

Configurer l'application de sécurité cloud pour IBM QRadar

Table des matières

[Introduction](#)

[Aperçu](#)

[Exigences](#)

[Exigences Cisco Umbrella](#)

[Configuration requise pour IBM Security QRadar SIEM](#)

[Installation de l'application Cisco Cloud Security pour IBM QRadar](#)

[Configuration des applications de sécurité cloud Cisco : Ajout de la source du journal](#)

[Génération du jeton d'authentification](#)

[Configuration de l'application Cisco Cloud Security](#)

[Indexation dans QRadar](#)

Introduction

Ce document décrit comment configurer l'application Cisco Cloud Security avec IBM QRadar pour l'analyse des journaux.

Aperçu

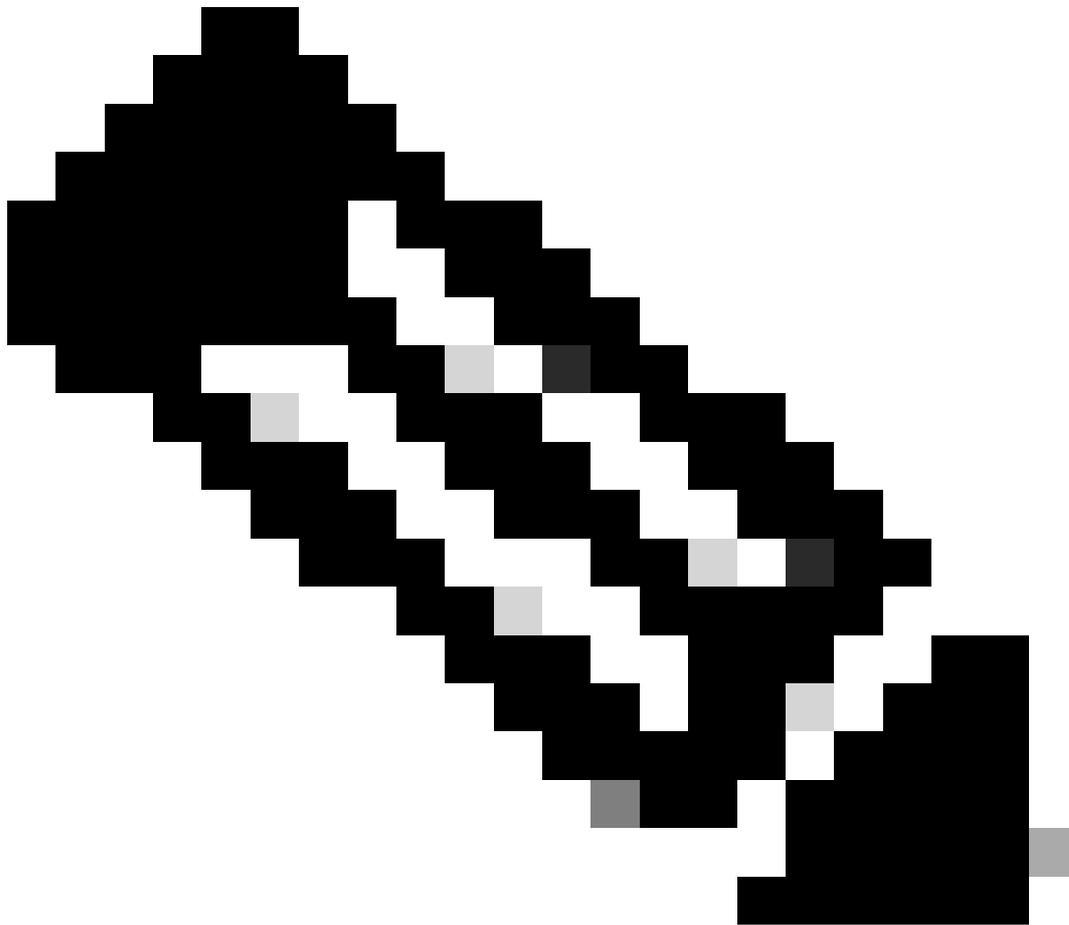
QRadar d'IBM est un SIEM populaire pour l'analyse des journaux. Il fournit une interface puissante pour analyser de grandes quantités de données, telles que les journaux fournis par Cisco Umbrella pour le trafic DNS de votre entreprise. L'application Cisco Cloud Security pour IBM QRadar fournit des informations sur plusieurs produits de sécurité (Investigate, Enforcement et CloudLock) et les intègre à QRadar. Il aide également l'utilisateur à automatiser la sécurité et à contenir les menaces plus rapidement et directement à partir de QRadar.

