IBM Security QRadar Incident Forensics
Version 7.3.1

Guide d'utilisation de QRadar Packet Capture

Important
Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations figurant à la section «Remarques», à la page 25.

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

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

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

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

Vous pouvez également consulter les serveurs Internet suivants :

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

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

Table des matières

Avis aux lecteurs canadiens . . . . . **v**

A propos du guide d'utilisation de Packet Capture . . . . . **vii**

1 Présentation de QRadar Packet Capture **1**

2 Configuration de QRadar Packet Capture **3**
Configuration de votre licence 4
Administration des utilisateurs 5
Changement du mot de passe du compte de système d'exploitation 5
Synchronisation de l'heure serveur QRadar Packet Capture avec l'heure système QRadar Console 5

3 Utilisation de Capture - Présentation **7**

4 Cluster **9**
Activation des noeuds de données 9

5 Graphiques QRadar Packet Capture **11**

6 Recherche de paquets pendant une période donnée pour des tests de diagnostic . . **13**

7 Configuration de filtres de pré-capture **15**

8 Configuration de déclencheurs actifs **17**

9 Traitement des incidents liés à QRadar Packet Capture **19**

Remarques **25**
Marques 26
Dispositions relatives à la documentation du produit 26
Déclaration IBM de confidentialité en ligne 27

Avis aux lecteurs canadiens

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

Illustrations

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

Terminologie

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

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

Claviers

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

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

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

Nomenclature

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

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

Brevets

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

Assistance téléphonique

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

A propos du guide d'utilisation de Packet Capture

Cette documentation inclut les informations dont vous avez besoin pour installer et configurer IBM® Security QRadar Packet Capture.

Public visé

Les administrateurs système chargés de l'installation de QRadar Packet Capture doivent bien connaître les concepts de sécurité réseau et les configurations d'unité.

Documentation technique

Pour trouver la documentation du produit IBM Security QRadar dans la bibliothèque de produits QRadar, voir Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Contacter le service clients

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

Instructions relatives aux pratiques de bonne 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, service ou mesure de sécurité ne doit empêcher l'utilisation ou l'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, PRODUITS OU SERVICES NI L'IMMUNITE DE VOTRE ENTREPRISE CONTRE LES CONDUITES MALVEILLANTES OU ILLICITES DE TIERS.

Remarque/Commentaire :

L'utilisation de ce programme peut impliquer différentes 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 fait en sorte de s'y conformer. Le détenteur de licence déclare qu'il détiendra ou qu'il a obtenu les agréments, les autorisations ou les licences nécessaires pour une utilisation réglementaire d'IBM Security QRadar.

1 Présentation de QRadar Packet Capture

IBM Security QRadar Packet Capture est une application de recherche et de capture de trafic réseau. Le dispositif QRadar Packet Capture possède un seul port de capture (DNA0) et vous pouvez installer un émetteur-récepteur SFP 10G ou 1G.

QRadar Packet Capture permet de capturer les paquets d'un réseau avec un débit de 10 gigabits par seconde à l'aide d'une interface réseau active pour les placer dans des fichiers sans perte de données.

Vous pouvez utiliser QRadar Packet Capture pour effectuer des recherches dans le trafic réseau en fonction d'une période et de données d'enveloppe de paquet. Si vous avez des ressources de dispositif suffisantes et des recherches personnalisées, vous pouvez utiliser simultanément les données de recherche et d'enregistreur sans perte de données.

Les dispositifs QRadar Packet Capture dotés d'un émetteur-récepteur 10G prennent en charge les clusters, ce qui permet d'étendre le stockage de données global et les fonctions de calcul d'un serveur autonome unique. Les dispositifs QRadar Packet Capture dotés d'un émetteur-récepteur 1G ne prennent pas en charge les clusters.

Fonctionnalités QRadar Packet Capture

Certaines fonctions incluses dans QRadar Packet Capture sont présentées ci-dessous :

Format de fichier PCAP standard

Format de fichier utilisé pour stocker le trafic réseau. Le format de fichier est intégré à des outils d'analyse tiers existants.

Enregistrement de paquet sur disque hautes performances

Capture de paquets réseau depuis un réseau actif.

Support multicoeur

QRadar Packet Capture est conçu pour être utilisé avec des architectures multicoeur.

Accès E-S direct aux disques

QRadar Packet Capture utilise l'accès E-S direct aux disques afin d'obtenir le débit maximal d'écriture sur disque.

Indexation en temps réel

QRadar Packet Capture peut générer automatiquement un index lors de la capture de paquet. L'index peut être interrogé avec une syntaxe de type BPF (Berkeley Packet Filter) et/ou des chaînes de domaine HTTP ou d'URL de base afin de rapidement extraire les paquets intéressants sur une période spécifique.

Ajout d'un cluster pour augmenter les capacités de capture des données (édition 10G uniquement)

Vous pouvez activer les noeuds de données pour créer un cluster et augmenter les capacités de stockage.

Format de vidage

Les fichiers de capture sont sauvegardés au format PCAP standard avec des horodatages définis en microsecondes. Les fichiers de capture sont stockés dans l'ordre séquentiel en fonction de la taille du fichier. Les fichiers de capture sont stockés dans des répertoires. Lorsque le répertoire ne dispose plus d'espace, les fichiers de capture sont écrasés, en fonction des paramètres d'enregistrement préconfigurés.

