IBM Security QRadar

Master Console

Version 0.10.0

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations figurant à la section «Remarques», à la page 19.

Table des matières

Avis aux lecteurs canadiens

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

Illustrations

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

Terminologie

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

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

Claviers

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

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

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

Nomenclature

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

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

Brevets

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

Assistance téléphonique

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

Présentation de Master Console

Les administrateurs d'IBM® Security QRadar utilisent la Master Console (console maître) pour afficher les informations d'intégrité et d'autres informations sur les déploiements et les hôtes.

Public visé

Ce guide est destiné à tous les utilisateurs de QRadar chargés d'étudier et de gérer la sécurité réseau. Pour utiliser ces informations, vous devez disposer d'un accès QRadar et de connaissances sur le réseau de votre entreprise et les technologies de mise en réseau.

Documentation technique

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

Pour savoir comment accéder à plus de documentation technique dans la bibliothèque produit QRadar, voir Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Contacter le service clients

Pour plus d'informations sur la façon de contacter le service clients, consultez la note technique Support and Download Technical Note (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

Déclaration de pratiques de sécurité recommandées

La sécurité des systèmes informatiques implique la protection des systèmes et des informations par la prévention par la détection et la réponse aux accès non autorisés depuis l'intérieur ou l'extérieur de votre entreprise. L'accès incorrect peut engendrer la modification, la destruction, le détournement la mauvaise utilisation des informations ou peut engendrer l'endommagement ou la mauvaise utilisation des systèmes, en particulier pour l'utilisation dans les attaques ou autres. Aucun système informatique ou produit ne doit être considéré comme entièrement sécurisé et aucun produit unique, service ou aucune mesure de sécurité ne peut être entièrement efficace dans la prévention d'une utilisation ou d'un accès incorrect. Les systèmes, les produits et les services IBM sont conçus pour s'intégrer à une approche de sécurité complète, qui implique nécessairement des procédures opérationnelles supplémentaires, et peuvent avoir besoin d'autres systèmes, produit ou services pour optimiser leur efficacité. IBM NE GARANTIT EN AUCUN CAS L'IMMUNITE DES SYSTEMES, PRODUITS OU SERVICES NI L'IMMUNITE DE VOTRE ENTREPRISE CONTRE LE COMPORTEMENT MALVEILLANT OU ILLEGAL DE L'UNE DES PARTIES.

Remarque/Commentaire :

L'utilisation de ce programme peut impliquer différents lois ou réglementations, concernant notamment la confidentialité, la protection des données, l'emploi, ainsi que les communications électroniques et le stockage. IBM Security QRadar peut

être utilisé uniquement de façon réglementaire. Le client accepte d'utiliser ce programme conformément aux lois, réglementations et règles en vigueur et veille à s'y conformer. Le détenteur de licence déclare qu'il détiendra ou qu'il a obtenu les agréments, les autorisations ou les licences nécessaires pour une utilisation réglementaire d'IBM Security QRadar.

Master Console

Utilisez Master Console pour surveiller les déploiements de IBM Security QRadar.

Master Console s'avère particulièrement utile dans un environnement de fournisseurs de services de sécurité (MSSP). L'utilisation du tableau de bord permet de surveiller simultanément plusieurs déploiements.

La représentation visuelle des données opérationnelles (utilisation d'UC, activité réseau et disque, utilisateur de mémoire, débits d'événements et de flux, par exemple) simplifie la surveillance de la santé de vos déploiements.

La vue centralisée de gestion des infractions affiche les infractions provenant de l'ensemble des déploiements, par ordre de magnitude. Vous explorez les informations puis vous vous connectez à un déploiement QRadar spécifique afin d'obtenir des informations supplémentaires sur une infraction.

Master Console - Nouveautés pour les utilisateurs

Découvrez les nouvelles fonctionnalités de chaque édition de Master Console.

Nouveautés de Master Console V0.10.0

Master Console V0.10.0 a introduit la connaissance des titulaires et des domaines, les fonctions de recherche et de filtrage dans la liste d'utilisateurs, la conservation des informations basées sur le domaine dans les mises à niveau ultérieures, etc.

Recherche et filtrage d'utilisateurs Master Console

A l'aide de la nouvelle barre de recherche, vous pouvez créer des requêtes basées sur du texte et des zones pour filtrer la liste d'utilisateurs Master Console, qui s'affiche dans la fenêtre **Gestion des utilisateurs**.

 En savoir plus sur le filtrage de la liste d'utilisateurs Master Console...

Connaissance des titulaires et des domaines

Master Console affiche maintenant des informations sur les titulaires et les domaines configurés pour chaque déploiement que vous surveillez. Pour afficher l'événement et les limites de débit de flux pour chaque titulaire, cliquez sur l'onglet **Titulaires** de la page **Hôtes gérés**.

 En savoir plus sur l'affichage des informations sur vos déploiements QRadar...

Amélioration de la gestion des informations sur le domaine dans les mises à niveau ultérieures

Lorsque des fournisseurs d'authentification tiers sont configurés, les mises à niveau Master Console ultérieures conserveront les paramètres du domaine. Pour tirer parti de cette amélioration, vous devez ajouter les informations de domaine au

fichier `shiro.realms` lorsque vous effectuez la mise à niveau vers Master Console V0.10.0 ou lorsque vous configurez un fournisseur d'authentification tiers pour la première fois.

 En savoir plus sur la configuration des fournisseurs d'authentification...

Master Console est installé en utilisant le gestionnaire de package YUM

Master Console est maintenant installé en utilisant la commande YUM (Yellowdog Updater Modified), qui offre des fonctions de vérification des liens de dépendance et de gestion des packages.

 En savoir plus sur l'installation de Master Console...

Amélioration de la validation des données et des messages

Les fenêtres **Ajouter un déploiement**, **Modifier un déploiement** et **Gestion des utilisateurs** repensées offrent une amélioration de la validation des données et des messages d'information lorsque vous gérez les déploiements et les comptes d'utilisateur.

Nouveautés de Master Console version 0.9.1

Master Console version 0.9.1 comporte des mises à jour qui corrigent le débit de mise à jour de la fenêtre Déploiement, et qui garantissent la compatibilité de Master Console avec les dernières versions de IBM Security QRadar.