Lorsque vous configurez l'application Cisco Cloud Security pour QRadar, elle intègre toutes les données de la plate-forme Cisco Cloud Security et vous permet de visualiser les données sous forme graphique dans la console QRadar. À partir de l'application, les analystes peuvent :

- Étudier les domaines, les adresses IP et les adresses e-mail
- Bloquer et débloquer des domaines (application)
- Affichez les informations de tous les incidents du réseau.

Cet article décrit les procédures de base pour configurer et exécuter QRadar afin qu'il puisse extraire les journaux de votre bucket S3 et les consommer.

Exigences



Remarque : La prise en charge de QRadar doit provenir d'IBM, car Cisco n'est pas en mesure de prendre directement en charge le matériel ou les logiciels tiers. Pour tout problème de connexion de votre tableau de bord Umbrella à votre compartiment S3, nous pouvons vous fournir une assistance. La plupart des informations disponibles ici se trouvent également sur le site Web d'IBM :

[https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/c_dsm_guide_microsoft_Cisco Umb](https://www.ibm.com/support/knowledgecenter/SS42VS_DSM/c_dsm_guide_microsoft_Cisco_Umbrella.html)

Exigences Cisco Umbrella

Ce document suppose que votre godet Amazon AWS S3 a été configuré dans Umbrella (Paramètres > Gestion des journaux) et s'affiche en vert avec les journaux récents ayant été téléchargés.

Pour plus d'informations sur la façon de configurer cette fonctionnalité, lisez ici : [Gérer vos](#)

[journaux](#).

Configuration requise pour IBM Security QRadar SIEM

L'administrateur doit disposer de droits d'administration sur le ou les appareils QRadar, la configuration d'Amazon S3 et le tableau de bord Umbrella. Ces instructions supposent que l'administrateur QRadar est familiarisé avec la création de fichiers LSX (Log source Extension).

Sachez que l'application Cisco Cloud Security App v1.0.3 fonctionne uniquement jusqu'à IBM QRadar 7.2.8. La nouvelle version, v1.0.6, fonctionne avec la version actuelle de QRadar 7.4.2 et ultérieure.

Installation de l'application Cisco Cloud Security pour IBM QRadar

1. Téléchargez et installez l'application de sécurité cloud Cisco pour IBM QRadar, disponible ici : [Cisco Cloud Security App v1.0.3](#) (pour IBM QRadar v7.2.8) ou [Cisco Cloud Security App v1.0.6](#) (pour IBM QRadar v7.4.8).
2. Après l'installation, déployez les modifications dans QRadar.

Configuration des applications de sécurité cloud Cisco : Ajout de la source du journal



