IBM Security QRadar Incident Forensics
Version 7.3.0

QRadar Packet Capture - Aide-mémoire

Important
Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations figurant à la section «Remarques», à la page 7.

Ce document s'applique à IBM QRadar Security Intelligence Platform version 7.3.0 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

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 de cet aide-mémoire 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.

Utilisateurs concernés

Les administrateurs système chargés de l'installation de QRadar Packet Capture doivent maîtriser 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 la note technique Accessing IBM Security Documentation (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Contacter le service clients

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

Instructions relatives aux bonnes pratiques de sécurité

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.

Chapitre 1. Mise à niveau de QRadar Packet Capture

Pour effectuer une mise à niveau depuis QRadar Packet Capture V7.2.8 vers version 7.3.0, installez un groupe de correctifs logiciel cumulé sur un dispositif QRadar Packet Capture. La version logicielle installée sur le dispositif doit être la version 7.2.6.241.

Procédure

1. Vérifiez qu'il ne s'agit pas d'une capture de paquet ou d'activités de recherche en cours.
2. Utilisez SSH pour vous connecter à votre système comme utilisateur `root`.
3. Téléchargez le groupe de correctifs `7.3.0-QRadar-PCAP-build<numéro_build>.sfs` depuis IBM Fix Central (http://www.ibm.com/support/fixcentral/).
4. Copiez le groupe de correctifs dans le répertoire `/tmp`.

   Si le répertoire `/tmp` dispose d'un espace limité, copiez-le dans un autre emplacement ayant un espace suffisant.
5. Créez le répertoire `/updates` en saisissant la commande suivante :

   ```
   mkdir -p /updates
   ```
6. Utilisez la commande **cd** pour vous déplacer vers le répertoire contenant le fichier du groupe de correctifs.

   ```
   cd /tmp
   ```
7. Pour monter le fichier du groupe de correctifs dans le répertoire `/updates`, entrez la commande suivante :

   ```
   mount -o loop -t squashfs 7.3.0-QRadar-PCAP-build<numéro_build>.sfs
   /updates
   ```
8. Pour exécuter le programme d'installation du groupe de correctifs, déplacez-vous dans le répertoire `/updates` et entrez la commande suivante :

   ```
   sh installer.sh
   ```
9. Redémarrez le système.

Chapitre 2. QRadar Packet Capture - Référence rapide

Avant de pouvoir capturer des paquets, vous devez configurer les paramètres réseau et de connexion IBM Security QRadar Packet Capture.

Liste de compatibilité Intel SFP+ et SFP

Le dispositif QRadar Packet Capture ne possède qu'un seul port de capture (DNA0). QRadar Packet Capture n'est pas équipé d'un émetteur-récepteur SFP. Vous devez donc installer soit un SFP+ 10G ou un SFP 1G (Copper RJ45) dans le port de capture.

Pour acquérir des modules SFP pour bvotre dispositif QRadar Packet Capture, voir les sites Web de fournisseur suivants :

- Le site Web Digi-Key (http://www.digikey.com)
- Le site Web Mouser Electronics (http://www.mouser.com)
- Le site Web CDW (http://www.cdw.com)
- Le site Web Newegg (https://www.newegg.com)
- Le site Web Amazon (http://amazon.com)

Lorsque le SFP 1G est installé, il tronque le taux de capture à 1 Gbps.

Si vous désirez avoir plusieurs connexions 1G, vous pouvez placer un commutateur ou un regroupeur à l'avant de la connexion entre le port de communications sortantes 10G et le port SFP+ 10G de QRadar Packet Capture. Ainsi, de multiples ports d'1 Go seront ajoutés à l'interface 10G SFP+ de QRadar Packet Capture.

