhel-temp           253:2    0     8G  0 lvm  /temp
  ├─rhel-storetmp       253:3    0    15G  0 lvm  /storetmp
  ├─rhel-opt            253:4    0    14G  0 lvm  /opt
  ├─rhel-home           253:5    0     6G  0 lvm  /home
  └─rhel-var_log_audit  253:6    0   7.8G  0 lvm  /var/log/audit
sdb                      8:16   0    32G  0 disk
└─sdb1                   8:17   0    32G  0 part /mnt/resource
sdc                      8:32   0     6T  0 disk
└─sdc1                   8:33   0  1022G  0 part
  ├─data-transient      253:7    0 204.4G  0 lvm  /transient
  └─data-store          253:8    0 817.6G  0 lvm  /store
```

6. Devenez superutilisateur en entrant la commande suivante ainsi que votre mot de passe lorsque vous y êtes invité :

```
sudo -i
```

7. Arrêtez les services en exécutant les commandes suivantes :

```
systemctl stop ecs-ec-ingress
```

```
systemctl stop ecs-ep
```

```
systemctl stop hostservices
```

```
systemctl stop systemStabMon
```

```
systemctl stop crond
```

8. Accédez au répertoire racine en entrant la commande suivante :

```
cd /
```

9. Créez une sauvegarde du système de fichiers `/store` en entrant la commande suivante :

```
tar -czhpf storetmp/storebackup.tgz store
```

La sortie peut inclure un message similaire à "tar: store/tmp/storebackup.tgz: file is the archive; not dumped". Il n'indique pas un problème grave. S'il s'affiche, ignorez-le et passez à l'étape suivante.

10. Créez une sauvegarde du système de fichiers `/transient` en entrant la commande suivante :

```
tar -czhpf storetmp/transientbackup.tgz transient
```

11. Ouvrez l'invite **parted** en entrant la commande suivante :

```
parted /dev/<device_name>
```

Exemple de commande :

```
parted /dev/sdc
```

12. Affichez la taille des unités présentées en mébioctets en entrant la commande suivante :

```
unit mib
```

```
p
```

13. Lorsque le message "Error: The backup GPT table is not at the end of the disk..." s'affiche, entrez `Fix`.
14. Lorsque le message "Warning: Not all of the space available ..." s'affiche, entrez `Fix`.
15. Redimensionnez la partition pour remplir le disque en entrant la commande suivante :

```
resizepart <partition_number> 100%
```

Exemple de commande :

```
resizepart 1 100%
```

16. Quittez parted en entrant la commande suivante :

```
quit
```

17. Assurez-vous que le noyau reconnaît les nouvelles informations de partition en entrant la commande suivante :

```
partprobe /dev/<device_name><partition_number>
```

Exemple de commande :

```
partprobe /dev/sdc1
```

Si l'étape aboutit, aucune sortie n'est générée. Si une sortie indique que **partprobe** n'a pas détecté les nouvelles partitions, réamorcez le système avant de passer à l'étape suivante.

18. Augmentez la taille du volume physique pour remplir l'espace disque supplémentaire en entrant la commande suivante :

```
pvresize /dev/<device_name><partition_number>
```

Exemple de commande :

```
pvresize /dev/sdc1
```

Exemple de sortie indiquant que l'étape a abouti :

```
Physical volume "/dev/sdc1" changed
  1 physical volume(s) resized / 0 physical volume(s) not resized
```

La sortie peut inclure un message similaire à "File descriptor 63 (pipe:[102103]) leaked on pvresize invocation. Parent PID 6636: -bash". Il n'indique pas un problème grave. S'il s'affiche, ignorez-le et passez à l'étape suivante.

19. Développez `/transient` pour augmenter sa taille de 20 % de l'espace disque supplémentaire en entrant la commande suivante :

    ```
    lvextend -l +20%FREE /dev/<volume_group>/transient
    ```

    Exemple de commande :

    ```
    lvextend -l +20%FREE /dev/data/transient
    ```

    Exemple de sortie indiquant que l'étape a abouti :

    ```
    Size of logical volume data/transient changed from <204.40 GiB (52326 extents) to 1.20 TiB
    (314573 extents).
      Logical volume data/transient successfully resized.
    ```

20. Développez `/store` dans l'espace disque supplémentaire restant en entrant la commande suivante :

    ```
    lvextend -l +100%FREE /dev/<volume_group>/store
    ```

    Exemple de commande :

    ```
    lvextend -l +100%FREE /dev/data/store
    ```

    Exemple de sortie indiquant que l'étape a abouti :

    ```
    Size of logical volume data/store changed from <817.60 GiB (209305 extents) to 4.00 TiB
    (1048985 extents).
      Logical volume data/store successfully resized.
    ```

21. Reformatez le système de fichiers `/store` :

    a) Démontez le système de fichiers `/store` en entrant la commande suivante :

    ```
    umount /dev/mapper/<volume_group>-store
    ```

    Exemple de commande :

    ```
    umount /dev/mapper/data-store
    ```

    b) Construisez le système de fichiers XFS pour `/store` en entrant la commande suivante :

    ```
    mkfs.xfs -f /dev/mapper/<volume_group>-store
    ```

    Exemple de commande :

    ```
    mkfs.xfs -f /dev/mapper/data-store
    ```

    Exemple de sortie indiquant que l'étape a abouti :

    ```
    meta-data=/dev/mapper/data-store isize=512    agcount=5, agsize=268435455 blks
             =                       sectsz=4096  attr=2, projid32bit=1
             =                       crc=1        finobt=0, sparse=0
    data     =                       bsize=4096   blocks=1074160640, imaxpct=5
             =                       sunit=0      swidth=0 blks
    naming   =version 2              bsize=4096   ascii-ci=0 ftype=1
    log      =internal log           bsize=4096   blocks=521728, version=2
             =                       sectsz=4096  sunit=1 blks, lazy-count=1
    realtime =none                   extsz=4096   blocks=0, rtextents=0
    ```

    c) Vérifiez que le système de fichiers XFS pour `/store` n'est pas endommagé en entrant la commande suivante :

    ```
    xfs_repair /dev/mapper/<volume_group>-store
    ```

    Exemple de commande :

    ```
    xfs_repair /dev/mapper/data-store
    ```

Exemple de sortie indiquant que l'étape a abouti :

```
Phase 1 - find and verify superblock...
Phase 2 - using internal log
        - zero log...
        - scan filesystem freespace and inode maps...
        - found root inode chunk
Phase 3 - for each AG...
        - scan and clear agi unlinked lists...
        - process known inodes and perform inode discovery...
        - agno = 0
        - agno = 1
        - agno = 2
        - agno = 3
        - agno = 4
        - process newly discovered inodes...
Phase 4 - check for duplicate blocks...
        - setting up duplicate extent list...
        - check for inodes claiming duplicate blocks...
        - agno = 0
        - agno = 1
        - agno = 3
        - agno = 4
        - agno = 2
Phase 5 - rebuild AG headers and trees...
        - reset superblock...
Phase 6 - check inode connectivity...
        - resetting contents of realtime bitmap and summary inodes
        - traversing filesystem ...
        - traversal finished ...
        - moving disconnected inodes to lost+found ...
Phase 7 - verify and correct link counts...
done
```

d) Montez le système de fichiers `/store` en entrant la commande suivante :

```
mount /dev/mapper/<volume_group>-store
```

Exemple de commande :

```
mount /dev/mapper/data-store
```

22. Reformatez le système de fichiers `/transient` :

a) Démontez le système de fichiers `/transient` en entrant la commande suivante :

```
umount /dev/mapper/<volume_group>-transient
```

Exemple de commande :

```
umount /dev/mapper/data-transient
```

b) Construisez le système de fichiers XFS pour `/transient` en entrant la commande suivante :

```
mkfs.xfs -f /dev/mapper/<volume_group>-transient
```

Exemple de commande :

```
mkfs.xfs -f /dev/mapper/data-transient
```

Exemple de sortie indiquant que l'étape a abouti :

```
meta-data=/dev/mapper/data-transient isize=512    agcount=4, agsize=80530688 blks
         =                       sectsz=4096  attr=2, projid32bit=1
         =                       crc=1        finobt=0, sparse=0
data     =                       bsize=4096   blocks=322122752, imaxpct=5
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0 ftype=1
log      =internal log           bsize=4096   blocks=157286, version=2
         =                       sectsz=4096  sunit=1 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
```

c) Vérifiez que le système de fichiers XFS pour `/transient` n'est pas endommagé en entrant la commande suivante :

```
xfs_repair /dev/mapper/<volume_group>-transient
```

Exemple de commande :

```
xfs_repair /dev/mapper/data-transient
```

Exemple de sortie indiquant que l'étape a abouti :

```
Phase 1 - find and verify superblock...
Phase 2 - using internal log
        - zero log...
        - scan filesystem freespace and inode maps...
        - found root inode chunk
Phase 3 - for each AG...
        - scan and clear agi unlinked lists...
        - process known inodes and perform inode discovery...
        - agno = 0
        - agno = 1
        - agno = 2
        - agno = 3
        - process newly discovered inodes...
Phase 4 - check for duplicate blocks...
        - setting up duplicate extent list...
        - check for inodes claiming duplicate blocks...
        - agno = 0
        - agno = 1
        - agno = 2
        - agno = 3
Phase 5 - rebuild AG headers and trees...
        - reset superblock...
Phase 6 - check inode connectivity...
        - resetting contents of realtime bitmap and summary inodes
        - traversing filesystem ...
        - traversal finished ...
        - moving disconnected inodes to lost+found ...
Phase 7 - verify and correct link counts...
done
```

d) Montez le système de fichiers `/transient` en entrant la commande suivante :

```
mount /dev/mapper/<volume_group>-transient
```

Exemple de commande :

```
mount /dev/mapper/data-transient
```

23. Vérifiez que les nouvelles tailles des systèmes de fichiers étendus sont correctes en entrant la commande suivante :

```
df -h
```

Exemple de sortie indiquant que l'étape a abouti :