Nouveautés de Master Console version 0.9.0

Master Console version 0.9.0 introduit la recherche et le filtrage des infractions et supprime la prise en charge de Microsoft Internet Explorer 10.

Recherche et filtrage des infractions

La nouvelle barre de recherche permet de générer des requêtes textuelles et basées sur des zones afin de filtrer les infractions figurant dans a liste consolidée des infractions  En savoir plus...

Mise à jour des navigateurs pris en charge

La prise en charge du navigateur Microsoft Internet Explorer 10 a été abandonnée dans cette édition  En savoir plus...

Nouveautés de Master Console version 0.8.1

Master Console version 0.8.1 introduit la gestion et la prise en charge des utilisateurs locaux pour vos fournisseurs de sécurité Active Directory et LDAP.

Gestion des utilisateurs

Vous pouvez accorder et contrôler les accès des utilisateurs locaux à Master Console. Immédiatement après la mise à niveau vers Master Console version 0.8.1 ou ultérieure, tous les utilisateurs QRadar existants sont migrés vers Master Console en tant qu'utilisateurs locaux. Vous gérez les utilisateurs, notamment en

ajoutant des utilisateurs et en changeant les mots de passe, dans Master Console.

 En savoir plus....

Intégration du fournisseur de sécurité

Vous pouvez utiliser votre infrastructure de sécurité LDAP ou Active Directory existante pour configurer l'authentification utilisateur.  En savoir plus...

Initiation à Master Console

Installez Master Console afin de surveillez la santé et le système de tous les hôtes QRadar de votre déploiement IBM Security QRadar.

Environnements pris en charge

Avant d'installer et d'utiliser Master Console, vérifiez que votre environnement dispose du matériel et des logiciels pris en charge.

Configuration matérielle requise

Master Console s'exécute sur le dispositif QRadar 3105.

Avant que vous installiez Master Console, confirmez que le dispositif virtuel ou physique satisfait les spécifications matérielles suivantes :

Tableau 1. Dispositif QRadar 3105 - Présentation

Description	Valeur
Processeurs	8
Interfaces	Deux interfaces de surveillance réseau 10/100/1000 Base-T Une interface de gestion 10/100/1000 Base-T QRadar Une interface de module de gestion intégrée 10/100 Base-T Integrated Management Module 2 ports SFP + 10 Go par seconde
Mémoire	RDIMM, 64 Go (8 x 8 Go) 1600 MHz
Stockage	9 x 8,9 cm (3,5"), 1 To, 7 200 tr/min, NL SAS, 9 To au total, 6,2 To utilisables (Raid 5)
Alimentation électrique	Alimentation CA 750 W double redondant
Dimensions	74,9 cm (29,5") (P) x 44,9 cm (17,7") (L) x 6 cm (2,4") (H)

Configuration logicielle requise

Pour héberger Master Console, vous devez installer IBM Security QRadar avec la clé d'activation 8500 (3L0C3S-2M0F3Q-6B1N0W-5N737F). Vous n'avez pas besoin d'une clé de licence distincte.

Vous pouvez utiliser Master Console pour surveiller un déploiement QRadar Log Manager, mais la vue centralisée de gestion des infractions est vide. Cette vue affiche uniquement les infractions pour les systèmes surveillant les infractions, par exemple QRadar SIEM.

La version QRadar requise pour héberger Master Console peut être différente des versions QRadar que Master Console peut surveiller. Avant d'installer Master Console, passez en revue la configuration logicielle requise dans le tableau ci-après.

Tableau 2. Configuration logicielle requise pour Master Console

Version de Master Console	**Installation sur**	**Surveille**	**Navigateurs pris en charge**
Master Console v0.10.0*	QRadar V7.2.7	QRadar version 7.2.6 ou version ultérieure	Microsoft Internet Explorer 11 Mozilla Firefox 38 Extended Support Release Google Chrome (version la plus récente)
Master Console v0.9.1	QRadar version 7.2.6 ou version ultérieure	QRadar version 7.2.6 ou version ultérieure	Microsoft Internet Explorer 11 Mozilla Firefox 38 Extended Support Release Google Chrome (version la plus récente)
Master Console version 0.9.0	QRadar version 7.2.6	QRadar version 7.2.6 ou version ultérieure	Microsoft Internet Explorer 11 Mozilla Firefox 38 Extended Support Release Google Chrome (version la plus récente)
Master Console version 0.8.1	QRadar version 7.2.5 ou version 7.2.6	QRadar version 7.2.5 ou version 7.2.6	Microsoft Internet Explorer 11 Microsoft Internet Explorer 10 Mozilla Firefox 38 Extended Support Release Google Chrome (version la plus récente)
* Support produit limité à la dernière version publiée de Master Console.			

Pour plus d'informations sur l'installation du composant QRadar, reportez-vous au document *IBM Security QRadar Installation Guide*.

Installation de Master Console

Master Console est automatiquement installé quand IBM Security QRadar version 7.2.5 ou une version ultérieure est installé avec la clé d'activation 8500 (3L0C3S-2M0F3Q-6B1N0W-5N737F). Ce composant ne requiert pas de clé de licence distincte. Pour plus d'informations sur l'installation du composant QRadar, reportez-vous au document *IBM Security QRadar Installation Guide*.

Vous pouvez télécharger les fonctionnalités et améliorations de Master Console les plus récentes depuis IBM Fix Central.

Avant de commencer

Assurez-vous que le dispositif sur lequel vous effectuez l'installation satisfait les spécifications matérielles minimales requises. Pour plus d'informations, voir «Environnements pris en charge», à la page 3.

Vous devez disposer d'un logiciel de copie de fichier tel que WinSCP pour copier le fichier du groupe de correctifs Master Console depuis votre système local vers le dispositif QRadar.

Pourquoi et quand exécuter cette tâche

La première fois que vous effectuez la mise à jour vers Master Console version 0.8.1 ou ultérieure, le processus de mise à jour importe les utilisateurs depuis la console QRadar. L'importation écrase les mots de passe de tous les utilisateurs Master Console existants, y compris l'administrateur, et les définit sur une même valeur (définie dans la console QRadar). Le processus d'importation a lieu une seule fois. Les mises à jour suivantes vers Master Console n'importent pas les utilisateurs et n'écrasent pas les mots de passe.

