IBM Security QRadar
Version 7.3.0

# *Guide d'architecture et de déploiement*

**Important**
Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations figurant à la section «Remarques», à la page 45.

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.

# Présentation des déploiements QRadar

Les informations du guide de déploiement d'IBM® Security QRadar vous permettent de planifier plus facilement l'installation de QRadar.

## Utilisateurs concernés

Ces informations sont destinées aux administrateurs de sécurité responsables de l'examen et de la gestion de la sécurité réseau. Pour utiliser ce guide, vous devez connaître l'infrastructure réseau de votre société et maîtriser les technologies de réseau.

## Documentation technique

Pour savoir comment accéder à plus de documentation technique, aux notes techniques et aux notes sur l'édition, voir Accessing IBM Security Documentation Technical Note (http://www.ibm.com/support/docview.wss?rs=0 &uid=swg21612861).

## 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?rs=0&uid=swg21612861).

## 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. Présentation de l'architecture QRadar

Lorsque vous planifiez ou créez votre déploiement IBM Security QRadar, il est utile de bien connaître l'architecture QRadar pour pouvoir évaluer le fonctionnement des composants QRadar dans votre réseau, puis planifier et créer votre déploiement QRadar.

IBM Security QRadar collecte, traite, agrège et stocke des données réseau en temps réel. QRadar utilise ces données pour gérer la sécurité du réseau en fournissant des informations et une surveillance en temps réel, des alertes et des infractions, ainsi que des réponses aux menaces auxquelles le réseau est confronté.

IBM Security QRadar SIEM (Security Information and Event Management) est une architecture modulaire qui fournit une visibilité en temps réel de votre infrastructure informatique, que vous pouvez utiliser pour la détection et la hiérarchisation des menaces. Vous pouvez adapter QRadar à vos besoins en matière de collecte de journaux et de flux, ainsi que d'analyse. Vous pouvez ajouter des modules intégrés à votre plateforme QRadar, comme QRadar Risk Manager, QRadar Vulnerability Manager et QRadar Incident Forensics.

La plateforme QRadar Security Intelligence fonctionne avec trois couches qui s'appliquent à toute structure de déploiement QRadar, quelle que soit sa taille et sa complexité. Le diagramme ci-dessous illustre les couches constituant l'architecture de QRadar.

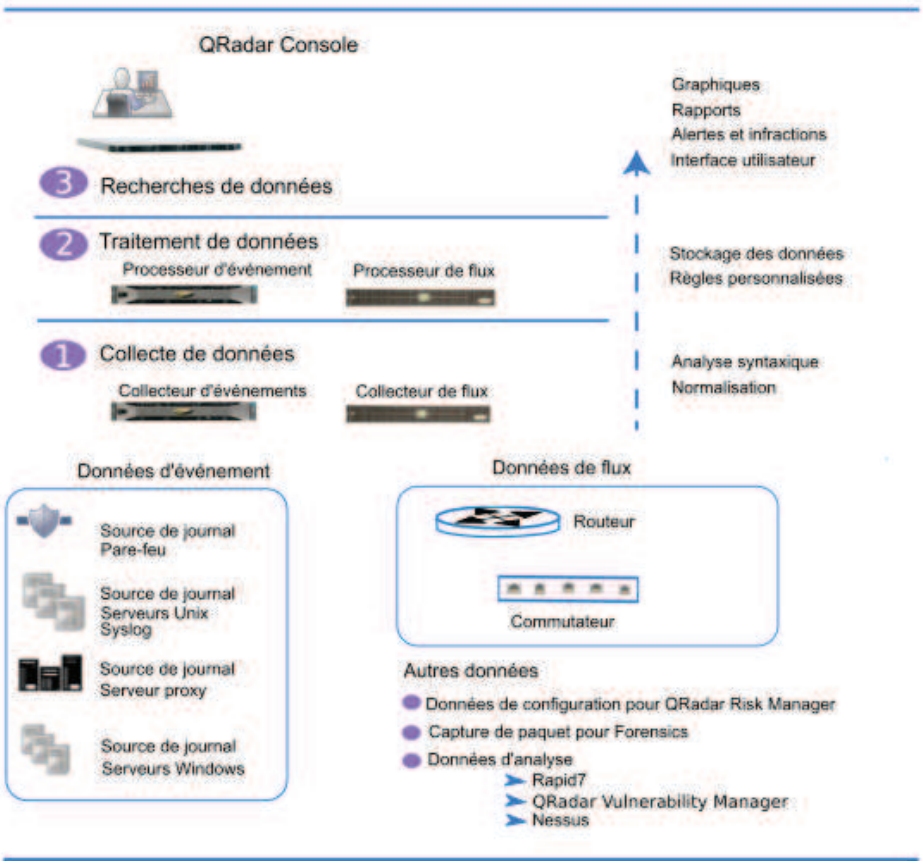



*Figure 1. Architecture de QRadar*

L'architecture de QRadar fonctionne de la même façon quelle que soit la taille des composants ou quel que soit leur nombre dans un déploiement. Les trois couches ci-après illustrées dans le diagramme représentent la fonctionnalité de base de tout système QRadar.

## Collecte de données

La collecte de données constitue la première couche, où des données telles que des événements ou des flux sont collectées depuis votre réseau. Le dispositif tout-en-un vous permet de collecter les données directement depuis votre réseau ; vous pouvez aussi utiliser des collecteurs tels que QRadar Event Collectors ou collecteurs QRadar QFlow Collector pour collecter des données d'événement ou de flux. Les données sont analysées et normalisées avant d'être transmises à la couche de traitement. Lorsque les données brutes sont analysées, elles sont normalisées en vue de leur présentation dans un format structuré et utilisable.

La fonctionnalité de base de QRadar SIEM couvre principalement la collecte de données et de flux.

Les données d'événement représentent des événements qui surviennent à un moment donné dans l'environnement de l'utilisateur. Il peut s'agir de connexions utilisateur, de courriers électroniques, de connexions VPN, de refus de pare-feu, de connexions proxy et de tout autre événement que vous décidez de consigner dans vos journaux d'unité.

Les données de flux sont des informations relatives à l'activité du réseau ou des informations de session qui sont transmises entre deux hôtes sur un réseau, que QRadar traduit en enregistrements de flux. QRadar traduit ou normalise des données brutes en adresses IP, ports, nombres d'octets et de paquets, et d'autres informations en enregistrements de flux, qui représentent effectivement une session entre deux hôtes. En plus de collecter des informations de flux avec un collecteur de flux, il est possible de capturer des paquets complets avec le composant QRadar Incident Forensics.

## Traitement des données

Après la collecte de données, dans la deuxième couche ou couche de traitement des données, les données d'événement et de flux sont exécutées dans le moteur de règles personnalisées (CRE), qui génère des infractions et des alertes, puis les données sont enregistrées dans l'espace de stockage.

Les données d'événement et de flux peuvent être traitées par un dispositif tout-en-un sans qu'il ne soit nécessaire d'ajouter des processeurs d'événement ou des processeurs de flux. Si la capacité de traitement du dispositif tout-en-un est dépassée, il peut être nécessaire d'ajouter des processeurs d'événement, des processeurs de flux ou tout autre dispositif de traitement afin de gérer les exigences supplémentaires. Il se peut également que vous ayez besoin de plus de capacité de stockage, que vous pouvez obtenir en ajoutant des noeuds de données.

D'autres fonctions telles que QRadar Risk Manager (QRM), QRadar Vulnerability Manager (QVM) ou QRadar Incident Forensics permettent de collecter différents types de données et fournissent d'autres options.

QRadar Risk Manager collecte les informations de configuration de l'infrastructure réseau et fournit une carte de la topologie de votre réseau. Vous pouvez utiliser ces données pour gérer les risques en simulant divers scénarios de réseau en altérant les configurations et en implémentant des règles sur votre réseau.

Utilisez QRadar Vulnerability Manager pour analyser votre réseau et rechercher les données de vulnérabilité ou gérer les données de vulnérabilité qui sont collectées par d'autres scanners tels que Nessus et Rapid7. Les données de vulnérabilité collectées sont utilisées pour identifier les divers risques de sécurité sur votre réseau.

Utilisez QRadar Incident Forensics pour procéder à des enquêtes d'expert approfondies et réexécuter des sessions réseau complètes.

## Recherches de données

Dans la troisième couche ou couche supérieure, les données qui ont été collectées et traitées par QRadar (recherches, analyses, rapports, alertes et enquêtes sur les infractions) sont mises à la disposition des utilisateurs. Les utilisateurs peuvent rechercher et gérer les tâches d'administration de la sécurité pour leur réseau depuis l'interface utilisateur dans QRadar Console.

Dans un système tout-en-un, toutes les données sont collectées, traitées et stockées sur le dispositif tout-en-un.

Dans les environnements répartis, QRadar Console ne procède pas au traitement des événements et des flux, ni à leur stockage. A la place, la console est utilisée principalement comme interface utilisateur, dont les utilisateurs peuvent se servir

pour les recherches, les rapports, les alertes et les enquêtes.

## Composants QRadar

Les composants IBM Security QRadar permettent d'échelonner un déploiement QRadar et de gérer la collecte et le traitement des données sur des réseaux répartis.

**Important :** les niveaux de version et de groupe de correctifs des logiciels, pour tous les dispositifs IBM Security QRadar dans un déploiement, doivent être identiques. Les déploiements qui utilisent des versions différentes des logiciels ne sont pas pris en charge car les environnements qui utilisent des versions mixtes peuvent empêcher le déclenchement de certaines règles et la création ou la mise à jour d'infractions, et générer des erreurs dans les résultats de recherche.

Les déploiements de QRadar peuvent inclure les composants suivants :

**QRadar Console**

QRadar Console fournit l'interface utilisateur de QRadar ainsi que des vues présentant les événements et les flux en temps réel, des rapports, des infractions, des informations sur les actifs et des fonctions d'administration.

Dans les déploiements de QRadar répartis, utilisez QRadar Console pour gérer les hôtes incluant d'autres composants.

**QRadar Event Collector**

Ce composant collecte des événements depuis des sources de journal locales et distantes et normalise les événements de source de journal bruts afin de les formater en vue de leur utilisation par QRadar. Le dispositif Event Collector regroupe ou fusionne les événements identiques afin de conserver l'utilisation du système et envoie les informations au dispositif Event Processor

- Utilisez QRadar Event Collector 1501 dans les emplacements distants avec des liaisons WAN lentes. Les dispositifs Event Collector n'enregistrent pas les événements en local. A la place, ils collectent et analysent les événements avant de les envoyer à un dispositif Event Processor en vue de leur stockage.
- Le dispositif Event Collector peut utiliser des limiteurs de bande passante et des planifications pour l'envoi des événements au dispositif Event Processor afin d'éviter les limitations de réseau étendu telles qu'une connectivité intermittente.
- Le dispositif Event Collector est affecté à une licence imposant un nombre maximal d'événements par seconde qui correspond au dispositif Event Processor auquel il est connecté.

**QRadar Event Processor**

Le dispositif Event Processor traite les événements collectés à partir d'un ou de plusieurs composants Event Collector. Il traite les événements à l'aide du moteur de règles personnalisées (CRE). Si des événements sont mis en correspondance avec les règles personnalisées du moteur de règles personnalisées qui sont prédéfinies dans la console, le dispositif Event Processor exécute l'action définie pour la réponse à la règle.

Chaque dispositif Event Processor dispose d'un stockage local et les données d'événement sont stockées sur le processeur ; elles peuvent également être stockées sur un noeud de données.

Le taux de traitement des événements est déterminé par votre licence, qui définit le nombre d'événements par seconde. Si vous dépassez la limite

imposée pour le nombre d'événements par seconde, les événements sont placés en mémoire tampon et restent dans les files d'attente source du dispositif Event Collector jusqu'à ce que le taux baisse. Toutefois, si vous continuez de dépasser le nombre d'événements par seconde défini par votre licence et que la file d'attente est remplie, votre système supprime des événements et QRadar émet un avertissement signalant le dépassement du nombre d'événements par seconde imposé par votre licence.

Lorsque vous ajoutez un composant Event Processor à un dispositif tout-en-un, la fonction de traitement des événements assurée jusqu'alors par le dispositif tout-en-un est transférée au composant Event Processor.

**QRadar QFlow Collector**

Ce composant collecte des flux en se connectant à un port SPAN ou à un tap réseau. IBM Security QRadar QFlow Collector prend également en charge la collecte de sources de données reposant sur des flux externes, comme NetFlow à partir de routeurs.

Les collecteurs QRadar QFlow Collector ne sont pas des systèmes de capture de paquet complet. Pour la capture de paquet complet, envisagez l'option QRadar Incident Forensics. Le dispositif QRadar QFlow Collector 1310 notamment peut acheminer des paquets à un dispositif QRadar Packet Capture, qui permet la collecte de flux et de paquets depuis une source de paquets simple.

Vous pouvez installer une instance de QRadar QFlow Collector sur votre propre matériel ou utiliser l'un des dispositifs QRadar QFlow Collector.

**Restriction :** QRadar Log Manager ne prend pas en charge la collecte de flux ni les collecteurs de flux, qui ne sont pris en charge que dans les déploiements de QRadar SIEM.

**QRadar Flow Processor**

Ce composant traite les flux provenant d'un ou de plusieurs dispositifs QRadar QFlow Collector. Le dispositif processeur de flux peut également collecter des flux réseau externes tels que NetFlow, J-Flow et sFlow directement depuis des routeurs sur votre réseau. Vous pouvez utiliser le dispositif processeur de flux pour échelonner votre déploiement QRadar afin de gérer des taux de flux par minute plus élevés. Les processeurs de flux comportent un dispositif processeur de flux intégré et un stockage interne pour les données de flux. Lorsque vous ajoutez un dispositif processeur de flux à un dispositif tout-en-un, la fonction de traitement assurée jusqu'alors par le dispositif tout-en-un est transférée au composant processeur de flux.