```
Filesystem                      Size  Used Avail Use% Mounted on
/dev/sda2                        20G  1.2G   18G   7% /
devtmpfs                        7.9G     0  7.9G   0% /dev
tmpfs                           7.9G     0  7.9G   0% /dev/shm
tmpfs                           7.9G  9.1M  7.9G   1% /run
tmpfs                           7.9G     0  7.9G   0% /sys/fs/cgroup
/dev/sda1                       976M  127M  783M  14% /boot
/dev/sda3                       200M  8.0K  200M   1% /boot/efi
/dev/mapper/rhel-var            8.0G  178M  7.9G   3% /var
/dev/mapper/rhel-opt             14G  3.5G   11G  25% /opt
/dev/mapper/rhel-storetmp        15G   33M   15G   1% /storetmp
/dev/mapper/rhel-temp           8.0G   33M  8.0G   1% /temp
/dev/mapper/rhel-home           6.0G   33M  6.0G   1% /home
/dev/mapper/rhel-var_log         18G   44M   18G   1% /var/log
/dev/mapper/rhel-var_log_audit  7.8G   70M  7.8G   1% /var/log/audit
/dev/sdb1                        32G   13G   20G  38% /mnt/resource
tmpfs                           1.6G     0  1.6G   0% /run/user/1000
/dev/mapper/data-store          4.0T   33M  4.0T   1% /store
/dev/mapper/data-transient      1.2T   33M  1.2T   1% /transient
```

24. Restaurez votre sauvegarde du système de fichiers `/store` en entrant la commande suivante :

```
tar -xphf storetmp/storebackup.tgz store
```

25. Restaurez votre sauvegarde du système de fichiers `/transient` en entrant la commande suivante :

```
tar -xphf storetmp/transientbackup.tgz transient
```

26. Démarrez les services en exécutant les commandes suivantes :

```
systemctl start crond
```

```
systemctl start systemStabMon
```

```
systemctl start ecs-ep
```

```
systemctl start ecs-ec-ingress
```

```
systemctl start hostservices
```

27. Réamorcez la machine virtuelle.
28. Connectez-vous à votre machine virtuelle.
    - Pour vous connecter en utilisant SSH et votre paire de clés, entrez la commande suivante :

      ```
      ssh -i <key.pem> user@<public_IP_address>
      ```

    - Pour vous connecter en utilisant SSH et votre mot de passe, entrez la commande suivante :

      ```
      ssh user@<public_IP_address>
      ```

Résultats

Si vous avez augmenté le stockage du système de fichiers, l'avertissement suivant peut s'afficher lorsque vous vous connectez au système :

```
WARNING:*****************************************************************
WARNING: QRadar requires 4092M of swap space but was only able to find
WARNING: 0M, please increase swap space by at least 4092M. Without this
WARNING: additional swap space, some components of QRadar will not function
WARNING: properly (such as complex queries or reports). Please contact
WARNING: Customer Support for further details and assistance in resolving
WARNING: this issue.
WARNING:*****************************************************************
```

Cet avertissement émis suite à l'augmentation du stockage du système de fichiers sur un nouvel hôte géré dans Microsoft Azure est bénin. Il s'affiche car l'espace de permutation pour la machine virtuelle est mis à jour dans l'infrastructure Microsoft Azure. Vous pouvez poursuivre l'installation.

Que faire ensuite

Suivez la procédure décrite dans «Installation de la passerelle de données», à la page 16.

Installation de la passerelle de données

Procédure

1. Entrez la commande suivante :

```
sudo /root/setup_mh 7000
```

2. Le système vous invite à définir un mot de passe root. Le mot de passe doit répondre aux critères suivants :
   - Contient au moins 5 caractères
   - Ne contient pas d'espace
   - Il ne peut pas comporter les caractères spéciaux suivants : @, #, ^ et *.

Vous ne pouvez pas changer ce mot de passe une fois l'installation terminée. Le mot de passe root est aussi celui de l'hôte de la passerelle.

3. Mettez à niveau la passerelle de données vers la même version de QRadar que votre console.
   a) Connectez-vous à la console.
   b) Cliquez sur le menu de navigation (☰), puis sur **A propos de**.
   c) Téléchargez à partir de Fix Central (https://www.ibm.com/support/fixcentral) le fichier SFS correspondant à la version QRadar de la console.
   d) Copiez le fichier SFS de la mise à jour sur votre passerelle de données.
   e) Déplacez le fichier SFS vers le répertoire `/storetmp` en entrant la commande suivante :

   ```
   sudo mv <version_number>_QRadar_patchupdate-<full_version_number>.sfs /storetmp
   ```

   f) Ouvrez le shell superutilisateur en entrant la commande suivante :

   ```
   sudo su -
   ```

   g) Créez le répertoire `/media/updates` en entrant la commande suivante :

   ```
   mkdir /media/updates
   ```

   h) Montez le fichier SFS en entrant la commande suivante :

   ```
   mount -o loop -t squashfs /storetmp/<version_number>_QRadar_patchupdate-
   <full_version_number>.sfs /media/updates
   ```

   i) Lancez le programme d'installation de la mise à jour en entrant la commande suivante :

   ```
   /media/updates/installer
   ```

4. Utilisez l'application QRadar on Cloud Self Serve afin de générer un jeton pour votre passerelle de données et inclure l'adresse IP de la passerelle de données dans la liste autorisée. Pour plus d'informations, voir «Gestion des accès à la console», à la page 39.
5. Une fois le marqueur reçu :
   a) Le dispositif ayant été redémarré après l'étape précédente, ouvrez à nouveau le shell du superutilisateur en entrant la commande suivante :

   ```
   sudo su -
   ```

   b) Pour terminer la configuration initiale de la passerelle de données, entrez la commande suivante :

   ```
   /opt/qradar/bin/setup_qradar_host.py mh_setup interactive -p
   ```

6. Mettez à jour le fichier de licence pour traiter le problème décrit dans l'APAR IJ30161 (https://www.ibm.com/support/pages/apar/IJ30161) en entrant la commande suivante :

   ```
   echo -n "QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" | tee /opt/
   qradar/ecs/license.txt /opt/ibm/si/services/ecs-ec-ingress/current/eventgnosis/
   license.txt /opt/ibm/si/services/ecs-ep/current/eventgnosis/license.txt /opt/ibm/si/services/
   ecs-ec/current/eventgnosis/license.txt /usr/eventgnosis/ecs/license.txt /opt/qradar/conf/
   templates/ecs_license.txt
   ```

7. Quittez le shell superutilisateur en entrant la commande suivante :

   ```
   exit
   ```

Que faire ensuite

Si vous avez augmenté le stockage du système de fichiers, supprimez l'archive de sauvegarde.

1. Connectez-vous avec votre paire de clés en entrant la commande suivante :

```
ssh -i <key.pem> ec2-user@<public_IP_address>
```

2. Supprimez l'archive de sauvegarde en entrant la commande suivante :

```
sudo rm /storetmp/storebackup.tgz
```

3. Supprimez l'archive de sauvegarde `/transient` en entrant la commande suivante :

```
sudo rm /storetmp/transientbackup.tgz
```

Installation d'une passerelle de données QRadar sur Microsoft Azure Government Cloud

Vous vous connectez à IBM QRadar on Cloud via une passerelle de données. Vous pouvez installer la passerelle de données dans Microsoft Azure Government Cloud.

Avant de commencer

Vérifiez que votre dispositif respecte la configuration système requise de la passerelle de données. Voir «Configuration système requise pour les passerelles de données», à la page 3.

Programmez une fenêtre de maintenance pour cette tâche et assurez-vous que les utilisateurs ne déploient pas de changements pendant que la passerelle de données est ajoutée à votre déploiement.

Vous devez connaître le nom d'hôte complet de la console à laquelle vous vous connectez à travers votre dispositif de passerelle.

Pourquoi et quand exécuter cette tâche

Pour tout problème lié au logiciel QRadar, contactez le support IBM. Si des problèmes liés à l'infrastructure Microsoft Azure surviennent, consultez la documentation du support Microsoft Azure. Si le support IBM détermine que le problème est provoqué par l'infrastructure Microsoft Azure, vous devez contacter Microsoft pour obtenir de l'aide concernant la résolution de ce problème.

Vous devez utiliser des adresses IP statiques privées et publiques.

Les passerelles de données doivent être installées l'une après l'autre. Si vous installez plusieurs passerelles de données, attendez que l'installation en cours soit terminée avant d'effectuer la suivante.

N'effectuez pas de changement de configuration, tel que l'ajout d'entrées DNS supplémentaires, tant que l'installation n'est pas terminée.

Procédure

1. Accédez à Microsoft Azure Government Cloud Marketplace (https://portal.azure.us/#blade/Microsoft_Azure_Marketplace/MarketplaceOffersBlade/selectedMenuItemId/) et recherchez "QRadar".
2. Sélectionnez **QRadar SIEM (BYOL)**.
3. Cliquez sur **Créer** pour créer une instance pour la passerelle de données.
4. Configurez les paramètres de la machine virtuelle.
   a) Entrez un nom.

      Remarque : Le nom de la machine virtuelle ne doit pas comporter plus de huit caractères.

   b) Cliquez sur **Change size** et vérifiez que votre machine virtuelle remplit les conditions minimales requises.

      Pour plus d'informations, voir «Intégration de QRadar on Cloud», à la page 2.

   c) Entrez un nom d'utilisateur ssh.
   d) Choisissez un élément dans la zone **SSH public key** ou **Password**.

Pour plus d'informations sur la création et l'utilisation d'une paire de clés publique-privée SSH pour les machines virtuelles Linux dans Azure, reportez-vous à la documentation Microsoft.

5. Configurez les règles de pare-feu du réseau Azure pour permettre l'accès uniquement à partir des plages CIDR de votre infrastructure interne.
   a) Cliquez sur **Settings** > **Choose network security group** > **Create network security group**.
   b) Cliquez sur **Advanced**.
   c) Sélectionnez le groupe de sécurité réseau que vous avez créé à l'étape précédente.
   d) Cliquez sur la règle **default-allow-ssh**.
   e) Dans le panneau d'édition, sélectionnez **IP addresses** dans la liste **Source**.
   f) Dans la zone **Source IP addresses/CIDR ranges**, entrez la plage d'adresses autorisées à accéder à la machine virtuelle.
   g) Entrez les ports 22 et 443 dans la zone **Choose network security group**.
   h) Cliquez sur **Save**.
   i) Cliquez sur **OK**.
   j) Sur l'onglet **Settings**, cliquez sur **OK**.
6. Cliquez sur **Review + Create**.
7. Cliquez sur **Create** pour déployer l'instance.
8. Une fois votre machine virtuelle déployée dans Azure, définissez les adresses IP publique et privée comme statiques :
   a) Cliquez sur **Go to resource**.
   b) Cliquez sur l'adresse IP publique.
   c) Sélectionnez **Static** pour **Assignment**.
   d) Cliquez sur **Save**.
   e) Cliquez sur **Overview**.
   f) Cliquez sur le lien **Associated to**.
   g) Cliquez sur **IP configurations**.
   h) Dans la liste des configurations IP, cliquez sur la ligne de configuration dans laquelle l'option Primary est sélectionnée pour **Type**.
   i) Sélectionnez **Static** pour l'affectation d'adresse IP privée.
   j) Cliquez sur **Save**.
9. Pour afficher les informations de connexion SSH pour l'adresse IP publique du dispositif virtuel, procédez comme suit :
   a) Cliquez sur **Virtual Machines** > **<nom_machine_virtuelle>**.
   b) Cliquez sur **Connect**.
10. Connectez-vous à votre machine virtuelle.
    - Pour vous connecter en utilisant SSH et votre paire de clés, entrez la commande suivante :

      ```
      ssh -i <key.pem> user@<public_IP_address>
      ```

    - Pour vous connecter en utilisant SSH et votre mot de passe, entrez la commande suivante :

      ```
      ssh user@<public_IP_address>
      ```

11. Entrez la commande suivante :

    ```
    sudo /root/setup_mh 7000
    ```

12. Mettez à niveau la passerelle de données vers la même version de QRadar que votre console.
    a) Connectez-vous à la console.

b) Cliquez sur le menu de navigation (☰), puis sur **A propos de**.

c) Téléchargez à partir de Fix Central (https://www.ibm.com/support/fixcentral) le fichier SFS correspondant à la version QRadar de la console.

d) Copiez le fichier SFS de la mise à jour sur votre passerelle de données.

e) Déplacez le fichier SFS vers le répertoire `/storetmp` en entrant la commande suivante :

