

IBM Security QRadar

*Guide d'utilisation des sources de
journal*
Avril 2016

IBM

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section «Remarques», à la page 63.

Ce document s'applique à IBM QRadar Security Intelligence Platform version 7.2.5 et à toutes les versions et modifications ultérieures sauf indication contraire dans les nouvelles éditions.

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

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

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

Vous pouvez également consulter les serveurs Internet suivants :

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

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

© Copyright IBM France 2016. Tous droits réservés.

© **Copyright IBM Corporation 2007, 2016.**

Table des matières

Avis aux lecteurs canadiens v

A propos de ce guide vii

Chapitre 1. Présentation de la gestion de sources de journal 1

Ajout d'une source de journal.	1
Options de configuration du protocole d'API REST Blue Coat Web Security Service	3
Options de configuration du protocole Cisco NSEL	3
Options de configuration du protocole EMC VMware	4
Options de configuration du protocole Forwarded	4
Options de configuration du protocole IBM Tivoli Endpoint Manager SOAP	5
Options de configuration du protocole JDBC	5
Options de configuration du protocole SiteProtector	7
Options de configuration du protocole Juniper Networks NSM	9
Options de configuration du protocole Juniper Security Binary Log Collector	10
Options de configuration du protocole de fichier journal	10
Options de configuration du protocole Microsoft DHCP	12
Options de configuration du protocole Microsoft Exchange	12
Options de configuration du protocole Microsoft IIS	13
Options de configuration du protocole Microsoft Security Event Log	14
Options de configuration du protocole MQ.	15
Options de configuration du protocole d'API REST Okta.	15
Options de configuration du protocole OPSEC/LEA	16
Options de configuration du protocole Oracle Database Listener	17
Options de configuration du protocole PCAP Syslog Combination	17
Options de configuration du protocole SDEE	17
Options de configuration du protocole SMB Tail	18
Options de configuration du protocole SNMPv2	19
Options de configuration du protocole SNMPv3	19
Options de configuration du protocole d'API REST Seculert Protection	19
Options de configuration du protocole Sophos Enterprise Console JDBC	20
Options de configuration du protocole Sourcefire Defense Center Estreamer	22

Présentation du protocole Syslog Redirect	23
Options de configuration du protocole TCP Multiline Syslog	23
Options de configuration du protocole TLS Syslog	24
Options de configuration du protocole UDP Multiline Syslog	25
Options de configuration du protocole VMware vCloud Director	26
Ajout de sources de journal en bloc	27
Ajout d'un ordre d'analyse syntaxique de source de journal	27

Chapitre 2. Extensions de source de journal 29

Exemples d'extensions de source de journal sur le forum QRadar	29
Motifs dans les documents d'extension de source de journal	30
Groupes de correspondance	30
Comparateur (matcher)	31
Modificateur d'événements multiples (event-match-multiple)	36
Modificateur d'événement unique (event-match-single)	36
Modèle de document d'extension	37
Création d'un document d'extension de source de journal	40
Construction d'un DSM universel	41
Exportation des journaux.	41
Expressions régulières courantes	43
Construction de motifs d'expression régulière	44
Téléchargement de documents d'extension à QRadar.	46
Mappage d'événements inconnus	46
Problèmes et exemples d'analyse syntaxique	48
Analyse d'un format de journal CSV	51
ID de type de source de journal	52

Chapitre 3. Gestion des extensions de sources de journal 61

Ajout d'une extension de source de journal. 61

Remarques 63

Marques	65
Remarques sur les règles de confidentialité.	65

Index 67

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

Brevets

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

Assistance téléphonique

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

A propos de ce guide

Les sources de journal sont des périphériques tiers qui envoient des événements à IBM® Security QRadar en vue de leur collecte, stockage, analyse et traitement.

Public concerné

Les administrateurs doivent disposer d'un accès à QRadar et connaître le réseau de l'entreprise et les technologies de réseau.

Documentation technique

Pour rechercher la documentation produit IBM Security QRadar sur le Web, y compris toute la documentation traduite, accédez à IBM Knowledge Center (<http://www.ibm.com/support/knowledgecenter/SS42VS/welcome>).

Pour savoir comment accéder à d'autres documents techniques dans la bibliothèque produit QRadar, voir Accessing IBM Security Documentation Technical Note (en anglais) (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Contactez le service clients

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

Déclaration de pratiques de sécurité recommandées

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

Vous pouvez configurer IBM Security QRadar pour accepter les journaux d'événements provenant de sources de journal se trouvant sur votre réseau. Une *source de journal* est une source de données créant un journal d'événement.

Par exemple, un pare-feu ou un système IPS (intrusion protection system) consigne des événements basés sur la sécurité, et les commutateurs et routeurs consignent les événements basés sur le réseau.

Pour recevoir des événements bruts des sources de journal, QRadar prend en charge un large éventail de protocoles. Les *protocoles passifs* écoutent les événements sur des ports spécifiques. Les *protocoles actifs* utilisent des API ou d'autres méthodes de communication pour se connecter aux systèmes externes qui interrogent et extraient les événements.

Suivant les limites de votre licence, QRadar peut lire et interpréter les événements de plus de 300 sources de journal.

Pour configurer une source de journal pour QRadar, procédez comme suit :

1. Téléchargez et installez un module de support de périphérique (DSM) prenant en charge la source de journal. Un *DSM* est une application logicielle contenant les modèles d'événements requis pour identifier et analyser les événements, initialement dans le format original du journal d'événements, puis dans le format que QRadar peut utiliser. Pour plus d'informations sur les DSM et les sources de journal pris en charge, reportez-vous au *Guide de configuration DSM*.
2. Si la détection automatique est prise en charge pour le DSM, attendez que QRadar ajoute automatiquement la source de journal à votre liste de sources de journal configurées.
3. Si la détection automatique n'est pas prise en charge pour le DSM, vous devez créer la configuration des sources de journal manuellement.

Ajout d'une source de journal

Si aucune source de journal n'est détectée automatiquement, vous pouvez en ajouter une manuellement afin de recevoir les événements de vos dispositifs et périphériques réseau.

Pourquoi et quand exécuter cette tâche

Le tableau suivant décrit les paramètres communs à tous les types de sources de journal :

Tableau 1. Paramètres d'une source de journal

Paramètre	Description
Identificateur de la source de journal	<p>Adresse IPv4 ou nom d'hôte identifiant la source de journal.</p> <p>Si votre réseau contient plusieurs périphériques rattachés à une seule console de gestion, spécifiez l'adresse IP du périphérique ayant créé l'événement. Un identificateur unique pour chacun, tel qu'une adresse IP, évite que les recherches d'événements identifient la console de gestion comme la source de tous les événements.</p>
Activé	Lorsque cette option est désactivée, la source de journal ne collecte pas les événements et n'est pas comptabilisée dans la limite de licence.
Crédibilité	La crédibilité est une représentation de l'intégrité ou de la validité des événements créés par une source de journal. La valeur de crédibilité affectée à une source de journal peut augmenter ou diminuer en fonction des événements entrants ou être réglée en réponse aux règles d'événements créées par les utilisateurs. La crédibilité des événements provenant de sources de journal contribue au calcul de l'ampleur de l'infraction et elle peut augmenter ou diminuer la valeur ampleur d'une infraction.
Collecteur d'événement cible	<p>Spécifie le collecteur d'événements QRadar interrogeant la source de journal distante.</p> <p>Utilisez ce paramètre dans un déploiement réparti pour améliorer les performances du système Console en transférant la tâche d'interrogation à un collecteur d'événements.</p>
Événements en coalescence	<p>Augmente le nombre d'événements lorsque le même événement se produit plusieurs fois durant un intervalle de temps réduit. Les événements regroupés offrent la possibilité d'afficher et de déterminer la fréquence avec laquelle un type d'événement unique se produit dans l'onglet Activité du journal.</p> <p>Lorsque cette case est décochée, les événements s'affichent individuellement et ne sont pas regroupés.</p> <p>Les sources de journal nouvelles et détectées automatiquement héritent de la valeur de cette case de la configuration de Paramètres système dans l'onglet Admin. Vous pouvez utiliser cette case pour ignorer le comportement par défaut des paramètres système d'une source de journal individuelle.</p>

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Sources de journal**.
3. Cliquez sur **Ajouter**.
4. Configurez les paramètres communs de votre source de journal.
5. Configurez les paramètres spécifiques au protocole de votre source de journal.
6. Cliquez sur **Sauvegarder**.
7. Sur l'onglet **Admin**, cliquez sur **Déployer les changements**.

Options de configuration du protocole d'API REST Blue Coat Web Security Service

Pour recevoir des événements depuis le service Blue Coat Web Security Service, configurez une source de journal pour l'utilisation du protocole d'API REST Blue Coat Web Security Service.

Le protocole d'API REST Blue Coat Web Security Service interroge l'API de synchronisation Blue Coat Web Security Service Sync et extrait les données de journal récemment renforcées depuis le cloud.

Le tableau suivant décrit les paramètres spécifiques au protocole pour le protocole d'API REST Blue Coat Web Security Service.

Tableau 2. Paramètres du protocole d'API REST Blue Coat Web Security Service

Paramètre	Description
API Username	Nom d'utilisateur utilisé pour l'authentification avec le service Blue Coat Web Security Service. Le nom d'utilisateur de l'API est configuré via le portail Blue Coat Threat Pulse Portal.
Password	Mot de passe utilisé pour l'authentification avec le service Blue Coat Web Security Service.
Confirm Password	Confirmation de la zone Password .
Use Proxy	Lorsque vous configurez un proxy, tout le trafic de la source de journal transite par le proxy pour l'accès de QRadar au service Blue Coat Web Security Service. Configurez les zones Proxy IP or Hostname , Proxy Port , Proxy Username et Proxy Password . Si le proxy ne requiert pas d'authentification, vous pouvez laisser les zones Proxy Username et Proxy Password à vide.
Automatically Acquire Server Certificate(s)	Si vous sélectionnez Oui (Yes) dans la liste, QRadar télécharge le certificat et fait confiance au serveur cible.
Recurrence	Vous pouvez spécifier quand le journal collecte des données. Le format est M/H/D pour Months/Hours/Days (mois/heures/jours). La valeur par défaut est 5 M.
EPS Throttle	Limite supérieure du nombre d'événements maximal par seconde (EPS). La valeur par défaut est 5000.

Options de configuration du protocole Cisco NSEL

Pour surveiller les flux de paquets en provenance d'un dispositif Cisco Adaptive Security Appliance (ASA), configurez la source de protocole Cisco Network Security Event Logging (NSEL).

Pour intégrer Cisco NSEL à QRadar, vous devez créer manuellement une source de journal pour recevoir les événements NetFlow. QRadar ne détecte ou ne crée pas les sources de journal de façon automatique pour les événements Syslog provenant de Cisco NSEL. Pour plus d'informations, voir le Guide de configuration *DSM*.

Le tableau suivant décrit les paramètres spécifiques au protocole Cisco NSEL :

Tableau 3. Paramètres du protocole Cisco NSEL

Paramètre	Description
Protocol Configuration	Cisco NSEL
Log Source Identifier	Si le réseau contient des périphériques rattachés à la console de gestion, vous pouvez indiquer l'adresse IP du périphérique ayant créé l'événement. Un identificateur unique pour chacun, tel qu'une adresse IP, évite que les recherches d'événements identifient la console de gestion comme la source de tous les événements.
Collector Port	Numéro de port UDP utilisé par Cisco ASA pour réacheminer les événements NSEL. QRadar utilise le port 2055 pour les données de flux sur QRadar QFlow Collectors. Vous devez attribuer un port UDP différent sur Cisco ASA pour NetFlow.

Options de configuration du protocole EMC VMware

Pour recevoir des données d'événements du service Web VMWare pour les environnements virtuels, configurez une source de journal de façon à utiliser le protocole EMC VMWare.

Le tableau suivant décrit les paramètres spécifiques au protocole EMC VMware :

Tableau 4. Paramètres du protocole EMC VMware

Paramètre	Description
Protocol Configuration	EMC VMware
Log Source Identifier	La valeur de ce paramètre doit correspondre à celle du paramètre VMware IP .
VMware IP	Adresse IP du serveur VMWare ESXi, par exemple, 1.1.1.1. Le protocole VMware ajoute l'adresse IP de votre serveur VMware ESXi avec HTTPS avant que le protocole ne demande les données d'événement.

Options de configuration du protocole Forwarded

Pour recevoir des événements d'une autre console dans votre déploiement, configurez une source de journal de façon à utiliser le protocole Forwarded.

Le protocole Forwarded est généralement utilisé pour transférer des événements vers une autre console QRadar. Par exemple, la console A a la console B configurée comme cible hors site. Les données provenant des sources de journal détectées automatiquement sont transférées à la console B. Les sources de journal créées manuellement sur la console A doivent également être ajoutées en tant que source de journal dans la console B avec le protocole Forwarded.

Options de configuration du protocole IBM Tivoli Endpoint Manager SOAP

Pour recevoir des événements au format Log Extended Event Format (LEEF) des dispositifs IBM Tivoli Endpoint Manager, configurez une source de journal qui utilise le protocole IBM Tivoli Endpoint Manager SOAP.

Ce protocole requiert IBM Tivoli Endpoint Manager versions V8.2.x ou suivantes et l'application Web Reports pour Tivoli Endpoint Manager.

Le protocole Tivoli Endpoint Manager SOAP extrait les événements par intervalles de 30 secondes sur HTTP ou HTTPS. Lorsque des événements sont extraits, IBM Tivoli Endpoint Manager DSM les analyse et les catégorise.

Le tableau suivant décrit les paramètres spécifiques au protocole IBM Tivoli Endpoint Manager SOAP :

Tableau 5. Paramètres de protocole IBM Tivoli Endpoint Manager SOAP

Paramètre	Description
Protocol Configuration	IBM Tivoli Endpoint Manager SOAP
Use HTTPS	Si un certificat doit être connecté avec HTTPS, vous devez copier les certificats requis dans le répertoire suivant : /opt/qradar/conf/trusted_certificates. Les certificats possédant les extensions .crt, .cert ou .der sont pris en charge. Copiez les certificats dans le répertoire des certificats de confiance avant que la source de journal ne soit sauvegardée et déployée.
SOAP Port	Par défaut, le port 80 est le numéro de port pour la communication avec IBM Tivoli Endpoint Manager. La plupart des configurations utilisent le port 443 pour les communications HTTPS.

Options de configuration du protocole JDBC

QRadar utilise le protocole JDBC pour rassembler des informations à partir de tableaux et de vues contenant des données d'événements issues de plusieurs types de bases de données.

Le tableau suivant décrit les paramètres spécifiques au protocole JDBC :

Tableau 6. Paramètres du protocole JDBC

Paramètre	Description
Database Type	Dans la zone de liste, sélectionnez le type de base de données contenant les événements.
Database Name	Le nom de la base de données doit correspondre au nom de base de données spécifié dans la zone Identificateur de source de journal .
Port	Le port JDBC doit correspondre au port d'écoute configuré sur la base de données distante. La base de données doit autoriser les connexions TCP entrantes. Si le paramètre Database Instance est utilisé avec le type de base de données MSDE, les administrateurs doivent laisser le paramètre Port vide dans la configuration de la source de journal.
Username	Compte utilisateur de QRadar dans la base de données.

Tableau 6. Paramètres du protocole JDBC (suite)

Paramètre	Description
Password	Mot de passe requis pour la connexion à la base de données.
Confirm Password	Mot de passe requis pour la connexion à la base de données.
Authentication Domain	Un domaine doit être configuré pour les bases de données MSDE qui se trouvent au sein d'un domaine Windows. Si votre réseau n'utilise pas de domaine, laissez cette zone vide.
Database Instance	Instance de base de données, si nécessaire. Les bases de données MSDE peuvent inclure plusieurs instances de serveur SQL sur un serveur. Lorsqu'un port non standard est utilisé pour la base de données ou que l'accès au port 1434 est bloqué pour la résolution de base de données SQL, le paramètre Database Instance doit être vide dans la configuration de la source de journal.
Predefined Query	Facultatif.
Table Name	Nom du tableau ou de la vue incluant les enregistrements d'événements. Le nom du tableau peut inclure les caractères spéciaux suivants : dollar (\$), dièse (#), trait de soulignement (_), tiret (-) et point (.).
Select List	Liste des zones à inclure lors de l'interrogation d'événements dans le tableau. Vous pouvez utiliser une liste séparée par des virgules ou entrer * pour sélectionner toutes les zones du tableau ou de la vue. Si une liste séparée par des virgules est définie, la liste doit contenir la zone définie sous Compare Field .
Compare Field	Zone de valeur numérique ou d'horodatage du tableau ou de la vue identifiant les nouveaux événements ajoutés au tableau entre chaque requête. Elle permet au protocole d'identifier les événements ayant été précédemment interrogés afin d'éviter la duplication des événements.
Use Prepared Statements	Les instructions préparées permettent à la source du protocole JDBC de configurer l'instruction SQL puis de l'exécuter plusieurs fois avec des paramètres différents. Pour des raisons de sécurité et de performance, la plupart des configurations de protocoles JDBC peuvent utiliser des instructions préparées.
Start Date and Time	Si aucune heure de début n'est définie, le protocole tente d'interroger les événements une fois que la configuration de la source de journal est sauvegardée et déployée.
Polling Interval	L'intervalle d'interrogation par défaut est de 10 secondes.
EPS Throttle	Limite supérieure du nombre d'événements par seconde (EPS) autorisé.
Database Locale	Pour toute installation en version multilingue, remplissez la zone Database Locale pour indiquer la langue à utiliser.
Database Codeset	Pour toute installation en version multilingue, remplissez la zone Database Codeset pour indiquer le jeu de caractères à utiliser.

Tableau 6. Paramètres du protocole JDBC (suite)

Paramètre	Description
Use Named Pipe Communication	Les connexions de pipe nommées pour les bases de données MSDE ont besoin que la zone de nom d'utilisateur et de la zone de mot de passe utilisent un nom et un mot de passe d'authentification Windows et non le nom d'utilisateur et le mot de passe de la base de données. La configuration de la source de journal doit utiliser le canal de communication nommé par défaut sur la base de données MSDE.
Use NTLMv2	La case Use NTLMv2 n'interrompt pas les communications des connexions MSDE qui n'ont pas besoin d'authentification NTLMv2.
Use Oracle Encryption	Paramètres de chiffrement Oracle et d'intégrité des données qui constituent la sécurité avancée Oracle. Si vous sélectionnez cette option, les connexions JDBC Oracle requièrent que le serveur prenne en charge des paramètres de chiffrement des données Oracle similaires à ceux du client.
SSL	Sélectionnez la case à cocher SSL si votre connexion prend en charge SSL. Cette option s'affiche uniquement pour MSDE.