Vitesse de capture

Pour les dispositifs de capture de paquets, la vitesse de trafic réseau dépend de la présence ou non de noeuds de données associés au noeud maître :

- Pour les dispositifs de capture de paquets ne comportant pas de noeuds de données associés, la vitesse de capture maximale peut atteindre 7 gigabits par seconde.
- Pour les dispositifs de capture de paquets comportant des noeuds de données associés au noeud maître, la vitesse de capture augmente et peut atteindre jusqu'à 10 gigabits par seconde.

Pour plus d'informations sur le transfert des paquets dans QRadar Packet Capture, consultez *IBM Security QRadar Administration Guide*.

Concepts associés:

3, «Utilisation de Capture - Présentation», à la page 7
Pour capturer le trafic sur disque, démarrez l'application de capture. Le composant Recorder sauvegarde les données du trafic réseau dans un répertoire préconfiguré. Lorsque le répertoire ne dispose plus d'espace, les fichiers existants sont écrasés.

2 Configuration de QRadar Packet Capture

Avant de pouvoir utiliser IBM Security QRadar Packet Capture, des étapes de configuration de base sont requises.

Navigateurs Web pris en charge

Les navigateurs Web suivants sont pris en charge :

- Google Chrome version 44.0.2403.157 ou ultérieure.
- Mozilla Firefox version 40.0.3 ou ultérieure.

Configuration de votre réseau

Pour que QRadar Packet Capture soit disponible à distance, il est nécessaire d'affecter une adresse IP à l'un des ports Ethernet, généralement eth2, eth3 ou eth4. Par défaut, le système est configuré pour utiliser DHCP. Pour la configuration initiale, vous pouvez avoir besoin de connecter un moniteur compatible VGA.

Pour la configuration initiale, procédez comme suit :

1. Mettez sous tension le dispositif QRadar Packet Capture.
2. Utilisez SSH et le port 4477 pour vous connecter en tant qu'utilisateur root.

   Le nom d'utilisateur par défaut est `root`. Le mot de passe par défaut est `P@ck3t08..`

   Pour changer le mot de passe par défaut, voir «Changement du mot de passe du compte de système d'exploitation», à la page 5.
3. Pour vérifier si le système est à jour, appliquez les correctifs de logiciels disponibles sur IBM Fix Central (www.ibm.com/support/fixcentral/).
4. Configurez une adresse IP statique pour votre propre réseau :
   a. Pour obtenir l'adresse MAC ou l'interface eth2, tapez la commande suivante :

      ```
      ifconfig | grep eth2
      ```

      Les interfaces eth0 et eth1 ne sont pas disponibles. Utilisez eth2 pour les composants matériels M4 xSeries.
   b. Notez l'adresse MAC.
   c. Editez les paramètres dans le fichier `/etc/sysconfig/network-scripts/ifcfg-eth2` :
      - Ajoutez le texte suivant sur la première ligne : `DEVICE=eth2`
      - Supprimez la mise en commentaire de l'adresse MAC du port eth2 : `HWADDR=xx:xx:xx:xx:xx`
      - Vérifiez que le paramètre suivant est configuré comme suit : `BOOTPROTO=static`
      - Vérifiez que vous utilisez les informations pertinentes pour votre réseau et que la sortie est identique à l'exemple statique suivant :

        ```
        DEVICE=eth2
        #HWADDR=xx:xx:xx:xx:xx
        BOOTPROTO="static"
        BROADCAST="192.168.1.255"
        DNS1="0.0.0.0"
        DNS2="0.0.0.0"
        GATEWAY="192.168.1.2"
        IPADDR="192.168.1.1"
        NETMASK="255.255.255.0"
        NM_CONTROLLED="no"
        ONBOOT="yes"
        ```
5. Sauvegardez le fichier.

6. Pour appliquer les paramètres, exécutez la commande suivante :
   `service network restart`
7. Vérifiez votre paramètre d'interface en exécutant cette commande :
   `ifconfig | more`

Exemple DHCP : Dans CentOS6.2, modifiez les paramètres suivants dans le fichier `/etc/sysconfig/network-scripts/ifcfg-eth0` ou `/etc/sysconfig/network-scripts/ifcfg-eth1`.

```
BOOTPROTO="dhcp"
NM_CONTROLLED="no"
ONBOOT="yes"
```

Connexion à distance

Après avoir configuré une adresse IP en local, vous pouvez administrer le dispositif en vous connectant à distance à l'aide du protocole SSH sur le port 4477.

Configuration de votre licence

Avant d'utiliser QRadar Packet Capture, vous devez configurer une licence pour le dispositif QRadar Packet Capture et le logiciel QRadar Packet Capture.