```
sudo mv <version_number>_QRadar_patchupdate-<full_version_number>.sfs /storetmp
```

f) Ouvrez le shell superutilisateur en entrant la commande suivante :

```
sudo su -
```

g) Créez le répertoire `/media/updates` en entrant la commande suivante :

```
mkdir /media/updates
```

h) Montez le fichier SFS en entrant la commande suivante :

```
mount -o loop -t squashfs /storetmp/<version_number>_QRadar_patchupdate-
<full_version_number>.sfs /media/updates
```

i) Lancez le programme d'installation de la mise à jour en entrant la commande suivante :

```
/media/updates/installer
```

13. Utilisez l'application QRadar on Cloud Self Serve afin de générer un jeton pour votre passerelle de données et inclure l'adresse IP de la passerelle de données dans la liste autorisée. Pour plus d'informations, voir «Gestion des accès à la console», à la page 39.
14. Une fois le marqueur reçu :
    a) Le dispositif ayant été redémarré après l'étape précédente, ouvrez à nouveau le shell du superutilisateur en entrant la commande suivante :

```
sudo su -
```

    b) Pour terminer la configuration initiale de la passerelle de données, entrez la commande suivante :

```
/opt/qradar/bin/setup_qradar_host.py mh_setup interactive -p
```

15. Mettez à jour le fichier de licence pour traiter le problème décrit dans l'APAR IJ30161 (https://www.ibm.com/support/pages/apar/IJ30161) en entrant la commande suivante :

```
echo -n "QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" | tee /opt/
qradar/ecs/license.txt /opt/ibm/si/services/ecs-ec-ingress/current/eventgnosis/
license.txt /opt/ibm/si/services/ecs-ep/current/eventgnosis/license.txt /opt/ibm/si/
services/ecs-ec/current/eventgnosis/license.txt /usr/eventgnosis/ecs/license.txt /opt/
qradar/conf/templates/ecs_license.txt
```

16. Quittez le shell superutilisateur en entrant la commande suivante :

```
exit
```

Information associée

Installation d'une passerelle de données QRadar sur Microsoft Hyper-V

Vous vous connectez à IBM QRadar on Cloud via une passerelle de données. Cette passerelle de données peut être installée surMicrosoft Hyper-V.

Vous devez utiliser une installation de logiciel plutôt qu'une installation de dispositif pour utiliser une passerelle de données sur Microsoft Hyper-V. Au cours de l'installation, sur l'écran relatif au type d'installation, appuyez sur **CTRL**+**K** pour entrer la clé d'activation de la passerelle de données.

Pour plus d'informations sur les installations de logiciel, voir la section sur les installations de dispositif virtuel dans le guide d'installation d'IBM QRadar (https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/c_siem_vrt_ap_inst.html).

Pour plus d'informations sur la configuration requise en termes de mémoire et de processeur, voir «Configuration système requise pour les passerelles de données», à la page 3.

Installation d'une passerelle de données QRadar sur Amazon Web Services à partir de l'image de la place de marché

Vous vous connectez à IBM QRadar on Cloud via une passerelle de données. Cette passerelle de données peut être installée dans une instance Amazon Web Services (AWS) à l'aide de l'AMI (Amazon Machine Image) fournie.

Avant de commencer

Vérifiez que votre dispositif respecte la configuration système requise de la passerelle de données. Voir «Configuration système requise pour les passerelles de données», à la page 3.

Programmez une fenêtre de maintenance pour cette tâche et assurez-vous que les utilisateurs ne déploient pas de changements pendant que la passerelle de données est ajoutée à votre déploiement.

Vous devez connaître le nom d'hôte complet de la console à laquelle vous vous connectez à travers votre dispositif de passerelle.

Pourquoi et quand exécuter cette tâche

Pour tout problème lié au logiciel QRadar, contactez le support IBM. Si des problèmes liés à l'infrastructure AWS surviennent, consultez la documentation AWS. Si le support IBM détermine que le problème est provoqué par l'infrastructure AWS, vous devez contacter Amazon pour obtenir de l'aide concernant la résolution de ce problème.

Vous devez utiliser des adresses IP statiques privées et publiques.

Les passerelles de données doivent être installées l'une après l'autre. Si vous installez plusieurs passerelles de données, attendez que l'installation en cours soit terminée avant d'effectuer la suivante.

N'effectuez pas de changement de configuration, tel que l'ajout d'entrées DNS supplémentaires, tant que l'installation n'est pas terminée.

Procédure

1. Allez sur AWS Marketplace (https://aws.amazon.com/marketplace/pp/B07TC8WXBG).
2. Cliquez sur **Continue to Subscribe**.
3. Cliquez sur **Accept Terms**.
4. Lorsque l'abonnement est prêt, cliquez sur **Continue to Configuration**.
5. Sélectionnez une région et cliquez sur **Continue to Launch**.
6. A partir de la liste **Choose Action**, sélectionnez **Launch from Website**.
7. Sélectionnez le type d'instance EC2 **m4.2xlarge**, ou un type plus grand remplissant les conditions minimales du système.

   Pour plus d'informations, voir «Intégration de QRadar on Cloud», à la page 2.
8. Créez ou sélectionnez un VPC (cloud privé virtuel).
9. Créez ou sélectionnez un sous-réseau pour votre VPC.
10. Créez ou sélectionnez un groupe de sécurité autorisant uniquement les connexions aux ports 22 et 443 depuis des adresses IP de confiance afin de créer une liste autorisée d'adresses IP pouvant accéder à votre déploiement QRadar.

11. Configurez une paire de clés. Vous l'utiliserez chaque fois que vous devrez vous connecter au dispositif en utilisant SSH.
12. Cliquez sur **Launch**.
13. Connectez-vous à l'instance AWS en utilisant la paire de clés créée lors de la configuration de l'instance. Entrez la commande suivante :

    ```
    ssh -i <key.pem> ec2-user@<public_IP_address>
    ```

14. Pour vérifier la longueur de votre nom de domaine complet, entrez la commande suivante :

    ```
    hostname -f | wc -c
    ```

    Si la commande renvoie une valeur supérieure à 63, l'installation échoue. Redémarrez cette procédure en utilisant un nom de machine virtuelle plus court.

Information associée

Augmentation du stockage du système de fichiers pour un nouvel hôte géré en recréant le disque de données avec une taille supérieure

Augmentez la taille du système de fichiers sur l'hôte géré en recréant le disque de données existant avec une taille supérieure et en utilisant le gestionnaire de volume logique (LVM) de Red Hat.

Avant de commencer

Servez-vous du document QRadar: Storage Performance Requirements (www.ibm.com/support/docview.wss?uid=swg21993402) et de la feuille de calcul disponible dans la section *Calculating Event Storage Requirements* de la page Event FAQ (https://developer.ibm.com/qradar/2017/08/22/1775/) pour déterminer vos besoins en stockage.

Pourquoi et quand exécuter cette tâche

Avertissement : Cette procédure est valable pour les nouvelles installations uniquement et doit être effectuée avant les étapes présentées dans «Installation de la passerelle de données», à la page 28. Suivre la procédure ci-après lorsque l'installation est terminée et entraîne des erreurs et une perte de données.

Procédure

1. Pour augmenter le stockage jusqu'à 16 To :
   a) Cliquez sur l'instance de votre machine virtuelle.
   b) Dans l'onglet de description, cliquez sur **/dev/sdb**.
   c) Cliquez sur l'ID EBS.
   d) Cliquez sur **Actions** > **Modifier un volume**.
   e) Modifiez la taille du volume pour qu'elle atteigne jusqu'à 16 384 Gio.
   f) Cliquez sur **Modifier**.
   g) Attendez que l'état change pour indiquer "in-use".
2. Une fois que l'état du disque de données indique `in-use`, connectez-vous à l'aide de votre paire de clés en entrant la commande suivante :

   ```
   ssh -i <key.pem> ec2-user@<public_IP_address>
   ```

3. Déterminez le nom d'unité et le numéro de partition pour les systèmes de fichiers `/store` et `/transient` en entrant la commande suivante :

```
lsblk
```

Dans cet exemple de sortie de **lsblk**, pour les systèmes de fichiers /store et /transient, le nom d'unité est xvdb, le numéro de partition est 2 et le groupe de volumes est storerhel.