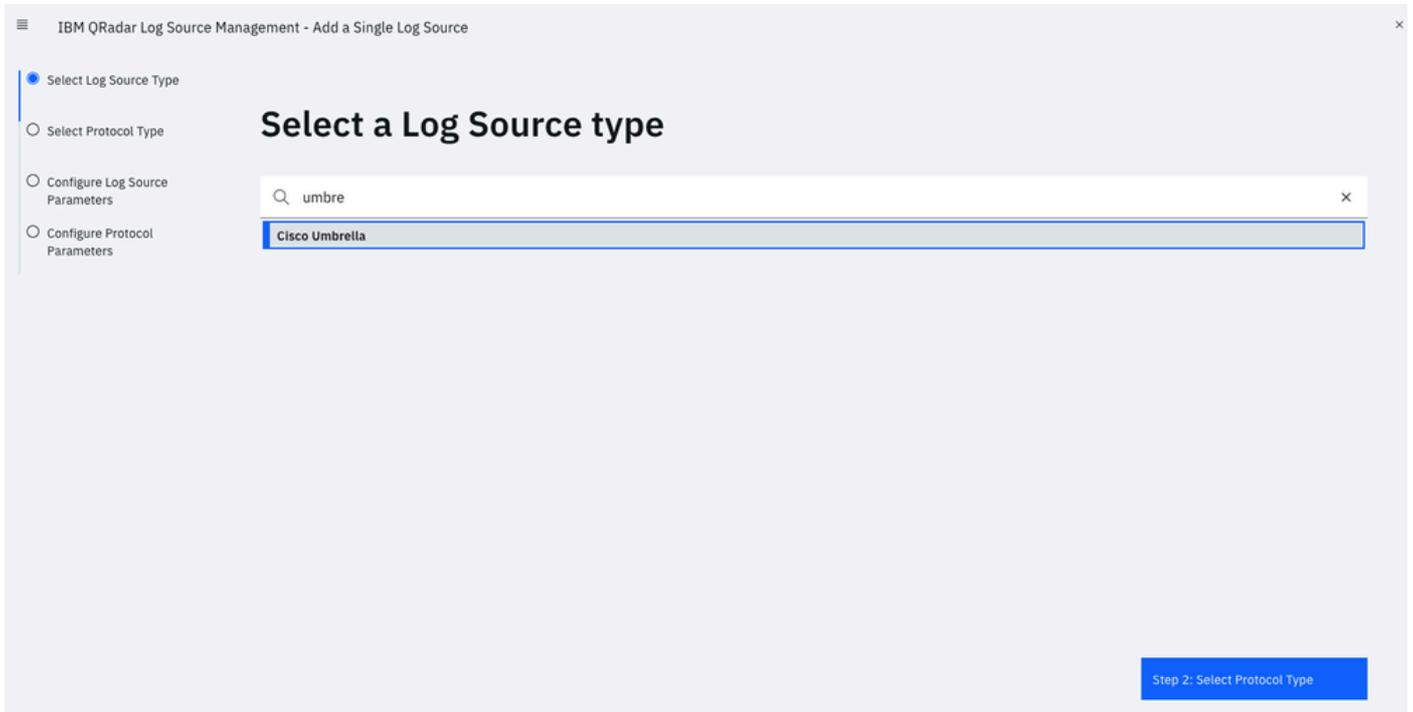
Remarque : Vous pouvez voir d'autres journaux dans S3, tels que Audit et Firewall, mais ils ne sont pas pris en charge. Configurez uniquement les trois éléments répertoriés ici. Toute tentative de configuration de ces autres journaux entraîne un échec.

Pour ajouter une source de journal, cliquez sur l'onglet Admin sur la barre de navigation QRadar, faites défiler vers le bas et cliquez sur QRadar Log Source Management, puis cliquez sur le bouton +New Log Source:

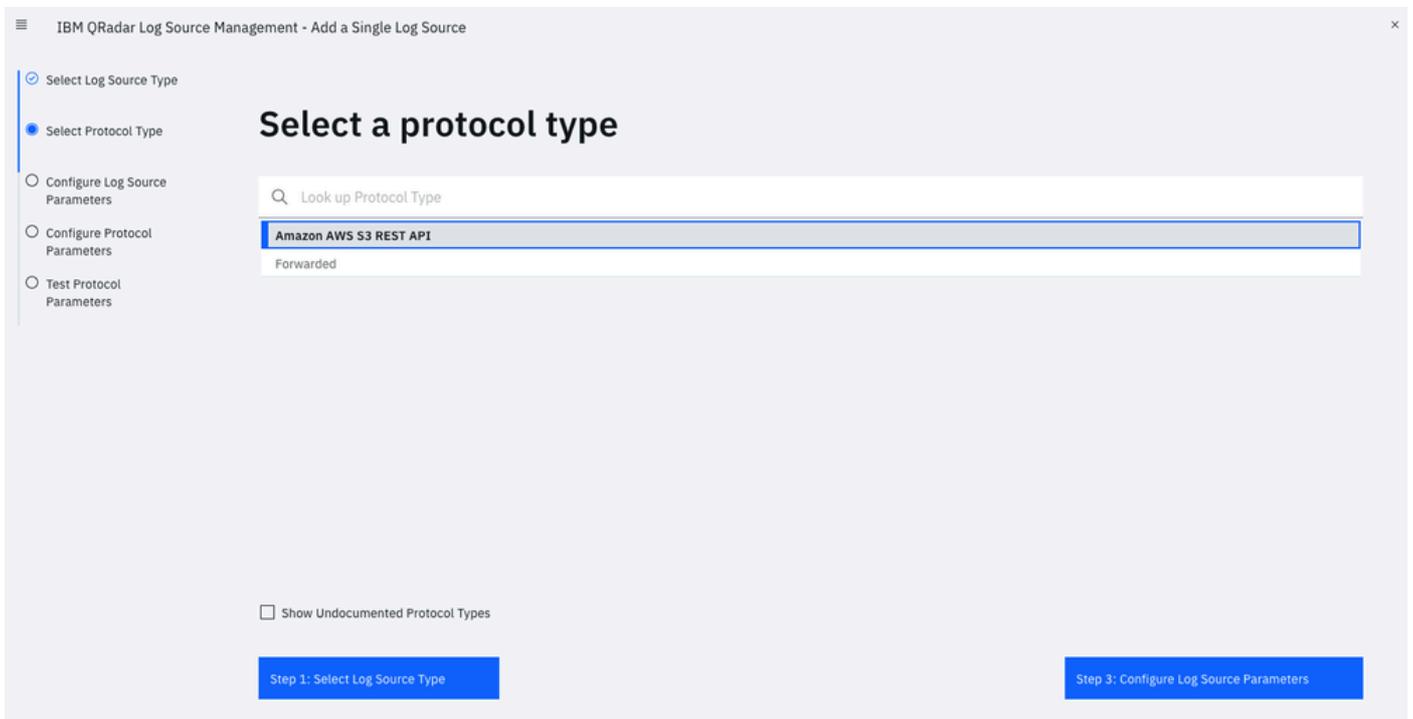
- Nom de la source du journal (les noms d'entrée doivent correspondre exactement à ceux répertoriés) :
 - Journaux DNS Cisco : `cisco_umbrella_dns_logs`
 - Journaux IP Cisco Umbrella : `cisco_umbrella_ip_logs`
 - Journaux de proxy Cisco Umbrella : `cisco_umbrella_proxy_logs`
- Format d'événement : Cisco Umbrella CSV
- Type de source du journal : Cisco Umbrella
- Configuration du protocole : API REST Amazon AWS S3
- Modèle de fichier : `.*?\.\csv\.\gz`

- Extension de la source du journal : CiscoUmbrella_ext **
- Sélectionnez les groupes dont vous souhaitez que cette source de journal soit membre : cisco_umbrella_logsource_group

Accédez à l'Assistant Ajout d'une source de journal unique :



4404306773524



4404306773268

IBM QRadar Log Source Management - Add a Single Log Source

Select Log Source Type

Select Protocol Type

Configure Log Source Parameters

Configure Protocol Parameters

Test Protocol Parameters

Configure the Log Source parameters

Name *
The name of the log source.

cisco_umbrella_dns_logs

Description
An optional description of the log source.

Enabled
Indicates whether the log source should be enabled.

On

Groups *
The groups that this log source will belong to.

cisco_umbrella_logsource_group

+ Add Group

Extension
Log Source Extensions perform post-processing of events after default parsing has occurred.