Procédure

1. Pour configurer l'octroi de licence pour un dispositif QRadar Packet Capture comportant un émetteur-récepteur SFP 1G, procédez comme suit :
   a. Pour obtenir la clé de licence pour le noeud principal, contactez le représentant IBM.
   b. Dans QRadar Packet Capture, cliquez sur **Help** > **Update Master License** (Aide -> Mettre à jour la licence maître).
   c. Pour appliquer une licence à un dispositif QRadar Packet Capture, collez la valeur dans la zone **License Key** (clé de licence).
   d. Collez les valeurs de **System ID** (ID système) et **License Key** (clé de licence) dans leurs zones respectives.
   e. Cliquez sur **Update Master License** (mettre à jour la licence maître) pour appliquer les changements.
2. Pour configurer l'octroi de licence pour un dispositif QRadar Packet Capture comportant un émetteur-récepteur SFP+ 10G, procédez comme suit :
   a. Pour obtenir une clé de licence pour vos noeuds de données, contactez le représentant IBM.
   b. Dans QRadar Packet Capture, pour appliquer la licence maître, cliquez sur **Help** > **Update Master License** (Aide -> Mettre à jour la licence maître).
   c. Collez les valeurs de **License Key** (clé de licence) et **System ID** (ID système) dans leurs zones respectives.
   d. Cliquez sur **Update Master License** (mettre à jour la licence maître) pour appliquer les changements.
   e. En fonction du nombre de noeuds de données dans un cluster, vous devez effectuer la mise à jour en cliquant sur **Help** > **Node1** (aide -> noeud1).
   f. Pour mettre à jour les licences de noeud de données, collez les valeurs de **License Key** (clé de licence) et **System ID** (ID système) dans leurs zones respectives.
   g. Pour mettre à jour le noeud de données, cliquez sur **Update Node1 License** (mettre à jour la licence de noeud1) pour appliquer les changements.

Administration des utilisateurs

Pour permettre aux utilisateurs d'accéder à IBM Security QRadar Packet Capture et de l'utiliser, vous devez créer un compte utilisateur, lui donner un rôle et configurer ses données d'identification de connexion.

Avant de commencer

Vous devez être connecté à QRadar Packet Capture en tant qu'utilisateur `root`. Vous pouvez aussi créer un utilisateur à l'aide d'une commande `sudo`.

Procédure

1. Pour créer un utilisateur, exécutez la commande suivante :

   `./usr/local/nc/bin/nc_user_manager add <nom_utilisateur> <mot_de_passe> <Admin|Guest>`

   Si le nom d'utilisateur <*nom_utilisateur*> existe déjà, la commande n'est pas exécutée.

   Elle ne l'est pas non plus si le rôle indiqué n'est ni admin, ni guest.

   Lorsqu'un utilisateur est créé, vous pouvez l'utiliser (même nom d'utilisateur et même mot de passe) pour la connexion au produit et à l'API REST.
2. Pour supprimer un utilisateur, exécutez la commande suivante :

   `./usr/local/nc/bin/nc_user_manager delete <nom_utilisateur> <mot_de_passe>`

   Si le nom d'utilisateur <*nom_utilisateur*> existe déjà, la commande n'est pas exécutée.

   La commande n'est pas exécutée si le nom d'utilisateur (<*nom_utilisateur)*> et le mot de passe (<*mot_de_passe)*>) ne correspondent pas à ceux qui sont enregistrés dans QRadar Packet Capture.

   Lorsqu'un utilisateur est supprimé, vous pouvez l'utiliser (même nom d'utilisateur et même mot de passe) pour la connexion au produit et à l'API REST.

Changement du mot de passe du compte de système d'exploitation

Après avoir configuré le dispositif, changez le mot de passe par défaut du système d'exploitation pour IBM Security QRadar Packet Capture.

Vous devez être un utilisateur `root` pour changer le compte de système d'exploitation.

Les mots de passe QRadar Packet Capture ne dépendent pas des mots de passe du système d'exploitation.

Procédure

1. Utilisez SSH et le port `4477` pour vous connecter en tant qu'utilisateur `root`.

   Le mot de passe par défaut de l'utilisateur `root` est `P@ck3t08..`
2. Pour modifier les mots de passe du compte utilisateur `root`, exécutez la commande **passwd**.

Synchronisation de l'heure serveur QRadar Packet Capture avec l'heure système QRadar Console

Pour garantir l'utilisation de paramètres d'heure cohérents lors des déploiements IBM Security QRadar afin que les recherches et les fonctions liées aux données s'exécutent correctement, il est nécessaire que les dispositifs se synchronisent avec le dispositif QRadar Console. Un administrateur doit mettre à jour les paramètres de tables IP sur le dispositif QRadar Console, puis les configurer afin qu'ils acceptent la communication rdate sur le port 37.

Avant de commencer

Vous devez connaître l'adresse IP ou le nom d'hôte de QRadar Console. Le nom d'hôte doit se résoudre correctement à l'aide de nslookup.

Par défaut, le fuseau horaire de l'unité QRadar Packet Capture est défini sur UTC (Coordinated Universal Time).

Important : Si vous changez le fuseau horaire par défaut sur l'unité QRadar Packet Capture, le reste de l'environnement QRadar peut ne pas fonctionner correctement.

Procédure

1. Avec SSH, connectez-vous au dispositif QRadar Packet Capture en tant qu'utilisateur `root`.
2. Pour désactiver le service Network Time Protocol (NTP), entrez la commande suivante : `service ntpd stop`.
3. Pour désactiver la vérification de la configuration de NTP, entrez la commande suivante : `chkconfig ntpd off`.
4. Planifiez la synchronisation en tant que travail cron en éditant le fichier `crontab` (crontable).
   a. Entrez la commande suivante : `crontab -e`.
   b. Pour configurer le dispositif afin qu'il se synchronise avec QRadar Console toutes les 10 minutes, entrez la commande suivante : `*/10 * * * * rdate -s` *`Console_IP_Address`*`.`

      Utilisez une adresse IP ou un nom d'hôte pour la variable *Console_IP_Address*.
   c. Sauvegardez vos modifications de configuration.
   d. Activez crond en tapant la commande suivante :

      ```
      service crond start
      chkconfig crond on
      ```
5. Mettez à jour les tables IP dans QRadar Console afin d'accepter le trafic rdate des unités QRadar Packet Capture.
   a. Avec SSH, connectez-vous au dispositif QRadar Console en tant qu'utilisateur `root`.
   b. Editez le fichier `/opt/qradar/conf/iptables.pre`.
   c. Entrez la commande suivante :

      ```
      -A QChain -m tcp -p tcp --dport 37 -j ACCEPT --src <PCAP_IP address>
      ```

      Si vous avez plusieurs dispositifs QRadar Packet Capture, ajoutez chaque adresse IP sur une seule ligne.