```
NAME                   MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
xvda                    202:0    0    98G  0 disk
├─xvda1                 202:1    0     1G  0 part /boot
├─xvda2                 202:2    0    20G  0 part /
├─xvda3                 202:3    0   200M  0 part
├─xvda4                 202:4    0     1K  0 part
└─xvda5                 202:5    0  76.8G  0 part
  ├─rhel-var_log_audit  253:0    0   7.8G  0 lvm  /var/log/audit
  ├─rhel-var_log       253:1    0    18G  0 lvm  /var/log
  ├─rhel-var            253:2    0     8G  0 lvm  /var
  ├─rhel-tmp            253:3    0     8G  0 lvm  /tmp
  ├─rhel-storetmp       253:4    0    15G  0 lvm  /storetmp
  ├─rhel-opt            253:5    0    14G  0 lvm  /opt
  └─rhel-home           253:6    0     6G  0 lvm  /home
xvdb                      202:16   0     6T  0 disk
├─xvdb1                 202:17   0    24G  0 part [SWAP]
└─xvdb2                   202:18   0   999G  0 part
  ├─storerhel-store     253:7    0 799.2G  0 lvm  /store
  └─storerhel-transient 253:8    0 199.8G  0 lvm  /transient
```

4. Devenez superutilisateur en entrant la commande suivante ainsi que votre mot de passe lorsque vous y êtes invité :

```
sudo -i
```

5. Arrêtez les services en exécutant les commandes suivantes :

```
systemctl stop ecs-ec-ingress
```

```
systemctl stop ecs-ep
```

```
systemctl stop hostservices
```

```
systemctl stop systemStabMon
```

```
systemctl stop crond
```

6. Accédez au répertoire racine en entrant la commande suivante :

```
cd /
```

7. Créez une sauvegarde du système de fichiers /store en entrant la commande suivante :

```
tar -czhpf storetmp/storebackup.tgz store
```

La sortie peut inclure un message similaire à "tar: store/tmp/storebackup.tgz: file is the archive; not dumped". Il n'indique pas un problème grave. S'il s'affiche, ignorez-le et passez à l'étape suivante.

8. Créez une sauvegarde du système de fichiers /transient en entrant la commande suivante :

```
tar -czhpf storetmp/transientbackup.tgz transient
```

9. Ouvrez l'invite **parted** en entrant la commande suivante :

```
parted /dev/<device_name>
```

Exemple de commande :

```
parted /dev/xvdb
```

10. Affichez la taille des unités présentées en mébioctets en entrant la commande suivante :

```
unit mib
```

```
p
```

11. Lorsque le message "Error: The backup GPT table is not at the end of the disk..." s'affiche, entrez `Fix`.
12. Lorsque le message "Warning: Not all of the space available ..." s'affiche, entrez `Fix`.
13. Redimensionnez la partition pour remplir le disque en entrant la commande suivante :

    ```
    resizepart <partition_number> 100%
    ```

    Exemple de commande :

    ```
    resizepart 2 100%
    ```

14. Quittez parted en entrant la commande suivante :

    ```
    quit
    ```

15. Assurez-vous que le noyau reconnaît les nouvelles informations de partition en entrant la commande suivante :

    ```
    partprobe /dev/<device_name><partition_number>
    ```

    Exemple de commande :

    ```
    partprobe /dev/xvdb2
    ```

    Si l'étape aboutit, aucune sortie n'est générée. Si une sortie indique que **partprobe** n'a pas détecté les nouvelles partitions, réamorcez le système avant de passer à l'étape suivante.
16. Augmentez la taille du volume physique pour remplir l'espace disque supplémentaire en entrant la commande suivante :

    ```
    pvresize /dev/<device_name><partition_number>
    ```

    Exemple de commande :

    ```
    pvresize /dev/xvdb2
    ```

    Exemple de sortie indiquant que l'étape a abouti :

    ```
    Physical volume "/dev/xvdb2" changed
      1 physical volume(s) resized / 0 physical volume(s) not resized
    ```

    La sortie peut inclure un message similaire à "File descriptor 63 (pipe:[102103]) leaked on pvresize invocation. Parent PID 6636: -bash". Il n'indique pas un problème grave. S'il s'affiche, ignorez-le et passez à l'étape suivante.
17. Développez `/transient` pour augmenter sa taille de 20 % de l'espace disque supplémentaire en entrant la commande suivante :

    ```
    lvextend -l +20%FREE /dev/<volume_group>/transient
    ```

    Exemple de commande :

    ```
    lvextend -l +20%FREE /dev/storerhel/transient
    ```

    Exemple de sortie indiquant que l'étape a abouti :

    ```
    Size of logical volume storerhel/transient changed from 199.80 GiB (51149 extents) to <1.20
    TiB (313345 extents).
      Logical volume storerhel/transient successfully resized.
    ```

18. Développez `/store` dans l'espace disque supplémentaire restant en entrant la commande suivante :

    ```
    lvextend -l +100%FREE /dev/<volume_group>/store
    ```

    Exemple de commande :

```
lvextend -l +100%FREE /dev/storerhel/store
```

Exemple de sortie indiquant que l'étape a abouti :

```
Size of logical volume storerhel/store changed from <799.20 GiB (204594 extents) to 4.00 TiB
(1048780 extents).
  Logical volume storerhel/store successfully resized.
```

19. Reformatez le système de fichiers `/store` :
    a) Démontez le système de fichiers `/store` en entrant la commande suivante :

    ```
    umount /dev/mapper/<volume_group>-store
    ```

    Exemple de commande :

    ```
    umount /dev/mapper/storerhel-store
    ```

    b) Construisez le système de fichiers XFS pour `/store` en entrant la commande suivante :

    ```
    mkfs.xfs -f /dev/mapper/<volume_group>-store
    ```

    Exemple de commande :

    ```
    mkfs.xfs -f /dev/mapper/storerhel-store
    ```

    Exemple de sortie indiquant que l'étape a abouti :

    ```
    meta-data=/dev/mapper/storerhel-store isize=512    agcount=5, agsize=268435455 blks
             =                       sectsz=512   attr=2, projid32bit=1
             =                       crc=1        finobt=0, sparse=0
    data     =                       bsize=4096   blocks=1073950720, imaxpct=5
             =                       sunit=0      swidth=0 blks
    naming   =version 2              bsize=4096   ascii-ci=0 ftype=1
    log      =internal log           bsize=4096   blocks=521728, version=2
             =                       sectsz=512   sunit=0 blks, lazy-count=1
    realtime =none                   extsz=4096   blocks=0, rtextents=0
    ```

    c) Vérifiez que le système de fichiers XFS pour `/store` n'est pas endommagé en entrant la commande suivante :

    ```
    xfs_repair /dev/mapper/<volume_group>-store
    ```

    Exemple de commande :

    ```
    xfs_repair /dev/mapper/storerhel-store
    ```

    Exemple de sortie indiquant que l'étape a abouti :

    ```
    Phase 1 - find and verify superblock...
    Phase 2 - using internal log
            - zero log...
            - scan filesystem freespace and inode maps...
            - found root inode chunk
    Phase 3 - for each AG...
            - scan and clear agi unlinked lists...
            - process known inodes and perform inode discovery...
            - agno = 0
            - agno = 1
            - agno = 2
            - agno = 3
            - agno = 4
            - process newly discovered inodes...
    Phase 4 - check for duplicate blocks...
            - setting up duplicate extent list...
            - check for inodes claiming duplicate blocks...
            - agno = 0
            - agno = 2
            - agno = 3
            - agno = 1
            - agno = 4
    Phase 5 - rebuild AG headers and trees...
            - reset superblock...
    Phase 6 - check inode connectivity...
            - resetting contents of realtime bitmap and summary inodes
            - traversing filesystem ...
    ```

```
        - traversal finished ...
        - moving disconnected inodes to lost+found ...
Phase 7 - verify and correct link counts...
done
```

d) Montez le système de fichiers `/store` en entrant la commande suivante :

```
mount /dev/mapper/<volume_group>-store
```

Exemple de commande :

```
mount /dev/mapper/storerhel-store
```

20. Reformatez le système de fichiers `/transient` :

a) Démontez le système de fichiers `/transient` en entrant la commande suivante :

```
umount /dev/mapper/<volume_group>-transient
```

Exemple de commande :

```
umount /dev/mapper/storerhel-transient
```

b) Construisez le système de fichiers XFS pour `/transient` en entrant la commande suivante :

```
mkfs.xfs -f /dev/mapper/<volume_group>-transient
```

Exemple de commande :

```
mkfs.xfs -f /dev/mapper/storerhel-transient
```

Exemple de sortie indiquant que l'étape a abouti :

```
meta-data=/dev/mapper/storerhel-transient isize=512    agcount=4, agsize=80216320 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=1        finobt=0, sparse=0
data     =                       bsize=4096   blocks=320865280, imaxpct=5
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0 ftype=1
log      =internal log           bsize=4096   blocks=156672, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
```

c) Vérifiez que le système de fichiers XFS pour `/transient` n'est pas endommagé en entrant la commande suivante :

```
xfs_repair /dev/mapper/<volume_group>-transient
```

Exemple de commande :

```
xfs_repair /dev/mapper/storerhel-transient
```

Exemple de sortie indiquant que l'étape a abouti :

```
Phase 1 - find and verify superblock...
Phase 2 - using internal log
        - zero log...
        - scan filesystem freespace and inode maps...
        - found root inode chunk
Phase 3 - for each AG...
        - scan and clear agi unlinked lists...
        - process known inodes and perform inode discovery...
        - agno = 0
        - agno = 1
        - agno = 2
        - agno = 3
        - process newly discovered inodes...
Phase 4 - check for duplicate blocks...
        - setting up duplicate extent list...
        - check for inodes claiming duplicate blocks...
        - agno = 0
        - agno = 2
        - agno = 3
        - agno = 1
Phase 5 - rebuild AG headers and trees...
```

```
        - reset superblock...
Phase 6 - check inode connectivity...
        - resetting contents of realtime bitmap and summary inodes
        - traversing filesystem ...
        - traversal finished ...
        - moving disconnected inodes to lost+found ...
Phase 7 - verify and correct link counts...
done
```

d) Montez le système de fichiers `/transient` en entrant la commande suivante :

```
mount /dev/mapper/<volume_group>-transient
```

Exemple de commande :

```
mount /dev/mapper/storerhel-transient
```

21. Vérifiez que les nouvelles tailles des systèmes de fichiers étendus sont correctes en entrant la commande suivante :

```
df -h
```

Exemple de sortie indiquant que l'étape a abouti :

