IBM Security QRadar
Version 7.2.6

Packet Capture - Guide d'utilisation

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

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

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

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

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

Vous pouvez également consulter les serveurs Internet suivants :

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

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

© Copyright IBM France 2015. Tous droits réservés.

© Copyright IBM Corporation 2012, 2015.

Table des matières

© Copyright IBM Corp. 2012, 2015

A propos du guide d'utilisation Packet Capture

Cette documentation inclut les informations dont vous avez besoin pour installer et configurer IBM® Security QRadar Packet Capture. QRadar Packet Capture est pris en charge par IBM Security QRadar SIEM.

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 des 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 clients, voir Support and Download Technical Note (http://www.ibm.com/support/docview.wss?uid=swg21616144).

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.

© Copyright IBM Corp. 2012, 2015

Chapitre 1. Nouveautés pour les utilisateurs de QRadar Packet Capture version 7.2.6

IBM Security QRadar Incident Forensics version 7.2.6 offre une récupération de capture de paquet plus rapide ainsi que des filtres de collecte et de stockage de données de réglage.

Résultats de recherche QRadar Packet Capture renvoyés plus rapidement et dans des segments de données discrets

Les données de capture de paquets sont téléchargées dans des segments discrets. De cette façon, les temps de transfert sont plus courts et vous pouvez afficher les données plus rapidement. Vous pouvez accéder aux données recherchées plus rapidement car celles-ci sont divisées en segments plus petits.  En savoir plus...

Affinage de la collecte et du stockage de données à l'aide de filtres de paquets de pré-capture

Vous pouvez conserver l'espace disque en définissant le type de données à capturer. Si vous disposez d'un espace de stockage de capture de paquets limité, vous pouvez capturer uniquement le trafic qui vous semble le plus risqué. Vous pouvez affiner la capacité de collecte de données de paquets afin de l'adapter à vos ressources de stockage.

© Copyright IBM Corp. 2012, 2015

Chapitre 2. Présentation de QRadar Packet Capture

IBM Security QRadar Packet Capture est une application de recherche et de capture de trafic réseau.

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. QRadar Packet Capture utilise le format de fichier PCAP standard pour stocker le trafic réseau. Le format du fichier PCAP facilite l'intégration avec les outils d'analyse tiers existants.

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. Cette application permet également d'effectuer un enregistrement à hautes performances de type paquet vers disque.

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 pour extraire rapidement les paquets intéressants pendant une période définie.

Ajout d'un cluster pour augmenter les capacités de capture de stockage des données capturées.

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

© Copyright IBM Corp. 2012, 2015

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.

Concepts associés:

Chapitre 4, «Utilisation de Capture - Présentation», à la page 9
Pour capturer le trafic sur disque, démarrez l'application de capture. Le composant Recorder sauvegarde les données du trafic dans un répertoire préconfiguré. Lorsque le répertoire ne dispose plus d'espace, les fichiers existants sont écrasés.

Chapitre 3. 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
- Mozilla Firefox
- Microsoft Internet Explorer version 10 et 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. Toutefois, pour la configuration initiale, vous devrez peut-être connecter un écran VGA, démarrer le système en local, vous connecter et configurer une adresse IP statique pour votre propre réseau. Après avoir démarré le système, connectez-vous en tant qu'utilisateur `root` à l'aide des données d'identification suivantes :

```
username: root
password: P@ck3t08..)
```

Pour la configuration initiale, procédez comme suit.

1. Connectez-vous à un moniteur compatible VGA.
2. Mettez sous tension le dispositif QRadar Packet Capture.
3. Connectez-vous au système d'exploitation Linux en tant qu'utilisateur `root`.