Procédure

1. Téléchargez le groupe de correctifs de Master Console depuis Fix Central (http://www.ibm.com/support/fixcentral).
2. Utilisez un logiciel type WinSCP pour copier le groupe de correctifs Master Console sur l'hôte QRadar où est installé Master Console.
3. Utilisez le protocole SSH pour vous connecter en tant qu'utilisateur root à l'hôte QRadar sur lequel vous avez copié le correctif logiciel Master Console.
4. Arrêtez le service Tomcat en entrant la commande suivante :

   ```
   service tomcat stop
   ```

5. Dans la fenêtre de console pour le dispositif QRadar, installez Master Console en entrant la commande suivante :

   ```
   yum -y install masterconsole-<version#>.rpm
   ```

6. Redémarrez le service Tomcat en entrant la commande suivante :

   ```
   service tomcat start
   ```

Résultats

Master Console est installé et les services sur le dispositif QRadar sont redémarrés.

Ouverture de Master Console

Quand Master Console est installé, utilisez l'adresse IP de la console QRadar pour ouvrir Master Console.

Avant de commencer

Assurez-vous que QRadar est installé avec la clé d'activation 8500 (3L0C3S-2M0F3Q-6B1N0W-5N737F).

Pourquoi et quand exécuter cette tâche

La première fois que vous effectuez la mise à jour vers Master Console version 0.8.1 ou ultérieure, le processus de mise à jour importe les utilisateurs depuis la console QRadar. L'importation écrase les mots de passe de tous les utilisateurs Master Console existants, y compris l'administrateur, et les définit sur une même valeur (définie dans la console QRadar). Le processus d'importation a lieu une seule fois. Les mises à jour suivantes vers Master Console n'importent pas les utilisateurs et n'écrasent pas les mots de passe.

Procédure

1. Ouvrez un navigateur Web et entrez l'URL suivante :

   `https://`*`adresse_IP`*

   où *adresse_IP* est l'adresse IP de l'hôte QRadar sur lequel vous avez installé Master Console.
2. Connectez-vous à Master Console.

   Si vous êtes connecté à Master Console pour la première fois, utilisez le compte admin et le mot de passe root sur le système.

Que faire ensuite

Pour ajouter des déploiements QRadar à surveiller, voir «Ajout de déploiements à Master Console».

Création d'un jeton d'autorisation pour Master Console

Vous devez créer un jeton d'autorisation afin que Master Console puisse se connecter à vos déploiements IBM Security QRadar.

Procédure

1. Dans l'onglet **Admin**, sous **Configuration du système**, cliquez sur **Services autorisés**.
2. Cliquez sur **Ajouter un service autorisé** et configurez les paramètres.
   a. Dans la zone **Nom du service**, indiquez un nom pour le service. Le nom peut comporter 255 caractères maximum.
   b. Dans le menu **Rôle utilisateur**, sélectionnez **Admin**.

      Les rôles utilisateur affectés à un service autorisé déterminent les fonctions auxquelles peut accéder ce service dans QRadar. Le jeton d'autorisation pour Master Console doit avoir le rôle utilisateur **Admin**.
   c. Dans le menu **Profil de sécurité**, sélectionnez **Admin**.

      Le profil de sécurité détermine les réseaux et les sources de journal auxquels ce service peut accéder dans QRadar. Le jeton d'autorisation pour Master Console doit avoir le profil de sécurité **Admin**.
   d. Dans la zone **Date d'expiration**, sélectionnez une date à laquelle vous voulez que le jeton arrive à expiration ou bien cochez la case **Pas d'expiration**.
3. Cliquez sur **Créer un service** et enregistrez la valeur du jeton.

Ajout de déploiements à Master Console

Un administrateur Master Console doit ajouter les déploiements IBM Security QRadar que vous souhaitez surveiller.

Avant de commencer

- Vous devez avoir un jeton d'autorisation. Pour plus d'informations, voir «Création d'un jeton d'autorisation pour Master Console», à la page 6.
- Si votre organisation doit utiliser le SSL sécurisé, assurez-vous que le certificat SSL non accrédité est remplacé par un certificat accrédité ou auto-signé sur tous les déploiements QRadar que vous souhaitez surveiller dans Master Console.
- Seuls les administrateurs QRadar peuvent ajouter, éditer ou retirer des déploiements QRadar dans Master Console.

Procédure

1. Pour ajouter un déploiement, cliquez sur l'icône d'ajout (**+**) dans le coin supérieur droit de l'écran.
2. Entrez un nom de déploiement.
3. Entrez l'adresse IP ou le nom d'hôte de la console.
4. Entrez le jeton d'autorisation.
5. Cliquez sur **Add Deployment** (ajouter le déploiement).
6. Si vous ajoutez un déploiement avec SSL non sécurisé et que votre entreprise n'exige pas de protocole SSL sécurisé, sélectionnez la case à cocher **Ignore insecure SSL** (ignorer le SSL non sécurisé) puis cliquez sur **Submit** (soumettre).

Surveillance des déploiements

Master Console affiche une représentation graphique, appelée *carte de déploiement*, de la santé et des données opérationnelles de chaque déploiement IBM Security QRadar qui lui est connecté.

Vous pouvez afficher les cartes de déploiement sur la page Deployments by Severity (déploiements par gravité). Pour vous aider à rapidement déterminer quels déploiements nécessitent votre attention, les cartes sont triées en fonction de groupes : **Critical** (critique), **Warning** (avertissement) et **Healthy** (en bonne santé).