La liste suivante décrit les exigences de module SFP+ et SFP :

Numéro de référence	**Description**
E10GSFPSR	Dual Rate 10GBASE-SR/1000BASE-SX, Intel Ethernet SFP+ SR Optical
E10GSFPLR	Dual Rate 10GBASE-LR/1000BASE-LX, Intel Ethernet SFP+ LR Optical
FCLF8522P2BTL	1000BASE-T, Emetteur-récepteur Finisar Gigabit Ethernet
453153-001	Emetteur-récepteur HP Gigabit SX

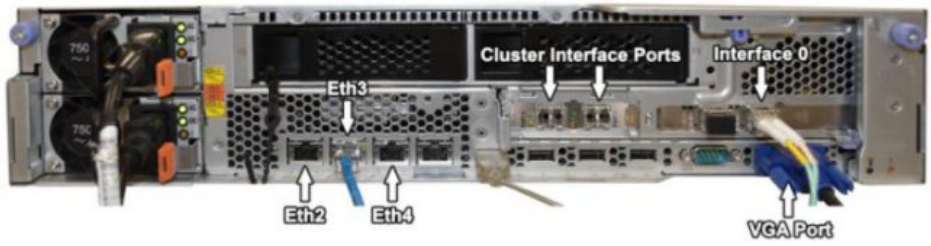
Configuration réseau

Pour configurer le réseau, vous devez disposer d'un écran, d'un clavier et d'une connexion Ethernet à un port intégré. Par défaut, le système a des ports DHCP actifs.

Si vous connaissez l'adresse IP du port Ethernet utilisé, consultez la section Lancement de l'enregistrement.

1. Indiquez une connexion réseau pour l'accès distant au serveur.

   Indiquez une connexion Ethernet à l'un des ports Ethernet embarqués, eth2, eth3 ou eth4, comme le montre le schéma ci-dessous.



2. Indiquez une connexion réseau pour la capture de réseau.

   Indiquez des connexions 10 Gbits fibre en utilisant les ports 0 d'interface qui sont présentés dans le schéma suivant.

   Important : Veillez à ce qu'il y ait 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.

3. 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..`

4. Notez l'adresse IP.

   Une fois que vous êtes connecté, ouvrez un terminal puis entrez la commande suivante : `#ifconfig -a`

   Cette commande fournit l'adresse IP du port Ethernet qui est connecté.

   Remarque : Pour plus d'informations sur la configuration d'une adresse IP statique, consultez le guide d'utilisation de *IBM Security QRadar Packet Capture.*

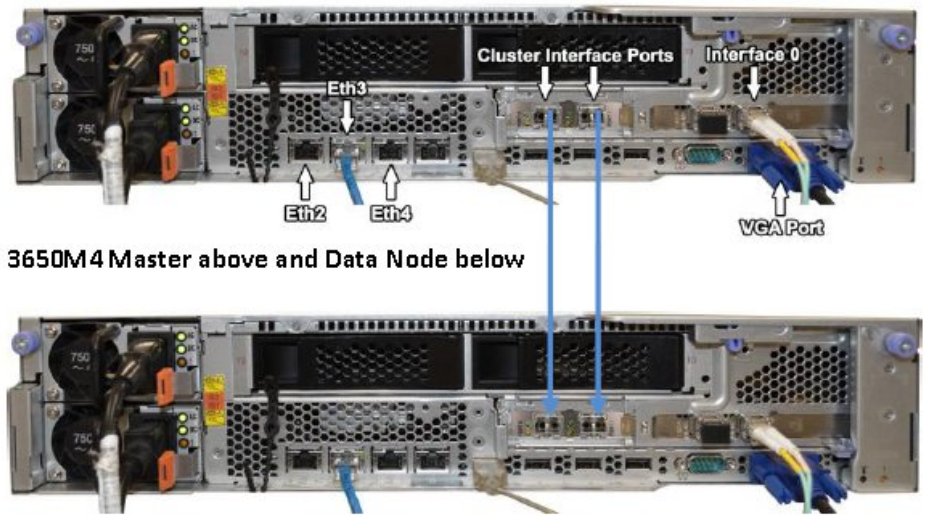
5. Testez la connexion.

   Pour tester la connexion, utilisez la commande ping sur votre réseau interne ou connectez-vous à distance en utilisant SSH sur le port 4477. Assurez-vous de disposer d'une connexion fiable avant de continuer.