   `Username: root`

   `Password: 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 6.
4. Pour vérifier si le système est à jour, appliquez les correctifs de logiciels disponibles sur IBM Fix Central (www.ibm.com/support/fixcentral/).
5. 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`

© Copyright IBM Corp. 2012, 2015

- 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"
```

6. Sauvegardez le fichier.
7. Pour appliquer les paramètres, exécutez la commande suivante :

   ```
   service network restart
   ```

8. 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.

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. Les utilisateurs des comptes `adminusername` et `continuum` doivent changer leurs mots de passe lorsqu'ils se connectent pour la première fois.

Procédure

1. Utilisez SSH pour vous connecter en tant qu'utilisateur `root`.

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

2. Pour changer les mots de passe des comptes utilisateur `continuum` et `root`, utilisez la commande **`passwd`** *nom_utilisateur*.

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 device est défini sur UTC (Coordinated Universal Time).

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:

Chapitre 4, «Utilisation de Capture - Présentation», à la page 9
Pour capturer le trafic sur disque, démarrez l'application de capture. Le composant Recorder sauvegarde les données du trafic dans un répertoire préconfiguré. Lorsque le répertoire ne dispose plus d'espace, les fichiers existants sont écrasés.

Chapitre 4. Utilisation de Capture - Présentation

Pour capturer le trafic sur disque, démarrez l'application de capture. Le composant Recorder sauvegarde les données du trafic 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 le navigateur et entrez l'adresse IP de votre périphérique.
2. Connectez-vous en utilisant les informations utilisateur suivantes :

   Utilisateur : `continuum`

   Mot de passe : `P@ck3t08..`

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

Conseil : Vous pouvez voir le numéro de version du produit en haut à droite de la fenêtre.

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.`

© Copyright IBM Corp. 2012, 2015

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:

Chapitre 2, «Présentation de QRadar Packet Capture», à la page 3
IBM Security QRadar Packet Capture est une application de recherche et de capture de trafic réseau.

Tâches associées:

«Synchronisation de l'heure serveur QRadar Packet Capture avec l'heure système QRadar Console», à la page 7
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.

Chapitre 5. Activation des noeuds de données

Après avoir connecté physiquement le dispositif IBM Security QRadar Packet Capture maître aux noeuds de données QRadar Packet Capture, vous devez activer les noeuds de données QRadar Packet Capture. L'activation des noeuds de données QRadar Packet Capture crée un cluster pour augmenter les capacités de stockage.

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

Restriction : Lorsque vous désactivez un noeud de données QRadar Packet Capture, la procédure de reprise Forensics ne peut pas accéder aux données capturées sur ce noeud.

Procédure

1. Dans l'onglet Tableau de bord, démarrez puis arrêtez la capture de trafic
2. Dans l'onglet Cluster, pour chaque noeud de données, sélectionnez **Activer**. Le statut affiché est **Connecté**.
3. Redémarrez la capture

   Les noeuds de données QRadar Packet Capture sont maintenant activés. Si les noeuds de données QRadar Packet Capture sont connectés et en cours d'exécution, le statut des noeuds de données QRadar Packet Capture dans le cluster devient “connecté”.

   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.

   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.

© Copyright IBM Corp. 2012, 2015

Chapitre 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. Comme vous pouvez le voir dans la colonne **Action** de la page de recherche, les demandes de recherche sont divisées en segments de données plus petits. De cette façon, vous pouvez accéder aux données pendant que la demande de

© Copyright IBM Corp. 2012, 2015

recherche complète est en cours d'exécution. Vous pouvez demander une recherche en indiquant le numéro du fichier PCAP, puis en cliquant sur le bouton **Download PCAP File**.

La taille des segments de données est de 128 Mo et le dernier segment peut être de toute taille.

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.

Chapitre 7. 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.

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"
  ```

© Copyright IBM Corp. 2012, 2015

- 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.

L'interface REST fonctionne-t-elle ?