Options de configuration du protocole SiteProtector

Vous pouvez configurer les sources de journal à utiliser le protocole Java™ Database Connectivity (JDBC) SiteProtector pour l'interrogation à distance des bases de données IBM Proventia® Management SiteProtector® pour les événements.

Le protocole JDBC - SiteProtector associe les informations des tables SensorData1 et SensorDataAVP1 dans la création du contenu de source de journal. Les tables SensorData1 et SensorDataAVP1 figurent dans la base de données IBM Proventia® Management SiteProtector®. Le nombre maximum de lignes que le protocole JDBC - SiteProtector peut interroger dans une seule requête est de 30 000.

Le tableau suivant décrit les paramètres spécifiques au protocole JDBC - SiteProtector :

Tableau 7. Paramètres du protocole JDBC - SiteProtector

Paramètre	Description
Protocol Configuration	JDBC - SiteProtector
Database Type	Dans la liste, sélectionnez MSDE comme type de base de données à utiliser pour la source d'événement.
Database Name	Entrez RealSecureDB en tant que nom de la base de données à laquelle le protocole peut se connecter.
IP or Hostname	Adresse IP ou nom d'hôte du serveur de base de données.

Tableau 7. Paramètres du protocole JDBC - SiteProtector (suite)

Paramètre	Description
Port	Numéro de port utilisé par le serveur de base de données. Le port de configuration JDBC SiteProtector doit correspondre au port d'écoute de la base de données. La base de données doit avoir activé les connexions TCP entrantes. Si vous définissez le paramètre Database Instance et que le type de base de données est MSDE, vous devez laisser le paramètre Port vide dans la configuration de votre source de journal.
Username	Si vous souhaitez contrôler l'accès à une base de données par le protocole JDBC, vous pouvez créer un utilisateur spécifique pour votre système QRadar.
Authentication Domain	Si vous sélectionnez MSDE et si la base de données est configurée pour Windows, vous devez définir un domaine Windows. Si votre réseau n'utilise pas de domaine, laissez cette zone vide.
Database Instance	Si vous sélectionnez MSDE et que vous disposez de plusieurs instances de serveur SQL sur un serveur, définissez l'instance à laquelle vous souhaitez vous connecter. Si vous utilisez un port non standard dans votre configuration de base de données ou si l'accès au port 1434 est bloqué pour la résolution de base de données SQL, le paramètre Database Instance doit être laissé vide dans votre configuration.
Predefined Query	Requête de base de données prédéfinie pour votre source de journal. Les requêtes de base de données prédéfinies sont uniquement disponibles pour les connexions de sources de journal spéciales.
Table Name	SensorData1
AVP View Name	SensorDataAVP
Response View Name	SensorDataResponse
Select List	Entrez * pour inclure tous les champs du tableau ou de la vue.
Compare Field	SensorDataRowID
Use Prepared Statements	Les instructions préparées permettent à la source du protocole JDBC de configurer l'instruction SQL puis d'exécuter l'instruction SQL plusieurs fois avec des paramètres différents. Pour des raisons de sécurité et de performance, utilisez des instructions préparées. Vous pouvez désélectionner cette case pour utiliser une méthode alternative d'interrogation n'utilisant pas d'instructions précompilées.
Include Audit Events	Indique les événements d'audit doivent être collectés d'IBM SiteProtector®.
Start Date and Time	Facultatif. Date et heure de début à laquelle le protocole peut commencer à interroger la base de données.

Tableau 7. Paramètres du protocole JDBC - SiteProtector (suite)

Paramètre	Description
Polling Interval	Intervalle entre les requêtes envoyées à la table d'événement. Vous pouvez définir un intervalle d'interrogation plus long en ajoutant à la valeur numérique un H pour les heures ou un M pour les minutes. Les valeurs numériques sans identificateur H ou M interrogent en secondes.
EPS Throttle	Nombre d'événements par seconde (EPS) que vous ne souhaitez pas que ce protocole dépasse.
Database Locale	Pour toute installation en version multilingue, remplissez la zone Database Locale pour indiquer la langue à utiliser.
Database Codeset	Pour toute installation en version multilingue, remplissez la zone Database Codeset pour indiquer le jeu de caractères à utiliser.
Use Named Pipe Communication	Si vous choisissez MSDE comme type de base de données, sélectionnez la case pour utiliser une méthode alternative à une connexion de port TCP/IP. Lorsque vous utilisez une connexion de pipe nommé, le nom d'utilisateur et le mot de passe doivent être le nom d'utilisateur et le mot de passe Windows appropriés et non le nom d'utilisateur et le mot de passe de la base de données. La configuration de la source de journal doit utiliser le canal de communication nommé par défaut.
Database Cluster Name	Nom du cluster devant assurer que les communications du canal de communication nommé fonctionnent correctement.
Use NTLMv2	Force les connexions MSDE à utiliser le protocole NTLMv2 avec les serveurs SQL nécessitant une authentification NTLMv2. La case Use NTLMv2 n'interrompt pas les communications des connexions MSDE qui n'ont pas besoin d'authentification NTLMv2.
Use SSL	Active le chiffrement SSL pour le protocole JDBC.
Log Source Language	Sélectionnez le langage des événements générés par la source de journal. Le langage de la source de journal aide le système à analyser les événements provenant de dispositifs externes ou de systèmes d'exploitation pouvant créer des événements dans plusieurs langages.

Options de configuration du protocole Juniper Networks NSM

Pour recevoir des événements de journaux Juniper Networks NSM et Juniper Networks Secure Service Gateway (SSG), configurez une source de journal pour l'utilisation du protocole Juniper Networks NSM.

Le tableau suivant décrit les paramètres spécifiques au protocole Juniper Networks NSM (Network and Security Manager) :

Tableau 8. Paramètres du protocole Juniper Networks NSM

Paramètre	Description
Log Source Type	Juniper Networks Network and Security Manager
Protocol Configuration	Juniper NSM

Options de configuration du protocole Juniper Security Binary Log Collector

Vous pouvez configurer une source de journal de façon à utiliser le protocole Security Binary Log Collector. Avec ce protocole, les dispositifs Juniper peuvent envoyer des événements des audits, du système, du pare-feu et du système de prévention contre les intrusions (IPS) au format binaire à QRadar.

Le format de journal binaire provenant des dispositifs Juniper SRX ou J Series est transmis à l'aide du protocole UDP. Vous devez spécifier un port unique pour la transmission des événements au format binaire. Le port Syslog standard 514 ne peut pas être utilisé pour les événements au format binaire. Le port affecté par défaut pour recevoir les événements binaires en continu des dispositifs Juniper est le port 40798.

Le tableau suivant décrit les paramètres spécifiques au protocole Juniper Security Binary Log Collector :

Tableau 9. Paramètres du protocole Juniper Security Binary Log Collector

Paramètre	Description
Protocol Configuration	Security Binary Log Collector
XML Template File Location	Chemin d'accès au fichier XML utilisé pour décoder le flux binaire provenant de votre dispositif Juniper SRX ou Juniper J Series. Par défaut, le module de support de périphérique (DSM) inclut un fichier XML pour le décodage des flux binaires. Le fichier XML se trouve dans le répertoire suivant : /opt/qradar/conf/security_log.xml.

Options de configuration du protocole de fichier journal

Pour recevoir des événements des hôtes distants, configurez une source de journal de façon à utiliser le protocole de fichier journal.

Le protocole de fichier journal est conçu pour les systèmes générant des journaux d'événements quotidiens. Il n'est pas conseillé de l'utiliser pour les périphériques ajoutant des informations à leurs fichiers d'événements.

Les fichiers journaux sont extraits un à un. Le protocole de fichier journal peut gérer du texte brut, des fichiers compressés ou des archives de fichiers. Les archives doivent contenir des fichiers de textes bruts pouvant être traités ligne après ligne. Lorsque le protocole de fichier journal télécharge un fichier d'événement, l'information reçue dans le fichier met à jour l'onglet **Activité du journal**. Si des informations supplémentaires sont inscrites dans le fichier à la fin du téléchargement, celles-ci ne sont pas traitées.

Le tableau suivant décrit les paramètres propres au protocole de fichier journal :

Tableau 10. Paramètres du protocole de fichier journal

Paramètre	Description
Protocol Configuration	Fichier journal
Remote Port	Si l'hôte distant utilise un numéro de port non standard, vous devez régler la valeur du port pour extraire les événements.

Tableau 10. Paramètres du protocole de fichier journal (suite)

Paramètre	Description
SSH Key File	Chemin d'accès à la clé SSH, si le système est configuré pour utiliser l'authentification par clé. Lorsqu'un fichier de clés SSH est utilisé, la zone Remote Password est ignorée.
Remote Directory	Pour le protocole FTP, si les fichiers journaux se trouvent dans le répertoire d'accueil de l'utilisateur distant, vous pouvez laisser le répertoire distant vide. Ceci permet de prendre en charge les systèmes dans lesquels les modifications dans la commande répertoire de travail (CWD) sont restreintes.
Recursive	Activez cette case pour autoriser les connexions FTP ou SFTP à rechercher des sous-dossiers dans le répertoire distant des événements de données de manière récursive. Les données collectées depuis des sous-dossiers dépendent des correspondances avec l'expression régulière du masque de fichiers FTP. L'option Récursive n'est pas disponible pour les connexions SCP.
FTP File Pattern	Expression régulière (regex) requise pour identifier les fichiers à télécharger de l'hôte distant.
FTP Transfer Mode	Vous devez sélectionner NONE dans la zone Processor et LINEBYLINE dans la zone Event Generator .
Recurrence	Intervalle de temps indiquant la fréquence à laquelle le répertoire distant est scanné afin de détecter de nouveaux fichiers journaux d'événements. L'intervalle de temps peut inclure des valeurs en heures (H), en minutes (M) ou en jours (D). Par exemple, une récurrence de 2H scanne le répertoire distant toutes les deux heures.
Run On Save	Démarre l'importation de fichiers journaux dès que vous sauvegardez la configuration de la source de journal. Lorsque cette case est cochée, la liste des fichiers téléchargés et traités précédemment est effacée. Après la première importation de fichier, le protocole du fichier journal suit l'heure de début et la planification de récurrence définies par l'administrateur.
EPS Throttle	Nombre d'événements par seconde (EPS) que le protocole ne peut pas dépasser.
Change Local Directory?	Modifie le répertoire local du Collecteur d'événement cible où les journaux d'événements doivent être stockés avant d'être traités.
Local Directory	Répertoire local du Collecteur d'événement cible . Le répertoire doit exister avant que le protocole du fichier journal tente d'extraire les événements.
File Encoding	Codage de caractères utilisé par les événements dans votre fichier journal.
Folder Separator	Caractère utilisé pour séparer les dossiers de votre système d'exploitation. La plupart des configurations peuvent utiliser la valeur par défaut de la zone Folder Separator . Cette zone est prévue pour les systèmes d'exploitation utilisant un caractère différent pour définir les dossiers séparés. Par exemple, les points séparant les dossiers sur les systèmes mainframe.

Options de configuration du protocole Microsoft DHCP

Pour recevoir des événements des serveurs Microsoft DHCP, configurez une source de journal pour l'utilisation du protocole Microsoft DHCP.

Pour lire les fichiers journaux, les chemins de dossiers contenant un partage administratif (C\$) nécessitent des privilèges NetBIOS sur le partage administratif (C\$). Les administrateurs locaux ou de domaine possèdent les privilèges suffisants pour accéder aux fichiers journaux en cas de partage administratif.

Les zones du protocole Microsoft DHCP qui prennent en charge les chemins de fichier autorisent les administrateurs à définir une lettre de lecteur avec les informations de chemin. Par exemple, la zone peut contenir le répertoire c\$/LogFiles/ (en cas de partage administratif) ou le répertoire LogFiles/ (en cas d'accès à un dossier de partage public) mais ne peut pas contenir le répertoire c:/LogFiles.

Restriction : Le protocole d'authentification Microsoft NTLMv2 n'est pas pris en charge par le protocole Microsoft DHCP.

Le tableau suivant décrit les paramètres spécifiques au protocole Microsoft DHCP :

Tableau 11. Paramètres du protocole Microsoft DHCP

Paramètre	Description
Protocol Configuration	Microsoft DHCP
Domain	Facultatif.
Folder Path	Chemin d'accès au répertoire contenant les fichiers journaux DHCP.
File Pattern	Expression régulière (regex) identifiant les journaux d'événements. Les fichiers journaux doivent contenir une abréviation d'un jour de la semaine de trois caractères. Utilisez l'un des masques de fichiers suivants : <ul style="list-style-type: none">• Masque de fichiers IPv4 : DhcpSrvLog-(?:Sun Mon Tue Wed Thu Fri Sat) \.log.• Masque de fichiers: DhcpV6SrvLog-(?:Sun Mon Tue Wed Thu Fri Sat) \.log.• Masque de fichiers mixte IPv4 et IPv6 : Dhcp.*SrvLog-(?:Sun Mon Tue Wed Thu Fri Sat) \.log.

Options de configuration du protocole Microsoft Exchange

Pour recevoir des événements des serveurs SMTP, OWA et Microsoft Exchange 2007 et 2010, configurez une source de journal de façon à utiliser le protocole Microsoft Windows Exchange à prendre en charge.

Pour lire les fichiers journaux, les chemins de dossiers contenant un partage administratif (C\$) nécessitent des privilèges NetBIOS sur le partage administratif (C\$). Les administrateurs locaux ou de domaine possèdent les privilèges suffisants pour accéder aux fichiers journaux en cas de partage administratif.

Les zones du protocole Microsoft Exchange qui prennent en charge les chemins de fichier autorisent les administrateurs à définir une lettre de lecteur avec les informations de chemin. Par exemple, la zone peut contenir le répertoire

c\$/LogFiles/ (en cas de partage administratif) ou le répertoire LogFiles/ (en cas d'accès à un dossier de partage public) mais ne peut pas contenir le répertoire c:/LogFiles.

Important : Le protocole Microsoft Exchange ne prend pas en charge Microsoft Exchange 2003 ou la session NTLMv2 du protocole d'authentification Microsoft.

Le tableau suivant décrit les paramètres spécifiques au protocole Microsoft Exchange :

Tableau 12. Paramètres du protocole Microsoft Exchange

Paramètre	Description
Protocol Configuration	Microsoft Exchange
Domain	Facultatif.
SMTP Log Folder Path	Lorsque le chemin de dossier est vide, la collecte d'événements SMTP est désactivée.
OWA Log Folder Path	Lorsque le chemin de dossier est vide, la collecte d'événements OWA est désactivée.
MSGTRK Log Folder Path	Le suivi de message est disponible sur les serveurs Microsoft Exchange 2007 ou 2010 affectés au rôle de serveur Hub Transport, Mailbox ou Edge Transport.
File Pattern	Expression régulière (regex) identifiant les journaux d'événements. La valeur par défaut est *.*\.(?:log LOG).
Force File Read	Si la case est décochée, le fichier journal est uniquement lu lorsque QRadar détecte un changement au niveau de l'heure de modification ou de la taille du fichier.
Throttle Events/Second	Nombre maximal d'événements pouvant être transférés par le protocole Exchange par seconde.

Options de configuration du protocole Microsoft IIS

Vous pouvez configurer une source de journal de façon à utiliser le protocole Microsoft IIS. Ce protocole prend en charge un seul point de collecte pour les fichiers de journal au format W3C qui se trouvent sur un serveur WebMicrosoft IIS.

Pour lire les fichiers journaux, les chemins de dossiers contenant un partage administratif (C\$) nécessitent des privilèges NetBIOS sur le partage administratif (C\$). Les administrateurs locaux ou de domaine possèdent les privilèges suffisants pour accéder aux fichiers journaux en cas de partage administratif.

Les zones du protocole Microsoft IIS qui prennent en charge les chemins de fichier autorisent les administrateurs à définir une lettre de lecteur avec les informations de chemin. Par exemple, la zone peut contenir le répertoire c\$/LogFiles/ (en cas de partage administratif) ou le répertoire LogFiles/ (en cas d'accès à un dossier de partage public) mais ne peut pas contenir le répertoire c:/LogFiles.

Restriction : Le protocole d'authentification Microsoft NTLMv2 n'est pas pris en charge par le protocole Microsoft IIS.

Le tableau suivant décrit les paramètres spécifiques au protocole Microsoft IIS :

Tableau 13. Paramètres du protocole Microsoft IIS

Paramètre	Description
Protocol Configuration	Microsoft IIS
File Pattern	Expression régulière (regex) identifiant les journaux d'événements.
Throttle Events/Second	Nombre maximal d'événements pouvant être transférés par le protocole IIS par seconde.

Options de configuration du protocole Microsoft Security Event Log

Vous pouvez configurer une source de journal de façon à utiliser le protocole Microsoft Security Event Log. Vous pouvez utiliser Microsoft Windows Management Instrumentation (WMI) pour collecter des journaux d'événements personnalisés ou Windows Event Logs sans agent.

L'API WMI nécessite que les configurations du pare-feu acceptent les communications externes entrantes sur le port 135 ainsi que sur tous les ports dynamiques requis pour DCOM. La liste suivante décrit les limitations de source de journal qui utilisent le protocole Microsoft Security Event Log :

- Les systèmes dépassant 50 événements par seconde (EPS) peuvent dépasser les capacités de ce protocole. Utilisez WinCollect pour les systèmes dépassant 50 EPS.
- Une installation QRadar tout en un peut prendre en charge jusqu'à 250 sources de journal avec le protocole Microsoft Security Event Log.
- Les Collecteurs d'événement dédiés peuvent prendre en charge jusqu'à 500 sources de journal à l'aide du protocole Microsoft Security Event Log.

Le protocole Microsoft Security Event Log n'est pas recommandé pour les serveurs éloignées qui sont accessibles via des liaisons réseau, par exemple, les systèmes dont les délais d'aller-retour sont élevés, comme les satellites ou les réseaux WAN lents. Vous pouvez confirmer les délais d'aller-retour en examinant les requêtes et les temps de réponse entre ping serveur. Les délais de réseau créés par des connexions lentes diminuent la capacité de traitement des EPS sur ces serveurs distants. De même, la collecte d'événements de serveurs occupés ou de contrôleurs de domaine compte sur des délais d'aller-retour faibles pour continuer de répondre aux événements entrants. Si vous ne pouvez pas réduire votre délai d'aller-retour réseau, vous pouvez utiliser WinCollect pour traiter les événements Windows.