      Exemple :

      ```
      QChain -m tcp -p tcp --dport 37 -j ACCEPT --src 100.100.1.10
      QChain -m tcp -p tcp --dport 37 -j ACCEPT --src 100.100.1.11
      QChain -m tcp -p tcp --dport 37 -j ACCEPT --src 100.100.1.12
      ```
   d. Sauvegardez le fichier `iptables.pre`.
   e. Mettez à jour les tables IP dans QRadar Console en entrant la commande suivante :

      ```
      ./opt/qradar/bin/iptables_update.pl
      ```

Concepts associés:

3, «Utilisation de Capture - Présentation», à la page 7
Pour capturer le trafic sur disque, démarrez l'application de capture. Le composant Recorder sauvegarde les données du trafic réseau dans un répertoire préconfiguré. Lorsque le répertoire ne dispose plus d'espace, les fichiers existants sont écrasés.

3 Utilisation de Capture - Présentation

Pour capturer le trafic sur disque, démarrez l'application de capture. Le composant Recorder sauvegarde les données du trafic réseau dans un répertoire préconfiguré. Lorsque le répertoire ne dispose plus d'espace, les fichiers existants sont écrasés.

Traitement des incidents : Si vous constatez qu'aucune donnée n'est collectée, vérifiez qu'il y a du trafic sur les connexions. Pour capturer le trafic, vous devez utiliser un port TAP ou SPAN (miroir). Lorsque vous utilisez un port SPAN sur un commutateur, si ce dernier affecte une priorité plus faible au port SPAN, certains paquets peuvent être supprimés.

Initiation

Une fois la configuration du système terminée, connectez-vous à IBM Security QRadar Packet Capture en procédant comme suit.

1. Ouvrez un navigateur Web et entrez l'URL suivante :
   `https://adresse_IP_PCAP:41390`
2. Connectez-vous à l'aide des informations de compte suivantes :
   Utilisateur : `continuum`
   Mot de passe : `P@ck3t08..`

Traitement des incidents : Si un utilisateur ne parvient pas à donner le mot de passe correct cinq fois de suite dans un intervalle de 10 minutes, le compte est verrouillé pendant 30 minutes. Le compte utilisateur peut être déverrouillé manuellement par un administrateur système.

Par défaut, la page Capture State est affichée. Vous pouvez contrôler les enregistrements en cliquant sur **Start Capture** ou **Stop Capture**.

Etat des captures

Les informations suivantes sont fournies dans la page Capture State :

- **Interface capturing on (Interface de capture)**
- **Capture status (Etat des captures)**
- **Start/Stop time (Heure de démarrage/arrêt)**
- **Duration of time the system has been capturing (Durée de capture du système)**
- **Throughput rate (Débit)**
- **Packets Captured (Paquets capturés)**
- **Bytes Captured (Octets capturés)**
- **Packets Dropped (Paquets supprimés)**
- **Storage Space Available (Espace de stockage disponible)**

Dans une configuration en cluster, les capacités de stockage utilisées sont affichées pour chaque noeud de données activé. Si le noeud de données QRadar Packet Capture n'est pas accessible en raison d'un problème de configuration ou d'une connexion incorrecte, le message suivant s'affiche à la place des statistiques de stockage : `Slave node is enabled but is currently unreachable.`

Traitement des incidents

Pour afficher les informations système concernant les interfaces de capture configurées, cliquez sur **Troubleshooting** (identification et résolution des problèmes).

Informations sur le serveur

Pour afficher les informations d'espace de stockage du serveur, cliquez sur **Server information** (informations serveur).

Caractéristiques du réseau

Affichez le débit du réseau sous forme graphique.

Le débit de capture sur disque maximum par défaut est de 10 Gbits/s.

Historique des captures

Affichez l'historique des captures de paquets qui ont été effectuées ou qui sont en cours d'exécution.

Compression en ligne

Pour effectuer des investigations Forensics, vous pouvez conserver plus longtemps le contenu des paquets bruts en augmentant la capacité de stockage virtuelle disponible sans ajouter de disques physiques. Vous pouvez désormais utiliser la nouvelle option de compression en ligne pour stocker de plus grandes quantités de données sur le dispositif QRadar Packet Capture.

Le volume de compression est lié au volume de contenu vidéo compressé dans le contenu. Par exemple, si vous avez un volume de vidéo compressé égal à 5 % dans le contenu, vous obtenez un ratio de compression de 13:1. Le ratio compression:stockage est le ratio entre le volume non compressé et le volume compressé.