```
Filesystem                      Size  Used Avail Use% Mounted on
/dev/xvda2                       20G  1.1G   18G   6% /
devtmpfs                         32G     0   32G   0% /dev
tmpfs                            32G     0   32G   0% /dev/shm
tmpfs                            32G  9.0M   32G   1% /run
tmpfs                            32G     0   32G   0% /sys/fs/cgroup
/dev/xvda1                      976M  130M  780M  15% /boot
/dev/mapper/rhel-tmp            8.0G   33M  8.0G   1% /tmp
/dev/mapper/rhel-home           6.0G   33M  6.0G   1% /home
/dev/mapper/rhel-opt             14G  4.1G   10G  29% /opt
/dev/mapper/rhel-storetmp        15G   33M   15G   1% /storetmp
/dev/mapper/rhel-var             8.0G  765M  7.3G  10% /var
/dev/mapper/rhel-var_log         18G   42M   18G   1% /var/log
/dev/mapper/rhel-var_log_audit   7.8G   34M  7.8G   1% /var/log/audit
tmpfs                            6.3G     0  6.3G   0% /run/user/1000
/dev/mapper/storerhel-store      4.0T   33M  4.0T   1% /store
/dev/mapper/storerhel-transient  1.2T   33M  1.2T   1% /transient
```

22. Restaurez votre sauvegarde du système de fichiers `/store` en entrant la commande suivante :

```
tar -xphf storetmp/storebackup.tgz store
```

23. Restaurez votre sauvegarde du système de fichiers `/transient` en entrant la commande suivante :

```
tar -xphf storetmp/transientbackup.tgz transient
```

24. Démarrez les services en exécutant les commandes suivantes :

```
systemctl start crond
```

```
systemctl start systemStabMon
```

```
systemctl start ecs-ep
```

```
systemctl start ecs-ec-ingress
```

```
systemctl start hostservices
```

25. Redémarrez la machine virtuelle en entrant la commande suivante :

```
reboot
```

Que faire ensuite

Suivez la procédure décrite dans «Installation de la passerelle de données», à la page 28.

Installation de la passerelle de données

Procédure

1. Une fois l'instance prête, connectez-vous avec votre paire de clés en entrant la commande suivante :

   ```
   ssh -i <key.pem> ec2-user@<public_IP_address>
   ```

2. Entrez la commande suivante :

   ```
   sudo /root/setup_mh 7000
   ```

3. Le système vous invite à définir un mot de passe root. Le mot de passe doit répondre aux critères suivants :

   - Contient au moins 5 caractères
   - Ne contient pas d'espace
   - Il ne peut pas comporter les caractères spéciaux suivants : @, #, ^ et *.

   Vous ne pouvez pas changer ce mot de passe une fois l'installation terminée. Le mot de passe root est aussi celui de l'hôte de la passerelle.

4. Mettez à niveau la passerelle de données vers la même version de QRadar que votre console.
   a) Connectez-vous à la console.
   b) Cliquez sur le menu de navigation (☰), puis sur **A propos de**.
   c) Téléchargez à partir de Fix Central (https://www.ibm.com/support/fixcentral) le fichier SFS correspondant à la version QRadar de la console.
   d) Copiez le fichier SFS de la mise à jour sur votre passerelle de données.
   e) Déplacez le fichier SFS vers le répertoire `/storetmp` en entrant la commande suivante :

      ```
      sudo mv <version_number>_QRadar_patchupdate-<full_version_number>.sfs /storetmp
      ```

   f) Ouvrez le shell superutilisateur en entrant la commande suivante :

      ```
      sudo su -
      ```

   g) Créez le répertoire `/media/updates` en entrant la commande suivante :

      ```
      mkdir /media/updates
      ```

   h) Montez le fichier SFS en entrant la commande suivante :

      ```
      mount -o loop -t squashfs /storetmp/<version_number>_QRadar_patchupdate-
      <full_version_number>.sfs /media/updates
      ```

   i) Lancez le programme d'installation de la mise à jour en entrant la commande suivante :

      ```
      /media/updates/installer
      ```

5. Utilisez l'application QRadar on Cloud Self Serve afin de générer un jeton pour votre passerelle de données et inclure l'adresse IP de la passerelle de données dans la liste autorisée. Pour plus d'informations, voir «Gestion des accès à la console», à la page 39.
6. Une fois le marqueur reçu :
   a) Le dispositif ayant été redémarré après l'étape précédente, ouvrez à nouveau le shell du superutilisateur en entrant la commande suivante :

      ```
      sudo su -
      ```

   b) Pour terminer la configuration initiale de la passerelle de données, entrez la commande suivante :

      ```
      /opt/qradar/bin/setup_qradar_host.py mh_setup interactive -p
      ```

7. Mettez à jour le fichier de licence pour traiter le problème décrit dans l'APAR IJ30161 (https://www.ibm.com/support/pages/apar/IJ30161) en entrant la commande suivante :

```
echo -n "QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" | tee /opt/
qradar/ecs/license.txt /opt/ibm/si/services/ecs-ec-ingress/current/eventgnosis/
license.txt /opt/ibm/si/services/ecs-ep/current/eventgnosis/license.txt /opt/ibm/si/services/
ecs-ec/current/eventgnosis/license.txt /usr/eventgnosis/ecs/license.txt /opt/qradar/conf/
templates/ecs_license.txt
```

8. Quittez le shell superutilisateur en entrant la commande suivante :

```
exit
```

Que faire ensuite

Si vous avez augmenté le stockage du système de fichiers, supprimez l'archive de sauvegarde.

1. Connectez-vous avec votre paire de clés en entrant la commande suivante :

```
ssh -i <key.pem> ec2-user@<public_IP_address>
```

2. Supprimez l'archive de sauvegarde en entrant la commande suivante :

```
sudo rm /storetmp/storebackup.tgz
```

3. Supprimez l'archive de sauvegarde `/transient` en entrant la commande suivante :