Le protocole Microsoft Security Event Log prend en charge les versions de logiciels suivantes avec l'API Microsoft Windows Management Instrumentation (WMI) :

- Microsoft Windows 2000
- Microsoft Windows Server 2003
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008R3
- Microsoft Windows XP
- Microsoft Windows Vista
- Microsoft Windows 7

Le tableau suivant décrit les paramètres spécifiques au protocole Microsoft Security Event Log :

Tableau 14. Paramètres du protocole Microsoft Security Event Log

Paramètre	Description
Protocol Configuration	Windows Security Event Log

Options de configuration du protocole MQ

Pour recevoir des messages d'un service de file d'attente de messages (MQ), configurez une source de journal pour utiliser le protocole MQ. Le nom du protocole apparaît dans IBM Security QRadar en tant que **JMS MQ**.

IBM MQ n'est pas pris en charge.

Le protocole MQ peut surveiller plusieurs files d'attente de messages (jusqu'à 50 files au maximum par source de journal).

Le tableau suivant décrit les paramètres spécifiques au protocole MQ :

Tableau 15. Paramètres du protocole MQ

Paramètre	Description
Protocol Name	JMS MQ
IP or Hostname	Adresse IP ou nom d'hôte du gestionnaire de files d'attente principal
Port	Le port par défaut utilisé pour communiquer avec le gestionnaire de files d'attente principal est 1414.
Standby IP or Hostname	Adresse IP ou nom d'hôte du gestionnaire de files d'attente de secours
Standby Port	Port utilisé pour communiquer avec le gestionnaire de files d'attente de secours.
Queue Manager	Nom du gestionnaire de files d'attente.
Channel	Canal par lequel le gestionnaire de files d'attente envoie des messages. Le canal par défaut SYSTEM.DEF.SVRCONN.
Queue	La file d'attente ou liste de files d'attente à surveiller. Les files d'attente doivent être spécifiées dans une liste séparée par des virgules.
Username	Nom d'utilisateur utilisé pour l'authentification avec le service MQ.
Password	Facultatif : Mot de passe à utiliser pour l'authentification avec le service MQ.
EPS Throttle	Limite supérieure du nombre d'événements maximal par seconde (EPS).
Incoming Message Encoding	Codage de caractères utilisé par les messages entrants.

Options de configuration du protocole d'API REST Okta

Pour recevoir des événements depuis Okta, configurez une source de fichiers pour utiliser le protocole d'API REST Okta.

Le protocole d'API REST Okta interroge les noeuds finaux d'API Okta Events and Users pour extraire des informations sur les actions accomplies par les utilisateurs d'une organisation.

Le tableau suivant décrit les paramètres spécifiques au protocole d'API REST Okta.

Tableau 16. Paramètres du protocole d'API Okta

Paramètre	Description
IP or Hostname	oktaprise.okta.com
Jeton d'authentification	Jeton d'authentification unique généré par la console Okta et qui doit être utilisé par toutes les transactions d'API.
Use Proxy	Quand un proxy est configuré, tout le trafic de la source de journal transite par le proxy pour l'accès de QRadar à Okta. Configurez les zones Proxy IP or Hostname , Proxy Port , Proxy Username et Proxy Password . Si le proxy ne requiert pas d'authentification, vous pouvez laisser les zones Proxy Username et Proxy Password à vide.
Automatically Acquire Server Certificate(s)	Si vous sélectionnez Yes (Oui) dans la liste, QRadar télécharge le certificat et fait confiance au serveur cible.
Recurrence	Vous pouvez spécifier quand la source de journal collecte des données. Le format est M/H/D pour Months/Hours/Days (mois/heures/jours). La valeur par défaut est 1 M.
EPS Throttle	Limite maximale pour le nombre d'événements par seconde.

Options de configuration du protocole OPSEC/LEA

Pour recevoir des événements sur le port 18184, configurez une source de journal de façon à utiliser le protocole OPSEC/LEA.

Le tableau suivant décrit les paramètres spécifiques au protocole OPSEC/LEA :

Tableau 17. Paramètres du protocole OPSEC/LEA

Paramètre	Description
Protocol Configuration	OPSEC/LEA
Server Port	Vous devez vérifier que QRadar peut communiquer sur le port 18184 à l'aide du protocole OPSEC/LEA.
Statistics Report Interval	Intervalle, en secondes, pendant lequel les événements Syslog sont enregistrés dans le fichier qradar.log.
OPSEC Application Object SIC Attribute (SIC Name)	Le nom de SIC (Secure Internal Communications) est le nom distinctif de l'application, par exemple : CN=LEA, o=fwconsole..7psasx.
Log Source SIC Attribute (Entity SIC Name)	Nom SIC du serveur, par exemple : cn=cp_mgmt,o=fwconsole..7psasx.
OPSEC Application	Nom de l'application effectuant la demande de certificat.

Important : Après mise à jour, si vous recevez le message d'erreur **Unable to pull SSL certificate**, suivez ces étapes :

1. Décochez la case permettant d'**indiquer un certificat**.
2. Saisissez de nouveau le mot de passe correspondant au **mot de passe de certificat d'extraction**.

Options de configuration du protocole Oracle Database Listener

Pour collecter à distance les fichiers journaux qui sont générés à partir d'un serveur de base de données Oracle, configurez une source de journal de façon à utiliser la source de protocole Oracle Database Listener.

Avant de configurer le protocole Oracle Database Listener pour intercepter les fichiers journaux à traiter, vous devez obtenir le chemin d'accès au répertoire des fichiers journaux de la base de données Oracle.

Le tableau suivant décrit les paramètres spécifiques au protocole Oracle Database Listener :

Tableau 18. Paramètres du protocole Oracle Database Listener

Paramètre	Description
Protocol Configuration	Programme d'écoute de base de données Oracle
File Pattern	Expression régulière (regex) identifiant les journaux d'événements.

Options de configuration du protocole PCAP Syslog Combination

Pour collecter les événements de dispositifs Juniper Networks SRX Series transférant des données de capture de paquets (PCAP), configurez une source de journal de façon à utiliser le protocole PCAP Syslog Combination.

Avant de configurer une source de journal de façon à utiliser le protocole PCAP Syslog Combination, identifiez le port PCAP sortant configuré sur le dispositif Juniper Networks SRX. Les données PCAP ne peuvent pas être transférées au port 514.

Le tableau suivant décrit les paramètres spécifiques au protocole PCAP Syslog Combination :

Tableau 19. Paramètres du protocole PCAP Syslog Combination

Paramètre	Description
Protocol Configuration	PCAP Syslog Combination
Incoming PCAP Port	Si le port PCAP sortant est édité sur le dispositif Juniper Networks SRX Series, vous devez éditer la source de journal afin de mettre à jour le port PCAP entrant. Une fois que vous avez édité la zone Incoming PCAP Port , vous devez déployer vos modifications.

Options de configuration du protocole SDEE

Vous pouvez configurer une source de journal de façon à utiliser le protocole SDEE (Security Device Event Exchange). QRadar utilise le protocole pour collecter les événements des dispositifs utilisant des serveurs SDEE.

Le tableau suivant décrit les paramètres spécifiques au protocole SDEE :

Tableau 20. Paramètres du protocole SDEE

Paramètre	Description
Protocol Configuration	SDEE
URL	URL HTTP ou HTTPS requise pour accéder à la source de journal, par exemple, https://www.mysdeeserver.com/cgi-bin/sdee-server . Pour SDEE/CIDEE (Cisco IDS v5.x et les versions ultérieures), l'URL doit se terminer par /cgi-bin/sdee-server. Pour les administrateurs avec RDEP (Cisco IDS v4.x), l'URL doit se terminer par /cgi-bin/event-server.
Force Subscription	Si la case est cochée, le protocole impose au serveur d'abandonner la connexion la moins active et d'accepter la connexion à un nouvel abonnement SDEE pour la source de journal.
Maximum Wait To Block For Events	Lorsqu'une demande de collecte est envoyée et qu'aucun événement nouveau n'est disponible, le protocole active un blocage d'événement. Le blocage empêche qu'une nouvelle demande d'événement soit envoyée à un périphérique distant n'ayant eu aucun événement nouveau. L'objectif de ce délai est de préserver les ressources du système.

Options de configuration du protocole SMB Tail

Vous pouvez configurer une source de journal de façon à utiliser le protocole SMB Tail. Utilisez ce protocole pour surveiller les événements sur un partage Samba distant et recevoir des événements du partage Samba lorsque de nouvelles lignes sont ajoutées au journal d'événement.

Le tableau suivant décrit les paramètres spécifiques au protocole SMB Tail :

Tableau 21. Paramètres du protocole SMB Tail

Paramètre	Description
Protocol Configuration	SMB Tail
Log Folder Path	Chemin d'accès au répertoire contenant les fichiers journaux. Par exemple, les administrateurs peuvent utiliser le répertoire c\$/LogFiles/ en cas d'accès à un dossier de partage administratif ou le répertoire LogFiles/ en cas de chemin d'accès à un dossier de partage public. Toutefois, le répertoire c:/LogFiles n'est pas un chemin de dossier de journal pris en charge. Si un chemin de dossier de journal contient un partage administratif (C\$), les utilisateurs possédant un accès NetBIOS sur le partage administratif (C\$) ont les privilèges requis pour lire les fichiers journaux. Les privilèges d'administrateur de système local ou de domaine sont également suffisants pour accéder à un fichier journal se trouvant sur un partage administratif.
File Pattern	Expression régulière (regex) identifiant les journaux d'événements.
Force File Read	Si la case est décochée, le fichier journal est uniquement lu lorsque QRadar détecte un changement au niveau de l'heure de modification ou de la taille du fichier.

Tableau 21. Paramètres du protocole SMB Tail (suite)

Paramètre	Description
Throttle Events/Second	Nombre maximal d'événements envoyés par le protocole SMB Tail par seconde.

Options de configuration du protocole SNMPv2

Vous pouvez configurer une source de journal de façon à utiliser le protocole SNMPv2 pour recevoir les événements SNMPv2.

Le tableau suivant décrit les paramètres spécifiques au protocole SNMPv2 :

Tableau 22. Paramètres du protocole SNMPv2

Paramètre	Description
Protocol Configuration	SNMPv3
Community	Nom de communauté SNMP requis pour accéder au système contenant les événements SNMP.
Include OIDs in Event Payload	Indique que la charge d'événement SNMP est construite à l'aide de paires nom-valeur, et non dans le format utilisé par les charges d'événements. Lorsque vous sélectionnez des sources de journal spécifiques dans la liste Types de source de journal , des OID sont requis dans la charge d'événement pour le traitement des événements SNMPv2 ou SNMPv3.

Options de configuration du protocole SNMPv3

Vous pouvez configurer une source de journal de façon à utiliser le protocole SNMPv3 pour recevoir les événements SNMPv3.

Le tableau suivant décrit les paramètres spécifiques au protocole SNMPv3 :

Tableau 23. Paramètres du protocole SNMPv3

Paramètre	Description
Protocol Configuration	SNMPv3
Authentication Protocol	Algorithmes à utiliser pour authentifier les alertes SNMP
Include OIDs in Event Payload	Indique que la charge d'événement SNMP est construite à l'aide de paires nom-valeur, et non dans le format utilisé par les charges d'événements standard. Lorsque vous sélectionnez des sources de journal spécifiques dans la liste Types de source de journal , des OID sont requis dans la charge d'événement pour le traitement des événements SNMPv2 ou SNMPv3.

Options de configuration du protocole d'API REST Seculert Protection

Pour recevoir des événements depuis Seculert, configurez une source de fichiers pour utiliser le protocole d'API REST Seculert Protection.

Seculert Protection fournit des alertes sur des incidents confirmés de logiciels malveillants qui communiquent activement ou exfiltrent des informations.

Pour pouvoir configurer une source de journal pour Seculert, vous devez obtenir votre clé d'interface de programmation (API) du portail Web de Seculert.

1. Connectez-vous au portail Web Seculert.
2. Dans le tableau de bord, cliquez sur l'onglet **API**.
3. Copiez la valeur pour **Your API Key**.

Le tableau suivant décrit les paramètres spécifiques au protocole d'API REST Seculert Protection :

Tableau 24. Paramètres du protocole d'API Seculert Protection

Paramètre	Description
API Key	Clé d'interface de programmation utilisée pour l'authentification avec l'API REST Seculert Protection. La valeur de la clé d'API est obtenue du portail Web Seculert.
Use Proxy	Lorsque vous configurez un proxy, tout le trafic de la source de journal transite par le proxy pour l'accès de QRadar à l'API REST Seculert Protection. Configurez les zones Proxy IP or Hostname , Proxy Port , Proxy Username et Proxy Password . Si le proxy ne requiert pas d'authentification, vous pouvez laisser les zones Proxy Username et Proxy Password à vide.
Automatically Acquire Server Certificate(s)	Si vous sélectionnez Yes (Oui) dans la liste, QRadar télécharge le certificat et fait confiance au serveur cible.
Recurrence	Indiquez quand le journal collecte des données. Le format est M/H/D pour Months/Hours/Days (mois/heures/jours). La valeur par défaut est 1 M.
EPS Throttle	Limite supérieure du nombre d'événements maximal par seconde (eps) pour les événements reçus de l'API.

Options de configuration du protocole Sophos Enterprise Console JDBC

Pour recevoir des événements des consoles Sophos Enterprise Console, configurez une source de journal de façon à utiliser le protocole Sophos Enterprise Console JDBC.

Le protocole Sophos Enterprise Console JDBC combine les informations contenues dans les journaux de contrôle d'application, les journaux de contrôle de périphérique, les journaux de contrôle de données, les journaux de protection contre les falsifications et les journaux de pare-feu du tableau vEventsCommonData. Si la Sophos Enterprise Console ne dispose pas de l'interface de génération de rapports Sophos Reporting Interface, vous pouvez utiliser le protocole JDBC standard pour collecter les événements antivirus.

Le tableau suivant décrit les paramètres du protocole Sophos Enterprise Console JDBC :

Tableau 25. Paramètres du protocole Sophos Enterprise Console JDBC

Paramètre	Description
Protocol Configuration	Sophos Enterprise Console JDBC
Database Type	MSDE

Tableau 25. Paramètres du protocole Sophos Enterprise Console JDBC (suite)

Paramètre	Description
Database Name	Le nom de la base de données doit correspondre au nom de base de données spécifié dans la zone Identificateur de source de journal .
Port	Le port par défaut pour MSDE dans Sophos Enterprise Console est 1168. Le port de configuration JDBC doit correspondre au port d'écoute de la base de données Sophos pour pouvoir communiquer avec QRadar. La base de données Sophos doit avoir les connexions TCP entrantes activées. Si le paramètre Database Instance est utilisé avec le type de base de données MSDE, vous devez laisser le paramètre Port vide.
Authentication Domain	Si votre réseau n'utilise pas de domaine, laissez cette zone vide.
Database Instance	Instance de base de données, si nécessaire. Les bases de données MSDE peuvent inclure plusieurs instances de serveur SQL sur un serveur. Lorsqu'un port non standard est utilisé pour la base de données ou que les administrateurs bloquent l'accès au port 1434 pour la résolution de base de données SQL, le paramètre Database Instance doit être vide.
Table Name	vEventsCommonData
Select List	*
Compare Field	InsertedAt
Use Prepared Statements	Les instructions préparées permettent à la source du protocole de configurer l'instruction SQL puis de l'exécuter plusieurs fois avec des paramètres différents. Pour des raisons de sécurité et de performance, la plupart des configurations peuvent utiliser des instructions préparées. Désélectionnez cette case pour utiliser une méthode d'interrogation alternative n'utilisant pas les instructions précompilées.
Start Date and Time	Facultatif. Date et heure de début à laquelle le protocole peut commencer à interroger la base de données. Si aucune heure de début n'est définie, le protocole tente d'interroger les événements une fois que la configuration de la source de journal est sauvegardée et déployée.
Polling Interval	Intervalle d'interrogation, qui correspond à l'intervalle de temps séparant deux requêtes sur la base de données. Vous pouvez définir un intervalle d'interrogation plus long en ajoutant à la valeur numérique un H pour les heures ou un M pour les minutes. L'intervalle d'interrogation maximum est de 1 semaine sous tous les formats horaires. Les valeurs numériques sans identificateur H ou M interrogent en secondes.
EPS Throttle	Nombre d'événements par seconde (EPS) que vous ne souhaitez pas que ce protocole dépasse.

Tableau 25. Paramètres du protocole Sophos Enterprise Console JDBC (suite)

Paramètre	Description
Use Named Pipe Communication	<p>Si MSDE est configuré comme type de base de données, les administrateurs peuvent cocher cette case pour utiliser une méthode alternative à une connexion de port TCP/IP.</p> <p>Les connexions de pipe nommées pour les bases de données MSDE ont besoin de la zone de nom d'utilisateur et de la zone de mot de passe pour utiliser un nom d'utilisateur et un mot de passe Windows et non le nom d'utilisateur et le mot de passe de la base de données. La configuration de la source de journal doit utiliser le canal de communication nommé par défaut sur la base de données MSDE.</p>
Database Cluster Name	Si vous utilisez votre serveur SQL dans un environnement cluster, définissez le nom du cluster pour vous assurer que les communications du canal de communication nommé fonctionnent correctement.
Use NTLMv2	<p>Force les connexions MSDE à utiliser le protocole NTLMv2 avec les serveurs SQL nécessitant une authentification NTLMv2. La valeur par défaut de la case à cocher est sélectionnée.</p> <p>La case Use NTLMv2 n'interrompt pas les communications des connexions MSDE qui n'ont pas besoin d'authentification NTLMv2.</p>

Options de configuration du protocole Sourcefire Defense Center Estreamer

Pour recevoir des événements d'un service Sourcefire Defense Center Estreamer (Event Streamer), configurez une source de journal de façon à utiliser le protocole Sourcefire Defense Center Estreamer.

Les fichiers d'événements sont diffusés en continu sur QRadar pour y être traités après la configuration du DSM Sourcefire Defense Center.

Le tableau suivant décrit les paramètres spécifiques au protocole Sourcefire Defense Center Estreamer :

Tableau 26. Paramètres du protocole Sourcefire Defense Center Estreamer

Paramètre	Description
Protocol Configuration	Sourcefire Defense Center Estreamer
Server Port	Le port par défaut utilisé par QRadar pour Sourcefire Defense Center Estreamer est 8302.
Keystore Filename	Chemin de répertoire et nom de fichier de la clé privée du magasin de clés et du certificat associé. Par défaut, le script d'importation crée le fichier de clés dans le répertoire suivant : /opt/qradar/conf/estreamer.keystore.
Truststore Filename	Le magasin de clés de confiance contient les certificats sécurisés par le client. Par défaut, le script d'importation crée le magasin de clés de confiance dans le répertoire suivant : /opt/qradar/conf/estreamer.truststore.

