IBM Security QRadar
Version 7.2.2

Packet Capture - Guide d'utilisation

SC43-0904-00

Important
Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 9.

Réf. US : SC27-6512-00

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.can.ibm.com (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

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 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 (en anglais) (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

Déclaration de pratiques de sécurité recommandées

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

Chapitre 1. Présentation de QRadar Packet Capture

IBM Security QRadar Packet Capture est une application de recherche et de capture de trafic réseau. A l'aide de QRadar Packet Capture, vous pouvez capturer les paquets réseau à des débits de plusieurs gigaoctets à partir d'une interface réseau active et les placer dans des fichiers sans aucune perte de paquet.

QRadar Packet Capture peut rechercher le trafic réseau capturé par heure et données d'enveloppe de paquet. Utilisez la recherche simultanément avec l'enregistreur sans perte de données, si les recherches ont été personnalisées et que des ressources de dispositif appropriées ont été attribuées. 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-après.

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 à hautes performances de type paquet vers disque.

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

Accès au disque (E-S en accès direct).
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.

Format de vidage

Les fichiers de capture sont sauvegardés au format PCAP standard avec des horodatages définis en microsecondes. Ils sont stockés dans un ordre séquentiel avec une limite de taille par fichier, avec des répertoires et des fichiers recyclés selon les besoins en fonction des paramètres d'enregistrement préconfigurés.

Chapitre 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
- Mozilla Firefox
- Microsoft Internet Explorer

Configuration de votre réseau

Pour que QRadar Packet Capture soit disponible à distance, vous devez attribuer une adresse IP à eth0 ou à eth1. Par défaut, le système est configuré pour utiliser DHCP.

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"
```

Exemple statique : Modifiez les paramètres suivants dans le fichier `/etc/sysconfig/network-scripts/ifcfg-eth0` ou `/etc/sysconfig/network-scripts/ifcfg-eth1`.

```
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"
```

Chapitre 3. 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, en recyclant les fichiers déjà créés, si nécessaire.

Mise en route

Après le démarrage du système, connectez-vous en utilisant les informations suivantes :

Utilisateur : continuum

Mot de passe : P@ck3t08

Par défaut, la page Recorder State s'affiche. Vous pouvez contrôler les enregistrements en cliquant sur **Start Recorder** ou sur **Stop Recorder**.

Etat de Recorder

Les informations suivantes sont disponibles sur la page Recorder State :

- Recorder status - en cours d'exécution (oui/non)
- Interface recording on
- Directory where PCAP files are stored
- Maximum PCAP Size - taille en Mo
- Duration of system recording time - hr:min:sec
- Packets Captured
- Packets Dropped
- Total number of PCAPS that is created since start of recording
- Storage Space Available

Configuration de Recorder

Sur la page Recorder Configuration, pour capturer le trafic réseau à un débit plus élevé, vous pouvez changer les paramètres de stockage de capture pour une session d'enregistrement. Vous pouvez avoir des débits plus élevés en réduisant le pourcentage de stockage de capture utilisé. Soyez vigilant lors de l'utilisation de cette fonction. L'augmentation du débit de capture maximal provoque la suppression de toutes les données d'index et de capture. Une fois que vous êtes prêt à enregistrer une session, cliquez sur **Start Recorder**.

Caractéristiques du réseau

Pour déterminer le débit de capture maximal ne provoquant aucune suppression, utilisez cette page pour voir le débit du réseau.

Bibliothèque Recorder

La bibliothèque IBM Security QRadar Packet Capture contient un historique des captures en cours et des captures terminées.

Chapitre 4. Obtention de licences

Pour obtenir des licences, vous devez exécuter l'utilitaire d'octroi de licence client en tant qu'utilisateur root.

Avant de commencer

Une connexion réseau est requise.

Procédure

1. Connectez-vous à une session de terminal en tant qu'utilisateur root.
2. Pour exécuter l'utilitaire d'octroi de licence, entrez la commande suivante : `./permkey`
3. Indiquez le type de licence, en entrant la commande suivante : `License type (p = permanent, d = demo)`

   Si l'installation de la licence aboutit, les messages suivants s'affichent :

   ```
   License successfully installed for MAC address your MAC address
   License successfully installed for System ID your system ID
   ```
4. Redémarrez le système.

   Les résultats sont consignés dans le fichier `/var/log/permkey.res`.

   si le message suivant s'affiche après 25 secondes environ, vérifiez que vous disposez d'une connexion Internet et que vous pouvez exécuter la commande ping sur nextcomputing.com.

   ```
   500 Can't connect to nextcomputing.com:80 (Bad hostname 'nextcomputing.com')
   ```
5. Si vous avez installé des licences de démonstration, vous pouvez vérifier le temps restant dont vous disposez en entrant la commande suivante : `n2disk10g |more`

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.

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 ou des marques déposées d'International Business Machines Corporation aux États-Unis et/ou dans d'autres pays. Si ces marques et d'autres marques d'IBM sont accompagnées d'un symbole de marque (® ou ™), ces symboles signalent des marques d'IBM aux Etats-Unis à la date de publication de ce document. Ces marques peuvent également exister et éventuellement avoir été enregistrées dans d'autres pays. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web Copyright and trademark information (www.ibm.com/legal/copytrade.shtml).

Java™ ainsi que tous les logos et toutes les marques incluant Java sont des marques de Sun Microsystems, Inc. aux Etats-Unis et/ou dans certains autres pays.

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

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).