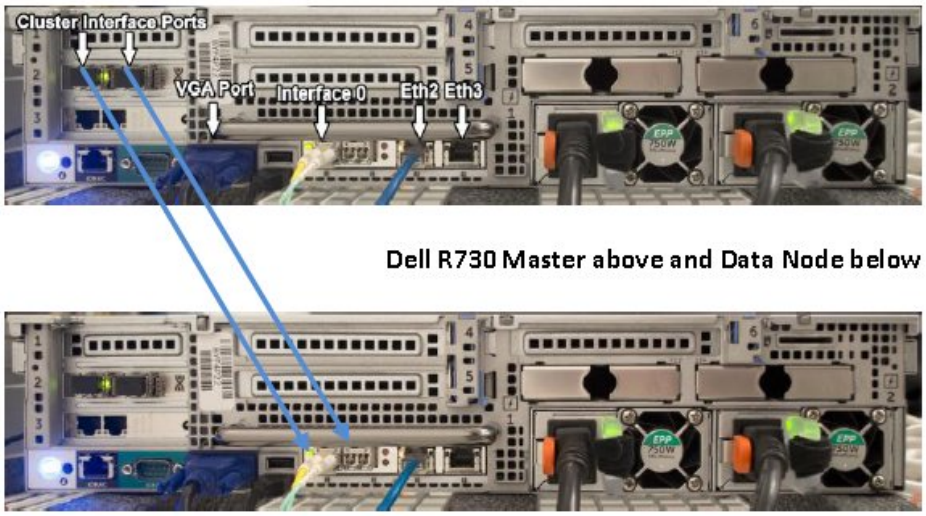
Connectez le cluster

Après avoir connecté avec succès le réseau au système autonome ou maître, branchez l'appareil de capture de paquets maître aux appareils QRadar Packet Capture Data Node. Si vous disposez uniquement d'un système de capture de paquets autonome, cette étape n'est pas nécessaire.

1. Reportez-vous au schéma de matériel pour votre périphérique de capture de paquets.
   - Périphérique de capture de paquet maître IBM System x3650 M4 et connexion Noeud de données QRadar Packet Capture



- Périphérique de capture de paquet Dell R730 et noeud de données QRadar Packet Capture



2. À l'arrière du périphérique de capture de paquets, connectez le port gauche de l'interface de cluster sur le maître au port gauche d'interface de cluster sur le premier nœud de données, comme indiqué par les flèches dans les schémas précédents.
3. S'il existe un deuxième noeud de données, connectez le port droit de l'interface de cluster sur le maître au port droit d'interface sur le second nœud de données.
4. A partir d'un terminal sur le système maître, vérifiez les connexions avec un test ping :

   ```
   ping 1.1.1.2
   ping 2.2.2.2
   ```

5. Si vous ne recevez pas de réponse de la commande ping, intervertissez les connexions de câbles uniquement sur les interfaces de noeuds de données.
   - Si un seul nœud de données est connecté, un seul ping doit répondre correctement.

- Si après avoir commuté les câbles, il n'y a toujours pas de réponse du test ping, commutez les câbles du contrôleur NIC de nœud de données vers le second contrôleur NIC Ethernet optique installé (s'il existe) et répétez le test de ping.

Lancement de l'enregistrement

Après avoir établi une connexion réseau avec le système, vous pouvez commencer à enregistrer les paquets réseau sur le disque et afficher les statistiques sur le trafic d'un réseau.

1. Ouvrez un navigateur Web et accédez au périphérique :

   `https://`*`adresse_IP_PCAP`*`:41390`
2. Connectez-vous en utilisant les informations utilisateur suivantes :

   Utilisateur : `continuum`

   Mot de passe : `P@ck3t08..`
3. Activez chaque nœud de données (esclave) que vous avez connecté physiquement.
4. Démarrez l'enregistrement.

   Après vous être connecté et avoir activé les noeuds de données, allez à la page **Capture State** et cliquez sur **Start Capture**.

   Remarque : Après le début de la capture, une fenêtre de statistiques qui contient tous les détails de capture apparaît.

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 services peuvent être des marques d'IBM ou d'autres sociétés. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web "Copyright and trademark information" à l'adresse www.ibm.com/legal/copytrade.shtml.

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).