Tableau 1. Taux de compression en ligne

Pourcentage (%) de contenu vidéo compressé	Taux d'amplification compression:stockage
0	17:1
5	13:1
10	6:1
20	4:1
40	2.4:1

Concepts associés:

1, «Présentation de QRadar Packet Capture», à la page 1
IBM Security QRadar Packet Capture est une application de recherche et de capture de trafic réseau. Le dispositif QRadar Packet Capture possède un seul port de capture (DNA0) et vous pouvez installer un émetteur-récepteur SFP 10G ou 1G.

Tâches associées:

«Synchronisation de l'heure serveur QRadar Packet Capture avec l'heure système QRadar Console», à la page 5
Pour garantir l'utilisation de paramètres d'heure cohérents lors des déploiements IBM Security QRadar afin que les recherches et les fonctions liées aux données s'exécutent correctement, il est nécessaire que les dispositifs se synchronisent avec le dispositif QRadar Console. Un administrateur doit mettre à jour les paramètres de tables IP sur le dispositif QRadar Console, puis les configurer afin qu'ils acceptent la communication rdate sur le port 37.

4 Cluster

Utilisez le dispositif QRadar Packet Capture comme serveur unique autonome ou comme cluster de serveurs.

Les éditions 10G prennent en charge les clusters qui développent la capacité globale de stockage des données et la fonction de calcul par rapport à un serveur autonome unique. Les clusters comportent un maître. Vous pouvez connecter jusqu'à deux dispositifs de noeud de données QRadar Packet Capture à chaque système maître QRadar Packet Capture.

L'onglet **Cluster** affiche deux noeuds de données, ainsi que leur statut en cours.

Les noeuds de données ne font pas partie du cluster par défaut et leur statut est "désactivé".

Activation des noeuds de données

Après avoir connecté physiquement des noeuds de données IBM Security QRadar Packet Capture au maître aux noeuds de données QRadar Packet Capture, vous devez activer les noeuds de données QRadar Packet Capture. Les noeuds de données QRadar Packet Capture activés et connectés forment un cluster pour la fonction de stockage ajoutée et les performances de capture améliorées.

Pour plus d'informations sur la connexion des dispositifs, voir *QRadar Packet Capture - Aide-mémoire.*

Avant de commencer

Assurez-vous que le serveur de capture est en cours d'exécution.

Procédure

1. Pour activer des noeuds de données, procédez comme suit :
   a. Dans l'onglet **Cluster**, pour chaque noeud de données, sélectionnez **Enable** (activer). Le statut affiché est **Connecté**.
   b. Redémarrez le serveur de capture. Les noeuds de données QRadar Packet Capture sont maintenant activés.

   Quand les noeuds de données QRadar Packet Capture sont connectés et en cours d'exécution, leur statut dans le cluster passe à "connectés".

   Une fois le noeud maître connecté au noeud de données, la taille du stockage (virtuel) compressée affichée sur le tableau de bord inclut celle des noeuds de données connectés.
2. Pour désactiver des noeuds de données, procédez comme suit :
   a. Dans l'onglet Cluster, pour chaque noeud de données, sélectionnez **Disable** (désactiver). Le statut affiché est **Disconnected** (déconnecté).
   b. Redémarrez le serveur de capture. Les noeuds de données QRadar Packet Capture sont à présent déconnectés et ne sont plus associés au maître.

   Un noeud de données déconnecté ne stocke plus les données.

   Une fois le noeud maître désactivé, la taille du stockage compressé (virtuel) affichée dans le tableau de bord diminue.

   Si le noeud de données 1 ou 2 est sous licence, la colonne destinée aux licences affiche soit **Permanent** ou **Evaluation**, en fonction du type de licence utilisé.

5 Graphiques QRadar Packet Capture

Dans IBM Security QRadar Packet Capture, utilisez un graphique en temps réel ou d'historique pour visualiser les statistiques de capture de paquet.

Graphique en temps réel

Le graphique en temps réel (Live graph) effectue le suivi des statistiques de capture de paquet suivantes concernant la capture de paquet en cours :

- Throughput in Gbps (débit en gigabits par seconde)
- Total packets per second (nombre total de paquets par seconde)
- TCP_packets per second (paquets TCP par seconde)
- UDP_packets per second (paquets UDP par seconde)
- Packets per second for non-UDP traffic (paquets par seconde pour le trafic non-UDP)
- Number of system events (nombre d'événements système)
- Packet compression ratio (taux de compression de paquet)

Déplacez la souris au dessus de du graphique pour obtenir les statistiques relatives au point sur le graphique.

Vous pouvez cliquer en un point du graphique point pour automatiquement générer une demande de recherche. Vous pouvez également cliquer sur les icônes de style d'affichage pour changer la vue de graphique.

Graphique d'historique

Le graphique d'historique fournit une vue d'ensemble sur le long terme de l'historique de capture de paquet. Les options de diagramme d'historique incluent 1 heure, 1 jour et 1 semaine.

Déplacez la souris au dessus de du graphique pour obtenir les statistiques relatives au point sur le graphique.

Cliquez en un point du graphique point pour automatiquement générer une demande de recherche.

6 Recherche de paquets pendant une période donnée pour des tests de diagnostic

Les données d'index créées lors de la capture permettent de générer un fichier de capture de paquet (pcap) contenant les paquets et les informations de métadonnées associées pendant la période indiquée.

Restriction : Ces recherches sont effectuées uniquement à des fins de diagnostic. Un nettoyage manuel est nécessaire pour éviter la saturation de la partition d'extraction.