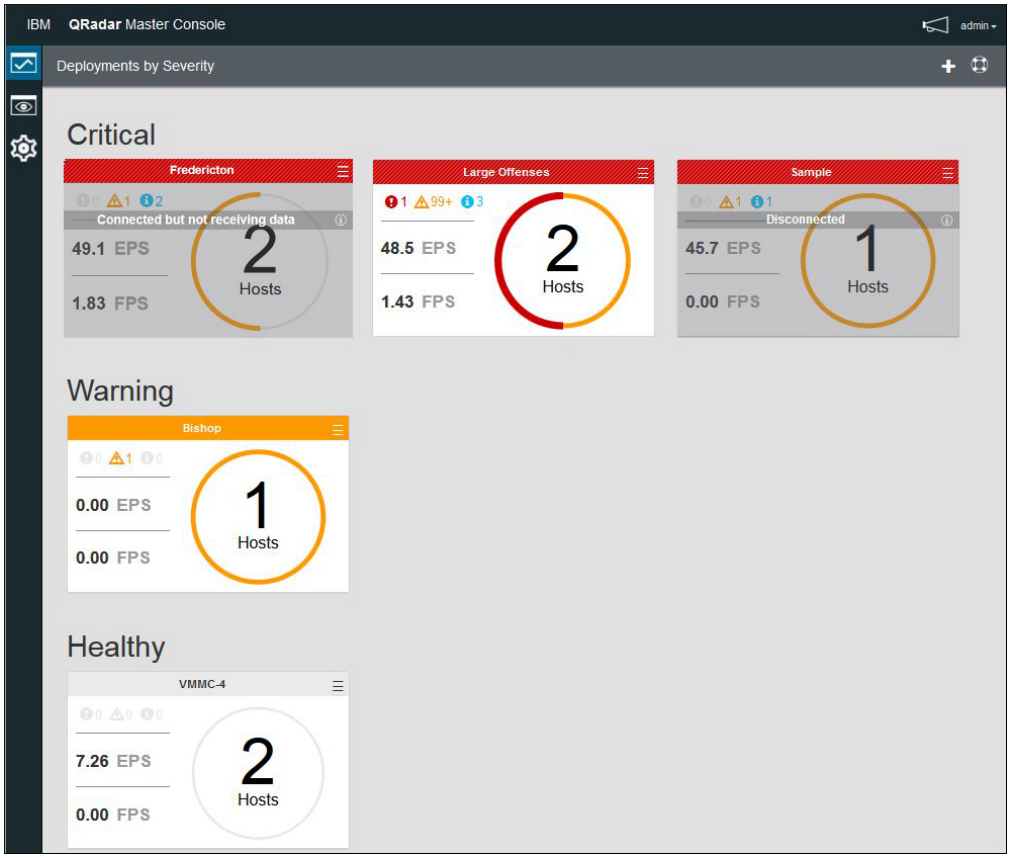

Figure 1. Cartes de déploiement dans Master Console

Chaque carte de déploiement affiche les informations suivantes :

- Nombre d'hôtes gérés dans le déploiement.
- Statut du déploiement, représenté par les couleurs autour du cercle. Si, par exemple, votre déploiement comporte deux hôtes gérés et que l'un d'entre eux a un statut critique, la moitié du cercle autour du nombre 2 est rouge.
- Nombre de notifications système de type Erreur critique, Avertissement et Information dans les 15 dernières minutes
- Débits d'événements et de flux, qui sont mesurés sous forme de moyenne sur les 15 dernières minutes.

Quand Master Console ne peut pas se connecter à un déploiement, la carte correspondante indique **Disconnected** (déconnecté). Ce statut peut signifier que le déploiement est hors tension. Quand un déploiement figure comme **Connected but not receiving data** (connecté mais ne recevant pas de données), le jeton d'autorisation a peut-être été révoqué ou est arrivé à expiration.

Vous pouvez exécuter les actions suivantes sur la carte de déploiement :

- Cliquer sur la carte de déploiement pour ouvrir la vue **Managed Hosts** (hôtes gérés).
- Cliquer sur l'icône de menu 'hamburger'  pour éditer les détails de déploiement ou pour déconnecter le déploiement de Master Console.

- Quand un déploiement est **Disconnected** (déconnecté) ou **Connected but not receiving data**, cliquez sur l'icône d'information de la carte de déploiement pour voir quand des données ont été reçues pour la dernière fois.

Surveillance des hôtes gérés

Utilisez la page Managed Hosts (hôtes gérés) pour voir les notifications système et les statistiques d'utilisation de la mémoire système et des UC pour tous les hôtes gérés connectés à un déploiement unique.

Pour vous aider à rapidement déterminer quels hôtes gérés nécessitent une certaine attention, la partie supérieure de la carte des hôtes gérés comporte un code couleurs : le rouge indique un statut **critique**, le jaune un statut d'**avertissement** et le gris correspond à un statut de **bonne santé**.