```
sudo rm /storetmp/transientbackup.tgz
```

Installation d'une passerelle de données QRadar sur Google Cloud Platform

Vous vous connectez à IBM QRadar on Cloud via une passerelle de données. Vous pouvez installer la passerelle de données sur une instance Google Cloud Platform (GCP) en utilisant l'image fournie.

Avant de commencer

Vérifiez que votre dispositif respecte la configuration système requise de la passerelle de données. Voir «Configuration système requise pour les passerelles de données», à la page 3.

Programmez une fenêtre de maintenance pour cette tâche et assurez-vous que les utilisateurs ne déploient pas de changements pendant que la passerelle de données est ajoutée à votre déploiement.

Vous devez connaître le nom d'hôte complet de la console à laquelle vous vous connectez à travers votre dispositif de passerelle.

Pourquoi et quand exécuter cette tâche

Pour tout problème lié au logiciel QRadar, contactez le support IBM. Si vous rencontrez des problèmes lors de l'utilisation de l'infrastructure GCP, consultez la documentation GCP. Si le support IBM détermine que le problème est provoqué par l'infrastructure GCP, vous devez contacter GCP pour obtenir de l'aide concernant la résolution du problème lié à l'infrastructure GCP.

Vous devez utiliser des adresses IP statiques privées et publiques.

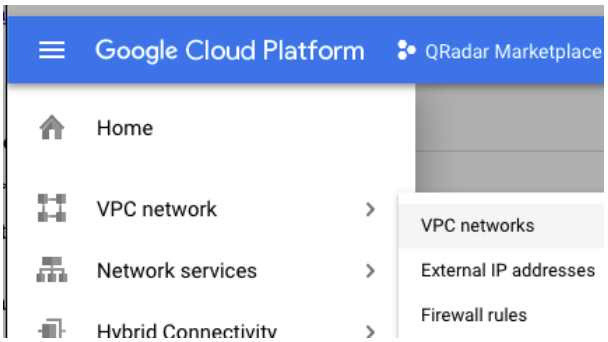
Les passerelles de données doivent être installées l'une après l'autre. Si vous installez plusieurs passerelles de données, attendez que l'installation en cours soit terminée avant d'effectuer la suivante.

N'effectuez pas de changement de configuration, tel que l'ajout d'entrées DNS supplémentaires, tant que l'installation n'est pas terminée.

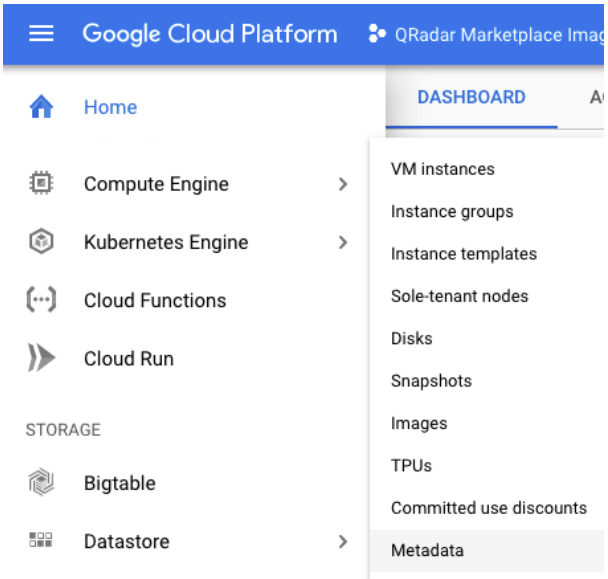
Procédure

1. Créez un nom de projet dans GCP de telle sorte que le nom de domaine complet (FQDN) ne comporte pas plus de 63 caractères. Le nom de domaine complet est composé du nom de déploiement suivi de "-vm", de la zone, de la région, du nom de projet et de l'extension ".internal".

   Par exemple, si votre nom de projet est `abc-stq-xyz`, le nom de déploiement du dispositif est `qr-con`, la zone est `us-east4-c`, la région est `c` et le nom FQDN est `qr-con-vm.us-east4-c.c.abc-stq-xyz.internal`. La zone peut comprendre entre 10 et 25 caractères. En fonction de la zone, vous disposez de 25 à 40 caractères à répartir entre le nom de projet et le nom de déploiement.
2. Dans le projet créé à l'étape 1, configurez votre interface réseau.
   a) Cliquez sur **Google Cloud Platform** > **VPC network** > **VPC networks**.



   b) Cliquez sur **CREATE VPC NETWORK**.
   c) Donnez un nom à votre réseau et configurez les paramètres selon vos besoins. Sélectionnez **No server policy** pour l'option **DNS server policy**.
   d) Cliquez sur **Create**.
3. Ajoutez une clé SSH au projet si vous ne l'avez pas déjà fait. La clé doit être créée pour un utilisateur appelé `cloud-user`.
   a) Cliquez sur **Google Cloud Platform** > **Compute Engine** > **Metadata**.



   b) Cliquez sur **SSH Keys**.
   c) Cliquez sur **Edit**.
   d) Cliquez sur **Add item**.

e) Entrez une clé SSH suivie de la mention `cloud-user`.

f) Cliquez sur **Save**.

4. Accédez à QRadar Security Intelligence Platform Managed Host v7.3.2 P1 (https://console.cloud.google.com/marketplace/details/ibm-security-public/qradar-mh?q=IBM%20qradar&id=19dda1c2-9483-4ddc-a7bf-43e5e0d2fc01).
5. Cliquez sur **LAUNCH**.
6. Définissez un nom de déploiement de telle sorte que le nom de domaine complet (FQDN) ne comporte pas plus de 63 caractères. Le nom de domaine complet est composé du nom de déploiement, de la zone, du nom de projet et de l'extension ".internal".

   Par exemple, si votre nom de projet est `abc-stq-xyz`, le nom de déploiement du dispositif est `qr-con`, la zone est `us-east4-c`, la région est c et le nom FQDN est `qr-con-vm.us-east4-c.c.abc-stq-xyz.internal`. La zone peut comprendre entre 10 et 25 caractères. En fonction de la zone, vous disposez de 25 à 40 caractères à répartir entre le nom de projet et le nom de déploiement.
7. Sélectionnez la zone dans laquelle se trouve votre projet.
8. Sélectionnez un **Type de machine** qui respecte la configuration système minimale requise.

   Pour plus d'informations, voir «Intégration de QRadar on Cloud», à la page 2.
9. Sélectionnez l'interface réseau que vous avez créée.
10. Définissez des règles de pare-feu pour votre dispositif autorisant uniquement les connexions aux ports 22 et 443 depuis des adresses IP de confiance afin de créer une liste autorisée d'adresses IP pouvant accéder à votre déploiement QRadar.

    Dans un déploiement QRadar à plusieurs dispositifs, la communication sur d'autres ports peut être autorisée entre les hôtes gérés. Pour plus d'informations sur les ports devant être autorisés dans votre déploiement, voir Ports et serveurs courants utilisés par QRadar.
11. Sélectionnez la case à cocher **I accept the GCP Marketplace Terms of Service**.
12. Cliquez sur **Deploy**.
13. Définissez une adresse IP statique pour votre dispositif.

    a) Cliquez sur **Google Cloud Platform** > **Compute Engine** > **VM instances**.

    b) Sélectionnez votre dispositif dans la liste.

    c) Cliquez sur **Edit**.

    d) Editez l'interface réseau.

    - Sélectionnez **Static** pour le paramètre **Internal IP type** et réservez une nouvelle adresse IP.
    - Sélectionnez ou créez une adresse IP externe.

    e) Cliquez sur **Done**.
14. Une fois que l'instance est prête, connectez-vous en utilisant **SSH** ainsi que votre paire de clés en entrant la commande suivante :

    ```
    ssh -i <key.pem> cloud-user@<public_IP_address>
    ```
15. Pour vérifier la longueur de votre nom de domaine complet, entrez la commande suivante :

    ```
    hostname -f | wc -c
    ```

    Si la commande renvoie une valeur supérieure à 63, l'installation échoue. Redémarrez cette procédure en utilisant un nom de machine virtuelle plus court.
16. Entrez la commande suivante :

    ```
    sudo /root/setup_mh 7000
    ```
17. Le système vous invite à définir un mot de passe root. Le mot de passe doit répondre aux critères suivants :

    - Contient au moins 5 caractères

- Ne contient pas d'espace
- Il ne peut pas comporter les caractères spéciaux suivants : @, #, ^ et *.

Vous ne pouvez pas changer ce mot de passe une fois l'installation terminée. Le mot de passe root est aussi celui de l'hôte de la passerelle.

18. Mettez à niveau la passerelle de données vers la même version de QRadar que votre console.
    a) Connectez-vous à la console.
    b) Cliquez sur le menu de navigation (☰), puis sur **A propos de**.
    c) Téléchargez à partir de Fix Central (https://www.ibm.com/support/fixcentral) le fichier SFS correspondant à la version QRadar de la console.
    d) Copiez le fichier SFS de la mise à jour sur votre passerelle de données.
    e) Déplacez le fichier SFS vers le répertoire `/storetmp` en entrant la commande suivante :

    ```
    sudo mv <version_number>_QRadar_patchupdate-<full_version_number>.sfs /storetmp
    ```

    f) Ouvrez le shell superutilisateur en entrant la commande suivante :

    ```
    sudo su -
    ```

    g) Créez le répertoire `/media/updates` en entrant la commande suivante :

    ```
    mkdir /media/updates
    ```

    h) Montez le fichier SFS en entrant la commande suivante :

    ```
    mount -o loop -t squashfs /storetmp/<version_number>_QRadar_patchupdate-
    <full_version_number>.sfs /media/updates
    ```

    i) Lancez le programme d'installation de la mise à jour en entrant la commande suivante :

    ```
    /media/updates/installer
    ```

19. Utilisez l'application QRadar on Cloud Self Serve afin de générer un jeton pour votre passerelle de données et inclure l'adresse IP de la passerelle de données dans la liste autorisée. Pour plus d'informations, voir «Gestion des accès à la console», à la page 39.
20. Une fois le marqueur reçu :
    a) Le dispositif ayant été redémarré après l'étape précédente, ouvrez à nouveau le shell du superutilisateur en entrant la commande suivante :

    ```
    sudo su -
    ```

    b) Pour terminer la configuration initiale de la passerelle de données, entrez la commande suivante :

    ```
    /opt/qradar/bin/setup_qradar_host.py mh_setup interactive -p
    ```

21. Mettez à jour le fichier de licence pour traiter le problème décrit dans l'APAR IJ30161 (https://www.ibm.com/support/pages/apar/IJ30161) en entrant la commande suivante :

    ```
    echo -n "QRadar:Q1 Labs Inc.:0007634bda1e2:WnT9X7BDFOgB1WaXwokODc:12/31/20" | tee /opt/
    qradar/ecs/license.txt /opt/ibm/si/services/ecs-ec-ingress/current/eventgnosis/
    license.txt /opt/ibm/si/services/ecs-ep/current/eventgnosis/license.txt /opt/ibm/si/
    services/ecs-ec/current/eventgnosis/license.txt /usr/eventgnosis/ecs/license.txt /opt/
    qradar/conf/templates/ecs_license.txt
    ```

22. Quittez le shell superutilisateur en entrant la commande suivante :

    ```
    exit
    ```

Configuration de la règle de notification d'état de la passerelle de données

QRadar on Cloud fournit une règle permettant d'envoyer des notifications si des passerelles de données sont dans un état inconnu. La règle est configurée pour s'exécuter toutes les 5 minutes. Si une passerelle de données est à l'état inconnu, une notification système est générée. Vous pouvez personnaliser les options de réponse à la règle selon vos besoins.

Procédure

1. Depuis les onglets **Infractions**, **Activité du journal** ou **Activité réseau**, cliquez sur **Règles**.
2. Entrez QRoC dans **Recherche de règles** et appuyez sur Entrée.
3. Cliquez deux fois sur **QRoC Data Gateway Status check**.
4. Utilisez l'**Assistant Règle** pour modifier les options de réponse à la règle.

Connexion d'un dispositif QRadar Network Insights à QRadar on Cloud

Pour pouvoir utiliser un dispositif IBM QRadar Network Insights avec IBM QRadar on Cloud, vous devez utiliser un jeton et exécuter une commande pour connecter le dispositif à la console en utilisant un réseau privé virtuel (VPN).

Avant de commencer

Le dispositif doit être au même niveau de version que la console QRadar on Cloud. Sinon, il n'est pas possible de connecter le dispositif à la console.

Vous devez installer une passerelle de données afin que les flux collectés par QRadar Network Insights puissent être envoyés à QRadar on Cloud.

Procédure

1. Utilisez l'Application Self Serve afin de générer un nouveau jeton pour votre nouvel hôte.
2. Une fois que vous avez reçu votre jeton, entrez la commande suivante pour connecter le dispositif à QRadar on Cloud :