**QRadar Data Node**

Les noeuds de données permettent aux déploiements QRadar nouveaux et existants d'ajouter de la capacité de stockage et de traitement à la demande lorsque cela est nécessaire. Ils permettent d'augmenter la vitesse de recherche dans votre déploiement en fournissant des ressources matérielles supplémentaires sur lesquelles exécuter les requêtes de recherche.

Pour plus d'informations sur la gestion des composants QRadar, voir le manuel *IBM Security QRadar Administration Guide*.

### Spécifications du dispositif QRadar

Le tableau ci-dessous contient des indications concernant l'utilisation de dispositifs QRadar spécifiques dans votre déploiement.

*Tableau 1. Présentation des dispositifs QRadar*

| Dispositif | Description |
|---|---|
| QRadar 2100 | Solution ne pouvant pas être étendue pour les déploiements avec 10 à 200 employés. |
| QRadar 3105 (All-in-One) | Présente une capacité accrue par rapport au système QRadar 2100, et permet d'ajouter des processeurs d'événement et des processeurs de flux. |
| QRadar 3105 (Console) | Si votre déploiement traite plus de 5000 événements par seconde, vous devez utiliser un système QRadar 3105 (Console) avec des processeurs d'événement distribués. Le système QRadar 3105 (Console) utilise le traitement d'événement et le stockage externes afin de libérer des ressources pour la mise à disposition de rapports, de résultats de recherche et des actions d'interface utilisateur plus rapides. |
| QRadar 3128 (All-in-One) | Présente une capacité accrue par rapport au système QRadar 3105 (All-in-One). |
| QRadar 3128 (Console) | Présente une capacité accrue par rapport au système QRadar 3105 (Console). |
| Collecteurs et processeurs xx05 | 12 processeurs<br><br>64 Go de mémoire RAM<br><br>6,2 To d'espace de stockage utilisable |
| Collecteurs et processeurs xx28 | 28 processeurs<br><br>128 Go de mémoire RAM<br><br>40 To d'espace de stockage utilisable<br><br>Couplage de collecteurs et processeurs xx28 avec le système QRadar 3128 (Console) pour accroître les performances. |

Pour plus d'informations sur les dispositifs QRadar, voir le manuel *IBM Security QRadar Hardware Guide*.

## Evénements et flux QRadar

Les fonctions de base d'IBM Security QRadar SIEM permettent de gérer la sécurité du réseau en surveillant les flux et les événements.

La différence majeure entre les données d'événement et les données de flux est la suivante : un événement, en général un journal d'une action spécifique telle qu'une connexion utilisateur ou une connexion VPN, survient à une heure précise, et est consigné à ce moment-là. Un flux est l'enregistrement d'une activité réseau qui peut durer plusieurs secondes, minutes, heures ou jours, selon l'activité dans la session. Par exemple, une demande Web peut télécharger plusieurs fichiers tels que

des images, des annonces et des vidéos, et durer 5 à 10 secondes, ou la session d'un utilisateur qui regarde un film sur Netflix peut durer quelques heures. Le flux est un enregistrement d'activité réseau entre deux hôtes.

## Evénements

QRadar accepte les journaux d'événements des sources de journal qui se trouvent sur votre réseau. Une source de journal est une source de données telle qu'un pare-feu ou un système de prévention contre les intrusions qui crée un journal des événements.

QRadar accepte des événements des sources de journal à l'aide de protocoles tels que syslog, syslog-tcp et SNMP. Il peut également configurer des connexions sortantes pour extraire des événements à l'aide de protocoles tels que SCP, SFTP, FTP, JDBC, Check Point OPSEC et SMB/CIFS.

## Pipeline d'événements

Pour que vous puissiez consulter et utiliser les données d'événement dans QRadar Console, les événements sont collectés depuis des sources de journal, puis traités par le Event Processor. Un dispositif QRadar tout-en-un fonctionne comme le Event Collector et le Event Processor, en plus de remplir le rôle de QRadar Console.

QRadar peut collecter des événements à l'aide d'un dispositif Event Collector dédié ou en utilisant un dispositif tout-en-un où le service de collecte d'événements et le service de traitement des événements s'exécutent sur le dispositif tout-en-un.

Le diagramme ci-dessous illustre les couches du pipeline d'événements.

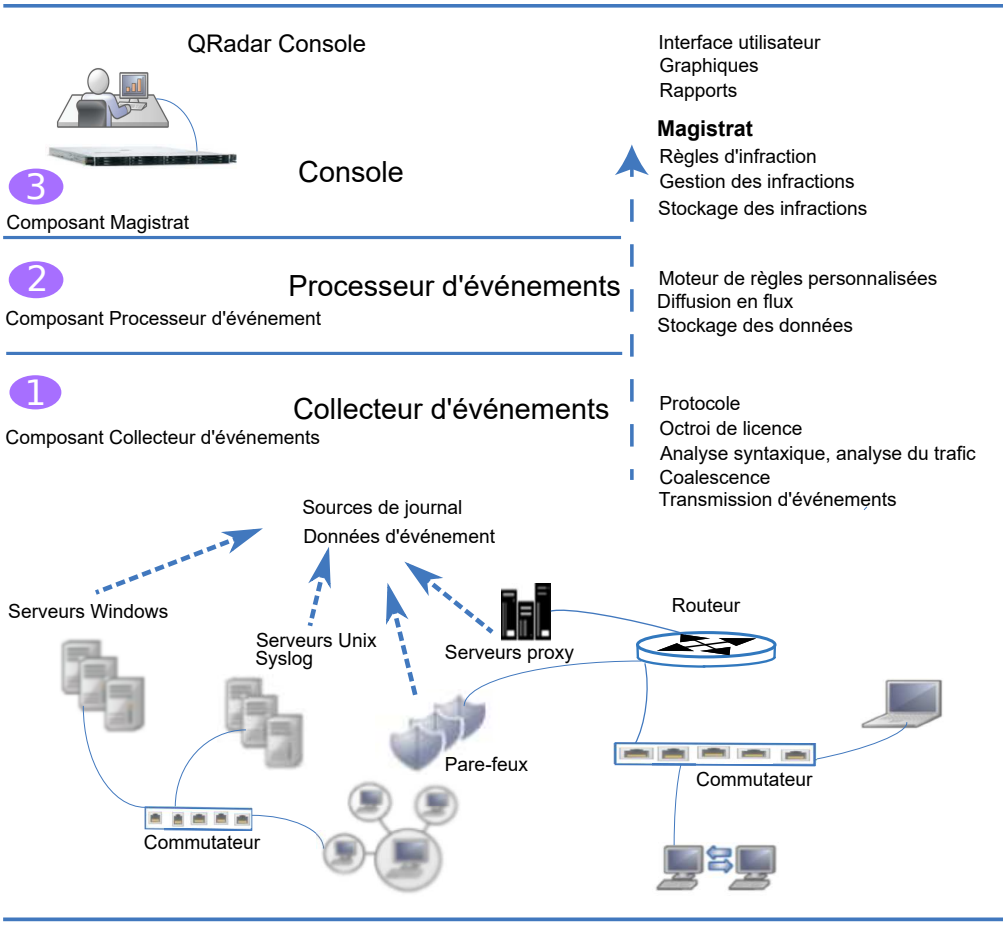



*Figure 2. Pipeline d'événements*

### Collecte d'événements

Le composant Event Collector assure les fonctions suivantes :

- Protocole

  Il collecte les données depuis des protocoles de source de journal tels que Syslog, JDBC, OPSEC, Log File et SNMP.
- Régulation de licence

  Il surveille le nombre d'événements entrants sur le système pour gérer les files d'entrée et l'octroi de licence définissant le nombre d'événements par seconde.
- Analyse syntaxique

  Il prend les événements bruts de l'unité source et analyse les zones dans un format utilisable par QRadar.
- Analyse du trafic de source de journal et détection automatique

  Il applique les données d'événement analysées et normalisées aux gestionnaires de services de données possibles qui prennent en charge la détection automatique.
- Coalescence

  Les événements sont analysés, puis fusionnés en fonction d'attributs d'événement communs.
- Transmission d'événements

Il applique les règles de routage pour le système afin d'acheminer des données vers des cibles hors site, des systèmes Syslog externes, des systèmes JSON et d'autres systèmes SIEM (Security Information and Event Management).

Lorsque le Event Collector reçoit les événements depuis des sources de journal tels que des pare-feux, les événements sont placés dans des files d'entrée en vue de leur traitement.
La taille des files d'attente varie en fonction de la méthode ou du protocole utilisé, et depuis ces files d'attente, les événements sont analysés et normalisés. Le processus de normalisation implique la conversion des données brutes dans un format comportant des zones telles que l'adresse IP, que QRadar peut utiliser.

QRadar reconnaît les sources de journal connues à l'aide du nom d'hôte ou de l'adresse IP source figurant dans l'en-tête.
QRadar analyse des événements provenant de sources de journal connues et les fusionne dans des enregistrements. Les événements provenant de sources de journal nouvelles ou inconnues qui n'ont pas encore été détectées sont redirigés vers le moteur d'analyse du trafic (détection automatique).

Lorsque de nouvelles sources de journal sont détectées, un message de demande de configuration requérant l'ajout de la source de journal est envoyé à QRadar Console. Si la détection automatique est désactivée ou si vous avez dépassé la limite imposée par votre licence pour les sources de journal, les nouvelles sources de journal ne sont pas ajoutées.

**Traitement des événements**

Le composant Event Processor assure les fonctions suivantes :

- Moteur de règles personnalisées (CRE)

  Le moteur de règles personnalisées est en charge du traitement des événements reçus par QRadar et de leur comparaison en fonction de règles définies, du suivi des systèmes impliqués dans les incidents au fil du temps, et de la génération de notifications envoyées aux utilisateurs. Lorsque des événements correspondent à une règle, une notification indiquant qu'un événement spécifique a déclenché une règle est envoyée depuis le Event Processor au magistrat dans QRadar Console. Le composant magistrat dans QRadar Console crée des infractions et les gère. Lorsque des règles sont déclenchées, des réponses ou des actions telles que des notifications, un syslog, un protocole SNMP, des courriers électroniques, de nouveaux événements et des infractions sont générées.

- Diffusion en flux

  Il envoie des données d'événement en temps réel à QRadar Console lorsqu'un utilisateur affiche des événements depuis l'onglet **Activité du journal** avec Temps réel (diffusion en flux). Les événements diffusés en flux ne proviennent pas de la base de données.

- Stockage des événements (Ariel)

  Base de données de série temporelle pour les événements, dans laquelle les données sont stockées toutes les minutes. Les données sont stockées à l'emplacement de traitement de l'événement.

Le Event Collector envoie des données d'événement normalisées au Event Processor où les événements sont traités par le moteur de règles personnalisées (CRE). Si des événements sont mis en correspondance avec

les règles personnalisées du moteur de règles personnalisées qui sont prédéfinies dans QRadar Console, le Event Processor exécute l'action qui est définie pour la réponse à la règle.

**Magistrat dans QRadar Console**

Le composant magistrat assure les fonctions suivantes :

- Règles d'infraction

  Il surveille les infractions et y réagit, par exemple en générant des notifications par courrier électronique.

- Gestion des infractions

  Il met à jour les infractions actives, change le statut des infractions et permet aux utilisateurs d'accéder aux informations sur les infractions depuis l'onglet **Infractions**.

- Stockage des infractions

  Il écrit des données d'infraction dans une base de données Postgres.

Le composant Magistrate Processing Core (MPC) est en charge de la corrélation des infractions avec des notifications d'événement provenant de plusieurs composants Event Processor. Seul QRadar Console ou le dispositif tout-en-un possède un composant magistrat.

## Flux

Les flux QRadar représentent une activité réseau en normalisant des adresses IP, des ports, des nombres d'octets et de paquets, ainsi que d'autres données, en enregistrements de flux, qui sont effectivement des enregistrements de sessions réseau entre deux hôtes. Le composant dans QRadar qui collecte et crée des informations de flux s'appelle QFlow.

La collecte de flux QRadar ne constitue pas une capture de paquet complet. Pour les sessions réseau qui s'étendent sur plusieurs intervalles de temps (minutes), le pipeline de flux génère un enregistrement à la fin de chaque minute avec les données en cours pour les mesures telles que les octets et les paquets. Il peut exister plusieurs enregistrements (par minute) dans QRadar avec la même valeur "Heure du premier paquet" ; toutefois, les valeurs "Heure du dernier paquet" sont incrémentées.

Un flux commence lorsque le collecteur de flux détecte le premier paquet possédant une adresse IP source, une adresse IP de destination, un port source, un port de destination et d'autres options de protocole spécifiques uniques.

Chaque nouveau paquet est évalué. Les nombres d'octets et de paquets sont ajoutés aux compteurs statistiques dans l'enregistrement de flux. A la fin d'un intervalle, un enregistrement de statut du flux est envoyé à un processeur de flux et les compteurs statistiques pour le flux sont réinitialisés. Un flux se termine lorsqu'aucune activité pour le flux n'est détectée pendant la durée configurée.

QFlow peut traiter des flux depuis les sources internes et externes suivantes :

- Les sources externes sont des sources de flux telles que netflow, sflow et jflow.

  Les sources externes peuvent être envoyées à un collecteur de flux dédié ou à un processeur de flux tel que le dispositif QRadar Flow Processor 1705. Elles ne requièrent pas autant de traitement sur l'UC car les paquets ne sont pas traités pour générer des flux. Dans cette configuration, vous pouvez disposer d'un collecteur de flux dédié et d'un processeur de flux qui, tous les deux, reçoivent

et créent des données de flux. Dans les environnements plus petits (moins de 50 mégabits par seconde), un dispositif tout-en-un peut gérer l'ensemble du traitement des données.