Exécutez la commande suivante et entrez le mot de passe approprié (différent de la valeur par défaut) pour l'utilisateur continuum :

```
curl -k -v -X POST -G -d "username=continuum&password=password&action
=ping" https://localhost/rest/forensics_fetch.php
```

Le résultat doit être comparable aux données suivantes :

```
About to connect() to localhost port 443 (#0)
* Trying ::1... connected
* Connected to localhost (::1) port 443 (#0)
* Initializing NSS with certpath: sql:/etc/pki/nssdb
* warning: ignoring value of ssl.verifyhost
* skipping SSL peer certificate verification
* SSL connection using TLS_DHE_RSA_WITH_AES_128_CBC_SHA
* Server certificate:
* subject: E=root@localhost.localdomain,CN=localhost.localdomain,
OU=SomeOrganizationalUnit,
O=SomeOrganization,L=SomeCity,ST=SomeState,C=--
* start date: Mar 27 17:10:01 2014 GMT
* expire date: Mar 27 17:10:01 2015 GMT
* common name: localhost.localdomain
* issuer: E=root@localhost.localdomain,CN=localhost.localdomain,
OU=SomeOrganizationalUnit,
O=SomeOrganization,L=SomeCity,ST=SomeState,C=--
> POST /rest/forensics_fetch.php?username=continuum&password=
test&action=ping HTTP/1.1
> User-Agent: curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.15.3
zlib/1.2.3 libidn/1.18 libssh2/1.4.2
> Host: localhost
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Mon, 13 Oct 2014 20:08:20 GMT
< Server: Apache/2.2.15 (Red Hat)
< X-Powered-By: PHP/5.3.3
< Set-Cookie: PHPSESSID=54cf36otmg899b6bau03lu6jh6; path=/
< Expires: Thu, 19 Nov 1981 08:52:00 GMT
< Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
< Pragma: no-cache
< Content-Length: 85
< Connection: close
< Content-Type: application/json
<
* Closing connection #0
{"status":"success","message":"QRadar Packet Capture (c), Version 7.2.4.209\n"}
```

Comment redéfinir le mot de passe utilisateur continuum ?

Vous pouvez modifier le mot de passe utilisateur continuum dans l'interface utilisateur QRadar Packet Capture. Pour rétablir la valeur par défaut du mot de passe définie en usine, vous devez utiliser le script `reset_default.sh`. L'utilisateur est invité à modifier le mot de passe à la prochaine connexion.

Pour exécuter le script `reset_default.sh`, connectez-vous à la ligne de commande en tant qu'utilisateur root et tapez la commande suivante :

```
sh /var/www/html/mysql/reset_default.sh continuum
```

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 paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales.

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 implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

© Copyright IBM Corp. 2012, 2015

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.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

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 Corporation
170 Tracer Lane,
Waltham MA 02451, USA

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 indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

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.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée 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. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

Si vous visualisez ces informations en ligne, il se peut que les photographies et illustrations en couleur n'apparaissent pas à l'écran.

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.

Les autres noms de sociétés, de produits et de services peuvent appartenir à des tiers.

Remarques sur les règles de confidentialité

Les produits IBM Software, notamment les logiciels sous forme de services (“Offres logicielles”), peuvent utiliser des cookies ou d'autres technologies pour collecter des informations d'utilisation en vue d'améliorer l'expérience de l'utilisateur final, d'ajuster les interactions avec l'utilisateur final ou à d'autres fins. Dans de nombreux cas, aucune information identifiant la personne n'est collectée par les offres logicielles. Certaines de nos Offres logicielles vous permettent de collecter des informations identifiant la personne. Si cette Offre logicielle utilise des cookies pour collecter des informations identifiant la personne, des informations spécifiques sur l'utilisation de cookies par cette offre sont énoncées ci-après.

Selon les configurations déployées, cette Offre logicielle peut utiliser des cookies de session qui collectent chaque ID de session à des fins de gestion de la 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 pour cette Offre logicielle vous fournissent à vous en tant que client la possibilité de collecter des informations identifiant d'autres personnes via des cookies et d'autres technologies, vous devez vous renseigner sur l'avis juridique et les lois applicables à ce type de collecte de données, notamment les exigences d'information et de consentement.

Pour plus d'informations sur l'utilisation de diverses technologies, notamment de cookies, à ces fins, reportez-vous aux Points principaux de la Déclaration IBM de confidentialité sur Internet (http://www.ibm.com/privacy/fr/fr) et à 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 qu'à 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).