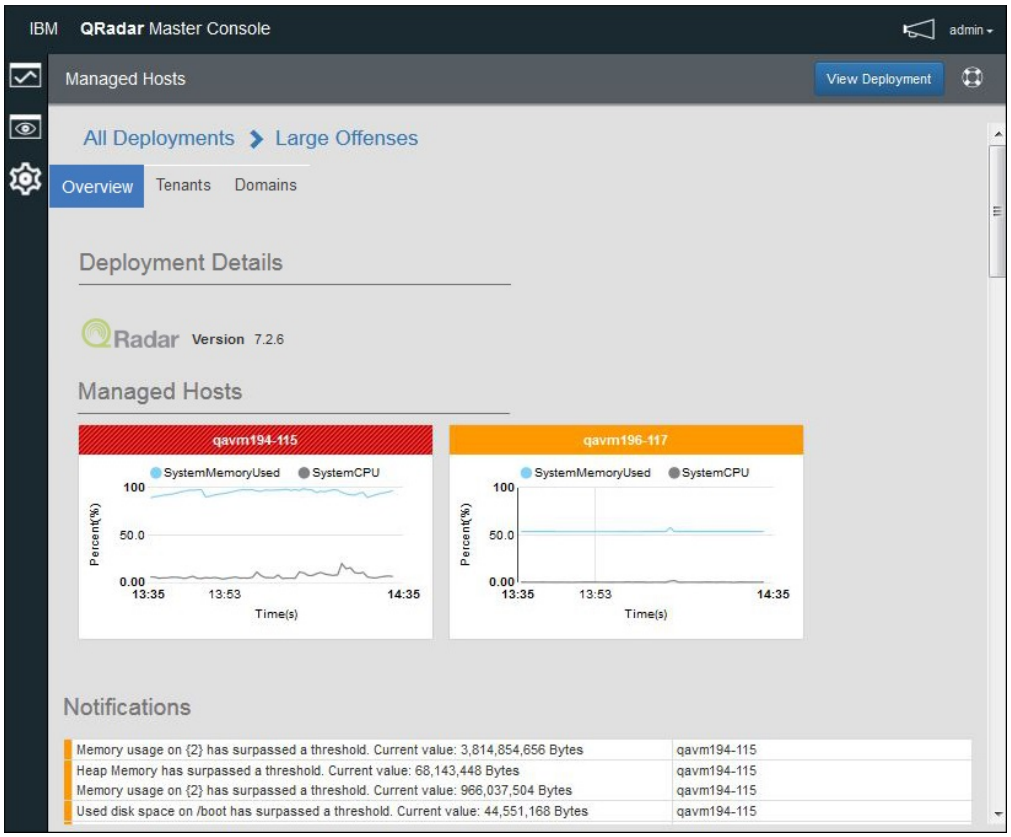

Figure 2. Page des hôtes gérés dans Master Console

Procédure

1. Pour afficher la page Managed Hosts (hôtes gérés), cliquez sur la carte de déploiement de la page Deployments by Severity (déploiements par gravité).
2. La page Managed Hosts permet également d'exécuter les actions suivantes :
   a. Cliquez sur **View Deployment** (afficher le déploiement) pour vous connecter à un déploiement QRadar.
   b. Pour afficher des informations sur les titulaires et les domaines configurés dans le déploiement, cliquez sur les onglets **Titulaires** et **Domaines**.
   c. Déplacez la souris au dessus des graphiques d'hôtes gérés pour afficher davantage d'informations sur les métriques de graphique.

d. Pour masquer une métrique du graphique d'hôtes gérés, cliquez sur l'icône de couleur correspondante. Ainsi, pour masquer la métrique **SystemCPU**, cliquez sur le cercle gris sous **System CPU** (UC système).

e. Pour afficher les données opérationnelles de l'hôte telles que l'utilisation d'UC et de mémoire, les opérations de lecture et d'écriture pour le réseau et le disque, ou encore les débits d'événements et de flux, cliquez sur la carte d'hôte géré.

Surveillance des infractions

Utilisez Master Console pour surveiller les infractions provenant de plusieurs déploiements IBM Security QRadar. Les infractions de tous les déploiements sont affichées dans une liste unique, les plus importantes figurant en haut.

Pourquoi et quand exécuter cette tâche

Les cartes d'infraction sont triées dans l'ordre suivant : magnitude, déploiement, et date/heure de dernière mise à jour.

La *magnitude* est un indicateur de l'importance relative de l'infraction. Elle est calculée d'après les valeurs de pertinence, gravité et crédibilité.

- La *pertinence* détermine l'impact de l'infraction sur votre réseau. Par exemple, si un port est ouvert, la pertinence est élevée.
- La *crédibilité* indique l'intégrité de l'infraction telle que déterminée par le classement de crédibilité configuré dans la source de journal. La crédibilité s'accroît lorsque plusieurs sources signalent le même événement.
- La *gravité* indique le niveau de menace créé par une source d'infraction par rapport à la préparation de la destination à l'attaque.

La magnitude est exprimée par une valeur numérique qui détermine la couleur de la carte associée à l'infraction. Déplacez la souris au dessus de la barre de couleur de la carte d'infraction pour afficher le chiffre correspondant à la magnitude.

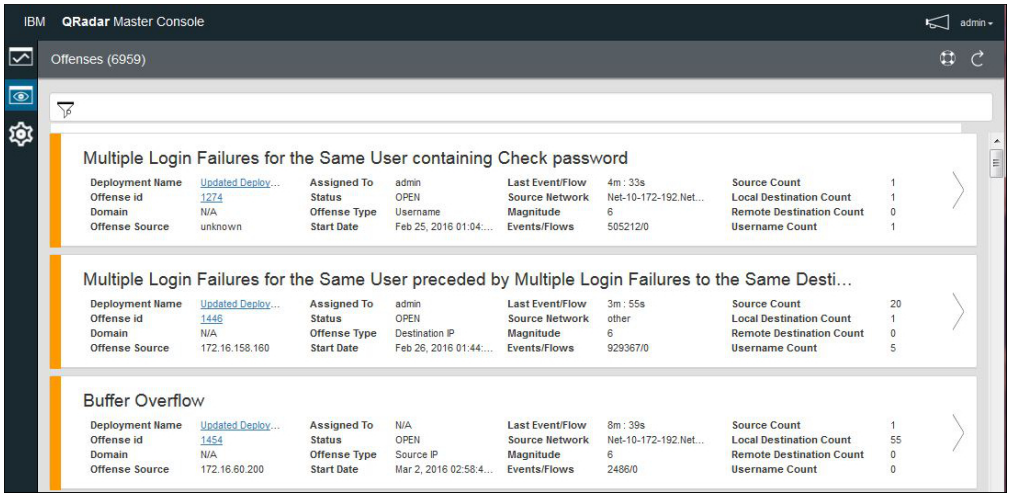

Figure 3. Cartes de déploiement dans Master Console

La carte d'infraction affiche les informations suivantes :