- Le collecteur de flux collecte des flux internes en se connectant à un port SPAN ou à un tap réseau.

  QRadar QFlow Collector 1310 peut réacheminer des paquets complets depuis sa carte de capture vers un dispositif de capture de paquet, mais ne capture pas les paquets complets lui-même.

Le diagramme ci-dessous présente les options de collecte de flux dans un réseau.

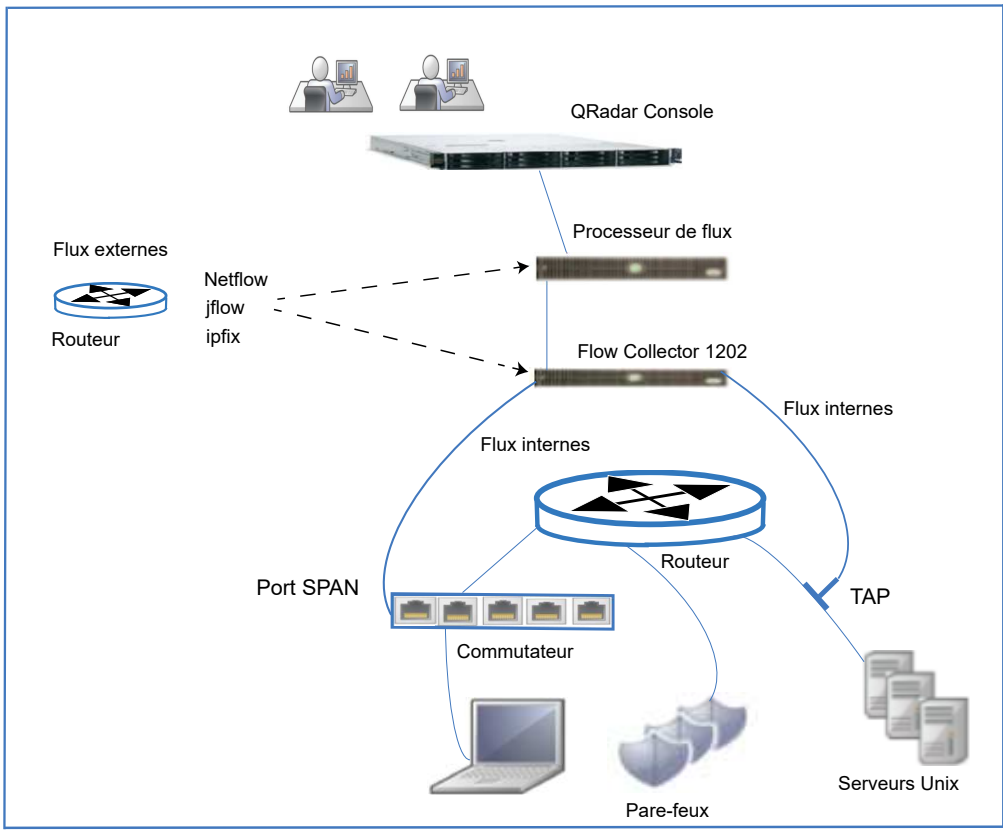



*Figure 3. Flux QRadar*

## Pipeline de flux

Le collecteur de flux génère des données de flux à partir de paquets bruts qui sont collectés depuis des ports de surveillance tels que des ports SPAN, des taps et des sessions de contrôle, ou depuis des sources de flux externes telles que netflow, sflow et jflow. Ces données sont ensuite converties au format de flux QRadar et envoyées dans le pipeline en vue de leur traitement.

Le processeur de flux assure les fonctions suivantes :

- Dédoublonnage de flux

  Le dédoublonnage de flux est un processus qui supprime les flux en double lorsque plusieurs collecteurs de flux fournissent des données à des dispositifs processeurs de flux.
- Recombinaison asymétrique

En charge de la combinaison des deux côtés de chaque flux lorsque les données sont fournies de façon asymétrique. Ce processus peut reconnaître les flux de chaque côté et les combiner en un seul enregistrement. Cependant, il n'existe parfois qu'un seul côté du flux.

- Régulation de licence

  Il surveille le nombre de flux entrants sur le système pour gérer les files d'entrée et l'octroi de licence.

- Réacheminement

  Il applique des règles de routage pour le système, comme l'envoi de données de flux à des cibles hors site, des systèmes Syslog externes, des systèmes JSON et d'autres systèmes SIEM (Security Information and Event Management).

Les données de flux transitent par le moteur de règles personnalisées (CRE) et sont corrélées en fonction des règles configurées, puis une infraction peut être générée en fonction de cette corrélation. Vous pouvez consulter les infractions dans l'onglet **Infractions**.

# Chapitre 2. Présentation des déploiements de QRadar

L'architecture d'IBM Security QRadar prend en charge des déploiements de diverses tailles et topologies, du déploiement d'hôte unique, où tous les composants logiciels s'exécutent sur un seul système, au déploiement de plusieurs hôtes, où des dispositifs tels que des collecteurs d'événement, des collecteurs de flux, des noeuds de données, des processeurs d'événement et des processeurs de flux possèdent des rôles spécifiques.

Le premier exemple de déploiement décrit un déploiement de dispositif tout-en-un unique pour une entreprise de taille moyenne. Les exemples suivants décrivent les options de déploiement dont l'entreprise dispose au fur et à mesure de sa croissance. Les exemples expliquent à quel moment ajouter des composants QRadar, comme des processeurs de flux, des collecteurs d'événement et des noeuds de données, et à quel moment il peut être nécessaire de colocaliser des composants spécifiques.

Les exigences à respecter pour votre déploiement QRadar dépendent de la capacité du déploiement que vous avez choisi pour traiter et stocker toutes les données que vous voulez analyser sur votre réseau.

Avant de planifier votre déploiement, répondez aux questions suivantes :

- De quelle façon votre entreprise utilise-t-elle Internet ? Envoyez-vous des données par téléchargement autant que vous en recevez ? Une utilisation accrue peut augmenter votre exposition à des problèmes de sécurité potentiels.
- Combien d'événements par seconde et de flux par minute devez-vous surveiller ?

  Les exigences de capacité de licence pour les événements par seconde et les flux par minute augmentent avec la croissance d'un déploiement.
- Quelle quantité d'informations devez-vous stocker, et pendant combien de temps ?

Le diagramme ci-dessous présente les composants QRadar que vous pouvez utiliser pour collecter, traiter et stocker les données d'événement et de flux dans votre déploiement QRadar. Un dispositif tout-en-un inclut les capacités de collecte de données, de traitement, de stockage, de surveillance, de recherche, de génération de rapports et de gestion des infractions.

Le Event Collector collecte des données d'événement depuis des sources de journal sur votre réseau, puis envoie les données d'événement au Event Processor. Le collecteur de flux collecte des données de flux depuis des périphériques réseau tels qu'un port SPAN de commutateur, puis envoie les données au processeur de flux. Les deux processeurs traitent les données provenant des collecteurs et les mettent à disposition dans QRadar Console. Les dispositifs de processeur peuvent stocker des données mais peuvent aussi utiliser les noeuds de données à cette fin. Le dispositif QRadar Console est utilisé pour la surveillance, les recherches de données, la génération de rapports, la gestion des infractions et l'administration de votre déploiement QRadar.

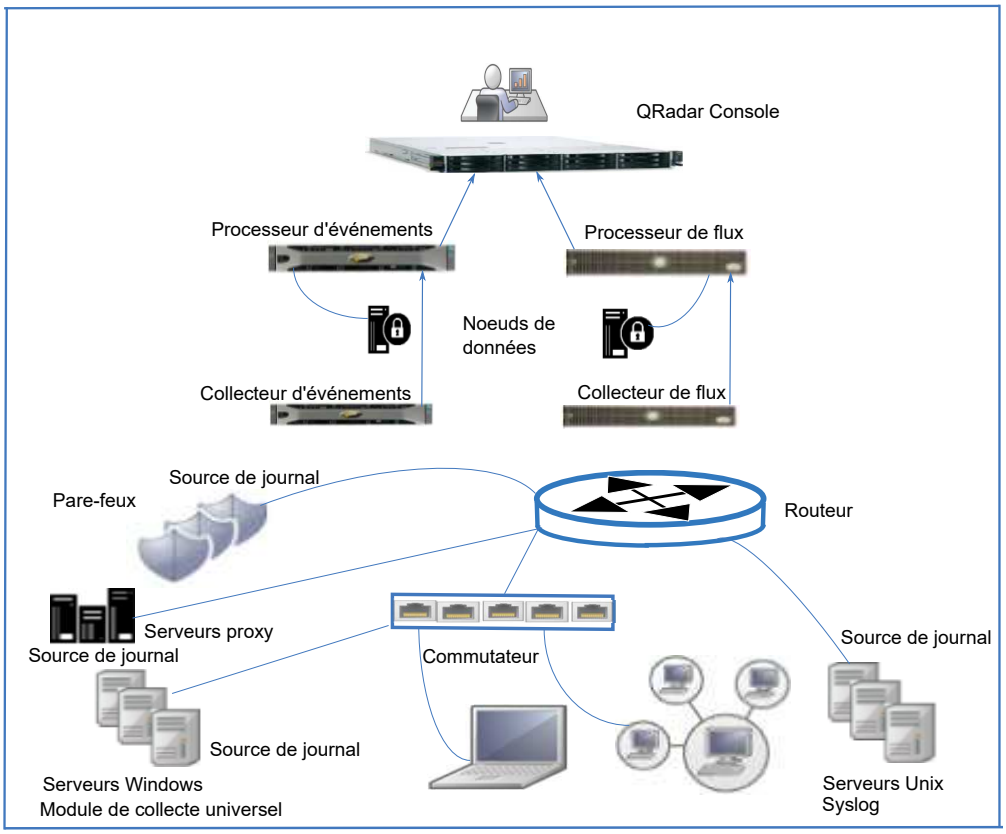



*Figure 4. Composants d'événement et de flux QRadar*

## Déploiement tout-en-un

Lors d'un déploiement QRadar d'hôte unique, vous pouvez utiliser un dispositif QRadar tout-en-un. Il s'agit d'un serveur unique collectant des données, comme des journaux de données d'événement syslog, des événements Windows ou encore des données de flux, depuis votre réseau.

Un dispositif tout-en-un est adapté aux entreprises de taille moyenne dont la visibilité est faible sur Internet, ou à des fins de test et d'évaluation. Les déploiements de serveur unique sont idéaux pour les entreprises qui surveillent l'activité réseau et les événements tels que les services d'authentification et l'activité de pare-feu.

Un dispositif tout-en-un fournit les capacités dont vous avez besoin, jusqu'à un certain point, déterminé par votre licence et les spécifications matérielles du système. Par exemple, un dispositif QRadar 3105 (All-in-One) traite généralement jusqu'à 5000 événements par seconde et 200 000 flux par minute, alors qu'un dispositif QRadar 3128 (All-in-One) traite généralement jusqu'à 15 000 événements par seconde et 300 000 flux par minute.

**Une entreprise de fabrication déploie un serveur QRadar unique**

Votre entreprise de fabrication compte moins de 1000 employés. Vous déployez un dispositif QRadar 3105 All-in-One pour collecter, traiter et surveiller des données

d'événement et de flux. Ce déploiement vous permet de collecter jusqu'à 5000 événements par seconde et 200 000 flux par minute.

Le diagramme ci-dessous illustre un dispositif tout-en-un qui collecte des données à partir de sources d'événements et de flux, traite les données, et fournit une application Web dans laquelle vous pouvez rechercher les menaces de sécurité, les surveiller et y répondre.

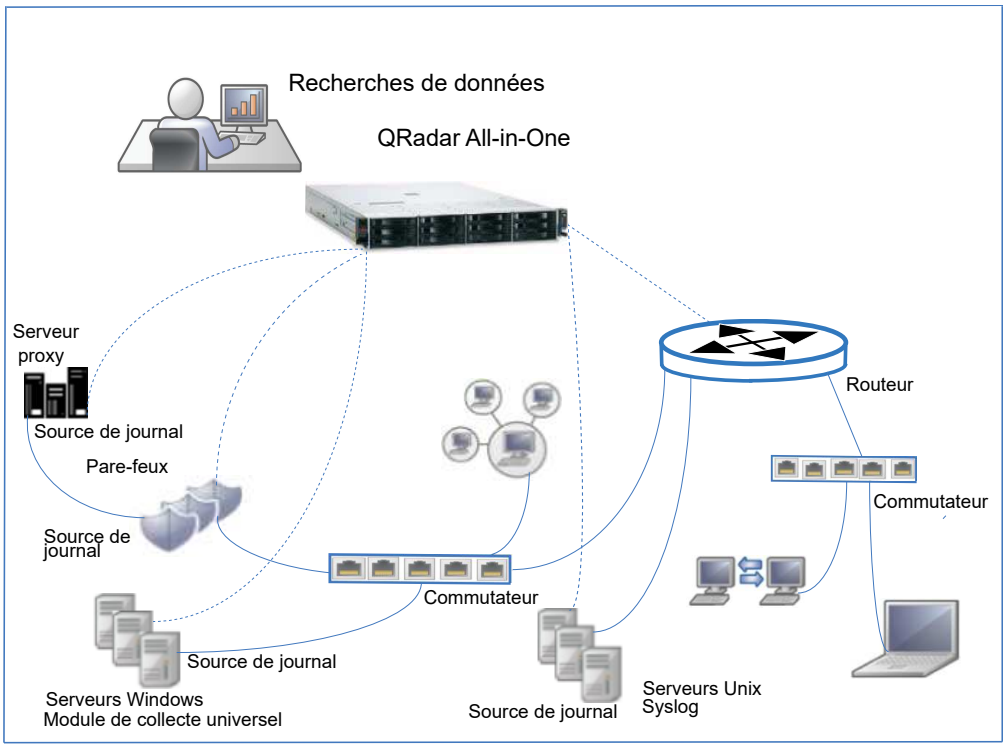



*Figure 5. Déploiement tout-en-un*

Le dispositif QRadar tout-en-un effectue les tâches suivantes :

- Il collecte des données d'événement et de flux réseau, puis normalise les données dans un format de données utilisable par QRadar.
- Il analyse et stocke les données, et identifie les menaces auxquelles l'entreprise est confrontée.
- Il fournit l'accès à l'application Web QRadar.