   ```
   /opt/qradar/bin/setup_qradar_host.py mh_setup interactive -p
   ```

3. Ouvrez un autre ticket auprès du support IBM pour connecter le dispositif à une passerelle de données.

   Vous devez indiquer à quelle passerelle de données vous souhaitez que le dispositif QRadar Network Insights soit connecté.

Tâches associées

«Installation d'une passerelle de données QRadar», à la page 6
Vous vous connectez à IBM QRadar on Cloud via une passerelle de données. Installez celle-ci sur un dispositif physique ou sur une machine virtuelle.

«Génération d'un nouveau marqueur pour une passerelle de données», à la page 40

Envoi de données syslog TLS à QRadar Console

Vous pouvez envoyer des informations de source de journal syslog directement à IBM QRadar on Cloud à l'aide du protocole de source de journal syslog TLS. Vous n'avez pas besoin d'utiliser une passerelle de données.

Procédure

1. Cliquez sur l'onglet **Admin**.

2. Cliquez sur l'icône **Sources de journaux**.
3. Cliquez sur **Ajouter**.
4. Configurez les paramètres communs de votre source de journaux.
5. Configurez les paramètres spécifiques au protocole de votre source de journaux.
   - Vous devez utiliser le port 6514 comme port d'écoute.
   - Si vous avez besoin d'une copie du certificat TLS généré par le serveur, vous devez la demander à l'aide d'un ticket de demande de service.
   - Si vous souhaitez fournir vos propres certificat et paire de clés, vous devez les télécharger à l'aide d'un ticket de demande de service.

   Pour plus d'informations sur la configuration du protocole, voir TLS syslog protocol configuration options
6. Cliquez sur **Enregistrer**.
7. Sur l'onglet **Admin**, cliquez sur **Déployer les modifications**.
8. Configurez le périphérique réseau pour envoyer le trafic à la même adresse IP ou adresse de nom de domaine complet (FQDN) que celle que vous utilisez pour accéder à votre instance QRadar on Cloud.

   Par exemple, configurez un pare-feu pour envoyer des informations syslog TLS à QRadar on Cloud. Si votre adresse de console est `console-#######.qradar.ibmcloud.com`, entrez `console-#######.qradar.ibmcloud.com` comme destination dans la configuration syslog du pare-feu.

Eléments de travail QRadar on Cloud nécessitant un ticket de demande de service

Votre infrastructure IBM QRadar on Cloud est gérée par des professionnels IBM de la sécurité. Pour qu'IBM puisse plus facilement vous aider, il est recommandé de fournir le plus d'informations possible.

Le tableau suivant décrit les éléments de travail pour lesquels un ticket de demande de service est requis.

Tableau 7. Eléments de travail QRadar on Cloud

Elément de travail	**Description**	**Informations à transmettre**
Authentification		Pour tout problème d'authentification, contactez le support.
Sauvegarde	La sauvegarde de la configuration est effectuée la nuit.	Heure à laquelle effectuer la configuration si cette dernière est planifiée en dehors des horaires de sauvegarde normaux.
Restauration	Restauration d'une sauvegarde quotidienne.	Date de la sauvegarde à restaurer, depuis la semaine dernière.
Paramètres système	Les paramètres système permettent de configurer les bases de données, l'authentification, les consoles, etc.	Paramètres et valeurs à changer. Pour plus d'informations sur les paramètres système, voir le document *IBM QRadar SIEM Administration Guide*.

Tableau 7. Eléments de travail QRadar on Cloud (suite)

Elément de travail	Description	Informations à transmettre
Destinations de réacheminement et règles de routage	Vous pouvez configurer les systèmes QRadar afin de transmettre des données à un ou plusieurs systèmes fournisseur (systèmes de demande de service ou d'alerte, par exemple). Vous pouvez également transmettre des données normalisées à d'autres systèmes QRadar. Le système cible qui reçoit des données de QRadar est appelé destination de réacheminement. Une fois que vous avez ajouté une ou plusieurs destinations de réacheminement, vous pouvez créer des règles de routage utilisant des filtres afin de transmettre de grandes quantités de données.	Détails sur les éléments à transmettre et sur l'emplacement de réacheminement. Pour plus d'informations sur les destinations de réacheminement, voir le document *IBM QRadar SIEM Administration Guide*. • Ajout de destinations de réacheminement • Configuration des profils de réacheminement • Configuration des règles de routage pour réacheminer des données
Création et édition de rôles utilisateur	Les rôles utilisateur définissent les droits octroyés aux utilisateurs.	Nom du rôle utilisateur à créer et droits que vous souhaitez lui affecter. Pour plus d'informations sur les droits disponibles, voir Création d'un rôle utilisateur.
Suppression de comptes utilisateur	Le compte utilisateur définit le nom d'utilisateur unique utilisé pour se connecter à IBM QRadar et spécifie le rôle utilisateur, le profil de sécurité et les affectations de titulaire affectés à l'utilisateur.	Pour plus d'informations sur les comptes utilisateur, voir «Gestion des utilisateurs», à la page 38.

Chapitre 2. Application Self Serve

Utilisez l'application QRadar on Cloud Self Serve pour effectuer des tâches d'administration liées à la mise à disposition et à la configuration de votre instance QRadar on Cloud.

L'application Self Serve est installée sur toutes les consoles QRadar on Cloud par défaut.

Configuration d'un mappage de proxy

Utilisez l'application QRadar on Cloud Self-Serve afin de configurer le mappage de proxy pour votre instance QRadar on Cloud.

De nombreuses applications requièrent l'accès au réseau pour pouvoir utiliser des unités, des serveurs ou des services sur le réseau client. Ces ressources ne sont normalement pas accessibles depuis Internet. Il convient donc d'utiliser un mappage de proxy de passerelle de données afin de créer un tunnel sécurisé entre les applications QRadar on Cloud et vos ressources réseau sur site. Seules les applications QRadar on Cloud utilisent le tunnel VPN permettant d'accéder à vos ressources.

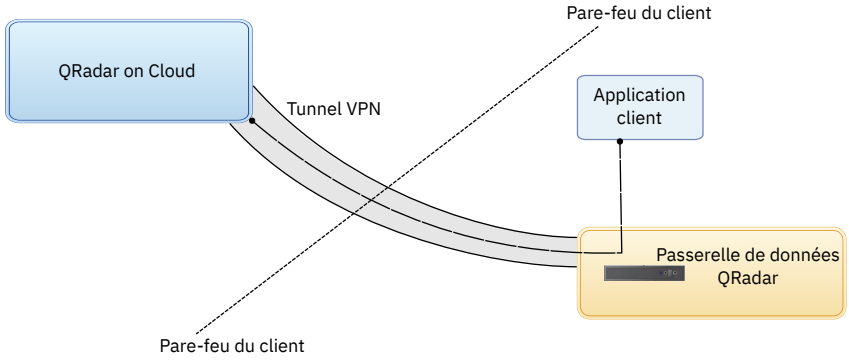


Figure 2. Tunnel VPN QRadar on Cloud

Par exemple, vous utilisez l'importateur de jeu de références LDAP pour importer des enregistrements LDAP en vue de l'analyse utilisateur. Vous pouvez créer un mappage de proxy qui indique la plage de routage CIDR dans laquelle se trouvent vos serveurs LDAP, ainsi que la passerelle de données utilisées par les applications QRadar on Cloud pour le tunnel. Vous pouvez aussi spécifier des adresses IP individuelles avec une extrémité de routage CIDR dans /32.

Important : Les mappages de proxy doivent utiliser les adresses IP de la ressource cible. Il n'est pas possible de limiter l'accès des applications QRadar on Cloud aux mappages de proxy.

Ajout d'un mappage de proxy

Ajoutez un mappage de proxy pour permettre aux applications QRadar d'accéder aux points d'extrémité d'API et aux autres intégrations dans votre réseau local.

Procédure

1. Ouvrez les paramètres **Admin** et cliquez sur **QRadar on Cloud Self Serve**.
2. Cliquez sur **Data Gateway Proxy Mapping**.
3. Cliquez sur **Add**.
4. Entrez un nom pour le mappage de proxy.
5. Entrez la plage CIDR voulue pour le mappage de proxy.
6. Sélectionnez la passerelle à laquelle s'applique le mappage de proxy.
7. Facultatif : Cliquez sur **Test** pour tester votre mappage de proxy.

8. Cliquez sur **Save**.

Edition d'un mappage de proxy

Vous pouvez éditer un mappage de proxy existant afin de changer son nom, le CIDR ou la passerelle.

Procédure

1. Cliquez sur un mappage de proxy.
2. Cliquez sur **Edit**.
3. Apportez les changements nécessaires dans les champs **Name**, **CIDR** et **Gateway**.
4. Facultatif : Cliquez sur **Test** pour tester votre mappage de proxy.
5. Cliquez sur **Save**.

Suppression d'un mappage de proxy

Si vous n'avez plus l'utilité d'un mappage de proxy, vous pouvez le supprimer.

Procédure

1. Cliquez sur un mappage de proxy.
2. Cliquez sur **Delete**.

Gestion des utilisateurs

Utilisez l'application QRadar on Cloud Self Serve pour gérer les utilisateurs de votre instance QRadar on Cloud.

Affichage des utilisateurs

La page Gestion des utilisateurs affiche vos utilisateurs QRadar on Cloud. Vous pouvez filtrer la liste d'utilisateurs par rôle ou par profil de sécurité. Vous pouvez également rechercher des noms d'utilisateur.

Procédure

1. Ouvrez les paramètres **Admin** et cliquez sur **QRadar on Cloud Self Serve**.
2. Cliquez sur **Gestion des utilisateurs**.

   La liste affiche tous vos utilisateurs QRadar on Cloud. Les rôles QRadar ne sont pas tous affichés dans la liste. Ainsi, les rôles de niveau élevé n'apparaissent pas.
3. Sélectionnez un filtre pour n'afficher que les utilisateurs que vous souhaitez voir. Ou saisissez un nom d'utilisateur dans la zone **Rechercher un utilisateur**.

Ajout d'un utilisateur

Vous pouvez ajouter des utilisateurs à votre instance QRadar on Cloud. Les utilisateurs doivent disposer d'un IBMid.

Procédure

1. Ouvrez les paramètres **Admin** et cliquez sur **QRadar on Cloud Self Serve**.
2. Cliquez sur **Gestion des utilisateurs**.
3. Cliquez sur **Ajouter**.
4. Saisissez l'IBMid de l'utilisateur dans **Nom d'utilisateur**.

   Si le nom d'utilisateur est déjà employé, un message indique qu'il est réservé.

5. Sélectionnez le **Rôle utilisateur** et le **Profil de sécurité** de l'utilisateur.
   - Les rôles utilisateur sont définis par un administrateur QRadar on Cloud. Les rôles QRadar ne sont pas tous affichés dans la liste. Ainsi, les rôles de niveau élevé n'apparaissent pas.
   - Les profils de sécurité sont les profils QRadar standard.
6. Cliquez sur **Enregistrer**.

   L'utilisateur est ajouté à la liste et l'**Etat** indique **EN ATTENTE** jusqu'à ce qu'il soit ajouté. L'état **ACTIF** concerne les utilisateurs actifs.

   Si l'IBMid n'est pas reconnu, l'**Etat** indique **ECHOUE**. Cliquez sur une valeur de nom d'utilisateur, puis sur le lien fourni pour créer un IBMid associé à l'utilisateur ou cliquez sur **Supprimer** pour retirer l'utilisateur.
7. Sur l'onglet **Admin**, cliquez sur **Déployer les modifications**.

Modification des paramètres utilisateur

Vous pouvez modifier le rôle ou le profil d'un utilisateur QRadar on Cloud.

Procédure

1. Ouvrez les paramètres **Admin** et cliquez sur **QRadar on Cloud Self Serve**.
2. Cliquez sur **Gestion des utilisateurs**.
3. Sélectionnez l'utilisateur et cliquez sur **Editer**.
4. Modifiez le rôle ou le profil comme vous le souhaitez, puis cliquez sur **Sauvegarder**.
5. Sur l'onglet **Admin**, cliquez sur **Déployer les modifications**.

Désactivation d'un compte utilisateur