+ Show More

CiscoUmbrella_ext

Step 2: Select Protocol Type

Step 4: Configure Protocol Parameters

4404313505300

Configure the protocol parameters

[AWS Authentication Configuration]

Log Source Identifier *

cisco_umbrella_dns_logs

Authentication Method *
- Access Key ID / Secret Key: Standard Access Key authentication

+ Show More

Access Key ID / Secret Key

Access Key ID *
The Access Key ID that is required to access the AWS S3 bucket.

XXXXXXXXXXXXXXXXXXXXXXXXXXXX

Secret Key *
The Secret Key that is required to access the AWS S3 bucket.

.....

[AWS S3 Collection Configuration]

S3 Collection Method *

Use a Specific Profile - Single Account/Region Only

Step 3: Configure Log Source Parameters

Step 5: Test Protocol Parameters

4404306774164

IBM QRadar Log Source Management - Add a Single Log Source

- Select Log Source Type
- Select Protocol Type
- Configure Log Source Parameters
- Configure Protocol Parameters**
- Test Protocol Parameters

Configure the protocol parameters

^ [AWS S3 Collection Configuration]

S3 Collection Method *
Choose how to collect the data.
[+ Show More](#)

Use a Specific Prefix - Single Account/Region Only

Bucket Name *
The name of the AWS S3 bucket where the log files are stored.

cisco-managed-eu-west-2

Directory Prefix *
The root directory location on the AWS S3 bucket from which the files are retrieved.
[+ Show More](#)

:3_51f2a158aad51ec7a68449a10400ba027acc00c3/dnslogs/

Region Name *
The Region the SQS Queue or S3 Bucket is in. Example: us-east-1, eu-west-1, ap-northeast-3

eu-west-2

Event Format *
Choose the format of the events that are contained in the files.
[+ Show More](#)

Cisco Umbrella CSV

Step 3: Configure Log Source Parameters

Step 5: Test Protocol Parameters

4404306897556

Test Protocol Parameters



[Restart](#)

Results (4):

- Testing DNS resolution of [s3.amazonaws.com]
- Testing TCP connection to [s3.amazonaws.com:443]
- Testing SSL connection to [s3.amazonaws.com:443]
- Testing access to S3 Bucket [cisco-managed-eu-west-2]

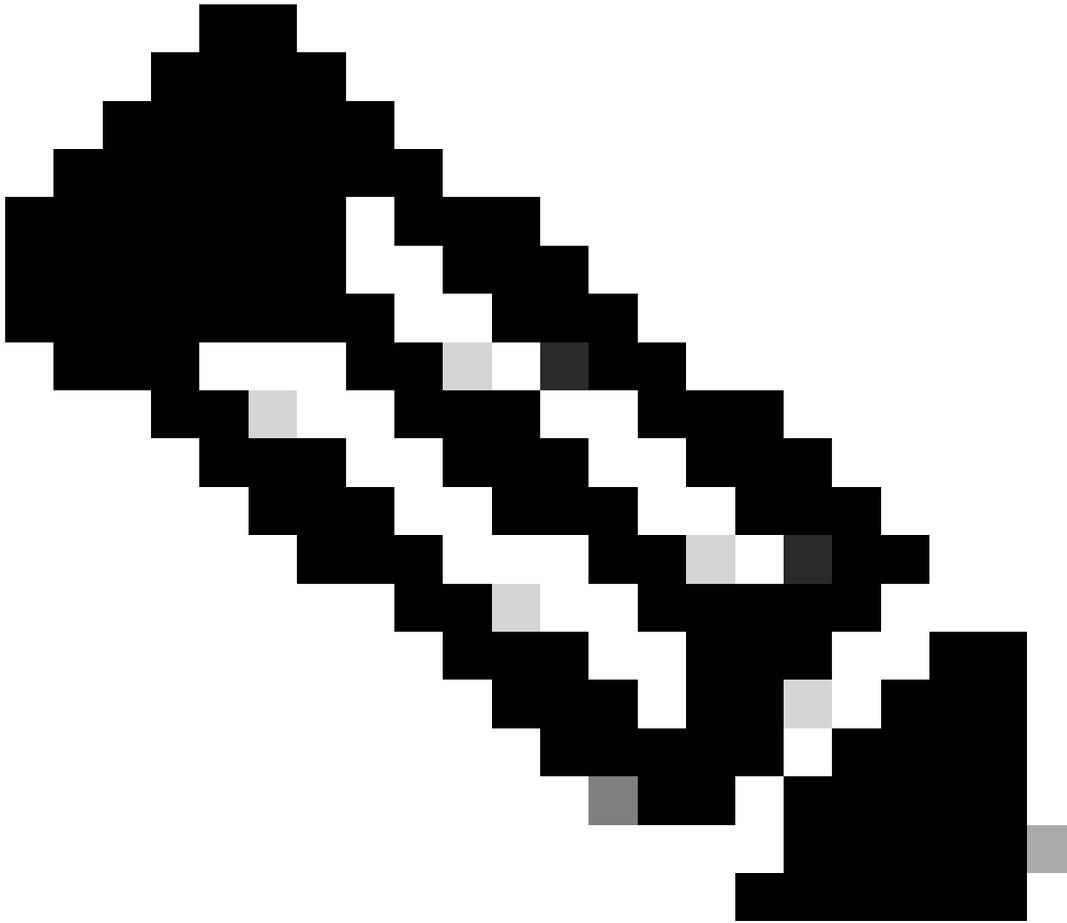
Events (5):