Au fur et à mesure que la taille de vos sources de données augmente, ou que vos besoins en matière de traitement ou de stockage deviennent plus importants, vous pouvez ajouter des dispositifs afin d'étendre votre déploiement.

## Extension de déploiements pour plus de capacité

Votre entreprise peut créer ou étendre un déploiement au-delà d'un dispositif tout-en-un IBM Security QRadar lorsque la capacité de traitement ou de stockage des données n'est pas suffisante ou lorsque vous avez des exigences spécifiques en matière de collecte de données.

La topologie et la composition de votre déploiement QRadar dépendent de la capacité de ce dernier en matière de collecte, de traitement et de stockage de l'ensemble des données à analyser sur votre réseau.

Pour obtenir des estimations approximatives des événements par seconde (EPS) ou des flux par minute (FPM) à traiter dans votre déploiement, utilisez la taille des journaux collectés dans les pare-feux, les serveurs proxy et les box Windows.

### Motifs d'ajout de collecteurs d'événement ou de flux dans un déploiement tout-en-un

Il peut être nécessaire d'ajouter des collecteurs d'événement ou de flux à votre déploiement dans les situations suivantes :

- La configuration requise pour la collecte de données va au-delà de la fonction de collecte du dispositif tout-en-un.
- Vous devez collecter des événements et des flux à un autre emplacement que l'emplacement d'installation de votre dispositif tout-en-un.
- Vous surveillez des sources de flux par paquets de grande taille ou à débit élevé qui sont plus rapides que la connexion 50 Mbps sur le dispositif tout-en-un

Un dispositif tout-en-un 3128 peut collecter jusqu'à 15 000 événements par seconde (EPS) et 300 000 flux par minute (FPM). Si vos exigences de collecte sont plus importantes, vous pouvez ajouter des collecteurs d'événement et des collecteurs de flux à votre déploiement. Par exemple, vous pouvez ajouter un composant QRadar QFlow Collector 1202, qui collecte jusqu'à 3 Gbps.

Un dispositif tout-en-un traite les événements et les flux collectés. En ajoutant des collecteurs d'événement et des collecteurs de flux, vous pouvez utiliser le traitement généralement effectué par le dispositif tout-en-un pour les recherches et les autres tâches de sécurité.

Pour les sources de flux par paquets, vous devez disposer d'un collecteur de flux connecté à un processeur de flux ou à un dispositif tout-en-un dans lequel il n'existe pas de dispositif processeur de flux. Vous pouvez collecter des sources de flux externes (NetFlow ou IPFIX, par exemple) sur un dispositif processeur de flux ou un dispositif tout-en-un.

## Ajout de collecteurs distants à un déploiement

Ajoutez des dispositifs QRadar Event Collector ou QRadar Flow Collector afin d'étendre un déploiement lorsque vous avez besoin de collecter plus d'événements localement et de collecter des événements et des flux provenant d'un emplacement distant.

Supposons que vous êtes une entreprise de fabrication disposant d'un déploiement tout-en-un QRadar et que vous ajoutez un système de commerce électronique et un bureau de vente à distance. Vous devez désormais surveiller s'il existe des menaces de sécurité et vous pouvez également subir des audits PCI.

Vous employez plus de personnel et l'utilisation d'Internet consiste maintenant principalement à effectuer des opérations de téléchargement entre vos employés et Internet. Voici quelques caractéristiques s'appliquant à votre entreprise.

- La licence d'événements par seconde (EPS) en cours est de 1 000 EPS.
- Vous souhaitez collecter des événements et des flux dans le bureau des ventes et des événements dans la plateforme de commerce électronique.
- La collecte d'événements dans la plateforme de commerce électronique requiert jusqu'à 2 000 événements par seconde (EPS).
- La collecte d'événements dans le bureau de vente à distance requiert jusqu'à 2 000 événements par seconde (EPS).

- La licence de flux par minute (FPM) est suffisante pour collecter des flux dans le bureau distant.

**Vous effectuez les actions suivantes :**

1. Vous ajoutez la plateforme de commerce électronique à votre siège principal puis vous ouvrez un bureau de vente à distance.
2. Vous installez un dispositif Event Collector et un collecteur de flux dans le bureau de ventes à distance qui envoie des données via Internet au dispositif tout-en-un de votre siège principal.
3. Vous mettez à niveau votre licence EPS en passant de 1 000 EPS à 5 000 EPS afin de répondre aux exigences pour les événements supplémentaires collectés dans le bureau distant.

Le diagramme suivant présente un exemple de déploiement lorsqu'un dispositif Event Collector et un collecteur de flux sont ajoutés dans un bureau distant.

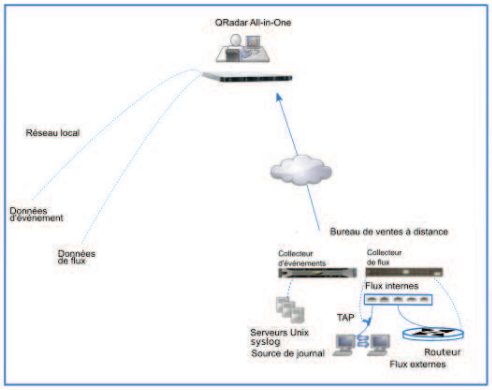



*Figure 6. Collecteurs dans le bureau distant*

Dans ce déploiement, les processus suivants ont lieu :

- Dans le bureau distant, le dispositif Event Collector collecte des données dans les sources de journal et le collecteur de flux collecte des données dans les routeurs et les commutateurs. Les collecteurs fusionnent et normalisent les données.
- Les collecteurs compressent et envoient les données au dispositif tout-en-un via le réseau étendu.
- Le dispositif tout-en-un traite et stocke les données.
- Votre entreprise surveille l'activité réseau en utilisant l'application Web QRadar pour les recherches, l'analyse, la génération de rapports ainsi que pour la gestion des alertes et des infractions.
- Le dispositif tout-en-un collecte et traite les événements du réseau local.

## Ajout de capacité de traitement à un déploiement tout-en-un

Ajoutez des processeurs d'événement et des processeurs de flux à votre déploiement QRadar afin d'augmenter la capacité de traitement et le stockage. L'ajout de processeurs libère des ressources sur votre console QRadar Console en transférant le traitement et le stockage sur des serveurs dédiés.

Lorsque vous ajoutez des processeurs d'événement ou des processeurs de flux à un dispositif tout-en-un, ce dernier se comporte comme une console QRadar Console. La puissance de traitement sur le dispositif tout-en-un est dédiée à la gestion et à la recherche de données envoyées par les processeurs et les données sont désormais stockées sur les processeurs d'événement et d'autres périphériques de stockage et non sur la console.

Vous ajoutez généralement des processeurs d'événement et des processeurs de flux à votre déploiement QRadar pour les raisons suivantes :

- Lorsque votre déploiement croît, la charge de travail dépasse la capacité de traitement du dispositif tout-en-un.
- Votre centre des opérations de sécurité emploie un plus grand nombre d'analystes qui effectuent un plus grand nombre de recherches simultanées.
- Le nombre de types de données surveillées et la durée de conservation augmentent, ce qui provoque une augmentation des exigences en matière de traitement et de stockage.
- Au fur et à mesure de la croissance de votre équipe d'analystes de sécurité, il est nécessaire de disposer de meilleures performances de recherche.

L'exécution de plusieurs recherches QRadar simultanées et l'ajout de types de source de journal que vous surveillez ont des conséquences sur les performances de traitement de votre dispositif tout-en-un. Lorsque vous augmentez le nombre de recherches et la quantité de données surveillées, ajoutez des processeurs d'événement et des processeurs de flux pour améliorer les performances de votre déploiement QRadar.

Lorsque vous définissez votre déploiement QRadar de telle sorte qu'il contienne plus de 15 000 EPS et de 300 000 FPM sur le dispositif tout-en-un le plus puissant, vous devez ajouter des dispositifs de processeur afin de traiter ces données.

## Exemple : Ajout d'un dispositif QRadar Event Processor à votre déploiement

Vous pouvez ajouter un dispositif QRadar Event Processor 1628, qui collecte et traite jusqu'à 40 000 EPS. Vous augmentez votre capacité en ajoutant 40 000 EPS supplémentaires dès que vous ajoutez un dispositif QRadar Event Processor 1628 à votre déploiement. Ajoutez un dispositif QRadar Flow Processor 1728, qui collecte et traite jusqu'à 1 200 000 FPM.

QRadar Event Processor 1628 est un collecteur et un processeur. Si vous avez un réseau distribué, il est recommandé d'ajouter des collecteurs d'événement pour répartir la charge et libérer des ressources système sur le dispositif Event Processor.

Dans le diagramme suivant, la capacité de traitement est ajoutée lorsqu'un dispositif Event Processor et un dispositif processeur de flux sont ajoutés à un dispositif QRadar 3128 (All-in-One) et que les modifications suivantes ont lieu :

- Le traitement d'événement et de flux est déplacé du dispositif tout-en-un vers les processeurs d'événement et de flux.
- La capacité de traitement d'événement est augmentée jusqu'à 40 000 EPS, ce qui inclut les 15 000 EPS qui se trouvaient dans le dispositif tout-en-un.
- La capacité de traitement de flux est augmentée jusqu'à 1 200 000 FPM, ce qui inclut les 300 000 FPM qui se trouvaient dans le dispositif tout-en-un.
- Les données envoyées par les collecteurs d'événement et de flux sont traitées et stockées sur les processeurs d'événement et de flux.

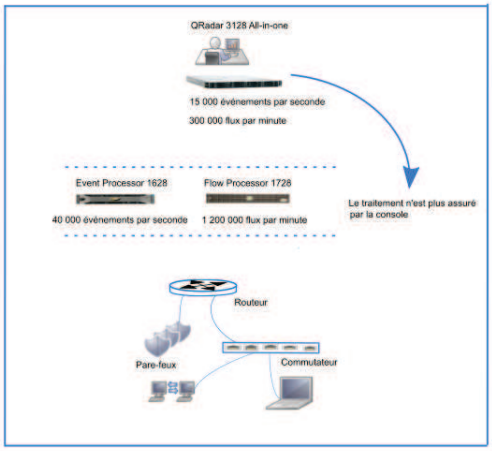



*Figure 7. Ajout de capacité de traitement*

Les performances de recherche sont plus rapides lorsque vous installez des processeurs d'événement et des processeurs de flux sur le même réseau que votre console QRadar Console.

L'ajout de processeurs et de collecteurs étend la capacité de traitement de votre déploiement QRadar. Vous pouvez également étendre la capacité de stockage de votre déploiement. Les besoins en matière de conservation de données de votre entreprise peuvent augmenter lorsque le trafic est plus important ou lorsque des modifications sont apportées aux règles de conservation. L'ajout de noeuds de données à votre déploiement étend la capacité de stockage de données et améliore les performances de recherche.

## Ajout de collecteurs à des processeurs

Ajoutez des collecteurs d'événement et des collecteurs de flux aux processeurs d'événement et aux processeurs de flux pour les même raisons que vous ajoutez des collecteurs à un dispositif tout-en-un :

- La configuration requise pour la collecte de données va au-delà de la fonction de collecte de votre processeur.
- Vous devez collecter des événements et des flux à un autre emplacement que celui où votre processeur est installé.
- Vous surveillez les sources de flux par paquet.

**Remarque :** collecteurs d'événement peut mettre en mémoire tampon des événements mais les collecteurs de flux ne peuvent pas mettre des flux en mémoire tampon.

Etant donné que les performances de recherche sont améliorées lorsque les processeurs sont installés sur le même réseau que la console, l'ajout de collecteurs à des emplacements distants puis l'envoi de ces données au processeur accélèrent vos recherches QRadar.

## Déploiements répartis géographiquement

Dans les déploiements répartis géographiquement, une faible connectivité ou une connectivité intermittente aux centres de données distants peut avoir des conséquences sur votre déploiement IBM Security QRadar. Les réglementations locales peuvent également affecter votre déploiement. Il peut par exemple être nécessaire de respecter les réglementations de certains pays imposant de conserver les données à leur emplacement d'origine. Cela implique de conserver les collecteurs sur site. Si vous devez conserver les données à leur emplacement d'origine, vous devez alors conserver le processeur sur site.

Par exemple, votre entreprise est en pleine expansion, ce qui implique non seulement une augmentation de l'activité sur le réseau mais également le développement du déploiement QRadar dans d'autres pays. Les lois concernant la conservation des données sont différentes en fonction des pays, ainsi vous devez prendre en compte ces réglementations lors de la planification du déploiement QRadar.

Prenez en compte les conditions suivantes :

- Votre entreprise doit collecter des données d'événement d'un site ayant une connectivité intermittente.
- Votre entreprise doit respecter les réglementations de conservation de données des pays dans lesquels les données sont collectées. Par exemple, si la réglementation allemande impose que les données restent dans le pays, ces dernières ne doivent pas être stockées dans d'autres pays.