Vous pouvez désactiver l'accès d'un utilisateur à IBM QRadar on Cloud.

Vous ne pouvez pas supprimer un utilisateur existant à l'aide de l'application IBM QRadar on Cloud Self Serve. Pour supprimer des comptes utilisateur, ouvrez un ticket de demande de service. Pour plus d'informations, voir «Eléments de travail QRadar on Cloud nécessitant un ticket de demande de service», à la page 34.

Procédure

1. Ouvrez les paramètres **Admin** et cliquez sur **QRadar on Cloud Self Serve**.
2. Cliquez sur **Gestion des utilisateurs**.
3. Sélectionnez l'utilisateur et cliquez sur **Editer**.
4. Cliquez sur **Désactiver**.
5. Sur l'onglet **Admin**, cliquez sur **Déployer les modifications**.

   Le compte reste à l'**Etat actif**. Mais le **Rôle utilisateur** indique **Désactivé**.

Gestion des accès à la console

Vous devez ajouter les adresses IP de tous les services qui doivent pouvoir accéder à la console IBM QRadar on Cloud.

Pour inclure les adresses IP dans la liste autorisée, ajoutez les valeurs de routage CIDR comprises entre /24 et /32 à l'écran **Allowlist Management** de l'application Self Serve.

Génération d'un nouveau marqueur pour une passerelle de données

Vous devez disposer d'un marqueur valide pour pouvoir installer une passerelle de données pour votre instance IBM QRadar on Cloud. Générez le marqueur à l'aide de l'outil de gestion de marqueurs de la passerelle de données de l'application Self Serve.

Avant de commencer

L'outil **Data Gateway Token Management** affiche les marqueurs en cours d'utilisation ainsi que les marqueurs arrivés à expiration. Il affiche également les marqueurs pouvant être utilisés avec une passerelle de données. Si aucun marqueur n'est disponible, ou que la date d'expiration est trop proche, vous pouvez générer un nouveau marqueur pour votre passerelle de données.

Procédure

1. Ouvrez les paramètres **Admin** et cliquez sur **QRadar on Cloud Self Serve**.
2. Cliquez sur **Data Gateway Token Management**.
3. Entrez l'adresse IP de la passerelle de données dans **Data Gateway Private IP**.
4. Entrez le nombre de jours pendant lequel vous souhaitez que le marqueur soit valide dans **Expires in (days)**.

   14 est le nombre de jours minimum que vous pouvez entrer dans **Expires in (days)**.
5. Cliquez sur **Generate Token**.

   La génération de marqueur peut prendre un certain temps.

   Vous pouvez cliquer sur l'icône de copie pour copier l'URL du marqueur ou du nom d'hôte.

Que faire ensuite

Vous devez veiller à ajouter l'adresse IP de la passerelle de données à la liste autorisée. Cliquez sur **Manage allowlists** dans l'écran **Data Gateway Token Management** pour ajouter la valeur de routage CIDR de la passerelle. Pour plus d'informations, voir «Placement d'une adresse IP sur liste autorisée», à la page 40.

Placement d'une adresse IP sur liste autorisée

Pour placer une adresse IP sur liste autorisée, ajoutez la valeur de routage CIDR sur la page **Allowlist Management**.

Procédure

1. Ouvrez les paramètres **Admin** et cliquez sur **QRadar on Cloud Self Serve**.
2. Cliquez sur **Allowlist Management**.

   La liste affiche toutes vos valeurs de routage CIDR QRadar on Cloud autorisées.
3. Cliquez sur **Ajouter**.
4. Entrez la valeur de routage CIDR.

   La valeur de routage CIDR doit être comprise entre /24 et /32.

   Les plages de valeurs de routage CIDR privées sont limitées. Vous ne pouvez pas y ajouter de valeurs dupliquées.
5. Cliquez sur **Enregistrer**.
6. Cliquez sur **Soumettre**, puis sur **Confirmer**.

   Lorsque vous cliquez sur **Soumettre**, toutes les modifications apportées dans la table sont mises à jour sur le serveur. Lors de la soumission, les plages d'adresses IP autorisées sont supprimées et la

liste est régénérée. Ce processus peut prendre un certain temps. Si vous devez faire plusieurs modifications, apportez-les toutes avant de cliquer sur **Soumettre**.

Les options de la table ne sont pas disponibles lors de la soumission.

Si la connexion au serveur est interrompue lors de la soumission, une erreur de serveur interne s'affiche, et vous devez entrer à nouveau les modifications.

L'accès à la console par l'adresse IP placée sur la liste autorisée peut être assez long. Si l'adresse IP ne peut toujours pas accéder à la console après quelques heures, contactez le support IBM.

Modification ou suppression d'une adresse IP placée sur liste autorisée

Vous pouvez mettre à jour l'entrée sur la page **Allowlist Management** si l'adresse IP d'un périphérique a été modifiée. Vous pouvez également supprimer les adresses IP placées sur liste autorisée si vous ne souhaitez plus qu'elles aient accès à la console.

Procédure

1. Ouvrez les paramètres **Admin** et cliquez sur **QRadar on Cloud Self Serve**.
2. Cliquez sur **Allowlist Management**.
3. Cliquez sur **Editer** pour modifier la valeur de votre choix.
4. Effectuez l'une des étapes suivantes.
   - Modifiez la valeur de routage CIDR, puis cliquez sur **Sauvegarder**.
   - Cliquez sur **Supprimer**.

     La table doit comprendre au moins une valeur de routage CIDR. Veillez à ce que la plage de valeurs de routage CIDR contenant votre adresse IP reste dans la table.
5. Cliquez sur **Soumettre**.

Marqueurs de service autorisés

Vous pouvez ajouter et gérer des marqueurs de service autorisé pour votre instance IBM QRadar on Cloud.

L'API RESTful QRadar utilise des services autorisés pour authentifier les appels d'API à la console. Pour plus d'informations sur l'API RESTful, consultez le QRadarGuide de l'API.

Ajout d'un marqueur de service autorisé

Lorsque vous ajoutez un marqueur de service autorisé, vous devez sélectionner un rôle utilisateur et un profil de sécurité. Vous pouvez également entrer la date d'expiration du marqueur.

Procédure

1. Ouvrez les paramètres **Admin** et cliquez sur **QRadar on Cloud Self Serve**.
2. Cliquez sur **Authorized Services Management**.
3. Cliquez sur **Ajouter**.
4. Dans **Nom du service**, entrez un nom pour ce service autorisé.
5. Dans **Rôle utilisateur**, sélectionnez le rôle utilisateur que vous souhaitez affecter à ce service autorisé.

   Les rôles utilisateur affectés à un service autorisé déterminent les fonctions auxquelles ce service peut accéder dans IBM QRadar on Cloud.
6. Dans **Profil de sécurité**, sélectionnez le profil de sécurité que vous souhaitez affecter à ce service autorisé.

   Le profil de sécurité détermine les réseaux et les sources de journal auxquels ce service peut accéder dans IBM QRadar on Cloud.

7. Dans **Date d'expiration**, entrez ou sélectionnez la date à laquelle vous souhaitez que ce service expire. Si aucune date d'expiration n'est requise, sélectionnez **Pas d'expiration**.
8. Cliquez sur **Enregistrer**.
9. Sur l'onglet **Admin**, cliquez sur **Déployer les modifications**.

Suppression d'un marqueur de service autorisé

Si vous n'avez plus besoin d'un marqueur, vous pouvez le supprimer.

Procédure

1. Ouvrez les paramètres **Admin** et cliquez sur **QRadar on Cloud Self Serve**.
2. Cliquez sur **Authorized Services Management**.
3. Cliquez sur le nom du service.

   Cochez les cases **Nom du service**, **Rôle utilisateur** ou **Profil de sécurité** pour filtrer les marqueurs de service autorisé.
4. Cliquez sur **Supprimer**.
5. Sur l'onglet **Admin**, cliquez sur **Déployer les modifications**.

Etat de la passerelle de données

Utilisez l'application QRadar on Cloud Self Serve pour afficher l'état de vos passerelles de données. Vous pouvez afficher les passerelles de données dans votre déploiement QRadar on Cloud. Vous pouvez également afficher les hôtes gérés par le client dans le tableau de bord QRadar.

Lorsque vous vous connectez à QRadar, une icône de nuage apparaît dans la zone **Notifications système**. Toutes les passerelles de données associées sont répertoriées dans la liste sous l'icône de nuage. Si des passerelles de données sont à l'état DOWN, une puce rouge apparaît en regard de l'icône de nuage pour indiquer les problèmes potentiels liés à votre déploiement.

Affichage de l'état de la passerelle de données

Utilisez l'application QRadar on Cloud Self Serve pour afficher l'état de vos passerelles de données.

Procédure

1. Cliquez sur l'icône de nuage pour afficher l'état des passerelles de données connectées à votre déploiement QRadar on Cloud.
2. Pour afficher les détails d'une passerelle de données, cliquez sur les en-têtes UP ou DOWN, puis cliquez sur la passerelle de données.
3. Sur la fenêtre **Deployment Hosts**, dans la colonne **Host Status**, cliquez sur l'icône d'état UNKNOWN **(?)** correspondant à votre passerelle de données.

Demande d'un ensemble de journaux pour votre instance QRadar on Cloud

Les ensembles de journaux sont des groupes de journaux compressés qui contiennent des détails spécifiques à votre déploiement IBM QRadar. Ces informations incluent des noms d'hôte, des adresses IP et des adresses électroniques. Vous pouvez également inclure dans votre ensemble de journaux des journaux d'application provenant de toutes les applications de votre QRadar Console.

Pourquoi et quand exécuter cette tâche

Utilisez l'application QRadar on Cloud Self Serve afin de demander des ensembles de journaux pour votre instance QRadar on Cloud. Sur demande du service clients, vous pouvez inclure des ensembles de

journaux dans vos tickets de demande de service. Seule une demande d'ensemble de journaux peut être émmise à la fois.

Procédure

1. Dans la fenêtre **Log Bundles**, cliquez sur **Request New Log Bundle**.
2. Facultatif : Pour inclure des journaux d'extension d'application dans l'ensemble de journaux, cochez la case **Include App Logs**.
3. Cliquez sur **Soumettre**.

Résultats

Une nouvelle ligne est créée dans la table **Log Bundles** et l'ensemble de journaux passe de l'état **PROCESSING** à l'état **COMPLETED**.

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 IBM 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 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.

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 distribuer ou publier tout ou partie de ces publications ou en faire 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 destinés à collecter l'identifiant de session 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 diverses technologies, y compris celles des cookies, consultez les Points principaux de la Déclaration IBM de confidentialité sur Internet à l'adresse http://www.ibm.com/privacy/fr/fr, la section Cookies, pixels espions et autres technologies de la Déclaration IBM de confidentialité sur Internet à l'adresse http://www.ibm.com/privacy/details/fr/fr.