Procédure

1. Cliquez sur la page **Rechercher**.

   Les valeurs par défaut sont déjà indiquées.
2. Sélectionnez l'interface du trafic capturé auquel la recherche doit s'appliquer.

   S'il n'y a qu'une seule configuration d'interface, elle est automatiquement sélectionnée.
3. Indiquez une valeur ou modifiez les valeurs par défaut définissant le début et la fin de la plage de recherche.
4. Indiquez le filtre BPF (Berkeley Packet Filter).

   Utilisez la syntaxe BPF pour indiquer des filtres BPF. Une expression se compose d'une ou de plusieurs primitives. Les expressions de filtre complexes sont créées à l'aide des opérateurs AND, OR et NOT.

   Les exemples ci-après sont des filtres de primitives :

   ```
   ether host 00:11:22:33:44:55
   ether src host 00:11:22:33:44:55

   ip host 192.168.0.1
   ip dst host 192.168.0.1

   ip6 host 2001:0db8:85a3:0042:0000:8a2e:0371:7334
   ip6 src host 2001:0db8:85a3:0042:0000:8a2e:0371:7334

   ip net 192.168.1.0/24
   ip src net 192.168.1

   port 80
   udp port 9000
   tcp src port 80
   ```

   Ces exemples sont des filtres complexes :

   ```
   ip host 192.168.1.1 and 192.168.1.2
   ip src 192.168.1.1 and dst 192.168.1.2
   ip host 192.168.1.1 and tcp port (80 or 443)
   (ip host 192.168.1.1 or 192.168.1.2) and (port 80 or 443)
   ```
5. Indiquez le nombre de paquets à extraire.

   Le nombre maximal de paquets par défaut est 10000. Si vous remplacez la valeur par 0, tous les paquets correspondant à la période et au filtre sont extraits.
6. Cliquez sur **Start Search**.
7. Dans la colonne **Action** de la page de recherche, utilisez l'option **Chunking** (granularisation) pour fractionner les demandes de recherche en segments de données plus petits afin de pouvoir accéder aux données tandis que la demande de recherche complète est toujours en cours d'exécution. Vous demandez une recherche en spécifiant d'abord le numéro de fichier PCAP puis en cliquant sur **Download PCAP File** (télécharger le fichier PCAP).

La taille des segments de données est de 128 Mo, et le dernier segment peut être d'une taille quelconque inférieure à 128 Mo.

8. Pour afficher l'état de la file d'attente des recherches, rendez-vous sur la page **Search request queue**.
9. Pour afficher l'historique de toutes les recherches terminées, cliquez sur **Request log**.
10. Nettoyez les recherches manuelles pour disposer d'un espace suffisant pour les procédures de reprise Forensics :
    a. Connectez-vous en tant qu'utilisateur root.
       nom d'utilisateur : root
       mot de passe : P@ck3t08..
    b. Exécutez la commande suivante :
       `rm -r /extraction/<nom_de_recherche>`
       La variable <*nom_de_recherche*> correspond à la colonne name de la page Completed Searches.

7 Configuration de filtres de pré-capture

Les filtres de pré-capture filtrent le trafic réseau avant l'écriture sur disque des données capturées.

Procédure

1. Créez un filtre de pré-capture.
   a. Cliquez sur le menu **Pre capture filter** (filtre de pré-capture).
   b. Entrez les paramètres pour les options de nom de filtre (Filter Name) et de filtre de recherche (Search Filter).

      Un filtre de capture prend la forme d'expressions primitives connectées par des conjonctions (et/ou, and/or) et éventuellement précédées de non (not).

      Dans l'exemple suivant, tout le trafic à destination du port 80 est supprimé.

      ```
      not dst port 80
      ```

      Dans l'exemple suivant, seul le trafic des deux hôtes est capturé et tout le reste du trafic est supprimé.

      ```
      host 1.2.3.4 or host 1.1.1.1
      ```

   c. Terminez la création du filtre de pré-capture en cliquant sur **Add** (ajouter). Le dernier filtre de pré-capture ajouté à la liste devient le filtre actif. L'historique des filtres précédent est également affiché.
2. Redémarrez le serveur de capture pour activer le filtre nouvellement ajouté.
3. Supprimez de manière permanente le filtre en sélectionnant **Delete** (supprimer). Vous devez redémarrer le serveur de capture.

8 Configuration de déclencheurs actifs

Les déclencheurs actifs vous alertent lorsqu'un événement spécifique survient sur votre réseau. Vous spécifiez, par exemple, une adresse IP comme filtre de recherche afin d'être alerté lorsque le trafic contenant l'adresse IP est capturé.

Procédure

1. Créez un déclencheur actif.
   a. Cliquez sur le menu **Active Trigger** (déclencheur actif).
   b. Entrez les paramètres pour les options de nom de déclencheur et de période (Time frame).
   c. Terminez la création du déclencheur actif en cliquant sur **Add** (ajouter).

   Restriction : Vous pouvez spécifier jusqu'à cinq déclencheurs actifs.
2. Examinez les événements de déclencheur dans le journal des événements (**Event Log**) lorsqu'ils se produisent. Le fait de cliquer sur un événement de déclencheur actif génère automatiquement une demande de recherche dans les paramètres de temps spécifiés autour de l'événement déclencheur. Le période de la recherche inclut des secondes avant et après l'événement.
3. Supprimez le déclencheur configuré en sélectionnant **Delete** (supprimer).