Tableau 26. Paramètres du protocole Sourcefire Defense Center Estreamer (suite)

Paramètre	Description
Request Extra Data	Sélectionnez cette option pour demander des données supplémentaires de Sourcefire Defense Center Estreamer, par exemple, des données supplémentaires comprennent l'adresse IP d'origine d'un événement.
Utilisation de requêtes étendues	Sélectionnez cette option pour utiliser une autre méthode pour extraire des événements à partir d'une source eStreamer. Les requêtes étendues sont prises en charge sur Sourcefire DefenseCenter Estreamer version 5.0 ou ultérieure.

Présentation du protocole Syslog Redirect

Le protocole Syslog Redirect est utilisé comme alternative au protocole Syslog. Utilisez ce protocole lorsque vous souhaitez que QRadar identifie nom d'unité spécifique envoyé par les événements. QRadar peut écouter de manière passive les événements Syslog sur le port UDP 517.

Le tableau suivant décrit les paramètres propres au protocole pour le protocole Syslog Redirect :

Tableau 27. Paramètres du protocole Syslog Redirect

Paramètre	Description
Protocol Configuration	Syslog Redirect
Log Source Identifier RegEx	devname=([\w-]+)
Listen Port	517
Protocol	UDP

Options de configuration du protocole TCP Multiline Syslog

Vous pouvez configurer une source de journal qui utilise le protocole TCP Multiline Syslog. Pour créer un événement à une seule ligne, ce protocole utilise les expressions régulières pour identifier les modèles de début et de fin des événements multi-lignes.

L'exemple suivant montre un événement multi-lignes :

```
06/13/2012 20:15:15
LogName=Security
SourceName=Microsoft Windows security auditing.
EventCode=5156
EventType=0
TaskCategory=Filtering Platform Connection
Keywords=Audit Success
Message=The Windows Filtering Platform permitted a connection.
Process ID: 4
Application Name: System
Direction: Inbound
Source Address: 1.1.1.1
Source Port: 80
Destination Address: 1.1.1.12
Destination Port:444
```

Le tableau suivant décrit les paramètres spécifiques au protocole TCP Multiline Syslog :

Tableau 28. Paramètres du protocole TCP Multiline Syslog

Paramètre	Description
Protocol Configuration	TCP Multiline Syslog
Listen Port	Le port d'écoute par défaut est 12468.
Event Formatter	Utilisez l'option Windows Multiline pour les événements multi-lignes formatés spécifiquement pour Windows.
Event Start Pattern	Expression régulière (regex) requise pour identifier le début d'une charge d'événement TCP multi-lignes. Les en-têtes Syslog commencent généralement par une date ou un horodatage. Le protocole peut créer un événement sur une seule ligne, basé uniquement sur un modèle de début, tel qu'un horodatage. Si seul un modèle de début est disponible, le protocole capture toutes les informations fournies entre chaque valeur de début pour créer un événement valide.
Event End Pattern	Expression régulière (regex) requise pour identifier le dernier champ d'une charge d'événement TCP multi-lignes. Si l'événement Syslog se termine par la même valeur, vous pouvez utiliser une expression régulière pour déterminer la fin d'un événement. Le protocole peut capturer des événements basés uniquement sur un modèle de fin d'événement. Si seul un modèle de fin est disponible, le protocole capture toutes les informations fournies entre chaque valeur de fin pour créer un événement valide.

Options de configuration du protocole TLS Syslog

Pour recevoir des événements Syslog chiffrés depuis plus de 50 périphériques réseau prenant en charge la transmission d'événements TLS Syslog, configurez une source de journal de façon à utiliser le protocole TLS Syslog.

La source de journal crée un port d'écoute pour les événements TLS Syslog entrants et génère un fichier certificat pour les périphériques réseau. 50 dispositifs réseau peuvent transmettre des événements au port d'écoute qui est créé pour la source de journal. Si vous avez besoin de plus de 50 périphériques réseau, créez des ports d'écoute supplémentaires.

Le tableau suivant décrit les paramètres propres au protocole TLS Syslog :

Tableau 29. Paramètres du protocole TLS Syslog

Paramètre	Description
Protocol Configuration	TLS Syslog
TLS Listen Port	La valeur par défaut du port d'écoute TLS est 6514.
Authentication Mode	Mode avec lequel votre connexion TLS est authentifiée. Si vous sélectionnez l'option TLS and Client Authentication , vous devez configurer les paramètres de certificat.
Client Certificate Path	Chemin d'accès absolu au certificat client sur le disque. Le certificat doit être stocké sur la console ou le Collecteur d'événements pour cette source de journal.

Tableau 29. Paramètres du protocole TLS Syslog (suite)

Paramètre	Description
Certificate Type	Type de certificat à utiliser pour l'authentification. Si vous sélectionnez l'option Provide Certificate , vous devez configurer les chemins de fichier pour certificat serveur et la clé privée.
Provided Server Certificate Path	Chemin d'accès absolu au certificat serveur.
Provided Private Key Path	Chemin d'accès absolu à la clé privée. Remarque : La clé privée correspondante doit être une clé PKCS8 codée DER. La configuration échoue avec un autre format de clé.
Maximum Connections	Le paramètre Maximum Connections contrôle le nombre de connexions simultanées que le protocole TLS Syslog peut accepter pour chaque Collecteur d'événements. Il existe une limite de 1000 connexions pour l'ensemble des configurations de source de journal TLS syslog par Collecteur d'événements. La valeur par défaut pour chaque connexion de dispositif est de 50. Remarque : Les sources de journal automatiquement reconnues qui partagent un programme d'écoute avec une source de journal sont prises en compte une seule fois pour cette limite. Par exemple, le même port sur le même collecteur d'événements.

Cas d'utilisation du protocole TLS

Les cas d'utilisation suivants représentent les configurations possibles que vous pouvez créer :

Authentification client

Vous pouvez fournir un certificat client qui permet au protocole de s'engager dans une authentification client. Si vous sélectionnez cette option et fournissez le certificat, les connexions entrantes sont validées par rapport au certificat client.

Certificats serveur fournis par l'utilisateur

Vous pouvez configurer votre propre certificat serveur et la clé privée correspondante. Le fournisseur TLS Syslog configuré utilise le certificat et la clé. Les connexions entrantes sont présentés avec le certificat fourni par l'utilisateur, au lieu d'un certificat TLS syslog généré automatiquement.

Authentification par défaut

Pour utiliser la méthode d'authentification par défaut, utilisez les valeurs par défaut pour les paramètres **Authentication Mode** et **Certificate Type**. Une fois la source de journal sauvegardée, un certificat `syslog-tls` est créé pour la source de journal. Le certificat doit être copié sur tous les périphériques de votre réseau configurés pour réacheminer les données Syslog chiffrées.

Options de configuration du protocole UDP Multiline Syslog

Pour créer un événement à une seule ligne à partir d'un événement multi-lignes, configurez une source de journal de façon à utiliser le protocole multi-lignes UDP.

Le protocole UDP Multiline Syslog utilise une expression régulière pour identifier et reconstituer les messages Syslog multi-lignes dans une charge d'événements unique.

L'événement d'origine doit contenir une valeur répétant une expression régulière capable d'identifier et de reconstituer l'événement multi-lignes. Par exemple, cet événement contient une valeur répétée :

```
15:08:56 1.1.1.1 slapd[517]: conn=2467222 op=2 SEARCH
RESULT tag=101
15:08:56 1.1.1.1 slapd[517]: conn=2467222 op=2 SRCH base="dc=iso-n,dc=com"
15:08:56 1.1.1.1 slapd[517]: conn=2467222 op=2 SRCH attr=gidNumber
15:08:56 1.1.1.1 slapd[517]: conn=2467222 op=1 SRCH base="dc=iso-n,dc=com"
```

Le tableau suivant décrit les paramètres spécifiques au protocole UDP Multiline Syslog :

Tableau 30. Paramètres du protocole UDP Multiline Syslog

Paramètre	Description
Protocol Configuration	UDP Multiline Syslog
Message ID Pattern	Expression régulière (regex) requise pour filtrer les messages de charges d'événements. Les messages d'événements multi-lignes UDP doivent contenir une valeur d'identification commune se répétant sur chaque ligne du message d'événement.

Une fois la source de journal sauvegardée, un certificat syslog-tls est créé pour la source de journal. Le certificat doit être copié vers tous les périphériques de votre réseau étant configurés pour réacheminer les événements Syslog chiffrés. Les autres périphériques réseau possédant un fichier certificat syslog-tls et le numéro du port d'écoute TLS peuvent être automatiquement reconnus comme source de journal TLS Syslog.

Options de configuration du protocole VMware vCloud Director

Pour collecter des événements des environnements virtuels VMware vCloud Director, vous pouvez créer une source de journal utilisant le protocole VMware vCloud Director.

Le tableau suivant décrit les paramètres spécifiques au protocole VMware vCloud Director :

Tableau 31. Paramètres du protocole VMware vCloud Director

Paramètre	Description
Protocol Configuration	VMware vCloud Director
vCloud URL	URL configurée sur le dispositif VMware vCloud pour accéder à l'API REST. L'URL doit correspondre à l'adresse configurée comme URL de base de l'API REST publique VCD sur le serveur vCloud, par exemple : <code>https://1.1.1.1.</code>
User Name	Nom d'utilisateur requis pour accéder au serveur vCloud à distance, par exemple : <code>console/user@organization</code> . Pour configurer un compte en lecture seule à utiliser avec le protocole vCloud Director, l'utilisateur doit posséder un droit d'accès à la console uniquement.

Ajout de sources de journal en bloc

Vous pouvez ajouter jusqu'à 500 sources de journal Microsoft Windows ou Universal DSM en une seule opération. Lorsque vous ajoutez plusieurs sources de journal à la fois, vous ajoutez une source de journal en vrac dans QRadar. Les sources de journal en vrac doivent partager une configuration commune.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Sources de journal**.
3. Dans la liste **Actions en vrac**, sélectionnez **Ajouter en vrac**.
4. Configurez les paramètres de la source de journal en vrac.
 - Téléchargement de fichier - Charger un fichier texte comportant un nom d'hôte ou une adresse IP par ligne
 - Manuel - Entrez le nom ou l'adresse IP de l'hôte à ajouter
5. Cliquez sur **Sauvegarder**.
6. Cliquez sur **Continuer** pour ajouter les sources de journal.
7. Sur l'onglet **Admin**, cliquez sur **Déployer les changements**.

Ajout d'un ordre d'analyse syntaxique de source de journal

Vous pouvez attribuer un ordre de priorité à suivre lorsque les événements sont analysés par le collecteur d'événements cible.

Pourquoi et quand exécuter cette tâche

Vous pouvez classer les sources de journal suivant leur importance en définissant un ordre d'analyse syntaxique pour les sources de journal partageant une adresse IP commune ou un nom d'hôte commun. La définition de l'ordre d'analyse des sources de journal permet d'analyser certaines sources de journal dans un ordre spécifique, indépendamment des modifications apportées à la configuration de la source de journal. L'ordre d'analyse évite que les performances du système ne soient affectées par les modifications apportées à la configuration de source de journal en évitant les analyses superflues. L'ordre d'analyse évite également que les sources d'événements de bas niveau ne soient analysées avant une source de journal plus importante.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Ordre d'analyse de la source de journal**.
3. Sélectionnez une source de journal.
4. Facultatif : Dans la liste **Collecteur d'événement sélectionné**, sélectionnez le collecteur d'événements à utiliser pour définir l'ordre d'analyse de la source de journal.
5. Facultatif : Dans la liste **Hôte de la source de journal**, sélectionnez une source de journal.
6. Définissez l'ordre d'analyse des sources de journal en fonction de leur priorité.
7. Cliquez sur **Sauvegarder**.

Chapitre 2. Extensions de source de journal

Un document d'extension peut étendre ou modifier la façon dont les éléments d'une source de journal particulière sont analysés. Vous pouvez utiliser le document d'extension pour corriger un problème d'analyse ou remplacer l'analyse par défaut d'un événement à partir d'un DSM existant.

Un document d'extension peut également fournir une prise en charge d'événements lorsqu'un module de support d'unité (DSM) n'existe pas pour analyser des événements pour un dispositif ou un périphérique de sécurité dans votre réseau.

Un document d'extension est un document formaté en XML (Extensible Markup Language) que vous pouvez créer ou modifier en utilisant n'importe quel texte commun, code ou éditeur de balisage. Vous pouvez créer plusieurs documents d'extension, mais un seul peut être appliqué à une source de journal.

Le format XML nécessite que tous les motifs d'expression régulière (regex) soient contenus dans les sections de données textuelles (CDATA) afin d'empêcher les caractères spéciaux requis par des expressions régulières d'interférer avec le format de balisage. Par exemple, le code suivant montre l'expression régulière pour rechercher des protocoles :

```
<pattern id="ProtocolPattern" case-insensitive="true" xmlns="">  
<![CDATA[(TCP|UDP|ICMP|GRE)]]></pattern>
```

(TCP|UDP|ICMP|GRE) est le modèle d'expression régulière.

La configuration d'extension de sources de journal se compose des sections suivantes :

Motif Motifs d'expressions régulières que vous associez à un nom de champ particulier. Les motifs sont référencés plusieurs fois dans le fichier d'extension de source de journal.

Groupes de correspondance

Entité au sein d'un groupe de correspondance qui est analysé, par exemple, EventName, et est appariée avec le motif et le groupe appropriés pour l'analyse. Tout nombre de groupes de correspondance peut apparaître dans le document d'extension.

Exemples d'extensions de source de journal sur le forum QRadar

Vous pouvez créer des extensions de source de journal (LSX) pour les sources du journal qui ne disposent pas d'un DSM pris en charge. Pour vous aider à créer vos propres extensions de source de journal (également appelées extensions DSM), vous modifiez celles existantes qui ont été créées.

Vous pouvez accéder aux exemples d'extension de source de journal (<https://www.ibm.com/developerworks/community/forums/html/topic?id=d15cac8d-b0fa-4461-bb1e-dc1b291de440&ps=25>) sur le forum de discussion sur les extensions DSM, les propriétés personnalisées et autres sujets connexes REGEX (<https://www.ibm.com/developerworks/community/forums/html/forum?id=11111111-0000-0000-0000-000000003046&ps=25>).

Le forum IBM Security QRadar est un site de discussion en ligne où les utilisateurs et les experts en la matière collaborent et partagent des informations.

Concepts associés:

«Création d'un document d'extension de source de journal», à la page 40
Créer des extensions de source de journal (LSX) pour les sources du journal qui ne disposent pas d'un DSM pris en charge, ou pour réparer un événement qui a des informations manquantes ou erronées, ou pour analyser un événement lorsque le DSM associé ne parvient pas à produire un résultat.

Motifs dans les documents d'extension de source de journal

Plutôt que d'associer une expression régulière directement à un nom de champ particulier, des motifs (patterns) sont déclarés séparément en tête du document d'extension. Ces motifs regex peuvent alors être référencés plusieurs fois dans le fichier d'extension de source de journal.

Tous les caractères entre la balise de début <pattern> et la balise de fin </pattern> sont considérés comme faisant partie du motif. N'utilisez pas d'espaces supplémentaires ou des retours fixes à l'intérieur ou autour de votre motif ou expression <CDATA>. Des caractères ou des espaces supplémentaires peuvent empêcher l'extension de DSM de correspondre à votre motif prévu.

Tableau 32. Description des paramètres de comparateur

Motif	Type	Description
id (obligatoire)	Chaîne	Chaîne régulière qui est unique dans le document d'extension.
case-insensitive (facultatif)	Booléen	Si la valeur est true, la casse est ignorée. Par exemple,, abc est identique à ABC. Sinon, ce paramètre par défaut devient faux.
trim-whitespace (facultatif)	Booléen	Si la valeur est true, les espaces blancs et les retours chariot sont ignorés. Si les sections CDATA sont réparties sur différentes lignes, des espaces supplémentaires et les retours chariot ne sont pas interprétés comme faisant partie du motif. Sinon, ce paramètre par défaut devient faux.

Groupes de correspondance

Un *groupe de correspondance* (match-group) est un ensemble de motifs utilisés pour l'analyse ou la modification d'un ou de plusieurs types d'événements.

Un *comparateur* est une entité au sein d'un groupe de correspondance qui est analysé, par exemple, EventName, et est appariée avec le motif et le groupe appropriés pour l'analyse. Tout nombre de groupes de correspondance peut apparaître dans le document d'extension.

Tableau 33. Description des paramètres de groupe de correspondance

Paramètre	Description
order (obligatoire)	Nombre entier supérieur à zéro qui définit l'ordre dans lequel les groupes de correspondance sont exécutés. Il doit être unique dans le document d'extension.
description (facultatif)	Description pour le groupe de correspondance, qui peut être une chaîne. Ces informations peuvent apparaître dans les journaux. Sinon, ce paramètre par défaut devient vide.
device-type-id-override (facultatif)	Définissez un ID d'unité différent afin de substituer QID. Permet au groupe de correspondance particulier de rechercher le type d'événement dans le dispositif spécifié. Il doit s'agir d'un ID type source de journal valide, représenté comme un entier. Une liste d'ID type source de journal est représentée dans tableau 40, à la page 52. Si non spécifié, ce paramètre est par défaut le type de source de journal de la source du journal à laquelle l'extension est attachée.

Les groupes de correspondance peuvent avoir ces entités :

- «Comparateur (matcher)»
- «Modificateur d'événement unique (event-match-single)», à la page 36
- «Modificateur d'événements multiples (event-match-multiple)», à la page 36

Comparateur (matcher)

Une entité de comparateur (matcher) est un champ qui est analysé, par exemple, EventName, et est jumelé avec le motif et le groupe appropriés pour l'analyse.

Les comparateurs ont un ordre associé. Si plusieurs comparateurs sont spécifiés pour le même nom de domaine, les comparateurs sont exécutés dans l'ordre qui est présenté, jusqu'à ce qu'une analyse syntaxique réussie soit trouvée ou qu'un échec se produise.

Tableau 34. Description des paramètres de comparateur

Paramètre	Description
field (obligatoire)	Champ auquel vous souhaitez appliquer le motif, par exemple, EventName, ou SourceIp. Vous pouvez utiliser l'un des noms de champs qui sont répertoriés dans le tableau Liste des noms de champs de comparateur valide .