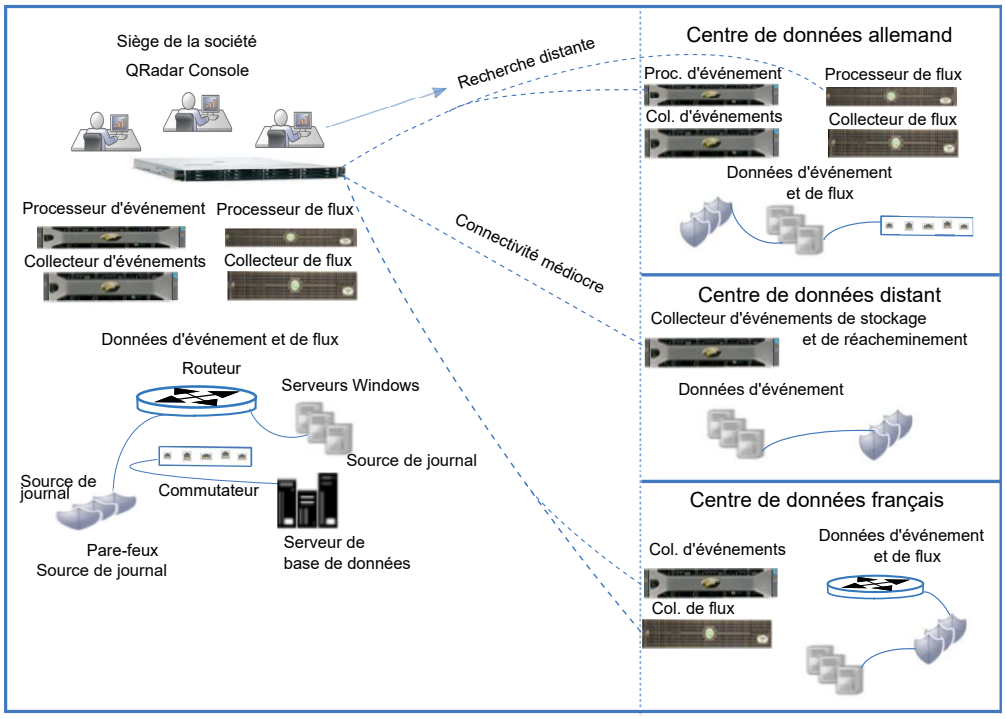



*Figure 8. Déploiement réparti géographiquement*

Dans un déploiement réparti géographiquement, les processus suivants se produisent.

- Votre entreprise installe des collecteurs et des processeurs dans le centre de données allemand en respectant les lois locales relatives aux données.
- Dans le centre de données français, votre entreprise installe des collecteurs, de telle sorte que les données soient envoyées au siège social par les collecteurs. Les données y sont ensuite traitées et stockées. Lorsque les dispositifs de processeur se trouvent sur le même segment de réseau à haute vitesse que la console QRadar Console, la vitesse des recherches est améliorée.
- Votre entreprise ajoute un dispositif Event Collector de stockage et de retransmission disposant de connexions de transmission planifiées et à débit limité dans le centre de données distant. Ces connexions compensent la connectivité réseau intermittente et permettent d'éviter des demandes de bande passante supplémentaires pendant les heures de bureau.

Si vous recherchez en permanence des données sur un processeur distant, il est préférable que ce dernier se trouve sur le même segment réseau à haut débit que la console QRadar Console. Si la bande passante entre la console QRadar Console et le processeur distant n'est pas suffisante, vos recherches peuvent être longues, particulièrement lorsque vous effectuez plusieurs recherches simultanées.

## Déploiements QRadar Vulnerability Manager

Recherchez et gérez les vulnérabilité de votre réseau en déployant IBM Security QRadar Vulnerability Manager. Améliorez la sécurité de votre réseau en intégrant des fonctions complémentaires, telles IBM BigFix et IBM Security SiteProtector.

IBM Security QRadar Vulnerability Manager détecte des vulnérabilités sur vos applications et vos périphériques réseau. Le logiciel ajoute du contexte aux vulnérabilités, définit les priorités pour le risque d'actif dans votre réseau et prend en charge la résolution des vulnérabilités détectées.

Pour une meilleure protection, vous pouvez intégrer QRadar Risk Manager, qui permet un ajustement des scores de risque pour les actifs à haut risque, les chemins d'attaque active et la topologie réseau par rapport à la conformité aux règles. QRadar Vulnerability Manager et QRadar Risk Manager sont rassemblés sous la même offre et dépendent de la même licence de base.

En fonction du produit que vous installez et selon que vous décidez de mettre à niveau IBM Security QRadar ou d'installer un nouveau système, l'onglet **Vulnérabilités** peut ne pas s'afficher. Accédez à IBM Security QRadar Vulnerability Manager en utilisant l'onglet **Vulnérabilités**. Si vous installez IBM Security QRadar SIEM, l'onglet **Vulnérabilités** est activé par défaut avec une clé de licence temporaire. Si vous installez QRadar Log Manager, l'onglet **Vulnérabilités** n'est pas activé. Vous pouvez utiliser l'option **Essayer** pour essayer QRadar Vulnerability Manager pendant 30 jours. Vous pouvez acheter la licence de QRadar Vulnerability Manager séparément ou l'activer à l'aide d'une clé de licence. Pour plus d'informations sur la mise à niveau, voir le document *IBM Security QRadar - Guide de mise à niveau*.

### Composants QRadar Vulnerability Manager

Les informations suivantes présentent le processeur QRadar Vulnerability Manager.

- Le processeur d'analyse prend en charge la planification et la gestion des analyses ainsi que la délégation des différentes tâches aux scanners de votre réseau.

- Vous ne pouvez avoir qu'un seul processeur d'analyse dans un déploiement QRadar.
- Lorsque vous installez QRadar Vulnerability Manager sous licence sur un système tout-en-un, un processeur de vulnérabilité incluant un composant d'analyse est automatiquement déployé sur votre console QRadar Console.
- Le processeur de vulnérabilité fournit par défaut un composant d'analyse. Si nécessaire, vous pouvez déplacer le processeur de vulnérabilité vers un autre hôte géré dans votre déploiement
- Si vous ajoutez un dispositif d'hôte géré 600 et que QRadar Vulnerability Manager est utilisé pour la première fois, le processeur d'analyse est alors affecté au dispositif d'hôte géré 600.
- Le processeur d'analyse est régi par la licence de traitement, qui détermine le nombre maximal d'actifs pouvant être traités par QRadar Vulnerability Manager.
- Le processeur d'analyse peut s'exécuter sur la console QRadar Console ou sur un hôte géré.

Les informations suivantes présentent le scanner QRadar Vulnerability Manager.

- Vous pouvez déployer un scanner sur une machine virtuelle ou en tant que logiciel uniquement.
- Vous pouvez déployer un dispositif de scanner dédié QRadar Vulnerability Manager (dispositif 610).
- Vous pouvez déployer un scanner sur une console QRadar Console ou sur les hôtes gérés suivants : collecteur de flux, processeur de flux, Event Collector, Event Processor ou noeud de données.
- Le nombre d'actifs que vous pouvez analyser à l'aide d'un scanner est déterminé par la capacité de ce dernier et nullement par la licence.

## Composants et processus d'analyse

Les travaux d'analyse sont effectués par un processeur et un composant de scanner. Le diagramme suivant présente les processus et les composants d'analyse qui s'exécutent.

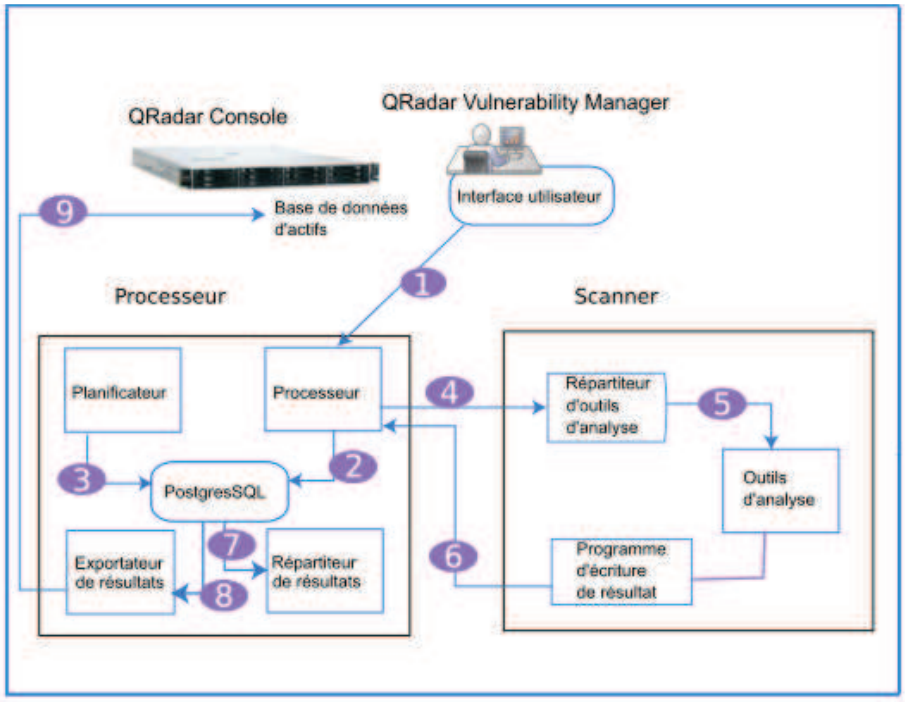



*Figure 9. Processus et composants d'analyse*

La liste suivante présente les différentes étapes du processus d'analyse :

1. Vous créez un travail d'analyse en définissant des paramètres, tels que les adresses IP des actifs, le type d'analyse et les données d'identification requises pour les analyses authentifiées.
2. Le travail d'examen est accepté par le processeur, consigné et ajouté à la base de données avec des informations de planification afin de déterminer quand le travail s'exécute.
3. Le composant de planificateur gère la planification des analyses. Lorsque le planificateur lance une analyse, il détermine la liste des outils requis et les place en file d'attente avant leur appel puis les outils sont affectés au scanner approprié.
4. Les scanners recherchent en permanence dans le processeur d'analyse des outils d'analyse à exécuter en envoyant un ID de scanner unique. Une fois que le planificateur a placé en file d'attente les outils adaptés au scanner spécifique, les outils sont envoyés au scanner pour appel.

   QRadar Vulnerability Manager utilise la méthodologie d'arborescence d'attaques pour gérer les analyses et déterminer quels sont les outils lancés. Les différentes phases sont les suivantes : reconnaissance d'actif, reconnaissance de port/service, analyse de service et analyse de correctif.
5. Le répartiteur exécute et gère chaque outil d'analyse de la liste. Pour chaque outil exécuté, le répartiteur envoie un message au processeur qui indique le début et la fin de l'exécution d'un outil d'analyse.
6. La sortie de l'outil d'analyse est lue par le programme d'écriture de résultat, qui transmet ensuite ces résultats au processeur.

7. Le répartiteur des résultats traite les résultats bruts des outils d'analyse et les enregistre dans la base de données Postgres.
8. Le programme d'exportation des résultats recherche dans la base de données du processeur les analyses terminées et exporte les résultats dans la console QRadar Console.
9. Les résultats exportés sont ajoutés dans la base de données QRadar dans laquelle les utilisateurs peuvent consulter et gérer les résultats de l'analyse.

## Déploiement tout-en-un

Vous pouvez exécuter QRadar Vulnerability Manager à partir d'un système tout-en-un dans lequel les fonctions d'analyse et de traitement se trouvent sur la console. Les informations suivantes présentent les tâches pouvant être effectuées dans une configuration standard :

- Analyse de 255 actifs ou moins.
- Analyses de reconnaissance illimitées.
- Utilisation du scanner hébergé pour l'analyse de zone démilitarisée.
- Gestion des données d'analyse provenant de scanners tiers intégrés à QRadar.
- Déploiement d'un scanner sur les hôtes gérés.
- Déploiement illimité de logiciels autonomes ou de scanners virtuels.

## Extension d'un déploiement

A mesure de la croissance de votre déploiement, il peut être nécessaire de déplacer la fonction de traitement hors de la console QRadar Console afin de libérer des ressources. Vous pouvez également souhaiter que le déploiement des scanners s'effectue à proximité de vos actifs.

Les différentes raisons pouvant vous amener à ajouter des scanners à votre déploiement sont présentées ci-dessous.

- Analyse des actifs à un autre emplacement que le processeur QRadar Vulnerability Manager.
- Analyse d'un grand nombre d'actifs simultanément pendant une courte période.
- Ajout d'un scanner afin d'éviter l'analyse via un pare-feu qui est une source de journal. Vous pouvez également ajouter le scanner directement au réseau en ajoutant une interface sur l'hôte de scanner qui ignore le pare-feu.

Le diagramme suivant présente un déploiement d'analyse avec une analyse externe et des scanners déployés sur les hôtes gérés.

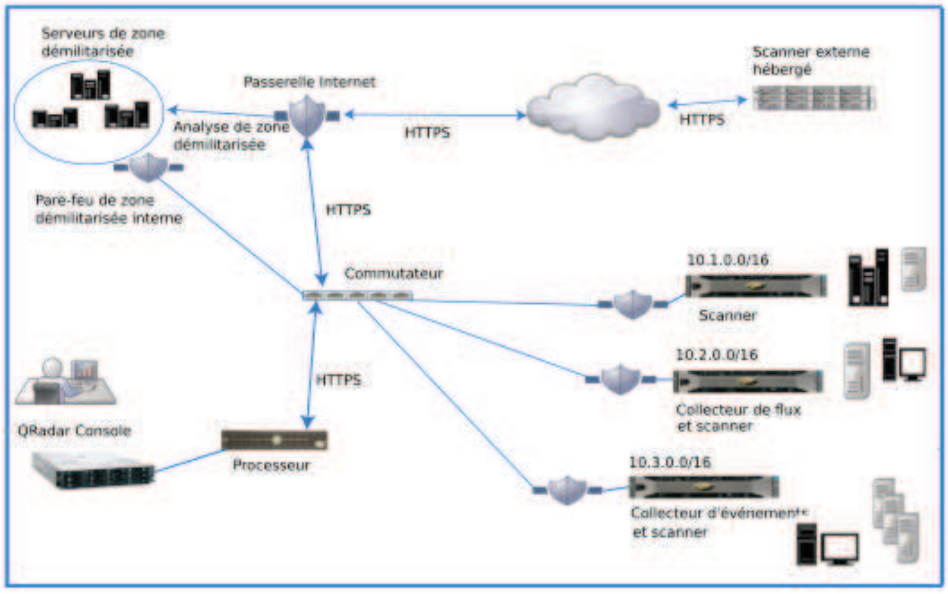



*Figure 10. Déploiement d'analyse*

## Scanner hébergé pour zone démilitarisée

Un scanner hébergé analyse votre zone démilitarisée à partir d'Internet en utilisant votre adresse IP publique. Pour analyser les actifs dans la zone démilitarisée afin de détecter des vulnérabilités, il n'est pas nécessaire de déployer un programme d'analyse dans votre zone démilitarisée. Vous devez configurer QRadar Vulnerability Manager avec un scanner IBM hébergé se trouvant hors de votre réseau. Pour plus d'informations, voir *IBM Security QRadar Vulnerability Manager - Guide d'utilisation*.