9 Traitement des incidents liés à QRadar Packet Capture

Le traitement des incidents est une approche systématique pour résoudre un incident. Il détermine les raisons pour lesquelles un élément ne fonctionne pas correctement et explique la démarche à suivre pour corriger le problème.

La dernière version du logiciel QRadar Packet Capture est-elle installée ?

Mettez toujours à niveau votre version actuelle vers la version logicielle la plus récente. Immédiatement après avoir mis à jour un logiciel, ou après toute nouvelle installation, assurez-vous de redémarrer votre système de façon à ce que les changements soient pris en compte. Dans les configurations de cluster, vérifiez toujours que le système de noeuds de données maître ainsi que tous les autres ont été mis à niveau vers la même version.

Disposez-vous du microprogramme suggéré pour le contrôleur RAID et les disques durs ?

Si vous rencontrez des problèmes de fiabilité ou de performance liés à la révision du microprogramme installée sur le contrôleur RAID 3650 M4 et les disques durs, assurez-vous de disposer des révisions de microprogramme minimales :

- Pour le système 3650 M4, la révision de microprogramme du contrôleur RAID M5200 doit être : version 24.7.0-0052 datant du 27 mai 2015 ou version ultérieure.

  Exécutez les fichiers `.bin` depuis la ligne de commande Red Hat Linux.
- Pour IBM Lenovo, la révision du 15 mai 2015 ou une version ultérieure.

  Exécutez les fichiers `.bin` depuis la ligne de commande Red Hat Linux.

HyperThreading est-il activé dans le BIOS ?

Le mécanisme HyperThreading est activé dans le BIOS par défaut. Exécutez la commande `lscpu` et vérifiez que la sortie indique “Thread(s) per core is equal to 2”. Voici un exemple de sortie de la commande pour IBM 3650-M4:

```
[root@3650M4-001 bin]# lscpu
Architecture:          x86_64
CPU op-mode(s):        32-bit, 64-bit
Byte Order:            Little Endian
CPU(s):                40
On-line CPU(s) list:   0-39
Thread(s) per core:    2
Core(s) per socket:    10
Socket(s):             2
NUMA node(s):          2
Vendor ID:             GenuineIntel
CPU family:            6
Model:                 62
Stepping:              4
CPU MHz:               2800.000
BogoMIPS:              5592.04
Virtualization:        VT-x
L1d cache:             32K
L1i cache:             32K
L2 cache:              256K
L3 cache:              25600K
NUMA node0 CPU(s):     0-9,20-29
NUMA node1 CPU(s):     10-19,30-39
```

Le port de capture est-il connecté correctement ?

Le périphérique IBM Security QRadar Packet Capture peut capturer uniquement des données sur l'interface 0.

La connexion au réseau Ethernet est-elle configurée correctement ?

Pour vérifier si l'interface Ethernet a été affectée à une adresse IP, exécutez la commande `ifconfig`.

Si aucune adresse n'est configurée, vous pouvez éditer le fichier correspondant `ifcfg-eth*`.

- Dans cet exemple utilisant un protocole DHCP, éditez les paramètres suivants dans `/etc/sysconfig/network-scripts/ifcfg-`*`eth2`* et remplacez *eth2* par le paramètre approprié.

  ```
  BOOTPROTO="dhcp"
  NM_CONTROLLED="no"
  ONBOOT="yes"
  ```

- Dans cet exemple utilisant une adresse IP statique, éditez les paramètres suivants dans `/etc/sysconfig/network-scripts/ifcfg-`*`eth2`* et remplacez *eth2* par le paramètre approprié.

  ```
  BOOTPROTO="static"
  BROADCAST="192.168.1.255"
  DNS1="0.0.0.0"
  DNS2="0.0.0.0"
  GATEWAY="192.168.1.2"
  IPADDR="192.168.1.1"
  NETMASK="255.255.255.0"
  NM_CONTROLLED="no"
  ONBOOT="yes
  ```

Après avoir changé les paramètres, exécutez la commande `ifconfig` pour configurer l'interface réseau.

L'heure système est-elle configurée correctement ?

Par défaut, l'heure système correspond à UTC (Coordinated Universal Time) et est configurée pour utiliser NDP (Network Time Protocol) et des serveurs publics afin de maintenir l'heure système correcte.

Existe-t-il des problèmes matériels liés au système ?

1. Vérifiez que le trafic est généré correctement et est reçu par la carte NIC (Network Interface Card).

   Examinez les voyants qui se trouvent à droite du port de connexion de l'Interface 0. Le premier voyant tout en bas doit être allumé et fixe. Il indique qu'il y a une connexion. Le premier voyant tout en haut doit clignoter. Il signale une activité de trafic.
2. Exécutez la commande `/usr/local/nc/bin/dpdk_nic_bind.py –status`.

   Le résultat de cette commande doit être comparable aux données suivantes :

```
Network devices using DPDK-compatible driver
============================================
0000:0f:00.0 '82599ES 10-Gigabit SFI/SFP+ Network Connection' drv=igb_uio
unused=ixgbe
0000:0f:00.1 '82599ES 10-Gigabit SFI/SFP+ Network Connection' drv=igb_uio
unused=ixgbe
Network devices using kernel driver
===================================
0000:07:00.0 'I350 Gigabit Network Connection' if=eth2 drv=igb unused=igb_uio
*Active*
0000:07:00.1 'I350 Gigabit Network Connection' if=eth3 drv=igb unused=igb_uio
0000:07:00.2 'I350 Gigabit Network Connection' if=eth4 drv=igb unused=igb_uio
Other network devices
=====================
<none>
```

Le système capture-t-il le trafic ?