Tableau 34. Description des paramètres de comparateur (suite)

Paramètre	Description
pattern-id (obligatoire)	Motif que vous souhaitez utiliser lorsque le champ est analysé à partir du contenu. Cette valeur doit correspondre (y compris la casse) au paramètre d'identification du motif qui est déjà défini dans un paramètre d'identification de motif (tableau 32, à la page 30).
order (obligatoire)	Ordre dans lequel vous souhaitez que ce motif fasse des tentatives parmi les comparateurs qui sont affectés à un même champ. Si deux comparateurs sont affectés au champ EventName, celui dont l'ordre est le plus faible est tenté en premier.
capture-group (facultatif)	<p>Référencé dans l'expression régulière entre parenthèses (). Ces captures sont indexées, à partir d'un et traitées de gauche à droite dans le motif. Le champ capture-group doit être un entier positif inférieur ou égal au nombre de groupes de capture qui figurent dans le motif. La valeur par défaut est zéro, ce qui constitue l'intégralité de la concordance.</p> <p>Par exemple, vous pouvez définir un motif unique pour une adresse IP source et le port ; où le comparateur SourceIp peut utiliser un groupe de capture de 1, et le comparateur SourcePort peut utiliser un groupe de capture de 2, mais uniquement un motif doit être défini.</p> <p>Ce champ a un double objectif lorsqu'il est combiné au paramètre enable-substitutions.</p> <p>Pour voir un exemple, consultez l'exemple de document d'extension.</p>

Tableau 34. Description des paramètres de comparateur (suite)

Paramètre	Description
enable-substitutions (facultatif)	<p>Booléen</p> <p>Lorsque vous sélectionnez true, un champ ne peut pas être correctement représenté avec une capture de groupe linéaire. Vous pouvez combiner plusieurs groupes avec le texte supplémentaire pour former une valeur.</p> <p>Ce paramètre change la signification du paramètre capture-groupe. Le paramètre capture-groupe crée la nouvelle valeur, et des substitutions de groupe sont spécifiées en utilisant \x où x est un numéro de groupe, 1 à 9. Vous pouvez utiliser des groupes à plusieurs reprises, et tout texte de forme libre peut également être inséré dans la valeur. Par exemple, pour former une valeur hors du groupe 1, suivie par un tiret, suivi par le groupe 2, un @, puis à nouveau le groupe 1, la syntaxe de capture-groupe appropriée est indiquée dans le code suivant :</p> <pre>capture-groupe="\1_\2@1"</pre> <p>Dans un autre exemple, une adresse MAC est séparée par des deux points, mais dans QRadar, les adresses MAC sont généralement séparées par des tirets. La syntaxe pour analyser et capturer les portions individuelles est indiquée dans l'exemple suivant :</p> <pre>capture-groupe="\1:\2:\3:\4:\5:\6"</pre> <p>Si aucun groupe n'est spécifié dans le groupe de capture lorsque des substitutions sont activées, un remplacement de texte direct se produit.</p> <p>La valeur par défaut est False.</p>
ext-data (facultatif)	<p>Un paramètre ext-data qui définit les informations de champ supplémentaire ou le formatage qu'un champ de comparateur peut fournir dans l'extension.</p> <p>Le seul champ qui utilise ce paramètre est DeviceTime.</p> <p>Par exemple, vous pourriez avoir un périphérique qui envoie des événements en utilisant un horodatage unique, mais vous souhaitez que l'événement soit reformaté à une heure du périphérique standard. Utilisez le paramètre ext-data inclus avec le champ DeviceTime pour reformater la date et l'heure de l'événement. Pour plus d'informations, voir la Liste des noms de champs de comparateur valide.</p>

Le tableau suivant répertorie les noms de champs de comparateur valides.

Tableau 35. Liste des noms de champs de comparateur valide

Nom de champ	Description
EventName (obligatoire)	Nom de l'événement à extraire à partir du QID pour identifier l'événement. Remarque : Ce paramètre n'apparaît pas en tant que champ dans l'onglet Activité de journal .
EventCategory	Une catégorie d'événement pour un événement avec une catégorie non gérée par une entité event-match-single ou une entité event-match-multiple. Combiné à EventName, EventCategory est utilisé pour rechercher l'événement dans le QID. Les champs qui sont utilisés pour les recherches QIDmap exigent le réglage d'un indicateur de remplacement lorsque les périphériques sont déjà connus de QRadar, par exemple, <pre><event-match-single event-name="Successfully logged in" force-qidmap-lookup-on-fixup="true" device-event-category="CiscoNAC" severity="4" send-identity="OverrideAndNeverSend" /></pre> force-qidmap-lookup-on-fixup="true" est la substitution de l'indicateur. Remarque : Ce paramètre n'apparaît pas en tant que champ dans l'onglet Activité de journal .
SourceIp	Adresse IP source pour le message.
SourcePort	Port source pour le message.
SourceIpPreNAT	Adresse IP source pour le message avant la traduction d'adresses réseau (NAT).
SourceIpPostNAT	Adresse IP source pour le message après la NAT.
SourceMAC	Adresse MAC source pour le message.
SourcePortPreNAT	Port source pour le message avant la NAT.
SourcePortPostNAT	Port source pour le message après la NAT.
DestinationIp	Adresse IP de destination pour le message.
DestinationPort	Port destination pour le message.
DestinationIpPreNAT	Adresse IP de destination pour le message avant la NAT.
DestinationIpPostNAT	Adresse IP de destination pour le message après la NAT.
DestinationPortPreNAT	Port de destination pour le message avant la NAT.
DestinationPortPostNAT	Port de destination pour le message après la NAT.

Tableau 35. Liste des noms de champs de comparateur valide (suite)

Nom de champ	Description
DestinationMAC	Adresse MAC de destination pour le message.
DeviceTime	<p>Temps et format utilisés par le périphérique. Cette date et l'heure représentent le moment où l'événement a été envoyé, selon le dispositif. Ce paramètre ne représente pas le moment où l'événement est arrivé. Le champ DeviceTime prend en charge la capacité d'utiliser une date et une heure personnalisées pour l'événement en utilisant l'attribut de comparateur ext-data.</p> <p>La liste suivante contient des exemples de formats de date et heure que vous pouvez utiliser dans le champ DeviceTime :</p> <ul style="list-style-type: none"> • ext-data="dd/MMM/YYYY:hh:mm:ss" 11/Mar/2015:05:26:00 • ext-data="MMM dd YYYY / hh:mm:ss" Mar 11 2015 / 05:26:00 • ext-data="hh:mm:ss:dd/MMM/YYYY" 05:26:00:11/Mar/2015 <p>Pour plus d'informations sur les valeurs possibles pour le format de date et heure, voir la page Web Joda-Time (http://www.joda.org/joda-time/key_format.html).</p> <p>DeviceTime est le seul champ d'événement qui utilise le paramètre facultatif ext-data.</p>
Protocole	Protocole qui est associé à l'événement ; par exemple, TCP, UDP, ou ICMP.
Nom d'utilisateur	Nom d'utilisateur qui est associé à l'événement.
HostName	Nom d'hôte qui est associé à l'événement. Typiquement, ce champ est associé à des événements d'identité.
GroupName	Nom de groupe associé à l'événement. Typiquement, ce champ est associé à des événements d'identité.
NetBIOSName	Nom NetBIOS associé à l'événement. Typiquement, ce champ est associé à des événements d'identité.
ExtraIdentityData	Toutes les données spécifiques à l'utilisateur associées à l'événement. Typiquement, ce champ est associé à des événements d'identité.
SourceIpv6	Adresse IP source IPv6 pour le message.
DestinationIpv6	Adresse IP de destination IPv6 pour le message.

Modificateur d'événements multiples (event-match-multiple)

Le modificateur d'événements multiples (event-match-multiple) correspond à une gamme de types d'événements puis les modifie comme spécifié par le paramètre pattern-id et le paramètre capture-group-index.

Cette correspondance ne se fait pas par rapport au contenu, mais se fait par rapport aux résultats du comparateur EventName analysé précédemment sur le contenu.

Cette entité permet la mutation d'événements réussis en changeant la catégorie de l'événement de périphérique, sa gravité ou la méthode que l'événement utilise pour envoyer des événements d'identité. capture-group-index doit être une valeur entière (les substitutions ne sont pas prises en charge) et pattern-ID doit faire référence à une entité de motif existante. Toutes les autres propriétés sont identiques à leurs contreparties dans le modificateur d'événement unique.

Modificateur d'événement unique (event-match-single)

Le modificateur d'événement unique (event-match-single) correspond, puis modifie exactement un type d'événement, comme spécifié par le paramètre requis, sensible à la casse EventName.

Cette entité permet la mutation d'événements réussis en changeant la catégorie de l'événement de périphérique, sa gravité ou sa méthode d'envoi des événements d'identité.

Lorsque des événements qui correspondent à ce nom d'événement sont analysés, la catégorie du périphérique, la gravité et les propriétés d'identité sont imposées sur l'événement qui en résulte.

Vous devez définir un attribut event-name et cette valeur d'attribut correspond à la valeur du champ **EventName**. En outre, une entité event-match-single se compose de ces propriétés facultatives :

Tableau 36. Description des paramètres d'événement unique

Paramètre	Description
device-event-category	Nouvelle catégorie pour rechercher un QID pour l'événement. Ce paramètre est un paramètre d'optimisation parce que certains dispositifs ont la même catégorie pour tous les événements.
severity	Gravité de l'événement. Ce paramètre doit être une valeur entière de 1 à 10. Si un niveau de gravité inférieur à 1 ou supérieur à 10 est spécifié, le valeur système par défaut est 5. Si rien n'est indiqué, la valeur par défaut est toute valeur trouvée dans le QID.

Tableau 36. Description des paramètres d'événement unique (suite)

Paramètre	Description
send-identity	<p>Indique l'envoi d'informations concernant le changement d'identité de l'événement. Choisissez l'une des options suivantes :</p> <ul style="list-style-type: none"> • UseDSMResults Si le DSM renvoie un événement d'identité, l'événement est transmis. Si le DSM ne renvoie pas d'événement d'identité, l'extension ne crée ni ne modifie les informations d'identité. Cette option est la valeur par défaut si aucune valeur n'est spécifiée. • SendIfAbsent Si le DSM crée des informations d'identité, l'événement de l'identité est traversé en restant inchangé. Si aucun événement d'identité n'est produit par le DSM, mais qu'il existe suffisamment d'informations dans l'événement pour créer un événement d'identité, un événement est généré avec tous les champs pertinents définis. • OverrideAndAlwaysSend Ignore tout événement d'identité qui est renvoyé par le DSM et crée un nouvel événement d'identité, s'il existe suffisamment d'informations. • OverrideAndNeverSend Supprime toute information d'identité qui sont renvoyées par le DSM. Option proposée sauf si vous traitez des événements que vous souhaitez intégrer dans les mises à jour d'actifs.

Modèle de document d'extension

L'exemple d'un document d'extension fournit des informations sur la façon d'analyser un type particulier de Cisco FWSM afin que les événements ne soient pas envoyés avec un nom d'événement incorrect.

Par exemple, si vous voulez résoudre le mot `session`, qui est intégré au milieu du nom de l'événement :

```
Nov 17 09:28:26 129.15.126.6 %FWSM-session-0-302015:
Built UDP connection for faddr 38.116.157.195/80
gaddr 129.15.127.254/31696 laddr 10.194.2.196/2157
duration 0:00:00 bytes 57498 (TCP FINs)
```

Cette condition entraîne le DSM à ne pas reconnaître d'événement et tous les événements sont non analysés et associés au consignateur générique.

Bien que seule une partie de la chaîne de texte (302015) est utilisée pour la recherche QID, toute la chaîne de texte (%FWSM-session-0-302015) identifie l'événement comme provenant d'un Cisco FWSM. Étant donné que toute la chaîne de texte n'est pas valide, le DSM suppose que l'événement n'est pas valide.

Exemple de document d'xtension pour analyser un type d'événement

Un périphérique FWSM possède de nombreux types d'événements et beaucoup avec des formats uniques. L'exemple de document d'extension suivant indique comment analyser un type d'événement.

Remarque : Les ID de motif ne doivent pas nécessairement correspondre aux noms de champ qu'ils analysent. Bien que l'exemple suivant duplique le motif, le champ SourceIp et le cab de champ SourceIpPreNAT utilisent le même modèle dans ce cas. Cette situation pourrait ne pas être vraie dans tous les événements FWSM.

```
<?xml version="1.0" encoding="UTF-8"?>
<device-extension xmlns="event_parsing/device_extension">
  <pattern id="EventNameFWSM_Pattern" xmlns=""><![CDATA[%FWSM[a-zA-Z\-\_]\d{1,6}]]></pattern>
  <pattern id="SourceIp_Pattern" xmlns=""><![CDATA[&gaddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([{\d}{1,5})]]></pattern>
  <pattern id="SourceIpPreNAT_Pattern" xmlns=""><![CDATA[&gaddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([{\d}{1,5})]]></pattern>
  <pattern id="SourceIpPostNAT_Pattern" xmlns=""><![CDATA[&laddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([{\d}{1,5})]]></pattern>
  <pattern id="DestinationIp_Pattern" xmlns=""><![CDATA[&raddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([{\d}{1,5})]]></pattern>
  <pattern id="Protocol_Pattern" case-insensitive="true" xmlns=""><![CDATA[({tcp|udp|icmp|gre})]]></pattern>
  <pattern id="Protocol_6_Pattern" case-insensitive="true" xmlns=""><![CDATA[protocol=6]]></pattern>
  <pattern id="EventNameId_Pattern" xmlns=""><![CDATA[(\d{1,6})]]></pattern>
  <match-group order="1" description="FWSM Test" device-type-id-override="6" xmlns="">
    <matcher field="EventName" order="1" pattern-id="EventNameFWSM_Pattern" capture-group="1" />
    <matcher field="SourceIp" order="1" pattern-id="SourceIp_Pattern" capture-group="1" />
    <matcher field="SourcePort" order="1" pattern-id="SourcePort_Pattern" capture-group="2" />
    <matcher field="SourceIpPreNAT" order="1" pattern-id="SourceIpPreNAT_Pattern" capture-group="1" />
    <matcher field="SourceIpPostNAT" order="1" pattern-id="SourceIpPostNAT_Pattern" capture-group="1" />
    <matcher field="SourcePortPreNAT" order="1" pattern-id="SourcePortPreNAT_Pattern" capture-group="2" />
    <matcher field="SourcePortPostNAT" order="1" pattern-id="SourcePortPostNAT_Pattern" capture-group="2" />
    <matcher field="DestinationIp" order="1" pattern-id="DestinationIp_Pattern" capture-group="1" />
    <matcher field="DestinationPort" order="1" pattern-id="DestinationIp_Pattern" capture-group="1" />
    <matcher field="Protocol" order="1" pattern-id="Protocol_Pattern" capture-group="1" />
    <matcher field="Protocol" order="2" pattern-id="Protocol_6_Pattern" capture-group="TCP" enable-substitutions=true />
    <event-match-multiple pattern-id="EventNameId" capture-group-index="1" device-event-category="Cisco Firewall" />
  </match-group>
</device-extension>

<?xml version="1.0" encoding="UTF-8"?>
<device-extension xmlns="event_parsing/device_extension">
  <!-- Do not remove the "allEventNames" value -->
  <pattern id="EventName-Fakeware_Pattern" xmlns=""><![CDATA[]]></pattern>
  <pattern id="SourceIp-Fakeware_Pattern" xmlns=""><![CDATA[]]></pattern>
  <pattern id="SourcePort-Fakeware_Pattern" xmlns=""><![CDATA[]]></pattern>
  <pattern id="SourceMAC-Fakeware_Pattern" xmlns=""><![CDATA[]]></pattern>
  <pattern id="DestinationIp-Fakeware_Pattern" xmlns=""><![CDATA[]]></pattern>
  <pattern id="DestinationPort-Fakeware_Pattern" case-insensitive="true" xmlns=""><![CDATA[]]></pattern>
  <pattern id="Protocol-Fakeware_Pattern" case-insensitive="true" xmlns=""><![CDATA[]]></pattern>
  <match-group order="1" description="FWSM Test" device-type-id-override="6" xmlns="">
    <matcher field="EventName" order="1" pattern-id="EventName-Fakeware_Pattern" capture-group="1" />
    <matcher field="SourceIp" order="1" pattern-id="SourceIp-Fakeware_Pattern" capture-group="1" />
    <matcher field="SourcePort" order="1" pattern-id="SourcePort-Fakeware_Pattern" capture-group="1" />
    <matcher field="SourceMAC" order="1" pattern-id="SourceMAC-Fakeware_Pattern" capture-group="1" />
    <matcher field="DestinationIp" order="1" pattern-id="DestinationIp-Fakeware_Pattern" capture-group="1" />
    <matcher field="DestinationPort" order="1" pattern-id="DestinationPort-Fakeware_Pattern" capture-group="1" />
    <matcher field="Protocol" order="1" pattern-id="Protocol-Fakeware_Pattern" capture-group="1" />
    <event-match-multiple pattern-id="EventNameId" capture-group-index="1" device-event-category="Cisco Firewall" />
  </match-group>
</device-extension>
```

Bases d'analyse syntaxique

L'exemple de document de l'extension précédent montre quelques-uns des aspects fondamentaux de l'analyse :

- Adresses IP
- Ports
- Protocol
- Plusieurs champs qui utilisent le même motif avec différents groupes

Cet exemple analyse tous les événements FWSM qui suivent le motif spécifié. Les champs qui sont analysés pourraient ne pas être présents dans ces événements lorsque les événements comprennent un contenu différent.

Les informations qui étaient nécessaires pour créer cette configuration qui n'étaient pas disponibles à partir de l'événement :

- Le nom de l'événement est uniquement les 6 derniers chiffres (302015) de la portion %FWSM-session-0-302015 de l'événement.

- Le FWSM a une catégorie d'événement de périphérique codée en dur de Cisco Firewall.
- Le DSM FWSM utilise le Cisco Pix QIDmap et comprend donc le paramètre `device-type-id-override="6"` dans le groupe de correspondance. L'ID de type de source de journal de pare-feu Pix est 6. Pour plus d'informations, voir «ID de type de source de journal», à la page 52).

Remarque : Si les informations QID ne sont pas spécifiées ou ne sont pas disponibles, vous pouvez modifier le mappage de l'événement. Pour plus d'informations, voir la section Modifier le mappage d'événement dans *IBM Security QRadar SIEM*.

Nom de l'événement et catégorie d'événement de périphérique

Un nom d'événement et une catégorie d'événement de périphérique sont nécessaires lorsque le QIDmap est recherché. Cette catégorie d'événement de périphérique est un paramètre de regroupement au sein de la base de données qui aide à définir des événements semblables dans un périphérique. `event-match-multiple` à la fin du groupe de correspondance comprend un codage en dur de la catégorie. `event-match-multiple` utilise le motif de `EventNameId` sur le nom de l'événement analysé pour correspondre jusqu'à 6 chiffres. Ce motif n'est pas exécuté sur le contenu complet, uniquement sur la partie analysée en tant que le champ `EventName`.