## Intégrations QRadar Vulnerability Manager

IBM Security QRadar Vulnerability Manager s'intègre à IBM BigFix afin de vous permettre de filtrer et de hiérarchiser les vulnérabilités pouvant être corrigées. BigFix offre une visibilité et un contrôle partagés entre les opérations informatiques et la sécurité. BigFix applique des fixlets aux vulnérabilités de priorité élevée identifiées et envoyées par QRadar Vulnerability Manager à BigFix. Les fixlets sont des packages que vous déployez dans vos actifs ou noeuds finaux pour résoudre des vulnérabilités spécifiques.

QRadar Vulnerability Manager s'intègre à IBM Security SiteProtector afin d'optimiser les règles du système de prévention des intrusions. Lorsque vous configurez IBM Security SiteProtector, les vulnérabilités détectées par les analyses

sont automatiquement transmises à IBM Security SiteProtector. IBM Security SiteProtector ne reçoit les données de vulnérabilité provenant des analyses QRadar Vulnerability Manager exécutées qu'après la configuration de l'intégration.

### Scanners tiers

QRadar Vulnerability Manager inclut une plateforme de gestion des vulnérabilités efficace, quelle que soit la source des données d'analyse. QRadar Vulnerability Manager est intégré en toute transparence à des scanners tiers, tels Nessus, nCircle et Rapid 7.

Vous devez disposer de la fonction d'analyse de QRadar Vulnerability Manager pour les actions suivantes :

- Analyse à la demande et pilotée par événements
- Analyse utilisant la liste de surveillance et la base de données d'actifs
- Analyse effectuée à partir d'hôtes gérés et de dispositifs QRadar existants
- Détection des vulnérabilités nouvellement publiées ne se trouvant dans aucun résultat d'analyse

Vous devez disposer de QRadar Risk Manager pour les actions suivantes :

- Gestion des vulnérabilités en fonction du trafic, des vulnérabilités et des actifs
- Ajustement des scores de vulnérabilité et de l'évaluation des risques en fonction du contexte.

## QRadar Risk Manager et QRadar Vulnerability Manager

Améliorez la sécurité de votre réseau en intégrant IBM Security QRadar Risk Manager à IBM Security QRadar Vulnerability Manager. Les sources de données, telles que les données d'analyse, permettent à QRadar Risk Manager d'identifier les risques de sécurité, de règles et de compatibilité dans votre réseau et de calculer la probabilité de l'exploitation des risques.

QRadar Vulnerability Manager et QRadar Risk Manager sont rassemblés sous la même offre et dépendent de la même licence de base.

Ajoutez un dispositif QRadar Risk Manager 700 pour bénéficier des fonctions suivantes :

- Evaluation de la conformité
- Politiques d'administration du risque dépendant des données de vulnérabilité et des scores de risque vous permettant d'identifier rapidement les vulnérabilités à haut risque.
- Visibilité dans la vue de topologie réseau des chemins d'exploitation potentiels pour les menaces éventuelles et les réseaux non sécurisés.
- Filtrage en fonction des politiques d'administration du risque.
- Visualisation des topologies
- Réduction du nombre de faux positifs dans les évaluations de vulnérabilité.
- Visibilité des vulnérabilités bloquées par des pare-feux et des systèmes de prévention contre les intrusions (IPS).

### Application QRadar Risk Manager

Installez QRadar Risk Manager séparément sur un dispositif QRadar Risk Manager 700.

Vous devez installer IBM Security QRadar Console avant de configurer le dispositif QRadar Risk Manager. Il est recommandé d'installer QRadar et QRadar Risk Manager sur le même commutateur réseau.

Un seul dispositif QRadar Risk Manager est requis par déploiement.

Le diagramme suivant présente un déploiement incluant un scanner et QRadar Risk Manager.

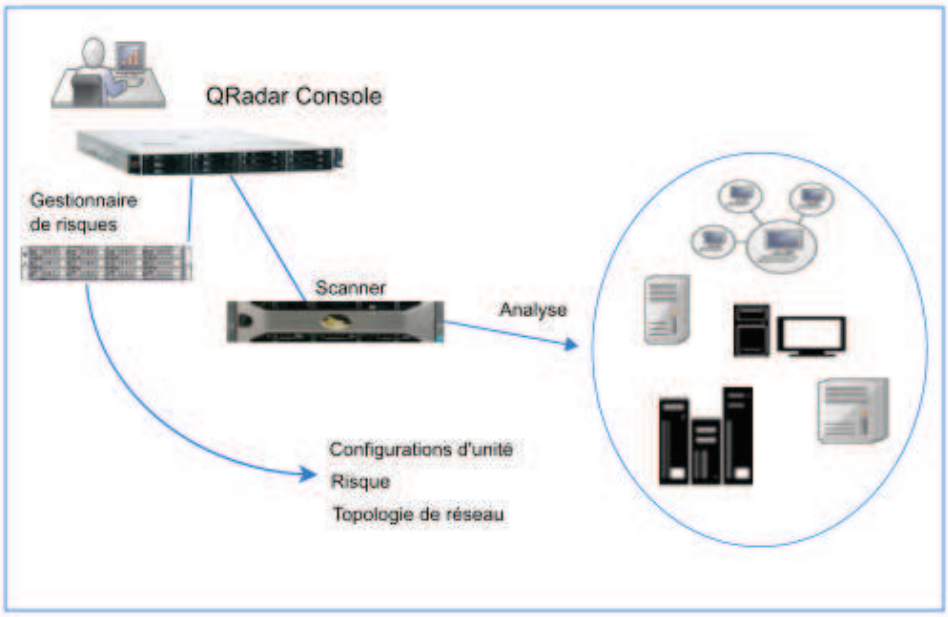



*Figure 11. Analyse du déploiement avec Risk Manager*

Utilisez Risk Manager pour effectuer les tâches suivantes :

- Gestion des risques centralisée
- Affichage et filtrage de votre topologie réseau
- Importation et comparaison des périphériques réseau
- Visualisation des connexions entre les unités réseau.
- Recherche parmi les règles de pare-feu.
- Visualisation des règles existantes et comptage des événements pour les règles déclenchées.
- Recherche de périphériques et de chemins
- Demande de connexions réseau

- Simulation des sorties possibles pour la mise à jour des configurations de périphérique.
- Surveillance et audit de votre réseau afin d'en garantir la conformité.
- Simulation de menaces ou d'attaques d'un modèle virtuel.
- Recherche des vulnérabilités.

## Forensics et collecte de paquet complet

Utilisez IBM Security QRadar Incident Forensics dans votre déploiement pour reproduire les actions étape par étape d'un pirate informatique potentiel et mener une enquête d'expert approfondie concernant les incidents de sécurité réseau malveillants suspectés.

QRadar Incident Forensics reconstruit les données réseau brutes liées à un incident de sécurité telles qu'elles étaient à l'origine.

QRadar Incident Forensics est intégré à IBM QRadar Security Intelligence Platform et est compatible avec un grand nombre d'offres de capture de paquet tierces.

QRadar Incident Forensics fournit un dispositif QRadar Packet Capture facultatif pour le stockage et la gestion des données utilisées par QRadar Incident Forensics si aucun autre périphérique PCAP (capture de paquets réseau) n'est déployé. Vous pouvez installer un nombre illimité de ces dispositifs en tant que dispositif TAP réseau ou sous-réseau pour collecter les données de paquets brutes.

### Composants QRadar Packet Capture

Les composants suivants peuvent être inclus dans un déploiement QRadar :

**QRadar Console**
Fournit l'interface utilisateur du produit QRadar. Lors de déploiements distribués, utilisez QRadar Console pour gérer plusieurs hôtes QRadar Incident Forensics Processor.

**QRadar Incident Forensics Processor**

Fournit l'interface utilisateur du produit QRadar Incident Forensics. Cette interface contient des outils permettant de retracer les actions étape par étape des cybercriminels, de reconstituer les données réseau brutes liées à un incident de sécurité, d'effectuer des recherches dans des données non structurées et de reproduire visuellement les sessions et les événements.

Vous devez ajouter QRadar Incident Forensics Processor en tant qu'hôte géré pour pouvoir utiliser les fonctions Forensics de sécurité intelligente.

**QRadar Incident Forensics Standalone**
Fournit l'interface utilisateur du produit QRadar Incident Forensics. L'installation de QRadar Incident Forensics Standalone fournit les outils dont vous avez besoin pour effectuer des études Forensics. Seules les fonctions d'étude et d'administration Forensics associées sont disponibles.

**QRadar Packet Capture**

Vous pouvez installer un dispositif QRadar Packet Capture facultatif. S'il n'existe aucun autre dispositif de capture de paquet réseau (PCAP) déployé, vous pouvez utiliser ce dispositif pour stocker les données utilisées par QRadar Incident Forensics. Vous pouvez installer un nombre illimité de ces dispositifs en tant que dispositif TAP réseau ou sous-réseau pour collecter les données de paquets brutes.

Si vous n'avez pas de périphérique de capture de paquet connecté, vous pouvez charger manuellement les fichiers de capture de paquet à l'aide de l'interface utilisateur ou de FTP.

En fonction des besoins de votre réseau et de la procédure de capture de paquet, vous pouvez connecter jusqu'à cinq périphériques de capture de paquet à un dispositif QRadar Incident Forensics.

**Dispositifs QRadar Packet Capture Data Node**

Pour disposer de capacités de stockage supplémentaires, vous pouvez connecter jusqu'à deux dispositifs QRadar Packet Capture Data Node à chaque système QRadar Packet Capture maître.

## Déploiement tout-en-un

Dans un déploiement autonome ou tout-en-un, vous installez le logiciel IBM Security QRadar Incident Forensics Standalone. Ces déploiements reviennent à installer le composant QRadar Console et l'hôte géré QRadar Incident Forensics sur un même dispositif sans les fonctions de gestion du journal, de surveillance de l'activité réseau ou d'autres fonctions de sécurité intelligente. Pour disposer d'une solution réseau Forensics autonome, installez QRadar Incident Forensics Standalone lors de déploiements de taille réduite et moyenne.

Le diagramme suivant présente un déploiement tout-en-un QRadar Incident Forensics.

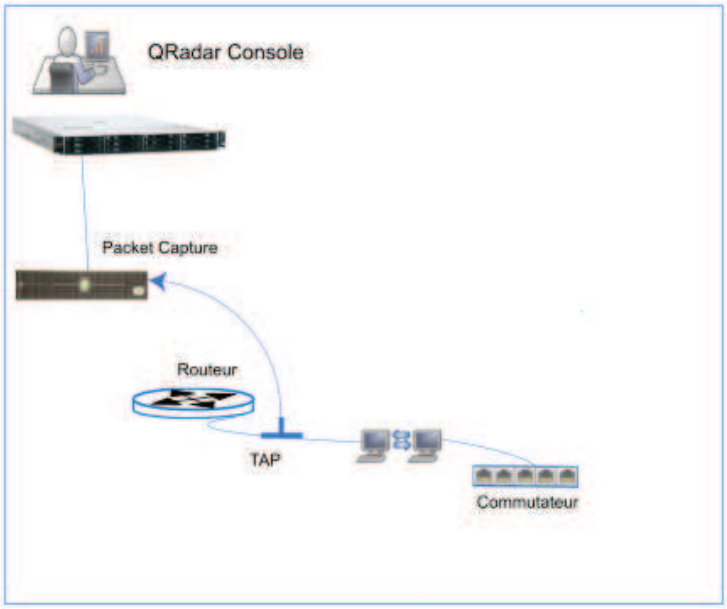



*Figure 12. Déploiement tout-en-un*

## Déploiement réparti

Dans un déploiement réparti, vous pouvez avoir les trois dispositifs suivants :

- QRadar Console
- Hôte géré QRadar Packet Capture (processeur QRadar Packet Capture)
- QRadar Packet Capture (facultatif)

Lors d'un déploiement, tous les dispositifs IBM Security QRadar doivent posséder un niveau de version et de correctif identique. Les déploiements qui utilisent des versions de logiciel différentes ne sont pas pris en charge.

Le diagramme suivant présente un déploiement réparti QRadar Incident Forensics.