Log Source Identifier	Payload
cisco_umbrella_dns_logs	{"sourceFile": "[REDACTED]68449a10400ba027acc00c3-dns logs-2021-06-26-2021-06-26-23-50-44ea.csv.gz"}
cisco_umbrella_dns_logs	{"sourceFile": "[REDACTED]68449a10400ba027acc00c3-dns logs-2021-06-26-2021-06-26-23-50-a6fd.csv.gz"}
cisco_umbrella_dns_logs	{"sourceFile": "[REDACTED]68449a10400ba027acc00c3-dns logs-2021-06-26-2021-06-26-23-50-cb6f.csv.gz"}

Step 4: Configure Protocol Parameters

Finish

4404306881812



Remarque : Si l'extension de la source du journal n'est pas mappée à « CiscoUmbrella_ext », sélectionnez le nom de la source du journal dans la liste :

The screenshot shows a web browser window titled "Log Source Extensions - Google Chrome". The address bar shows a URL starting with "Not secure" and "/core/genericsearchlist?appName=eventviewer&pageld=DeviceExtensionList". Below the browser window is a table with the following columns: Extension Name, Description, Enabled, and Default for Log Source Types. The table contains three rows, with the last row clearly visible as "CiscoUmbrella_ext" with "true" in the Enabled column and "Cisco Umbrella" in the Default for Log Source Types column.

Extension Name	Description	Enabled	Default for Log Source Types
[Redacted]	[Redacted]	true	[Redacted]
[Redacted]	[Redacted]	true	[Redacted]
CiscoUmbrella_ext	[Redacted]	true	Cisco Umbrella

360071157752

Edit a Log Source Extension
?

Name

Description

Log Source Types

Available

3Com 8800 Series Switch

APC UPS

AhnLab Policy Center APC

Akamai KONA

Amazon AWS CloudTrail

Amazon AWS Security Hub

Amazon GuardDuty

Ambiron TrustWave ipAngel Intrusion Prevention Sy:

Apache HTTP Server

Application Security DbProtect

→
←

Set to default for

Cisco Umbrella

Upload Extension: No file chosen

Extension Document

```

<ns2:device-extension xmlns:ns2="event_parsing/device_extension">
<pattern id="UserName-Pattern-1">"MostGranularIdentity": "(.*)", </pattern>
<pattern id="EventName-Pattern-1">(.*)</pattern>
<match-group device-type-id-override="431" order="1">
<matcher order="1" enable-substitutions="true" capture-group="1" pattern-id="UserName-Pattern-1" field="UserName" />
<matcher order="1" capture-group="1" pattern-id="EventName-Pattern-1" field="EventName" />
<event-match-multiple force-qidmap-lookup-on-fixup="false" send-identity="UseDSMResults" pattern-id="EventName-Pattern-1" />
</match-group>
</ns2:device-extension>