Pour confirmer si le système capture le trafic après le démarrage de la session de capture, utilisez l'une des méthodes suivantes :

- Examinez les voyants qui se trouvent à droite du port de connexion de l'Interface 0. Le premier voyant tout en haut doit clignoter. Il signale une activité de trafic.
- Dans la page Network Characterization, vous pouvez voir la sortie graphique.
- Depuis la ligne de commande, exécutez la commande `du –h /storage0/int0`.

  Le résultat doit s'apparenter aux données suivantes :

```
4.4G /storage0/int0/1_0
4.9G /storage0/int0/2_0
6.4G /storage0/int0/3_0
4.9G /storage0/int0/4_0
4.9G /storage0/int0/5_0
4.9G /storage0/int0/6_0
.
.
.
1.4T /storage0/int0/
```

  Si vous exécutez cette commande de façon répétitive, le nombre de sous-répertoires et les volumes d'allocation renvoyés augmentent.

Le noeud de données QRadar Packet Capture est-il activé ?

Lorsque le noeud de données QRadar Packet Capture est connecté physiquement au noeud principal, vous devez également vous assurer qu'il est activé dans l'interface utilisateur pour fonctionner avec le serveur principal. Pour le moment, le système prend en charge jusqu'à deux noeuds de données QRadar Packet Capture.

Si l'onglet **Cluster** indique que les noeuds de données QRadar Packet Capture sont connectés et activés et que le paramètre **System ID** manque dans l'écran **Update Node(n) License** sous l'onglet **Admin**, vous devez vous assurer que le noeud de données QRadar Packet Capture spécifique dispose de la même version du logiciel de noeud de donnéesQRadar Packet Capture que le noeud principal. Après la mise à jour vers la dernière version du logiciel, veillez à ce que cette exigence soit respectée.

En tant qu'utilisateur `root`, exécutez la commande ci-dessous pour vérifier que l a version du logiciel est installée sur le noeud de données QRadar Packet Capture et sur le noeud principal :

```
cat /root/version.txt
```

La version du logiciel du noeud de données QRadar Packet Capture doit être identique à la version installée sur le noeud principal.

Comment une licence pour le noeud de données QRadar Packet Capture est-elle appliquée à partir de la ligne de commande ?

Pour vous assurer que vous vous trouver sur le noeud de données QRadar Packet Capture, en tant qu'utilisateur `root`, exécutez la commande suivante :

```
cat /root/version.txt
```

Pour vérifier que vous êtes connecté au noeud de données QRadar Packet Capture, cherchez un "D" est ajouté à la fin du numéro de version, par exemple, 7.2.7.256D.

Pour appliquer la licence au noeud de données QRadar Packet Capture, en tant qu'utilisateur `root`, exécutez le script : `nc_set_license.sh` en tant qu'utilisateur `root`.

Remarques :

- Pour appliquer la nouvelle licence, vous devez redémarrer le noeud de données QRadar Packet Capture.
- Si le noeud de données QRadar Packet Capture dispose déjà d'une licence lors de la production, il n'est pas nécessaire d'exécuter le script. La licence est appliquée dès que le système démarre.

Si la licence que vous avez appliquée n'est pas valide, un message d'erreur s'affiche :

```
Avertissement : LicenseKey n'est *PAS* valide.
```

Qu'est-ce que le format de journalisation LEEF 2.0 ?

Les messages LEEF (Log Event Extended Format) sont ajoutés au fichier `/var/log/messages` au format suivant :

```
<DateTime> <ServerIP> LEEF: 2.0|IBM|QRadar Packet Capture|7.2.7.256|<ID>|cat=<catégorie>
msg=<message>
```

Par exemple, lorsque le serveur de capture de paquet démarre sur un système dont l'adresse IP est 10.91.170.20, le message LEEF ci-dessous est ajouté au fichier `/var/log/messages` :

```
May 24 22:27:49 IP_10_91_170_20 LEEF: 2.0|IBM|QRadar Packet
Capture|7.2.7.256|Started|cat=PacketCapture
```

Pourquoi la demande Create Search renvoie-t-elle une ereur `NoSpace` ?

Si le répertoire `/extraction` est saturé lorsque vous créez une recherche, le serveur renvoie une erreur `NoSpace`.

Que se passe-t-il lorsqu'une recherche est suspendue ?

Une recherche est suspendue lorsque l'espace utilisé dans le répertoire `/extraction` dépasse 6.7 Go. Un message LEEF est envoyé à `Syslog` pour indiquer que la recherche est suspendue. Le journal des événements affiche un message comme celui-ci :

```
!AVERTISSEMENT : Stockage d'extraction saturé ! Impossible de poursuivre la recherche !
```

Pour veiller à la reprise d'une recherche suspendue, vous devez créer de l'espace en supprimant les anciennes recherches effectuées précédemment. Pour supprimer une ancienne recherche, suivez cette procédure :

1. Dans le menu principal, cliquez sur l'option **Rechercher**.
2. Dans la zone **Journal des demandes de recherche**, supprimez les anciennes recherches en cliquant sur **Supprimer la recherche**.

Remarques

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

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

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

Pour le Canada, veuillez adresser votre courrier à :

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Marques

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

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).