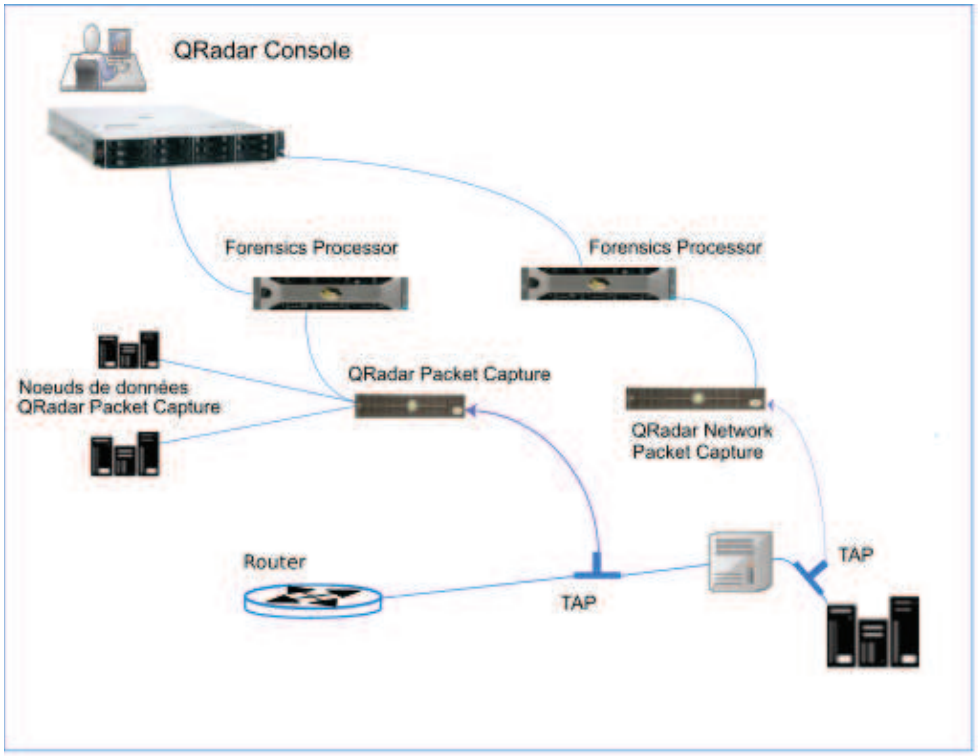



*Figure 13. Déploiement réparti*

Le diagramme suivant présente la transmission de paquet entre une instance IBM QRadar QFlow Collector 1310 avec une carte réseau Napatech 10G et un dispositif QRadar Packet Capture.

QRadar QFlow Collector utilise une carte de contrôle Napatech dédiée pour copier des paquets entrants d'un port de la carte sur un deuxième port qui se connecte à un dispositif IBM Security QRadar Packet Capture.

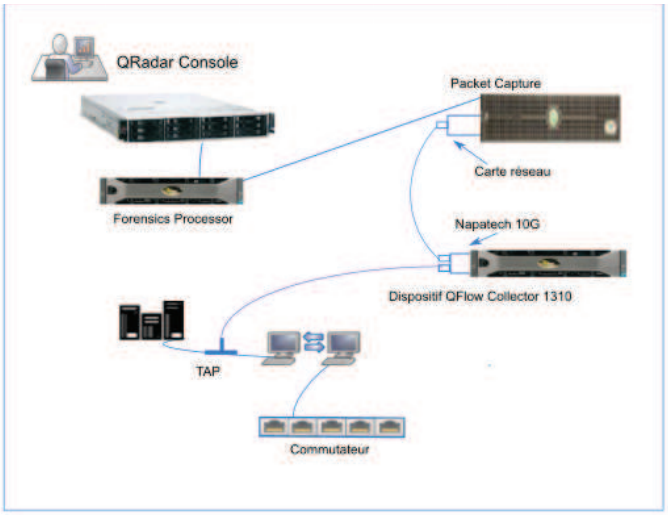



*Figure 14. Transmission de paquet*

## Transmission de paquets à QRadar Packet Capture

Vous pouvez surveiller le trafic réseau en envoyant des paquets de données brutes à un dispositif IBM Security QRadar QFlow Collector 1310. QRadar QFlow Collector utilise une carte de contrôle Napatech dédiée pour copier des paquets entrants d'un port de la carte sur un deuxième port qui se connecte à un dispositif IBM Security QRadar Packet Capture.

Si vous disposez déjà d'un dispositif QRadar QFlow Collector 1310 avec une carte réseau Napatech 10G, vous pouvez reproduire le trafic sur QRadar Packet Capture.

Comme présenté dans le diagramme suivant, si vous disposez déjà d'un dispositif QRadar QFlow Collector 1310 avec une carte réseau Napatech 10G, vous pouvez reproduire le trafic sur QRadar Packet Capture.

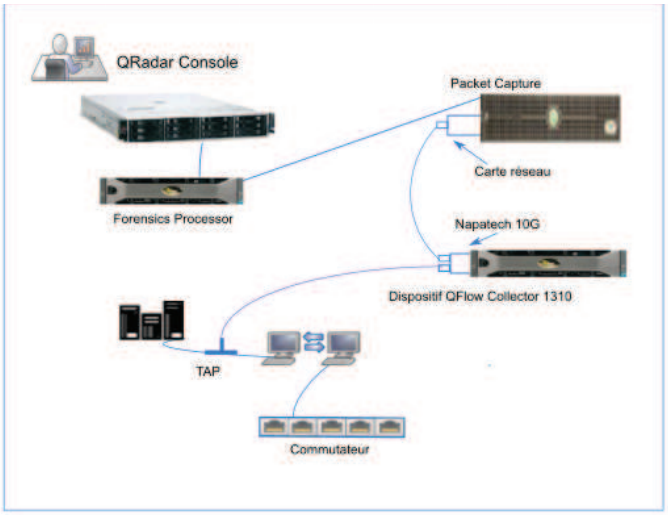



*Figure 15. Transmission de données de paquet à partir d'un dispositif QRadar QFlow Collector vers QRadar Packet Capture en utilisant la carte Napatech*

## Avant de commencer

Vérifiez que le matériel suivant est configuré dans votre environnement :

- Vous avez relié le câble au port 1 de la carte Napatech sur le dispositif QRadar QFlow Collector 1310.
- Vous avez relié le câble qui est connecté au port 2 de la carte Napatech (port de transmission) au dispositif QRadar Packet Capture.
- Vérifiez la connectivité de couche 2 à l'aide des voyants de liaison sur les deux dispositifs.

## Procédure

1. En utilisant SSH à partir de votre console IBM Security QRadar Console, connectez-vous à QRadar QFlow Collector en tant qu'utilisateur root. Sur le dispositif QRadar QFlow Collector, éditez le fichier suivant.

   `/opt/qradar/init/apply_tunings`

   a. Recherchez la ligne suivante aux alentours de la ligne 137.

   ```
   apply_multithread_qflow_changes()
   {
        APPLIANCEID=`$NVABIN/myver -a`
        if [ "$APPLIANCEID" == "1310" ]; then
             MODELNUM=$(/opt/napatech/bin/AdapterInfo 2>&1 | grep "Active FPGA Image" | cut -d'-' -f2)
             if [ "$MODELNUM" == "9220" ]; then..
   ```

   b. Dans les lignes `AppendToConf` qui suivent le code de l'étape précédente, ajoutez ces lignes :

   ```
   AppendToConf SV_NAPATECH_FORWARD YES
   AppendToConf SV_NAPATECH_FORWARD_INTERFACE_SRCDST "0:1"
   ```

   Ces instructions permettent la transmission de paquet et font transiter les paquets du port 0 au port 1.

   c. Vérifiez que le *traitement multitâche* est activé en vérifiant que la ligne suivante se trouve dans le fichier `/opt/qradar/conf/nva.conf` .

   ```
   MULTI_THREAD_ON=YES
   ```

2. Exécutez le script `apply_tunings` pour mettre à jour les fichiers de configuration sur QRadar QFlow Collector en entrant la commande suivante :

   ```
   ./apply_tunings restart
   ```

3. Redémarrez les services IBM Security QRadar en entrant la commande suivante :

   ```
   systemctl restart hostcontext
   ```

4. Facultatif : Vérifiez que la carte Napatech reçoit et transmet des données.
   a. Pour vérifier que la carte Napatech reçoit des données, entrez la commande suivante :

      ```
      /opt/napatech/bin/Statistics -dec -interactive
      ```

      Le paquet "RX" et les statistiques s'incrémentent si la carte reçoit des données.
   b. Pour vérifier que la carte Napatech transmet des données, entrez la commande suivante :

      ```
      /opt/napatech/bin/Statistics -dec -interactive
      ```

      Les statistiques "TX" s'incrémentent si la carte transmet des données.
5. Facultatif : Vérifiez que QRadar Packet Capture reçoit des paquets de votre dispositif QRadar QFlow Collector.
   a. En utilisant SSH depuis votre console QRadar Console, connectez-vous à votre dispositif QRadar Packet Capture en tant qu'utilisateur root sur le port 4477.
   b. Vérifiez que le dispositif QRadar Packet Capture reçoit des paquets en entrant la commande suivante :

      ```
      watch -d cat /var/www/html/statisdata/int0.txt
      ```

      Le fichier `int0.txt` se met à jour lorsque des données transitent par l'intermédiaire de votre dispositif QRadar Packet Capture.

   Pour plus d'informations sur la capture de paquet, voir le document *IBM Security QRadar Packet Capture Quick Reference Guide*.

# Chapitre 3. Noeuds de données et stockage de données

Les dispositifs de processeur IBM Security QRadar et les dispositifs tout-en-un peuvent stocker des données mais un grand nombre d'entreprises ont besoin du stockage autonome et des fonctions de traitement du noeud de données pour gérer leurs exigences spécifiques en matière de stockage et pour implémenter plus facilement les règles de conservation de données. Un grand nombre d'entreprises doivent appliquer des réglementations et des lois qui leur imposent de conserver des enregistrements de données pendant des périodes définies.

## Informations sur les noeuds de données

Vous trouverez ci-dessous des informations spécifiques aux noeuds de données :

- Les noeuds de données ajoutent une capacité de stockage et de traitement.
- Les noeuds de données sont plug-n-play et peuvent être ajoutés à tout moment à un déploiement.
- Les noeuds de données sont intégrés en toute transparence aux déploiements existants.
- Les noeuds de données permettent de réduire la charge des dispositifs de processeur, ces derniers n'ayant plus à assurer le stockage des données.
- Les utilisateurs peuvent échelonner le stockage et la puissance de traitement indépendamment de la collecte de données.
- A partir de la version 7.2.7 de QRadar, la compression de données natives permet de compresser les données lors de leur stockage. La compression des données natives permet de meilleures performances de recherche que les algorithmes de compression précédents qui étaient utilisés pour compresser les données dans les anciennes versions de QRadar.

Le diagramme suivant présente des exemples d'utilisation des noeuds de données dans un déploiement.

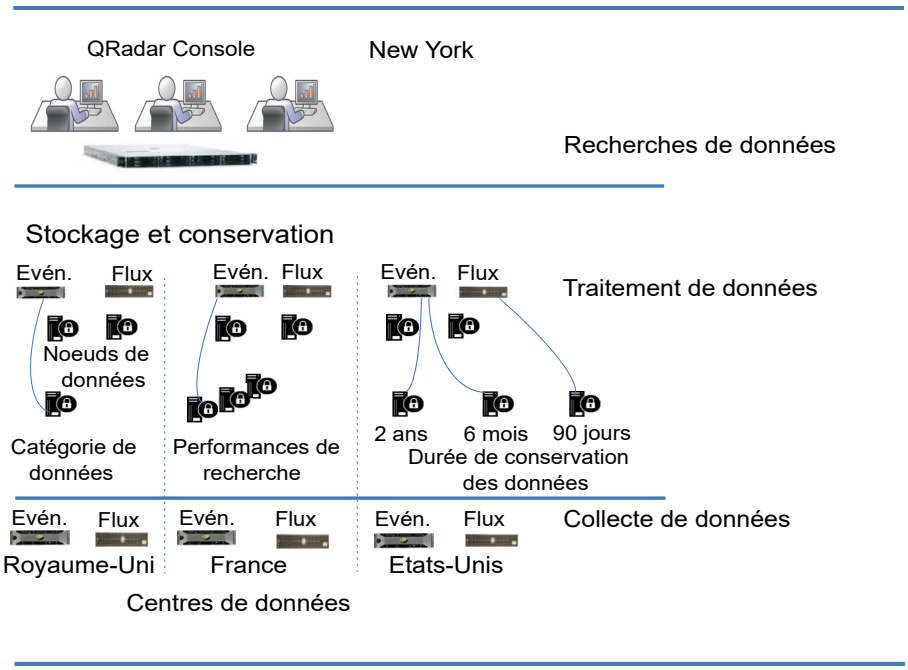



*Figure 16. Utilisation de dispositifs de noeud de données pour la gestion du stockage de vos données*

La liste suivante décrit les différents points à prendre en compte lors du déploiement des noeuds de données.

**Groupement des données**

Les noeuds de données ajoutent une capacité de stockage à un déploiement et améliorent également les performances en répartissant entre plusieurs volumes de stockage les données collectées. Lors d'une recherche de données, plusieurs hôtes, autrement dit un cluster, procèdent à la recherche. Le cluster peut améliorer les performances de la recherche mais sans qu'il soit nécessaire que vous ajoutiez plusieurs processeurs d'événements. Les noeuds de données multiplient le stockage pour chaque processeur.

**Remarque :** Vous ne pouvez connecter un noeud de données qu'à un seul processeur à la fois mais un processeur peut prendre en charge plusieurs noeuds de données.

**Remarques liées au déploiement**

Prenez en compte les informations suivantes lorsque vous configurez des noeuds de données dans un déploiement.

- Les noeuds de données sont disponibles à partir de la version 7.2.2 de QRadar.
- Les noeuds de données exécutent des fonctions de recherche et d'analyse similaires aux fonctions des processeurs d'événements et de flux dans un déploiement QRadar.