```

360071326791

Voici un exemple de ce à quoi ressemble un compartiment géré Cisco :

```

Bucket name: cisco-managed-us-west-1
ACCESS_KEY_ID: xxxxxxxxxxxxxxxx
SECRET_ACCESS_KEY: xxxxxxxxxxxxxxxx
Region: us-west-1
Your Directory Prefix is the key part of this. This is the customers folder,
followed by the appropriate log folder.
For example: xxxxxxx_cfa37bd906xxxxxx3aff94e205db7bxxxxxx/dnslogs

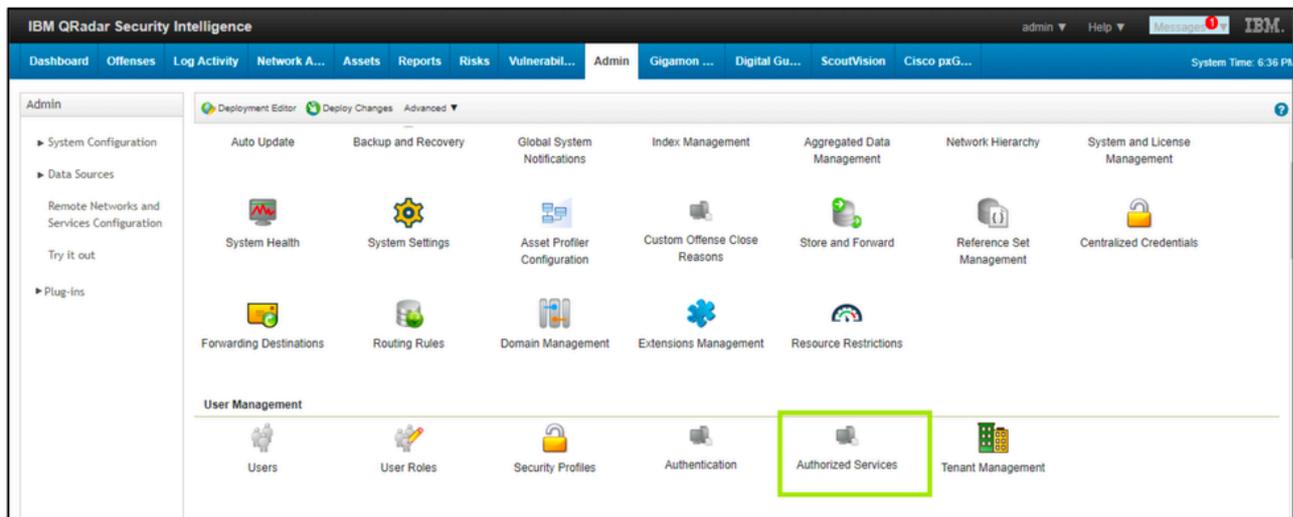
```

Revenez aux paramètres de l'application de sécurité cloud Cisco et définissez la fréquence d'actualisation du panneau en heures à une valeur minimale de « 1 » afin que les graphiques affichent les données.