Le motif `EventName` fait référence à la partie `%FWSM` des événements ; tous les événements Cisco FWSM contiennent la partie `%FWSM`. Le motif dans l'exemple correspond à `%FWSM` suivi par un nombre quelconque (zéro ou plus) de lettres et de tirets. Cette correspondance de motif résout le mot `session` qui est incorporé au milieu du nom de l'événement qui doit être retiré. La gravité de l'événement (selon Cisco), suivie d'un tiret, puis du vrai nom de l'événement comme attendu par QRadar. La chaîne `(\d{6})` est la seule chaîne dans le motif `EventNameFWSM` qui possède un groupe de capture.

Les adresses IP et les ports pour l'événement suivent tous le même modèle de base : une adresse IP suivie de deux-points, suivie du numéro de port. Ce motif analyse deux données (l'adresse IP et le port), et précise les différents groupes de capture dans la section `matcher`.

```
<device-extension>
<pattern id="EventName1">(logger):</pattern>
<pattern id="DeviceTime1">time=[(\d{2}/\w{3}/\d{4}:\d{2}:\d{2}:\d{2})\ ] </pattern>
<pattern id="Username">(TLsv1)</pattern>
<match-group order="1" description="Full Test">
  <matcher field="EventName" order="1" pattern-id="EventName1" capture-group="1"/>
  <matcher field="DeviceTime" order="1" pattern-id="DeviceTime1"
    capture-group="1" ext-data="dd/MMM/YYYY:hh:mm:ss"/>
  <matcher field="UserName" order="1" pattern-id="Username" capture-group="1"/>
</match-group>
</device-extension>
```

Adresse IP et motifs de port

L'adresse IP et les motifs de port sont quatre ensembles de un à trois chiffres, séparés par des points, suivis par un signe deux-points et le numéro de port. La section de l'adresse IP est dans un groupe, de même que le numéro de port, mais pas les deux points. Les sections `matcher` pour ces champs font référence au même nom de motif mais à un groupe de capture différent (l'adresse IP est le groupe 1 et le port est le groupe 2).

Le protocole est un motif commun qui recherche le contenu pour la première instance de TCP, UDP, ICMP, ou GRE. Le motif est marqué avec le paramètre insensible à la casse de sorte que toute occurrence correspond.

Bien qu'un second motif de protocole ne se produise pas dans l'événement utilisé dans l'exemple, il existe un second motif de protocole qui est défini par un ordre de deux. Si le motif de protocole le plus faible ne correspond pas, le suivant est tenté, et ainsi de suite. Le deuxième motif de protocole démontre également la substitution directe ; il n'existe pas de groupe de correspondances dans le motif, mais avec le paramètre enable-substitutions activé, le texte TCP peut être utilisé à la place du protocole=6.

Création d'un document d'extension de source de journal

Créer des extensions de source de journal (LSX) pour les sources du journal qui ne disposent pas d'un DSM pris en charge, ou pour réparer un événement qui a des informations manquantes ou erronées, ou pour analyser un événement lorsque le DSM associé ne parvient pas à produire un résultat.

Pour les sources de journal qui ne disposent pas d'un DSM officiel, utilisez un DSM universel, ou UDSM, pour intégrer les sources de journal. Une extension de source de journal (également appelée extension de périphérique) est ensuite appliquée au UDSM pour fournir la logique pour analyser les journaux. Le LSX est basé sur les expressions régulières Java et peut être utilisé sur tout protocole de journal, comme syslog, JDBC et LFPS. Les valeurs peuvent être extraites à partir des journaux et mappées à tous les champs communs au sein de QRadar.

Lorsque vous utilisez les extensions de source de journal pour réparer du contenu manquant ou incorrect, tous les nouveaux événements produits par les extensions de source de journal sont associés à la source de journal qui n'a pas pu analyser le contenu d'origine. La création d'une extension empêche les événements inconnus ou non catégorisés d'être stockés comme inconnus dans IBM Security QRadar.

Suivez cette procédure pour créer une extension de source de journal :

1. Assurez-vous qu'une source de journal est créée dans QRadar.
Utilisez le DSM universel comme type de source de journal pour gérer des éléments qui ne sont pas dans la liste. Vous pouvez également créer manuellement une source de journal pour empêcher les journaux d'être classés automatiquement.
2. Pour déterminer quels domaines sont disponibles, utilisez l'onglet **Activité du journal** pour exporter les journaux pour l'évaluation.
3. Utilisez le modèle exemple du document d'extension pour déterminer les champs que vous pouvez utiliser. («Modèle de document d'extension», à la page 37).
Il est pas nécessaire d'utiliser tous les champs dans le modèle. Déterminez les valeurs de la source de journal qui peuvent être mappées sur les champs dans le modèle de document d'extension. Pour plus d'informations, voir «Modèle de document d'extension», à la page 37.
4. Retirez tous les champs inutilisés et leur ID de motif correspondants du document d'extension de source de journal.
5. Téléchargez le document d'extension et appliquez l'extension à la source du journal.
6. Mappez les événements à leurs équivalents dans le QIDmap.

Cette action manuelle sur l'onglet **Activité du journal** permet de mapper des événements de source de journal inconnus sur des événements QRadar connus afin qu'ils puissent être classés et traités.

Concepts associés:

«Exemples d'extensions de source de journal sur le forum QRadar», à la page 29
Vous pouvez créer des extensions de source de journal (LSX) pour les sources du journal qui ne disposent pas d'un DSM pris en charge. Pour vous aider à créer vos propres extensions de source de journal (également appelées extensions DSM), vous modifiez celles existantes qui ont été créées.

Construction d'un DSM universel

La première étape dans la construction d'un DSM universel consiste à créer la source du journal dans IBM Security QRadar. Lorsque vous créez la source du journal, cela empêche les journaux d'être classés automatiquement et vous pouvez exporter les journaux pour examen.

Procédure

1. Dans l'onglet **Admin**, créez une source en cliquant sur l'icône **Sources de journal**.
2. Cliquez sur **Ajouter**.
3. Indiquez le nom dans le champ **Nom de source de journal**.
4. Dans la liste **Type de source de journal**, sélectionnez **Universal DSM**.
Vous ne pourrez peut-être pas voir l'**Extension de source de journal** à moins d'avoir déjà appliqué une extension de source de journal à la QRadar Console
5. Dans la liste **Configuration de protocole**, spécifiez le protocole que vous souhaitez utiliser.
Cette méthode est utilisée par QRadar pour obtenir les journaux de la source de journal non pris en charge.
6. Pour l'**Identificateur de source de journal**, entrez l'adresse IP ou le nom d'hôte de la source de journal non prise en charge.
7. Cliquez sur **Sauvegarder** pour enregistrer la nouvelle source de journal et fermer la fenêtre.
8. Dans l'onglet **Admin**, cliquez sur **Déployer les changements**.

Que faire ensuite

«Exportation des journaux»

Exportation des journaux

Exportez les journaux qui sont créés après que vous générez un DSM universel

Pourquoi et quand exécuter cette tâche

En général, vous souhaitez un nombre important de journaux pour examen. En fonction du débit EPS de la source de journal non prise en charge, cela peut prendre plusieurs heures pour obtenir un échantillon global de journal.

Quand QRadar ne peut pas détecter le type de source de journal, les événements sont collectés, mais ne sont pas analysés. Vous pouvez filtrer ces événements non analysés et puis examiner la dernière notification du système que vous avez reçue. Après avoir examiné la notification du système, vous pouvez créer une recherche qui est basée sur ce laps de temps.

Procédure

1. Pour consulter uniquement les événements qui ne sont pas analysés, filtrez les journaux.
 - a. Cliquez sur l'onglet **Activité du journal**.
 - b. Cliquez sur **Ajouter un filtre**.
 - c. Sélectionnez **L'événement n'est pas analysé**.

Conseil : Saisissez dans la zone **Paramètre** pour visualiser l'élément **L'événement n'est pas analysé**.

- d. Sélectionnez une période.
- e. Si vous voyez des événements **Information** dans les notifications système, cliquez avec le bouton droit de la souris pour les filtrer.
- f. Examinez la colonne **IP source** pour déterminer quel périphérique envoie les événements.

Vous pouvez afficher les contenus d'événement bruts. Généralement, les fabricants ont mis des noms de produits identifiables dans les en-têtes, de sorte que vous pouvez définir votre recherche sur **Afficher : Événements bruts** pour montrer les contenus sans avoir à ouvrir manuellement chaque événement. Le tri par réseau peut aussi vous aider à rechercher un dispositif spécifique d'où provient l'événement.

2. Créez une recherche pour exporter les journaux.
 - a. Dans l'onglet **Activité de journal**, sélectionnez **Recherche > Editer la recherche**
 - b. Pour l'**Intervalle**, spécifiez suffisamment de temps, par exemple six heures, à partir du moment où la source de journal a été créée.
 - c. Dans **Paramètres de recherche**, dans la liste **Paramètres**, sélectionnez **Source de journal (indexée)**, dans la liste **Opérateurs**, sélectionnez **Egale**, et dans la liste **Groupe de sources de journal**, sélectionnez **Autre**, spécifiez la source du journal qui a été créée lorsque vous avez généré le Universal DSM.

Parameter:	Operator:	Value:
Log Source [Indexed]	Equals	Log Source Group: Other

Log Source: Fakeware@100.100.100.1

Add Filter

Remarque : En fonction de vos paramètres, vous pourriez voir **Source de journal** dans la liste **Paramètres** plutôt que la **Source de journal (indexée)**.

- d. Cliquez sur **Recherche** pour afficher les résultats.
3. Examinez les résultats dans la console pour vérifier le contenu.
 4. En option, vous pouvez exporter les résultats en cliquant sur **Actions > Exporter au format XML > Exportation complète (toutes les colonnes)**.

Ne sélectionnez pas **Exporter au format CSV** parce que le contenu peut être réparti sur plusieurs colonnes, rendant difficile la recherche de contenu. XML est le format préféré des avis d'événements.

 - a. Vous êtes invité à télécharger un fichier compressé. Ouvrez le fichier compressé et ouvrez le fichier résultant.
 - b. Consultez les journaux.

Les contenus d'événements sont entre les balises suivantes :

```
<payloadAsUTF>
...
</payloadAsUTF>
```

Le code suivant montre un exemple de contenu :

```
<payloadAsUTF>ecs-ep (pid 4162 4163 4164) is running... </payloadAsUTF>
```

Une étape critique dans la création d'un DSM universel est l'examen des journaux pour le degré d'utilisation. Au minimum, les journaux doivent avoir une valeur qui peut être mappée sur un nom d'événement. Le nom de l'événement doit être une valeur unique qui peut distinguer les différents types de journaux.

Le code suivant montre un exemple de journaux utilisables :

```
May 20 17:16:14 dropbear[22331]: bad password attempt for 'root'
from 192.168.50.80:3364
May 20 17:16:26 dropbear[22331]: password auth succeeded for
'root' from 192.168.50.80:3364
May 20 16:42:19 kernel: DROP IN=vlan2 OUT=
MAC=00:01:5c:31:39:c2:08:00 SRC=172.29.255.121
DST=255.255.255.255 PROTO=UDP SPT=67 DPT=68
```

Les codes d'exemple suivants montrent les journaux un peu moins utilisables :

```
Oct 26 08:12:08 loopback 1256559128 autotrace[215824]: W: trace:
no map for prod 49420003, idf 010029a2, la1 00af0008
Oct 26 16:35:00 sxpgbd0081 last message repeated 7 times
Nov 24 01:30:00 sxpgbd0081 /usr/local/monitor-rrd/sxpgbd0081/.rrd
(rc=-1, opening '/usr/local/monitor-rrd/sxpgbd0081/.rrd':
No such file or directory)
```

Expressions régulières courantes

Utilisez des expressions régulières pour faire correspondre des modèles de texte dans le fichier source du journal. Vous pouvez analyser les messages pour les motifs de lettres, de chiffres, ou une combinaison des deux. Par exemple, vous pouvez créer des expressions régulières qui correspondent à des adresses IP source et de destination, des ports, des adresses MAC, et plus encore.

Les codes suivants montrent plusieurs expressions régulières communes :

```
\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3} \d{1,5}
(?:[0-9a-fA-F]{2}\:){5}[0-9a-fA-F]{2} (TCP|UDP|ICMP|GRE)
\w{3}\s\d{2}\s\d{2}:\d{2}:\d{2}
\s \t .*?
```

Le caractère d'échappement, ou "\", est utilisé pour désigner un caractère littéral. Par exemple, le caractère "." signifie "tout caractère unique" et correspond à A, B, 1, X, et ainsi de suite. Pour faire correspondre les caractères ".", une correspondance littérale vous devez utiliser "\".

Tableau 37. Expressions regex courantes

Type	Expression
Type	\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}
Adresse IP	\d{1,5}
Numéro de port	(?:[0-9a-fA-F]{2}\:){5}[0-9a-fA-F]{2}
Protocole	(TCP UDP ICMP GRE)
Heure de l'unité	\w{3}\s\d{2}\s\d{2}:\d{2}:\d{2}
Espace	\s
Tabulation	\t

Tableau 37. Expressions regex courantes (suite)

Type	Expression
Faire correspondre à tout élément	.*

Conseil : Pour garantir que vous ne faites pas correspondre accidentellement un autre caractère, mettez en échappement tout caractère non numérique ou non alphabétique.

Construction de motifs d'expression régulière

Pour créer un DSM universel, vous utilisez des expressions régulières (regex) pour faire correspondre des chaînes de texte à partir de la source de journal non prise en charge.

Pourquoi et quand exécuter cette tâche

L'exemple suivant montre une entrée de journal référencée dans les étapes.

```
May 20 17:24:59 kernel: DROP MAC=5c:31:39:c2:08:00
SRC=172.29.255.121 DST=10.43.2.10 LEN=351 TOS=0x00 PREC=0x00 TTL=64 ID=9582
PROTO=UDP SPT=67 DPT=68 LEN=331
May 20 17:24:59 kernel: PASS MAC=5c:14:ab:c4:12:59
SRC=192.168.50.10 DST=192.168.10.25 LEN=351 TOS=0x00 PREC=0x00 TTL=64
ID=9583 PROTO=TCP SPT=1057 DPT=80 LEN=331
May 20 17:24:59 kernel: REJECT
MAC=5c:ad:3c:54:11:07 SRC=10.10.10.5 DST=192.168.100.25 LEN=351
TOS=0x00 PREC=0x00 TTL=64 ID=9584 PROTO=TCP SPT=25212 DPT=6881 LEN=331
```

Procédure

1. Analysez visuellement la source de journal non prise en charge pour identifier des motifs uniques.

Ces motifs sont ensuite traduits en expressions régulières.

2. Recherchez les chaînes de texte à faire correspondre.

Conseil : Pour fournir un contrôle d'erreur de base, incluez des caractères avant et après les valeurs, afin d'empêcher des valeurs similaires d'être involontairement appariées. Vous pouvez ensuite isoler la valeur réelle des caractères supplémentaires.

3. Développez le pseudo-code pour les motifs correspondants et incluez le caractère d'espace pour indiquer le début et la fin d'un motif.

Vous pouvez ignorer les guillemets. Dans l'exemple d'entrée de journal, les noms d'événements sont DROP, PASS, et REJECT. La liste suivante montre les champs d'événement utilisables.

- EventName: " kernel: VALUE "
- SourceMAC: " MAC=VALUE "
- SourceIp: " SRC=VALUE "
- DestinationIp: " DST=VALUE "
- Protocol: " PROTO=VALUE "
- SourcePort: " SPT=VALUE "
- DestinationPort: " DPT=VALUE "

4. Remplacez un espace par l'expression régulière \s.

Vous devez utiliser un caractère d'échappement pour les caractères non numériques ou non alphabétiques. Par exemple, = devient \= et : devient \:.

5. Convertissez le pseudo-code en une expression régulière.

Tableau 38. Conversion du pseudo-code en expressions régulières

Zone	Pseudo-code	Expression régulière
EventName	" kernel: VALUE "	\skernel\:\s.*?\s
SourceMAC	" MAC=VALUE "	\sMAC\=(?:[0-9a-fA-F]{2}\:){5}[0-9a-fA-F]{2}\s
SourceIP	" SRC=VALUE "	\sSRC\=\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\s
DestinationIp	" DST=VALUE "	\sDST\=\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\s
Protocol	" PROTO=VALUE "	\sPROTO\ =(TCP UDP ICMP GRE)\s
SourcePort	" SPT=VALUE "	\sSPT\=\d{1,5}\s
DestinationPort	" DPT=VALUE "	\sDPT\=\d{1,5}\s

6. Indiquez des groupes de capture.

Un groupe de capture isole une certaine valeur dans l'expression régulière.

Par exemple, dans le motif SourcePort dans l'exemple précédent, vous ne pouvez pas transmettre toute la valeur car elle comprend des espaces et SRC=<code>. Au lieu de cela, vous spécifiez uniquement le numéro de port en utilisant un groupe de capture. La valeur dans le groupe de capture est ce qui est transmis au champ pertinent IBM Security QRadar.

Insérez les parenthèses autour des valeurs que vous souhaitez capturer :

Tableau 39. Mappage d'expressions régulières pour capturer des groupes pour les champs d'événements

Zone	Expression régulière	Groupe de capture
EventName	\skernel\:\s.*?\s	\skernel\:\s(?:)\s
SourceMAC	\sMAC\=(?:[0-9a-fA-F]{2}\:){5}[0-9a-fA-F]{2}\s	\sMAC\=(?:[0-9a-fA-F]{2}\:){5}[0-9a-fA-F]{2}(?)\s
SourceIP	\sSRC\=\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\s	\sSRC\=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})(?)\s
IP de destination	\sDST\=\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\s	\sDST\=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})(?)\s
Protocol	\sPROTO\ =(TCP UDP ICMP GRE)\s	\sPROTO\ =((TCP UDP ICMP GRE))(?)\s
SourcePort	\sSPT\=\d{1,5}\s	\sSPT\=(\d{1,5})(?)\s
DestinationPort	\sDPT\=\d{1,5}\s	\sDPT\=(\d{1,5})(?)\s

7. Migrez les motifs et les groupes de capture dans le document d'extensions de source de journal.

Le fragment de code suivant montre une partie du document que vous utilisez.

```
<device-extension xmlns="event_parsing/device_extension">
  <pattern id="EventNameFWSM_Pattern" xmlns=""><![CDATA[%FWSM[a-zA-Z-]*\d-(\d{1,6})]]></pattern>
  <pattern id="SourceIp_Pattern" xmlns=""><![CDATA[gaddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
  <pattern id="SourceIpPreNAT_Pattern" xmlns=""><![CDATA[gaddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
  <pattern id="SourceIpPostNAT_Pattern" xmlns=""><![CDATA[laddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
  <pattern id="DestinationIp_Pattern" xmlns=""><![CDATA[faddr (\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})/([\d]{1,5})]]></pattern>
  <pattern id="Protocol_Pattern" case-insensitive="true" xmlns=""><![CDATA[(TCP|UDP|ICMP|GRE)]]></pattern>
  <pattern id="Protocol_6_Pattern" case-insensitive="true" xmlns=""><![CDATA[protocol=6]]></pattern>
  <pattern id="EventNameId_Pattern" xmlns=""><![CDATA[(\d{1,6})]]></pattern>
</device-extension>
```

Téléchargement de documents d'extension à QRadar

Vous pouvez créer plusieurs documents d'extension, puis les télécharger et les associer à divers types de sources de journal. La logique de l'extension de source de journal (LSX) est alors utilisée pour analyser les journaux de la source de journal non pris en charge.