  La vitesse opérationnelle sur un cluster est affectée par le membre le plus lent d'un cluster. Les performances système du noeud de données s'améliorent si les noeuds de données sont redimensionnés de la même façon que les processeurs d'événement et les processeurs de flux dans un déploiement. Pour faciliter un redimensionnement similaire entre les

noeuds de données et les processeurs d'événements et de flux, les noeuds de données sont disponibles à la fois sur les dispositifs centraux XX05 et XX28.

- Les noeuds de données sont disponibles à trois formats : Logiciel (sur votre propre matériel), physique et dispositifs. Vous pouvez combiner plusieurs formats dans un seul cluster.

**Bande passante et temps d'attente**

Vérifiez que vous disposez d'une liaison 1 Gbps et que le temps d'attente est inférieur à 10 ms entre les hôtes du cluster. Les recherches renvoyant un grand nombre de résultats nécessitent une bande passante plus large.

**Compatibilité de dispositif**

Les noeuds de données sont compatibles avec tous les dispositifs QRadar existants ayant un composant Event Processor ou processeur de flux, y compris les dispositifs tout-en-un. Les noeuds de données ne sont pas compatibles avec les dispositifs QRadar Incident Forensics PCAP.

Les noeuds de données prennent en charge la haute disponibilité.

**Installation de noeuds de données**

Les noeuds de données utilisent les réseaux TCP/IP standard et n'ont pas besoin de matériel de connexion propriétaire ou spécialisé.

Installez chaque noeud de données que vous souhaitez ajouter à votre déploiement comme tout autre dispositif QRadar. Associez les noeuds de données aux processeurs d'événement ou de flux dans l'éditeur de déploiement QRadar. Pour plus d'informations, voir le document *IBM Security QRadar Administration Guide*.

Vous pouvez associer plusieurs noeuds de données à un seul dispositif Event Processor ou processeur de flux dans une configuration plusieurs à un.

Lorsque vous déployez des paires à haute disponibilité (HD) avec des dispositifs de noeud de données, installez, déployez et rééquilibrez les données avec les dispositifs à haute disponibilité avant de synchroniser la paire HD. L'effet combiné du rééquilibrage des données et du processus de réplication utilisé pour la haute disponibilité se traduit par une dégradation significative des performances. Si la haute disponibilité est configurée sur les dispositifs où se trouvent les noeuds de données, déconnectez la haute disponibilité sur les dispositifs puis reconnectez-la une fois le rééquilibrage du cluster terminé.

**Mise hors service des noeuds de données**

Retirez les noeuds de données de votre déploiement avec l'éditeur de déploiement, comme vous le feriez pour tout autre dispositif QRadar. La mise hors service ne supprime pas les données sur l'hôte, ni ne déplace les données vers vos autres dispositifs. Si vous avez toujours besoin d'accéder aux données se trouvant sur les noeuds de données, vous devez indiquer un emplacement vers lequel déplacer ces données.

**Rééquilibrage des données**

L'ajout d'un noeud de données à un cluster répartit les données sur chaque noeud de données. Lorsque cela est possible, le rééquilibrage de données tente de conserver le même pourcentage d'espace disponible sur chacun d'entre eux. L'ajout de nouveaux noeuds de données à un cluster démarre un rééquilibrage supplémentaire depuis les processeurs de flux et

d'événement du cluster afin de parvenir à une utilisation efficace des disques sur les dispositifs de noeud de données nouvellement ajoutés.

A partir de la version 7.2.3 de QRadar, le rééquilibrage de données est automatique et s'effectue parallèlement à d'autres activités de cluster, telles que les requêtes et la collecte de données. Aucune indisponibilité ne se produit pendant le rééquilibrage de données.

Les noeuds de données ne présentent aucune amélioration des performances du cluster tant que le rééquilibrage des données n'est pas terminé. Le rééquilibrage peut entraîner une dégradation mineure des performances lors des opérations de recherche, mais le traitement et la collecte des données ne sont pas affectés.

**Remarque :** La transmission des données chiffrées entre les noeuds de données et les processeurs d'événement n'est pas prise en charge. Les ports de pare-feu suivants doivent être ouverts pour la communication entre les noeuds de données et le Event Processor :

- Port 32006 entre les noeuds de données et le dispositif Event Processor.
- Port 32011 entre les noeuds de données et le Event Processor de la console.

**Gestion et opérations**

Les noeuds de données sont auto-gérés et ne nécessitent aucune intervention de l'utilisateur pour la gestion régulière des opérations normales. QRadar gère les activités, comme les sauvegardes de données, la haute disponibilité et les règles de conservation, pour tous les hôtes, y compris les dispositifs de noeud de données.

**Défaillance d'un noeud de données**

En cas de panne d'un noeud de données, les autres membres du cluster continuent à traiter les données.

Lorsque l'élément défaillant redevient opérationnel, l'équilibrage de données peut avoir lieu pour maintenir une répartition correcte des données dans le cluster. Le processus normal reprend alors. Lors de la période d'indisponibilité, les données se trouvant sur l'élément défaillant ne sont pas disponibles et les erreurs d'E-S survenant s'affichent dans les résultats de recherche du journal et dans les afficheurs d'activité réseau de l'interface utilisateur QRadar.

Pour les défaillances graves qui requièrent le remplacement du dispositif ou la réinstallation de QRadar, mettez hors service les noeuds de données dans le déploiement et remplacez-les à l'aide de la procédure d'installation standard. Copiez les données non perdues lors de la défaillance sur le nouveau noeud de données avant le déploiement. L'algorithme de rééquilibrage tient compte des données existantes sur un noeud de données et traite uniquement les données collectées pendant la défaillance.

Pour les noeuds de données déployés avec une paire haute disponibilité, une défaillance matérielle entraîne un basculement, et les opérations se poursuivent normalement.

## Présentation du réseau de stockage

Pour augmenter la quantité d'espace de stockage sur votre dispositif, vous pouvez déplacer une partie de vos données sur un périphérique de stockage externe. Vous pouvez déplacer vos systèmes de fichiers `/store`, `/store/ariel` ou `/store/backup`.

Plusieurs méthodes sont disponibles pour l'ajout de stockage externe, notamment iSCSI, Fiber Channel et NFS (Network File System). Vous devez utiliser iSCSI ou Fiber Channel pour stocker les données accessibles et consultables dans l'interface utilisateur (répertoire `/store/ariel`, par exemple) et réserver l'utilisation de NFS uniquement aux sauvegardes de données.

Le déplacement du système de fichiers `/store` vers un périphérique externe peut affecter les performances de QRadar.

Après la migration, les opérations d'E-S de données dans le système de fichiers `/store` ne sont plus effectuées sur le disque local. Avant de déplacer vos données QRadar vers un périphérique de stockage externe, vous devez prendre en compte les informations suivantes :

- Les recherches marquées comme sauvegardées se trouvent également dans le répertoire `/transient`. Si le disque local est défaillant, ces recherches ne sont pas sauvegardées.
- Une partition provisoire existant avant le déplacement de vos données peut être conservée après le déplacement et elle peut être montée sur un élément de stockage iSCSI ou Fiber Channel.

Pour plus d'informations sur le stockage externe, voir le document *IBM QRadar Security Intelligence Offboard Storage Guide*.

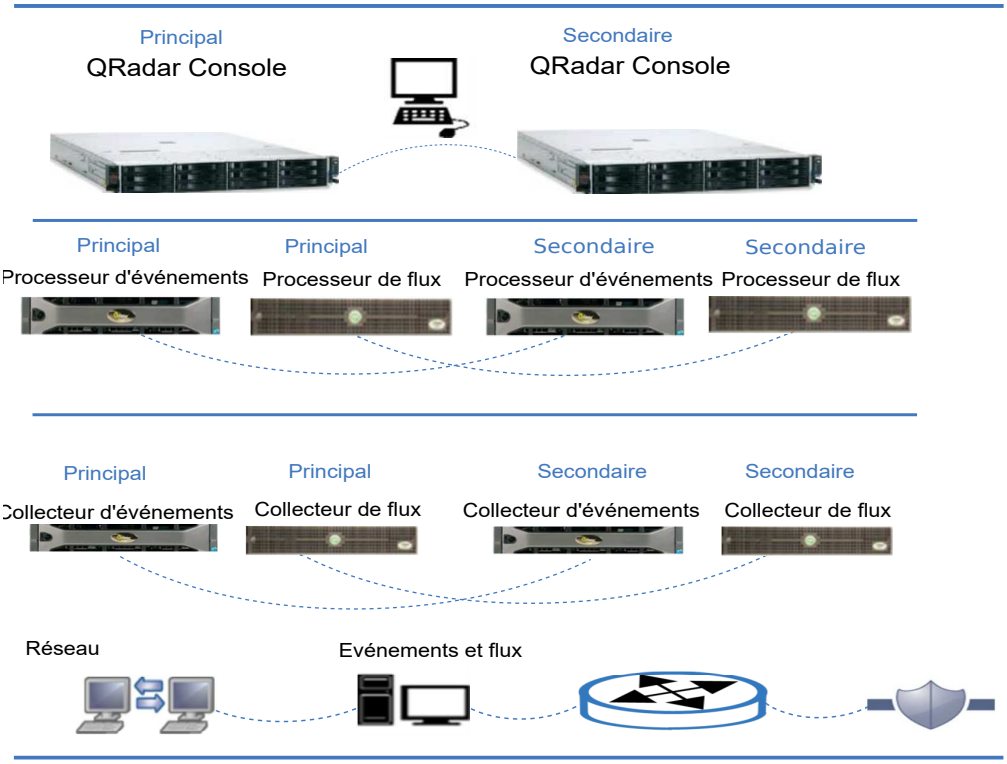
# Chapitre 4. Présentation du déploiement à haute disponibilité

Implémentez la haute disponibilité dans votre déploiement IBM Security QRadar afin que les fonctions QRadar soient toujours en cours d'exécution lorsqu'un problème matériel ou logiciel survient dans votre déploiement.

En utilisant la haute disponibilité, vous pouvez continuer de collecter, de stocker et de traiter les données d'événement et de flux en cas de défaillance.

Pour activer la haute disponibilité, QRadar connecte un hôte à haute disponibilité principal à un hôte à haute disponibilité secondaire afin de créer un cluster à haute disponibilité.

Le diagramme suivant présente une configuration à haute disponibilité standard.




## Présentation de la haute disponibilité

Dans un déploiement à haute disponibilité, vous installez et configurez un deuxième dispositif qui est utilisé en cas de défaillance du dispositif principal dans les situations suivantes :

- Panne d'alimentation
- Panne réseau détectée par des tests de connectivité réseau
- Dysfonctionnement du système d'exploitation qui retarde ou arrête les tests ping de signal de présence
- Défaillance RAID sur l'hôte à haute disponibilité principal
- Basculement manuel

- Défaillance de l'interface de gestion sur l'hôte à haute disponibilité principal

Pour de meilleures performances dans des déploiements de grande taille, il est fortement recommandé d'utiliser une interface 10 Gbps pour une connexion croisée à haute disponibilité. L'utilisation d'une interface 10 Gbps réduit la durée de la synchronisation système et garantit des performances optimales. Si vous n'avez pas d'interface 10 Gbps disponible, pensez à associer plusieurs interfaces 1 Gbps pour les connexions croisées.

Pour plus d'informations sur la haute disponibilité, voir le document *IBM Security QRadar SIEM High Availability Guide*.

# Chapitre 5. Stratégies de sauvegarde

Sauvegardez les informations stratégiques de votre entreprise afin de vous protéger contre la perte de données. Les stratégies de sauvegarde sont différentes en fonction des types de données.

## Sauvegarde des données QRadar

La classification des données est une étape importante des stratégies de sauvegarde pour les raisons suivantes :

- Les données telles que les informations identifiant la personne doivent être stockées de manière sécurisée et il peut être nécessaire de les conserver à un autre emplacement que les sauvegardes de données en masse et pendant plus longtemps pour des raisons de conformité.
- Pour des raisons de fiabilité, conservez les données de configuration système QRadar à un emplacement différent de celui de vos données de sécurité (événements, flux, etc.). Ainsi, il est plus facile de restaurer les données de configuration.
- Placez les données, telles que les données PCI, à un emplacement distinct afin de pouvoir y accéder facilement lorsque des auditeurs souhaitent les consulter.
- Prenez en compte les types de données et les durées de conservation lorsque vous développez vos stratégies de sauvegarde.
- Vous pouvez sauvegarder certains types de données plus fréquemment que d'autres et vous pouvez utiliser le stockage hors site pour certaines données afin de vous prémunir contre la perte de données.

## Paramètres de conservation

La valeur par défaut pour la conservation de la sauvegarde QRadar est de 7 jours. Vous pouvez également effectuer une sauvegarde à la demande une fois que vous avez apporté des modifications importantes à la configuration. Vous pouvez attribuer à cette sauvegarde un nom descriptif afin de trouver plus facilement vos modifications si vous souhaitez utiliser à nouveau la configuration précédente.

Les sauvegardes planifiées remplacent les sauvegardes planifiées plus anciennes. Les sauvegardes à la demande sont conservées indéfiniment. Une fois que le volume de sauvegarde QRadar atteint 75 % de sa capacité, les sauvegardes planifiées ne s'exécutent plus.

## Emplacement de la sauvegarde

L'emplacement de la sauvegarde constitue également un facteur crucial à prendre en compte lors du déploiement de QRadar. Si vos sauvegardes sont conservées sur un hôte et que ce dernier est défaillant, toutes les données de sauvegarde sont alors perdues.

Vous pouvez soit créer vos sauvegardes sur un système externe, soit copier vos sauvegardes sur un système externe.

Pour des raisons de sécurité, conservez des copies de vos données stratégiques en local et sur un système distant.

# 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.

Linux est une marque de Linus Torvalds aux Etats-Unis et/ou dans certains autres pays.

Java™ ainsi que tous les logos et toutes les marques incluant Java sont des marques d'Oracle et/ou de ses sociétés affiliées.


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).

## Politique de confidentialité

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).