Tableau 3. Informations sur les cartes des infractions

Paramètre	Description
Offense ID (ID infraction)	Lien vers le récapitulatif d'infraction.
Source de l'infraction	Les informations sur la source d'infraction varient en fonction du type d'infraction. Si, par exemple, **Offense Type** (type d'infraction) a pour valeur Source IP, la zone **Offense Source** (source de l'infraction) affiche l'adresse IP de la source de l'événement à l'origine de l'infraction. Si **Offense Type** a pour valeur Destination IP, la zone **Offense Source** affiche l'adresse IP de destination de l'événement.
Assigned To (affecté à)	Si aucun utilisateur n'est affecté à l'examen de l'infraction, vous pouvez affecter des infractions à des utilisateurs dans QRadar. Pour plus d'informations sur l'affectation d'infractions à QRadar, reportez-vous au document *IBM Security QRadar Users Guide*.
Status	Par défaut, le filtre affiche uniquement les infractions ouvertes.
Offense Type (type d'infraction)	Déterminé par la règle ayant créé l'infraction. Par exemple, si le type d'infraction correspond à l'événement de la source du journal (**Log source event**), la règle qui a généré l'infraction met en corrélation les événements basés sur l'unité qui a détecté l'événement.
Start Date (date de début)	Indique la date et l'heure du premier événement ou flux associé à l'infraction.
Last Event/Flow (dernier événement/flux)	Indique le temps écoulé depuis que le dernier événement ou flux a été observé pour cette infraction, catégorie, adresse IP source ou adresse IP de destination.
Source Network (réseau source)	Indique le réseau du périphérique qui a tenté de violer la sécurité d'un composant de votre réseau.
Event/Flow (événement/flux)	Indique le nombre d'événements ou de flux associés à l'adresse IP source, l'adresse IP de destination, le nom d'événement, le nom d'utilisateur, l'adresse MAC, la source de journal, le nom d'hôte, le port, la source de journal, l'adresse ASN, l'adresse IPv6, la règle ASN, l'application, le réseau ou la catégorie.
Source Count (nombre de sources)	Indique le nombre d'adresses IP source associées aux infractions dans la catégorie. Si une adresse IP source est associée à des infractions figurant dans cinq catégories de bas niveau différentes, l'adresse IP source n'est comptée qu'une seule fois.

Procédure

1. Ouvrez Master Console et cliquez sur l'icône d'infraction  .
2. Cliquez sur le lien en forme de flèche dans la carte d'infraction pour vous connecter au déploiement et ouvrez le récapitulatif d'infraction.
3. Pour afficher les infractions masquées ou fermées, cliquez sur l'icône de filtre  et sélectionnez les cases à cocher des infractions que vous souhaitez voir. Le nombre d'infractions correspondant au filtre appliqué s'affiche dans l'en-tête de page.
4. Cliquez sur l'icône d'actualisation pour mettre à jour les infractions répertoriées.

Tâches associées:

«Ouverture de Master Console», à la page 5
Quand Master Console est installé, utilisez l'adresse IP de la console QRadar pour ouvrir Master Console.

Filtrage de la liste des infractions

Créez une requête de recherche pour filtrer les cartes d'infraction qui figurent dans la liste consolidée des infractions. Vous pouvez, par exemple, filtrer la liste des infractions de sorte à afficher uniquement les infractions affectées à un individu ou de sorte à afficher uniquement les infractions d'un déploiement unique.

Pourquoi et quand exécuter cette tâche

Vous utilisez la zone de recherche en texte intégral dans la vue **Offenses** (infractions) afin de rapidement trouver les infractions qui sont des correspondances proches ou exactes et à les afficher sous forme de classement. Vous pouvez créer une requête pour rechercher un mot unique, une partie d'un mot ou plusieurs mots selon un ordre précis ou sans classement. Vous pouvez rechercher des données sur l'ensemble des zones de données de la carte d'infraction, ou bien limiter la recherche en spécifiant l'identificateur en fonction duquel vous souhaitez effectuer la recherche.

La fonction de recherche en texte intégral est basée sur le moteur de recherche Apache Lucene. Les recherches ne prennent pas en compte la distinction majuscules/minuscules. Pour rechercher en utilisant un caractère générique unique, utilisez le symbole `?`. Pour rechercher en utilisant plusieurs caractères génériques, utilisez le symbole `*`.

Vous pouvez limiter la recherche en indiquant la zone de la carte d'infraction sur laquelle effectuer la recherche. Le tableau suivant montre les identificateurs de zone pour les zones de la carte d'infraction.

Tableau 4. Identificateurs de zone pour la recherche de données sur la carte d'infraction

Description des cartes d'infraction	Identificateur de zone
Offense Description (description de l'infraction)	description
Deployment name (nom du déploiement)	deployment_name
Offense ID (ID infraction)	offense_id
Domain	domain_id
Offense source (source de l'infraction)	offense_source
Assigned to (affectée à)	assigned_to
Status (statut)	status
Offense type (type d'infraction)	offense_type Vous ne pouvez pas utiliser de caractère générique pour une recherche sur `offense_type`. Vous devez indiquer une correspondance exacte de texte dans la requête.
Start date (date de début)	start_time
Last Event/Flow (dernier événement/flux)	last_updated_time
Source Network (réseau source)	source_network
Magnitude	magnitude

Tableau 4. Identificateurs de zone pour la recherche de données sur la carte d'infraction (suite)

Description des cartes d'infraction	Identificateur de zone
Events/Flows (événements/flux)	event_count flow_count
Source Count (nombre de sources)	source_count
Local Destination Count (nombre de destinations locales)	local_destination_count
Remote Destination Count (nombre de destinations distantes)	remote_destination_count
Username Count (nombre de noms d'utilisateur)	username_count

Procédure

1. Cliquez sur l'icône d'infraction  .
2. Dans la zone de recherche, entrez la requête de recherche pour le texte à rechercher.
   - Pour rechercher les données figurant dans la carte d'infraction, entrez le texte dans la zone de recherche.
   - Pour rechercher des données d'une zone spécifique, entrez l'identificateur de la zone suivi d'un signe deux-points puis du terme que vous recherchez.
   - Pour mettre en échappement un caractère spécial, utilisez \ avant le caractère dans votre requête de recherche :

     `+ - && || ! ( ) { } [ ] ^ " ~ * ? : \`

     Exemples de requête de recherche :

     Le tableau suivant montre des exemples des requêtes que vous pouvez utiliser pour effectuer une recherche sur les données d'une carte d'infraction.