Les documents d'extension peuvent être stockés n'importe où avant de télécharger vers IBM Security QRadar.

Procédure

1. Dans l'onglet **Admin**, cliquez sur **Sources de données > Extensions de source de journal**.
2. Dans la fenêtre Ajout d'une extension de source de journal, cliquez sur **Ajouter**.
3. Attribuez un nom.
4. Si vous utilisez le DSM universel, ne sélectionnez pas le document d'extension par défaut pour un **Type de source de journal**.
En sélectionnant le DSM universel par défaut, il affecte toutes les sources de journaux associées. Un DSM universel peut être utilisé pour définir la logique d'analyse pour plusieurs sources d'événements personnalisées et non prises en charge.
5. Facultatif : Si vous souhaitez appliquer cette extension de source de journal à plusieurs instance d'un type de source de journal, sélectionnez le type de la source de journal à partir de la liste des **Types de la source de journal** disponibles et cliquez sur la flèche d'ajout pour le définir comme la valeur par défaut.
La définition du type de source de journal par défaut applique l'extension de source de journal à tous les événements d'un type de source de journal, y compris les sources de journaux qui sont détectées automatiquement.
Assurez-vous que vous testez l'extension pour le type de source de journal d'abord, pour garantir que les événements sont analysés correctement.
6. Cliquez sur **Parcourir** pour localiser le LSX que vous avez enregistré, puis cliquez sur **Charger**.
QRadar valide le document par rapport au XSD interne et vérifie la validité du document avant que le document d'extension soit téléchargé sur le système.
7. Cliquez sur **Enregistrer** puis fermez la fenêtre.
8. Associez l'extension de source de journal à une source du journal.
 - a. Dans l'onglet **Admin**, cliquez sur **Sources de données > Sources de journal**.
 - b. Double-cliquez sur le type de source de journal pour lequel vous avez créé le document d'extension.
 - c. Dans la liste **Extension de la source de journal**, sélectionnez le document que vous avez créé.
 - d. Cliquez sur **Enregistrer** puis fermez la fenêtre.

Mappage d'événements inconnus

Initialement, tous les événements du DSM universel apparaissent comme inconnus dans l'onglet **Activité du journal** dans QRadar. Vous devez mapper manuellement tous les événements inconnus à leurs équivalents dans la mappe QID.

Bien que les noms d'événements, tels que DROP, DENY, et ACCEPT, pourraient être des valeurs compréhensibles lorsque vous les visualisez dans les fichiers journaux, QRadar ne comprend pas ce que ces valeurs représentent. Pour QRadar,

ces valeurs sont des chaînes de texte qui ne sont pas mappées à des valeurs connues. Les valeurs apparaissent comme prévu et sont traitées comme des événements normalisés jusqu'à ce que vous les mappiez manuellement.

Dans certains cas, comme un système de détection d'intrusion (IDS) ou une détection d'intrusion et de prévention (IDP) des milliers d'événements existent et nécessitent le mappage. Dans ces situations, vous pouvez mapper une catégorie en tant que nom de l'événement au lieu de lui-même. Par exemple, dans l'exemple suivant, afin de réduire le nombre de mappages, au lieu d'utiliser le champ de nom pour le Nom d'événement, utilisez le champ de la catégorie à la place. Vous pouvez utiliser une propriété personnalisée pour afficher le nom de l'événement (Code Red v412) :

```
date: "Feb 25 2010 00:43:26"; name: "SQL Slammer v312"; category: "Worm Activity"; source ip: "100.100.200.200";  
date: "Feb 25 2015 00:43:26"; name: "Code Red v412"; category: "Worm Activity"; source ip: "100.100.200.200";  
date: "Feb 25 2015 00:43:26"; name: "Annoying Toolbar"; category: "Malware"; source ip: "100.100.200.200";
```

Au lieu d'utiliser le champ de nom pour le Nom d'événement, utilisez le champ de la catégorie. Le nom de l'événement réel, par exemple Code Red V412 peut être affiché en utilisant une propriété personnalisée.

Avant de commencer

Assurez-vous que vous avez téléchargé le document d'extension de source de journal et que vous l'avez appliqué au DSM universel. Pour plus d'informations, voir «Téléchargement de documents d'extension à QRadar», à la page 46.

Procédure

1. Dans l'onglet **Activité de journal**, cliquez sur **Recherche > Editer la recherche**
2. Dans les options **Intervalle**, choisissez suffisamment de temps, comme 15 minutes, à partir du moment où l'extension de source de journal a été appliquée au DSM universel.
3. Dans **Paramètres de recherche**, sélectionnez **Source de journal [Index]** dans la liste **Paramètres**, **Egale** dans la liste **Opérateurs**, puis sélectionnez la source de journal que vous avez créée dans le **Groupe de source de journal** et les **Listes de source de journal**.
4. Cliquez sur **Recherche** pour afficher les résultats.
Tous les événements apparaissent comme inconnus.
5. Double-cliquez sur une entrée inconnue pour afficher les détails de l'événement.
6. Cliquez sur **Mapper l'événement** dans la barre d'outils.
La valeur **ID d'événement de la source de journal** affiche une valeur **EventName**, par exemple, DROP, DENY, ou ACCEPT, à partir de l'extension de la source de journal. La valeur ne peut pas être vide. Une valeur vide indique qu'il existe une erreur dans le document d'extension de source de journal.
7. Mappez la valeur qui est affichée comme **ID d'événement de la source de journal** au QID approprié.

Utilisez **Parcourir par catégorie**, ou **Recherche de QID**, ou les deux pour rechercher une valeur qui correspond le mieux à la valeur **ID d'événement de la source de journal**. Par exemple, la valeur DROP peut être mise en correspondance avec le **QID Firewall Deny - Event CRE**.

Utilisez le QID avec l'Event CRE dans le nom.. La plupart des événements sont spécifiques à un type de source de journal particulier. Par exemple, lorsque

vous mappez à un pare-feu aléatoire, **Refuser QID** est similaire au mappage du DSM universel sur des événements provenant d'un autre type de source de journal. Les entrées QID qui contiennent le nom Event CRE sont génériques et ne sont pas liées à un type de source de journal particulier.

8. Répétez ces étapes jusqu'à ce que tous les événements inconnus soient mappés avec succès.

A partir de ce moment, d'autres événements du DSM universel qui contiennent cet ID d'événement source de journal particulier apparaît comme le QID spécifié. Les événements qui sont arrivés avant la mappage de QID restent inconnus. Il n'existe aucune méthode prise en charge pour le mappage des événements antérieurs à un QID actuel. Ce processus doit être répété jusqu'à ce que tous les types d'événements inconnus soient mappés avec succès à un QID.

Problèmes et exemples d'analyse syntaxique

Lorsque vous créez une extension de source de journal, vous pourriez rencontrer des problèmes d'analyse. Utilisez ces exemples XML pour résoudre les problèmes d'analyse spécifiques.

Conversion de protocole

L'exemple suivant illustre une conversion de protocole typique qui recherche TCP, UDP, ICMP, ou GRE partout dans le contenu. Le modèle de recherche est entouré par toute limite de mot, par exemple, onglet, espace, fin de ligne. De même, la casse est ignorée :

```
<pattern id="Protocol" case-insensitive="true" xmlns="">
<![CDATA[\b(TCP|UDP|ICMP|GRE)\b]>
</pattern>
<matcher field="Protocol" order="1" pattern-id="Protocol" capture-group="1" />
```

Effectuer une substitution unique

L'exemple suivant montre une substitution qui analyse l'adresse IP source, puis annule le résultat et définit l'adresse IP à 100.100.100.100, en ignorant l'adresse IP dans le contenu.

Cet exemple suppose que l'adresse IP source correspond à quelque chose de semblable à SrcAddress=10.3.111.33 suivi d'une virgule :

```
<pattern id="SourceIp_AuthenOK" xmlns="">
<![CDATA[SrcAddress=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}),]>
</pattern>

<matcher field="SourceIp" order="1" pattern-id="SourceIp_AuthenOK"
capture-group="100.100.100.100" enable-substitutions="true"/>
```

Génération d'une adresse MAC séparée par deux points

QRadar détecte les adresses MAC au format séparé par des virgules. Parce que tous les périphériques risquent de ne pas utiliser ce format, l'exemple suivant montre comment corriger cette situation :

```
<pattern id="SourceMACWithDashes" xmlns="">
<![CDATA[SourceMAC=([0-9a-fA-F]{2})-([0-9a-fA-F]{2})-([0-9a-fA-F]{2})-
([0-9a-fA-F]{2})-([0-9a-fA-F]{2})-([0-9a-fA-F]{2})]>
</pattern>
<matcher field="SourceMAC" order="1" pattern-id="
SourceMACWithDashes" capture-group="\1:\2:\3:\4:\5:\6" />
```


Dans l'exemple précédent, SourceMAC=12-34-56-78-90-AB est converti en adresse MAC 12:34:56:78:90:AB.

Si les tirets sont supprimés du motif, le motif convertit une adresse MAC et n'a pas de séparateurs. Si des espaces sont insérés, le motif convertit une adresse MAC séparée par des espaces.

Combinaison d'adresse IP et de port

Typiquement une adresse IP et le port sont combinés en un seul champ, qui est séparé par une virgule.

L'exemple suivant utilise plusieurs groupes de capture avec un motif :

```
pattern id="SourceIPColonPort" xmlns="">
<! [CDATA[Source=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}):([\d]{1,5})]]>
</pattern>

<matcher field="SourceIp" order="1" pattern-id="SourceIPColonPort" capture-group="1" />
<matcher field="SourcePort" order="1" pattern-id="SourceIPColonPort" capture-group="2" />
```

Modification d'une catégorie d'événement

Une catégorie d'événement de périphérique peut être codée en dur, ou la gravité peut être ajustée.

L'exemple suivant ajuste la gravité pour un seul type d'événement :

```
<event-match-single event-name="TheEvent" device-event-category="Actual
Category" severity="6" send-identity="UseDSMResults" />
```

Suppression des événements de changement d'identité

Un DSM peut inutilement envoyer des événements de changement d'identité.

Les exemples suivants montrent comment éviter que des événements de changement d'identité soient envoyés à partir d'un seul type d'événement et un groupe d'événements.

```
// Never send identity for the event with an EventName of Authen OK
<event-match-single event-name="Authen OK" device-event-category="ACS"
severity="6" send-identity="OverrideAndNeverSend" />

// Never send any identity for an event with an event name starting with 7,
followed by one to five other digits:
<pattern id="EventNameId" xmlns=""><![CDATA[(7\d{1,5})]]>
</pattern>

<event-match-multiple pattern-id="EventNameId" capture-group-index="1"
device-event-category="Cisco Firewall" severity="7"
send-identity="OverrideAndNeverSend"/>
```

Codage des journaux

Les formats de codage suivants sont pris en charge :

- US-ASCII
- UTF-8

Vous pouvez transférer les journaux au système dans un codage qui ne correspond pas aux formats US-ASCII ou UTF-8. Vous pouvez configurer un indicateur avancé pour assurer que l'entrée peut être recodée en UTF-8 à des fins d'analyse et de stockage.

Par exemple, si vous souhaitez vous assurer que les journaux de source arrivent en codage SHIFT-JIS (japonais ANSI/OEM), entrez le code suivant :

```
<device-extension source-encoding=SHIFT-JIS xmlns=event_parsing/device_extension>
```

Les journaux sont insérés au format UTF-8.

Formatage des dates d'événements et d'horodatages

Une extension de source de journal peut détecter plusieurs formats de date et d'horodatage différents sur les événements.

Etant donné que les fabricants de périphériques ne se conforment pas à un format d'horodatage standard, le paramètre optionnel ext-data est inclus dans l'extension de la source de journal pour permettre à DeviceTime d'être reformaté. L'exemple suivant montre comment un événement peut être reformaté pour corriger le formatage d'horodatage :

```
<device-extension>
<pattern id="EventName1">(logger):</pattern>
<pattern id="DeviceTime1">time=\[(\d{2})/\w{3}/\d{4}:\d{2}:\d{2}:\d{2})\]</pattern>
<pattern id="Username">(Tlsv1)</pattern>

<match-group order="1" description="Full Test">
  <matcher field="EventName" order="1" pattern-id="EventName1_Pattern" capture-group="1"/>
  <matcher field="DeviceTime" order="1" pattern-id="DeviceTime1_Pattern"
    capture-group="1" ext-data="dd/MMM/YYYY:hh:mm:ss"/>
  <matcher field="UserName" order="1" pattern-id="Username_Pattern" capture-group="1"/>
</match-group>
</device-extension>
```

Formats de journaux multiples dans une source de journal unique

Parfois, plusieurs formats de journaux sont inclus dans une source de journal unique.

```
May 20 17:15:50 kernel: DROP IN=vlan2 OUT= MAC= SRC=67.149.62.133
DST=239.255.255.250 PROTO=UDP SPT=1900 DPT=1900
May 20 17:16:26 dropbear[22331]: password auth succeeded for 'root' from 192.168.50.80:3364
May 20 17:16:28 dropbear[22331]: exit after auth (root): Exited normally <br>
May 20 17:16:14 dropbear[22331]: bad password attempt for 'root' from 192.168.50.80:3364
```

Par exemple, il existe deux formats de journal : l'un pour les événements de pare-feu, et un pour les événements d'authentification. Vous devez écrire plusieurs motifs pour analyser les événements. Vous pouvez spécifier l'ordre d'analyse. Typiquement, les événements les plus fréquents sont analysés en premier, suivis des événements les moins fréquents. Vous pouvez avoir autant de motifs que nécessaire pour analyser tous les événements. La variable de commande détermine dans quel ordre les motifs sont appariés.

L'exemple suivant montre de multiples formats pour les champs suivants EventName et UserName

Des motifs distincts sont écrits pour analyser chaque type de journal unique. Les deux motifs sont référencés lorsque vous affectez la valeur aux champs normalisés.

```
<pattern id="EventName-DDWRT-FW_Pattern" xmlns=""><![CDATA[kernel\:(.*)\s]]></pattern>
<pattern id="EventName-DDWRT-Auth_Pattern" xmlns=""><![CDATA[sdropbear\[\d{1,5}\]:\s(.*)\s]]>
</pattern>
```

```

<pattern id="UserName_DDWRt-Auth1_Pattern" xmlns=""><![CDATA[\\sfor\\s\\'(.*)\\'s]]></pattern>
<pattern id="UserName_DDWRt-Auth2_Pattern" xmlns=""><![CDATA[\\safter\\sauth\\s\\((.*)\\):]]></pattern>

<match-group order="1" description="DD-WRT Device Extensions xmlns="">
  <matcher field="EventName" order="1" pattern-id="EventName-DDWRt-FW_Pattern" capture-group="1"/>
  <matcher field="EventName" order="2" pattern-id="EventName-DDWRt-Auth_Pattern" capture-group="1"/>

  <matcher field="UserName" order="1" pattern-id="UserName-DDWRt-Auth1_Pattern" capture-group="1"/>
  <matcher field="UserName" order="2" pattern-id="UserName-DDWRt-Auth2_Pattern" capture-group="1"/>

```

Analyse d'un format de journal CSV

Un fichier journal au format CSV peut utiliser un seul analyseur qui possède plusieurs groupes de capture. Il n'est pas toujours nécessaire de créer plusieurs ID de motif lorsque vous analysez ce type de journal.

Pourquoi et quand exécuter cette tâche

L'échantillon de journal suivant est utilisé :

```

Event,User,Source IP,Source Port,Destination IP,Destination Port
Failed Login,bjones,192.168.50.100,1024,10.100.24.25,22
Successful Login,nlabadie,192.168.64.76,1743,10.100.24.25,110
Privilege Escalation,bjones,192.168.50.100,1028,10.100.1.100,23

```

Procédure

1. Créez un analyseur qui correspond à toutes les valeurs pertinentes en utilisant les motifs précédents.

```

.*?\\,.*?\\,\\d{1,3}\\.\\d{1,3}\\.\\d{1,3}\\.\\d{1,3}
\\,\\d{1,5}\\,\\d{1,3}\\.\\d{1,3} \\,\\d{1,3}\\.\\d{1,3}\\,\\d{1,5}

```

2. Placez les groupes de capture autour de chaque valeur :

```

(.*?)\\,(.*?)\\,(\\d{1,3}\\.\\d{1,3}\\.\\d{1,3}\\.
\\d{1,3})\\,(\\d{1,5})\\,(\\d{1,3} \\,\\d{1,3}\\.\\d{1,3}\\.\\d{1,3})\\,(\\d{1,5})

```

3. Mappez le champ auquel chaque groupe de capture est mappé, en incrémentant la valeur lorsque vous vous déplacez.

```

1 = Event, 2 = User, 3 = Source IP,
4 = Source Port, 5 = Destination IP, 6 = Destination Port

```

4. Incluez les valeurs dans l'extension de source de journal en mappant le groupe de capture à l'événement pertinent.

Le code suivant montre un exemple partiel de mappage du groupe de capture à l'événement pertinent.

```

<pattern id="CSV-Parser_Pattern" xmlns=""><![CDATA[9.*?\\,(.*?)\\,(\\d{1,3}\\.\\d{1,3}\\.\\d{1,3})]]></pattern>
<match-group order="1" description="Log Source Extension xmlns="">
  <matcher field="EventName" order="1" pattern-id="CSV-Parser_Pattern" capture-group="1"/>
  <matcher field="SourceIP" order="1" pattern-id="CSV-Parser_Pattern" capture-group="3"/>
  <matcher field="SourcePort" order="1" pattern-id="CSV-Parser_Pattern" capture-group="4"/>
  <matcher field="DestinationIP" order="1" pattern-id="CSV-Parser_Pattern" capture-group="5"/>
  <matcher field="DestinationPort" order="1" pattern-id="CSV-Parser_Pattern" capture-group="6"/>
  <matcher field="UserName" order="1" pattern-id="CSV-Parser_Pattern" capture-group="2"/>

```

5. Téléchargez l'extension de source de journal.
6. Mappez les événements.

Tâches associées:

«Mappage d'événements inconnus», à la page 46

Initialement, tous les événements du DSM universel apparaissent comme inconnus dans l'onglet **Activité du journal** dans QRadar. Vous devez mapper manuellement tous les événements inconnus à leurs équivalents dans la mappe QID.