Tableau 5. Expressions de recherche Master Console

Description	Requête de recherche
Recherche les infractions pour lesquelles `text` ou `test` figure dans l'une des zones.	`te?t`
Recherche les infractions contenant `test`, `tests` ou `tester`.	`test*`
Recherche les infractions pour lesquelles `password` figure dans une zone.	`*password*`
Recherche les infractions pour lesquelles une évaluation de magnitude est équivalente à 2, 3 ou 4.	`magnitude:[2 to 4]`
Recherche les infractions pour lesquelles une évaluation de magnitude équivaut à 3 ou 5.	`magnitude:(3 OR 5)`
Recherche les infractions pour lesquelles le type d'infraction (Offense Type) est égal à `Event Name` (nom de l'événement).	`offense_type: "Event Name"`

Tableau 5. Expressions de recherche Master Console (suite)

Description	Requête de recherche
Recherche les infractions mises à jour au cours des 10 derniers jours à compter de la date du jour.	`last_update_time:[NOW-10DAYS to NOW]`
Recherche les infractions du déploiement `Bishop` avec une magnitude de 3.	`deployment_name:Bishop AND magnitude:3`

3. Pour afficher les infractions masquées ou fermées, cliquez sur l'icône de filtre  et sélectionnez les cases à cocher des infractions que vous souhaitez voir.
   Le nombre d'infractions correspondant au filtre appliqué s'affiche dans l'en-tête de page.

Gestion des utilisateurs

Les utilisateurs de la console maître sont directement gérés dans Master Console.

La première fois que vous effectuez la mise à jour vers Master Console version 0.8.1 ou ultérieure, la mise à jour importe les utilisateurs depuis la console QRadar. Le processus d'importation a lieu une seule fois. Les mises à jour suivantes vers Master Console n'importent pas les utilisateurs. Une fois l'importation initiale effectuée, tous les comptes utilisateur sont gérés directement depuis Master Console.

Ajout d'un utilisateur local

Une fois Master Console installé et mis à jour vers la version la plus récente, les administrateurs ajoutent les nouveaux utilisateurs directement dans Master Console.

Procédure

1. Cliquez sur l'icône des paramètres  .
2. Cliquez sur **User Management** (gestion des utilisateurs).
3. Dans le coin supérieur droit de la fenêtre User Management, cliquez sur l'icône d'ajout (+) pour ouvrir la fenêtre Create user (créer un utilisateur).
4. Entrez les informations concernant le nouvel utilisateur.
5. Si le nouvel utilisateur est un administrateur, sélectionnez la case à cocher **Security Admin**.
6. Cliquez sur **Create User**.

Modification des paramètres utilisateur

Changez des paramètres, tels que les mots de passe utilisateur, d'un utilisateur local dans Master Console.

Pourquoi et quand exécuter cette tâche

Les mots de passe d'utilisateur local qui sont changés dans IBM Security QRadar ne sont pas automatiquement appliqués dans Master Console. Vous devez éditer le paramètre utilisateur et changer le mot de passe dans Master Console.

Vous ne pouvez pas changer les mots de passe LDAP et Active Directory dans Master Console.

Procédure

1. Cliquez sur l'icône des paramètres  .
2. Cliquez sur **User Management** (gestion des utilisateurs).
3. Sur la carte de l'utilisateur à éditer, cliquez sur l'icône de menu 'hamburger'  .
4. Sélectionnez **Edit User** (éditer l'utilisateur).
5. Modifiez les informations utilisateur dans la fenêtre Edit User.
6. Cliquez sur **Edit User** pour sauvegarder vos modifications.

Retrait d'un utilisateur local

Si l'utilisateur n'a plus besoin d'un accès, retirez l'utilisateur local de Master Console.

Procédure

1. Cliquez sur l'icône des paramètres  .
2. Cliquez sur **User Management** (gestion des utilisateurs) pour afficher les cartes de tous les utilisateurs.
3. Sur la carte de l'utilisateur à éditer, cliquez sur l'icône de menu 'hamburger'  .
4. Sélectionnez **Remove User** (retirer l'utilisateur).
5. Dans la fenêtre de confirmation, cliquez sur **Remove User**.

Filtrage de la liste d'utilisateurs

Créez une requête de recherche pour filtrer la liste d'utilisateurs Master Console qui s'affiche dans la page Gestion des utilisateurs. Par exemple, vous pouvez filtrer la liste d'utilisateurs pour n'afficher que les utilisateurs actifs ou que les utilisateurs disposant d'un profil de sécurité Administrateur.

Pourquoi et quand exécuter cette tâche

Vous utilisez la zone de recherche en texte intégral dans la page Gestion des utilisateurs pour rechercher rapidement les utilisateurs les plus proches ou les correspondances exactes des critères de recherche. La fonction de recherche en texte intégral est basée sur le moteur de recherche Apache Lucene. Pour effectuer une recherche en utilisant un caractère générique, utilisez un point d'interrogation (`?`). Pour effectuer une rechercher en utilisant plusieurs caractères génériques, utilisez un astérisque (`*`). Vous pouvez affiner la recherche en spécifiant la zone d'utilisateur à utiliser pour la rechercher.

Procédure

1. Cliquez sur l'icône des paramètres  .
2. Cliquez sur **User Management** (gestion des utilisateurs).

3. Dans la zone de recherche, entrez la requête de recherche pour le texte à rechercher.
   - Pour rechercher du texte libre, entrez le texte dans la zone de recherche. Vous devez utiliser des mots entiers dans une recherche libre. Vous ne pouvez pas utiliser de mots partiels ou de caractères génériques.
   - Pour chercher des données dans une zone spécifique, entrez l'identificateur de zone, suivi de deux points (:), puis entrez le terme recherché.

   Exemples de requête de recherche :

   Le tableau ci-dessous contient des exemples de requêtes que vous pouvez utiliser pour chercher des données utilisateur :

Tableau 6. Expressions de recherche de données utilisateur

Description	Chaîne recherchée
Recherche de texte dans la zone **Nom d'utilisateur**.	`name:John`
Recherche d'un nom de connexion unique. Les recherches dans cette zone dépendent des minuscules/majuscules.	`login:Coop1`
Recherche d'une adresse électronique. Vous devez indiquer l'adresse électronique intégrale. Vous ne pouvez pas effectuer une recherche sur une adresse électronique partielle.	`email:coop1@ca.ibm.com`
Recherche d'utilisateurs actifs actuellement sur le système.	`status:ACTIVE`
Recherche de tous les utilisateurs disposant de droits d'administrateur.	`role_name:admin`
Recherche d'utilisateurs dont le profil a été modifié au cours des 14 derniers jours.	`last_modified:[NOW-14DAYS TO NOW]`

Configuration de l'authentification Active Directory et LDAP dans Master Console

Pour configurer un fournisseur d'authentification Microsoft Active Directory ou LDAP pour la première fois, vous devez ajouter les informations de domaine au fichier `/opt/qradar/masterconsole/conf/shiro.realms`.