ID de type de source de journal

IBM Security QRadar prend en charge un certain nombre de sources de journal et chaque source de journal a un identifiant. Utilisez les ID de type de source de journal dans une instruction match-group :

Le tableau suivant indique le type de source de journal pris en charge et leurs identifiants.

Tableau 40. ID de type de source de journal

ID	Type de la source de journal
2	ID Open Source Snort
3	Point de contrôle pare-feu-1
4	Filtre de pare-feu configurable
5	Pare-feu et VPN de réseaux Juniper
6	Pare-feu PIX Cisco
7	Filtre de messages d'authentification configurable
9	IPS de réseau Enterasys Dragon
10	Serveur HTTP Apache
11	Système d'exploitation Linux
12	Journal d'événements de sécurité Microsoft Windows
13	IIS Windows
14	Pare-feu iptables de Linux
15	IBM Proventia Network Intrusion Prevention System (IPS)
17	Juniper Networks Intrusion Detection and Prevention (IDP)
19	TippingPoint Intrusion Prevention System (IPS)
20	Cisco IOS
21	Commutateur VPN Nortel Contivity
22	Routeur Multiprotocoles Nortel
23	Cisco VPN 3000 Series Cntrator
24	Messages d'authentification du système d'exploitation Solaris
25	Dispositif McAfee IntruShield Network IPS
26	Cisco CSA
28	Commutateur Enterasys Matrix E1
29	Journaux Sendmail du système d'exploitation Solaris
30	Intrusion Prevention System (IDS) Cisco
31	Firewall Services Module (FWSM) Cisco
33	IBM Proventia Management SiteProtector
35	Cyberguard FW/VPN KS Family

Tableau 40. ID de type de source de journal (suite)

ID	Type de la source de journal
36	Juniper Networks Secure Access (SA) SSL VPN
37	Commutateur VPN Nortel Contivity
38	Top Layer Intrusion Prevention System (IPS)
39	Universal DSM
40	Tripwire Enterprise
41	Dispositif Cisco Adaptive Security (ASA)
42	Niksun 2005 v3.5
45	Juniper Networks Network and Security Manager (NSM)
46	Squid Web Proxy
47	Système de prévention d'intrusions (IPS) Ambiron TrustWave ipAngel
48	Oracle RDBMS Audit Records
49	F5 Networks BIG-IP LTM
50	Journaux DHCP du système d'exploitation Solaris
55	Array Networks SSL VPN Access Gateway
56	Cisco CatOS for Catalyst Switches
57	Serveur ProFTPD
58	Linux DHCP Server
59	Contrôleur Infranet Juniper Networks
64	Plateforme Juniper JunOS
68	Commutateur Enterasys Matrix K/N/S
70	Système d'exploitation Extreme Networks ExtremeWare
71	Dispositif de sécurité Sidewinder G2
73	Passerelle de sécurité Fortinet FortiGate
78	Périphérique SonicWall UTM/Firewall/VPN
79	Vericept Content 360
82	Dispositif Symantec Gateway Security (SGS)
83	Juniper Steel Belted Radius
85	Serveur AIX IBM
86	MetaInfo MetaIP
87	SymantecSystemCenter
90	Cisco ACS
92	Forescout CounterACT
93	McAfee ePolicy Orchestrator
95	Dispositif CiscoNAC
96	Dispositifs TippingPoint X Series
97	Microsoft DHCP Server

Tableau 40. ID de type de source de journal (suite)

ID	Type de la source de journal
98	Microsoft IAS Server
99	Microsoft Exchange Server
100	Trend Interscan VirusWall
101	Microsoft SQL Server
102	MAC OS X
103	Dispositif Bluecoat SG
104	Nortel Switched Firewall 6000
106	Commutateur 3Com 8800 Series
107	Passerelle VPN Nortel
108	Détecteur d'intrusions Threat Protection System (TPS) Nortel
110	Commutateur Nortel Application
111	Plateforme Juniper DX Application Acceleration
112	SNARE Reflector Server
113	Routeurs Cisco série 12000
114	Commutateurs Cisco série 6500
115	Routeurs Cisco série 7600
116	Cisco Carrier Routing System
117	Routeur de services intégré Cisco
118	Juniper M-Series Multiservice Edge Routing
120	Nortel Switched Firewall 5100
122	Routeur Juniper MX-Series Ethernet Services
123	Plateforme Juniper T-Series Core
134	Nortel Ethernet Routing Switch 8300/8600
135	Nortel Ethernet Routing Switch 2500/4500/5500
136	Nortel Secure Router
138	Système d'exploitation OpenBSD
139	Commutateur Juniper Ex-Series Ethernet
140	Sysmark Power Broker
141	Programme d'écoute de base de données Oracle
142	Samhain HIDS
143	Contrôleur de service Bridgewater Systems AAA
144	Paire nom-valeur
145	Nortel Secure Network Access Switch (SNAS)
146	Starent Networks Home Agent (HA)
148	IBM AS/400 iSeries
149	Foundry Fastiron

Tableau 40. ID de type de source de journal (suite)

ID	Type de la source de journal
150	Passerelle de services Juniper SRX
153	CRYPTOCARD CRYPTOSHIELD
154	Imperva Securesphere
155	Contrôleur Aruba Mobility
156	Enterasys NetsightASM
157	Enterasys HiGuard
158	Motorola SymbolAP
159	Enterasys HiPath
160	Symantec Endpoint Protection
161	IBM RACF
163	Gestionnaire d'authentification RSA
164	Redback ASE
165	Trend Micro Office Scan
166	Routeurs Enterasys XSR Security
167	Commutateurs empilables et autonomes Enterasys
168	Juniper Networks AVT
169	OS Services Qidmap
170	Enterasys A-Series
171	Enterasys B2-Series
172	Enterasys B3-Series
173	Enterasys C2-Series
174	Enterasys C3-Series
175	Enterasys D-Series
176	Enterasys G-Series
177	Enterasys I-Series
178	Trend Micro Control Manager
179	Cisco IronPort
180	Hewlett Packard UniX
182	Cisco Aironet
183	Cisco Wireless Services Module (WiSM)
185	ISC BIND
186	IBM Lotus Domino
187	HP Tandem
188	Sentriigo Hedgehog
189	Sybase ASE
191	Microsoft ISA
192	Juniper SRC
193	Radware DefensePro
194	Pare-feu ACE Cisco

Tableau 40. ID de type de source de journal (suite)

ID	Type de la source de journal
195	IBM DB2
196	Oracle Audit Vault
197	Sourcefire Defense Center
198	Websense V Series
199	Oracle RDBMS OS Audit Record
206	Palo Alto PA Series
208	HP ProCurve
209	Microsoft Operations Manager
210	EMC VMWare
211	IBM WebSphere Application Server
213	F5 Networks BIG-IP ASM
214	FireEye
215	Avertissement juste
216	IBM Informix
217	CA Top Secret
218	Enterasys NAC
219	System Center Operations Manager
220	Passerelle Web McAfee
221	CA Access Control Facility (ACF2)
222	Application McAfee / contrôle des changements
223	Lieberman Random Password Manager
224	Sophos Enterprise Console
225	NetApp Data ONTAP
226	Sophos PureMessage
227	Cyber-Ark Vault
228	Itron Smart Meter
230	Bit9 Parity
231	IBM IMS
232	F5 Networks FirePass
233	Citrix NetScaler
234	F5 Networks BIG-IP APM
235	Juniper Networks vGW
239	Oracle BEA WebLogic
240	Dispositif de sécurité Web Sophos
241	Passerelle de sécurité Sophos Astaro
243	Infoblox NIOS
244	Tropos Control
245	Novell eDirectory
249	IBM Guardium

Tableau 40. ID de type de source de journal (suite)

ID	Type de la source de journal
251	Stonesoft Management Center
252	SolarWinds Orion
254	Great Bay Beacon
255	Damballa Failsafe
258	CA SiteMinder
259	IBM z/OS
260	Microsoft SharePoint
261	iT-CUBE agileSI
263	Commutateur Digital China Networks séries DCS et DCRS
264	Collecteur de journal Juniper Security Binary
265	Trend Micro Deep Discovery
266	Tivoli Access Manager for e-business
268	Verdasys Digital Guardian
269	Hauwei S Series Switch
271	HBGary Active Defense
272	APC UPS
272	Contrôleur LAN sans fil Cisco
276	IBM Customer Information Control System (CICS)
278	Barracuda Spam & Virus Firewall
279	Open LDAP
280	Application Security DbProtect
281	Barracuda Web Application Firewall
283	Routeur Huawei AR Series
286	IBM AIX Audit
289	IBM Tivoli Endpoint Manager
290	Juniper Junos WebApp Secure
291	Nominum Vantio
292	Commutateur Enterasys 800-Series
293	IBM zSecure Alert
294	IBM Security Network Protection (XGS)
295	IBM Security Identity Manager
296	F5 Networks BIG-IP AFM
297	IBM Security Network IPS (GX)
298	Fidelis XPS
299	Arpeggio SIFT-IT
300	Barracuda Web Filter
302	Brocade FabricOS
303	Plateforme ThreatGRID Malware Threat Intelligence

Tableau 40. ID de type de source de journal (suite)

ID	Type de la source de journal
304	IBM Security Access Manager for Enterprise Single Sign-On
306	Venustech Venusense Unified Threat Management
307	Venustech Venusense Firewall
308	Venustech Venusense Network Intrusion Prevention System
309	ObserveIT
311	Pirean Access: One
312	Venustech Venusense Security Platform
313	PostFix MailTransferAgent
314	Oracle Fine Grained Auditing
315	VMware vCenter
316	Moteur de services d'identité Cisco
318	Moniteur d'intégrité des fichiers Honeycomb Lexicon
319	Oracle Acme Packet SBC
320	Juniper WirelessLAN
330	Arbor Networks Peakflow SP
331	Zscaler Nss
332	Proofpoint Enterprise Protection/Enterprise Privacy
338	Microsoft Hyper-V
339	Cilasoft QJRN/400
340	Vormetric Data Security
341	SafeNet DataSecure/KeySecure
343	STEALTHbits StealthINTERCEPT
344	Juniper DDoS Secure
345	Arbor Networks Pravail
346	Trusteer Apex
348	IBM Security Directory Server
349	Enterasys A4-Series
350	Enterasys B5-Series
351	Enterasys C5-Series
354	Passerelle VPN Avaya
356	DG Technology MEAS
358	CloudPassage Halo
359	CorreLog Agent for IBM zOS
360	WatchGuard Fireware OS
361	IBM Fiberlink MaaS360
362	Trend Micro Deep Discovery Analyzer

Tableau 40. ID de type de source de journal (suite)

ID	Type de la source de journal
363	AccessData InSight
364	BM Privileged Session Recorder
367	Universal CEF
369	FreeRADIUS
370	Riverbed SteelCentral NetProfiler
372	SSH CryptoAuditor
373	IBM WebSphere DataPower
374	Symantec Critical System Protection
375	Kisco Information Systems SafeNet/i
376	IBM Federated Directory Server
378	Lastline Enterprise
379	genua genugate
383	Oracle Enterprise Manager

Chapitre 3. Gestion des extensions de sources de journal

Vous pouvez créer des extensions de sources de journal pour étendre ou modifier les routines d'analyse de certains périphériques.

Une *extension de source journal* est un fichier XML incluant tous les modèles d'expressions régulières requis pour identifier et classer les événements de la charge d'événements. Les fichiers d'extension peuvent être utilisés pour analyser les événements lorsque vous devez corriger un problème d'analyse syntaxique ou lorsque vous devez redéfinir l'analyse syntaxique par défaut d'un événement à partir d'un DSM. Si aucun DSM n'existe pour analyser les événements d'un dispositif ou d'un périphérique de sécurité dans votre réseau, une extension peut assurer la prise en charge des événements. L'onglet **Activité du journal** identifie trois types d'événements de sources de journal :

- Sources de journal analysant correctement l'événement. Les événements analysés correctement sont affectés à la catégorie et au type de source de journal corrects. Dans ce cas, aucune intervention ou extension n'est requise.
- Les sources de journal analysent les événements, mais ont une valeur **Inconnu** dans le paramètre **Source de journal**. Les événements inconnus sont des événements de source de journal où le type de source de journal est identifié, mais l'information de contenu n'est pas comprise par le DSM. Le système ne peut pas reconnaître l'identificateur de l'événement à partir de l'information disponible pour classer correctement l'événement. Dans ce cas, l'événement peut être mappé vers une catégorie ou une extension de source de journal peut être écrite pour réparer l'analyse syntaxique des événements inconnus.
- Les sources de journal ne peuvent pas identifier le type de source de journal et ont une valeur d'événement **Stocké** dans le paramètre **Source de journal**. Pour analyser un événement correctement, vous devez mettre à jour vos fichiers DSM ou écrire une extension de source de journal. Une fois que l'événement s'analyse, vous pouvez mapper les événements.

Avant de pouvoir ajouter une extension de source de journal, vous devez créer le document d'extension. Le document d'extension est un document XML que vous pouvez créer avec n'importe quel éditeur ou outil de traitement de texte commun. Plusieurs documents d'extension peuvent être créés, téléchargés et associés à différents types de sources de journal. Le format du document d'extension doit être conforme à un document de schéma XML standard (XSD). Pour développer un document d'extension, vous devez maîtriser la codification XML et posséder une expérience correspondante.

Ajout d'une extension de source de journal

Vous pouvez ajouter une extension de source de journal pour étendre ou modifier les routines d'analyse de certains périphériques.

Procédure

1. Cliquez sur l'onglet **Admin**.
2. Cliquez sur l'icône **Extensions de la source de journal**.
3. Cliquez sur **Ajouter**.
4. Dans la liste **Types de source de journal**, sélectionnez l'une des options suivantes :

Option	Description
Disponible	Sélectionnez cette option lorsque le module de support de périphérique (DSM) analyse correctement la plupart des zones de la source de journal. Les valeurs de zone analysées de façon incorrecte sont améliorées avec les nouvelles valeurs XML.
Définir sur la valeur par défaut pour	Sélectionnez les sources de journal à ajouter ou supprimer de l'analyse d'extension. Vous pouvez ajouter des extensions à une source de journal, ou les supprimer de celles-ci. Si une extension de source de journal est définie sur la valeur par défaut d'une source de journal, toutes les nouvelles sources de journal appartenant au même type de source de journal utiliseront l'extension de source de journal affectée.

5. Cliquez sur **Parcourir** pour localiser votre document XML d'extension de source de journal.
6. Cliquez sur **Charger**. Le contenu de l'extension de source de journal s'affiche afin de vérifier que le fichier d'extension téléchargé est bien le fichier correct. Le fichier d'extension est évalué à l'aide du XSD afin de détecter toute erreur lors du téléchargement du fichier.
7. Cliquez sur **Sauvegarder**.

Résultats

Si le fichier d'extension ne contient aucune erreur, la nouvelle extension de source de journal est créée et activée. Il est possible de télécharger une extension de source de journal sans appliquer l'extension à une source de journal. Toute modification de l'état d'une extension est appliquée immédiatement et les hôtes gérés ou consoles imposent les nouveaux paramètres d'analyse d'événements dans l'extension de la source de journal.

Que faire ensuite

Dans l'onglet **Activité du journal**, vérifiez que les modèles d'analyse des événements sont appliqués correctement. Si la source de journal classe les événements comme **Stockés**, les modèles d'analyse de l'extension de source de journal ont besoin d'être réglés. Vous pouvez comparer avec le fichier d'extension au événements de source de journal afin de repérer d'éventuels problèmes d'analyse syntaxique d'événement.

Remarques

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

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

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

Pour le Canada, veuillez adresser votre courrier à :

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

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

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

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

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

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

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

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

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

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, 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 indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

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

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

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

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

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

Marques

IBM, le logo IBM et ibm.com sont des marques d'International Business Machines Corp. dans de nombreux pays. Les autres noms de produits et de 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.

UNIX est une marque enregistrée de The Open Group 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.

Remarques sur les règles de confidentialité

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

Selon les configurations déployées, cette Offre logicielle peut utiliser des cookies de session qui collectent chaque ID de session à des fins de gestion de la session et d'authentification. Ces cookies peuvent être désactivés, mais leur désactivation empêchera l'utilisation de la fonctionnalité qui leur est associée.

Si les configurations déployées pour cette Offre logicielle vous fournissent à vous en tant que client la possibilité de collecter des informations identifiant d'autres

personnes via des cookies et d'autres technologies, vous devez vous renseigner sur l'avis juridique et les lois applicables à ce type de collecte de données, notamment les exigences d'information et de consentement.

Pour plus d'informations sur l'utilisation de diverses technologies, notamment de cookies, à ces fins, reportez-vous aux Points principaux de la Déclaration IBM de confidentialité sur Internet (<http://www.ibm.com/privacy/fr/fr>) et à la section "Cookies, pixels espions et autres technologies" de la Déclaration IBM de confidentialité sur Internet sur le site <http://www.ibm.com/privacy/details/fr/fr>, ainsi qu'à la section "IBM Software Products and Software-as-a-Service Privacy Statement" sur le site <http://www.ibm.com/software/info/product-privacy> (en anglais).

Index

A

administrateur réseau vii
ajout en bloc 27

C

Cisco NSEL 4

D

documents d'extension
traitement des incidents 48

E

exemples XML 48
extension de source de journal
activer une extension 61
désactiver une extension 61
extensions de sources de journal 61

G

gérer 61

I

IBM Proventia® Management
SiteProtector® 7
introduction vii

O

ordre d'analyse syntaxique 27

P

présentation 1
protocole d'IBM Tivoli Endpoint
Manager 5
protocole de fichier journal 10
protocole EMC VMware 4
protocole Forwarded 4
protocole JDBC 5
protocole JDBC SiteProtector 7
protocole Juniper Networks NSM 9
protocole Juniper Security Binary Log
Collector 10
protocole Microsoft DHCP 12
protocole Microsoft Exchange 12
protocole Microsoft IIS 13
protocole Microsoft Security Event
Log 14
protocole OPSEC/LEA 16
protocole Oracle Database Listener 17
protocole PCAP Syslog Combination 17
protocole SDEE 17

protocole SMB Tail 18
protocole SNMPv2 19
protocole Sophos Enterprise Console
JDBC 20
protocole Syslog Redirect 23
protocole TCP Multiline Syslog 23
protocole TLS Syslog 24
protocole UDP Multiline Syslog 26
protocole vCloud Director 26

S

source de journal
état 1
sources de journal 1