Si vous avez effectué dernièrement une mise à niveau vers Master Console V0.10.0, vous devez copier manuellement les informations de domaine du fichier de sauvegarde `shiro.ini` vers le fichier `/opt/qradar/masterconsole/conf/shiro.realms`. Les informations de domaine sont conservées pour les mises à niveau ultérieures vers Master Console.

Avant de commencer

Vérifiez que le fichier de sauvegarde `shiro.ini.<timestamp>` existe dans le répertoire `/opt/qradar/masterconsole/conf/`. Si le fichier de sauvegarde n'existe pas, créez-le.

Examinez la configuration sur votre serveur d'authentification. En fonction du type de fournisseur d'authentification que vous configurez, vous pouvez avoir besoin de fournir les valeurs de paramètre suivantes :

Tableau 7. Descriptions des paramètres d'authentification

Paramètre	Description
`searchBase`	Racine du répertoire Active Directory ou LDAP dans lequel les utilisateurs sont organisés.
`searchFilter`	Permet de rechercher le contexte de l'utilisateur Active Directory ou LDAP. Le compte est une classe d'objet par défaut utilisée par la plupart des serveurs, mais cette entrée varie en fonction de la configuration de serveur Active Directory ou LDAP spécifique.
`groupAttribute`	Identifie les groupes d'utilisateurs auxquels appartient l'utilisateur Active Directory ou LDAP.
`groupRolesMap`	Mappe des groupes Active Directory ou LDAP vers des rôles Apache Shiro.
`userDnTemplate`	Modèle de nom distinctif qui extrait un utilisateur du serveur Active Directory ou LDAP.
`contextFactory.url`	Numéro de port et adresse IP du serveur Active Directory ou LDAP.
`principalSuffix`	Indique un suffixe principal afin de simplifier les informations de connexion que les utilisateurs doivent spécifier. Ainsi, au lieu de `username@this.is.my.long.domain.name.in.canada.com`, vous pouvez créer un suffixe principal utilisateur appelé `canada`, et les utilisateurs pourront entrer `username@canada`.

Procédure

1. Modifiez le répertoire pour utiliser le répertoire `/opt/qradar/masterconsole/conf/`.
2. Créez une copie du fichier `shiro.realms` :

   ```
   cp shiro.realms.default shiro.realms
   ```

3. Ouvrez le fichier `shiro.realms`.
4. Pour configurer Microsoft Active Directory, procédez comme suit.
   a. Recherchez la section suivante et remplacez les exemples de valeur par les valeurs de votre environnement d'authentification :

   ```
   # ----------------------------------------------------------------------------
   # following section is for configuring ActiveDirectory realm. Replace example
   # values before add to securityManager.realm
   # ----------------------------------------------------------------------------
   adRealm = org.apache.shiro.realm.activedirectory.ActiveDirectoryRealm
   adRealm.url = ldap://{ad_server}:389
   adRealm.groupRolesMap = "CN=the_users,CN=Users,DC=department,DC=company,DC=com":"admin"
   adRealm.searchBase = "DC=department,DC=company,DC=com"
   adRealm.systemUsername= user_name
   adRealm.systemPassword= password
   adRealm.principalSuffix= @company.com
   ```

   b. Ajoutez `$adRealm` à l'entrée `securityManager.realms` :

   ```
   securityManager.realms = $localRealm, $adRealm
   ```

5. Pour configurer LDAP, procédez comme suit.
   a. Recherchez la section suivante et remplacez les exemples de valeur par les valeurs de votre environnement d'authentification :

```
#-------------------------------------------------------------------------
# following section is for configuring OpenLdap realm. Replace example
# values before add to securityManager.realm
#-------------------------------------------------------------------------
ldapRealm = com.ibm.si.mc.security.shiro.realm.LdapRealm
ldapRealm.searchBase = "dc=company,dc=com"
ldapRealm.searchFilter = (&(objectClass=account)(uid={0}))
ldapRealm.groupAttribute = ou
ldapRealm.groupRolesMap = "Manager":"admin"
ldapRealm.userDnTemplate = uid={0},dc=company,dc=com
ldapRealm.contextFactory.url = ldap://{ldap_server}:389
```

b. Ajoutez `$ldapRealm` à l'entrée `securityManager.realms` :

   ```
   securityManager.realms = $localRealm, $ldapRealm
   ```

6. Enregistrez le fichier `/opt/qradar/masterconsole/conf/shiro.realms`.
7. Entrez la commande ci-dessous pour ajouter les informations de domaine au fichier shiro.ini :

   ```
   /opt/qradar/masterconsole/bin/generateShiroIni.py
   ```

8. Redémarrez le serveur tomcat en utilisant la commande suivante :

   ```
   service tomcat restart
   ```

Que faire ensuite

Testez la configuration en vous connectant à Master Console à l'aide d'une authentification Microsoft Active Directory ou LDAP.

Remarques

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

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

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

Pour le Canada, veuillez adresser votre courrier à :

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

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

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

LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU IMPLICITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES INFORMATIONS EN CAS DE CONTREFAÇON AINSI QU'EN CAS DE 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.

Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation aux Etats-Unis et/ou dans certains autres pays.

Dispositions relatives à la documentation du produit

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

Applicabilité

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

Utilisation personnelle

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

Utilisation commerciale

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

Droits

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

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

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

IBM N'OCTROIE AUCUNE GARANTIE SUR LE CONTENU DE CES PUBLICATIONS. LE PRESENT DOCUMENT EST LIVRE EN L'ETAT SANS AUCUNE GARANTIE EXPLICITE OU TACITE. IBM DECLINE NOTAMMENT TOUTE RESPONSABILITE RELATIVE A CES PUBLICATIONS EN CAS DE

CONTREFAÇON AINSI QU'EN CAS DE DEFAUT D'APTITUDE A L'EXECUTION D'UN TRAVAIL DONNE.

Déclaration IBM de confidentialité en ligne

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

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

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

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