Génération du jeton d'authentification

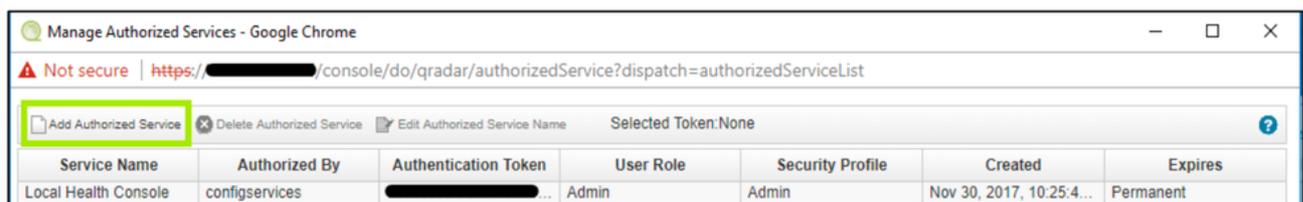
L'administrateur doit générer un jeton de service à ajouter à votre application de sécurité Cisco. Conformément aux meilleures pratiques, a recréé le jeton de service autorisé tous les 90 jours :

1. Connectez-vous à QRadar > Onglet Admin > Authorized Services.



360071965571

2. Ajouter des services autorisés.

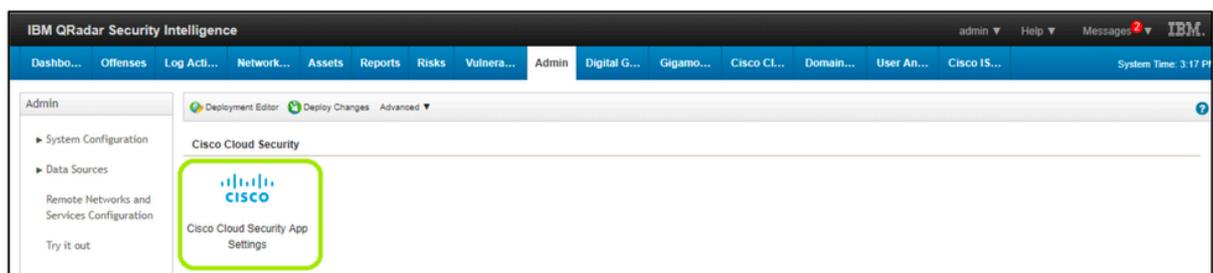


360071965551

3. Entrez les détails et générez le jeton d'authentification.
4. Après avoir généré le jeton, cliquez sur « Déployer les modifications ».

Configuration de l'application Cisco Cloud Security

1. Dans l'onglet Admin sur la barre de navigation QRadar, faites défiler vers le bas et ouvrez Paramètres de l'application de sécurité du cloud Cisco.



360071754732

2. Saisissez le jeton d'authentification généré à l'étape précédente.

Qradar Settings

QRadar Server IP

QRadar Server port

QRadar service token

360072462992

3. Modifiez les paramètres Api comme suit :

- URL de base Cisco Investigate : <https://investigate.api.umbrella.com/>
- Jeton API Cisco Investigate : générer via le tableau de bord Umbrella -> Examiner -> Clés API -> Créer un nouveau jeton ; pour plus d'informations, consultez la page <https://docs.umbrella.com/deployment-umbrella/docs/create-investigate-api-key>
- URL de base d'application Cisco : <https://s-platform.api.opendns.com/1.0/>
- Cisco Enforce CustomerKey : générer via le tableau de bord Umbrella -> Composants de stratégie -> Intégrations -> Ajouter ; pour plus d'informations, consultez la page <https://docs.umbrella.com/umbrella-user-guide/docs/set-up-custom-integrations>
- URL de base Cisco Cloudlock : `https://{YourCloudlockAPIServer}/api/v2` (par exemple, <https://api-demo.cloudlock.com/api/v2/>. Veuillez confirmer votre URL de base Cloudlock ou URL d'API Cloudlock Enterprise en envoyant un e-mail à support@cloudlock.com.)
- Jeton API Cisco Cloudlock : générer via Cloudlock -> Paramètres -> Authentification et API -> Générer ; pour plus d'informations, consultez la page <https://developer.cisco.com/docs/cloud-security/cloudlock-api-getting-started/#authentication>

Api Settings

Show Cisco Cloudlock incident details to end user Yes No

Show Cisco Cloudlock UEBA Panels Yes No

Cisco Investigate Base URL

Cisco Investigate API token

Cisco Enforce Base URL

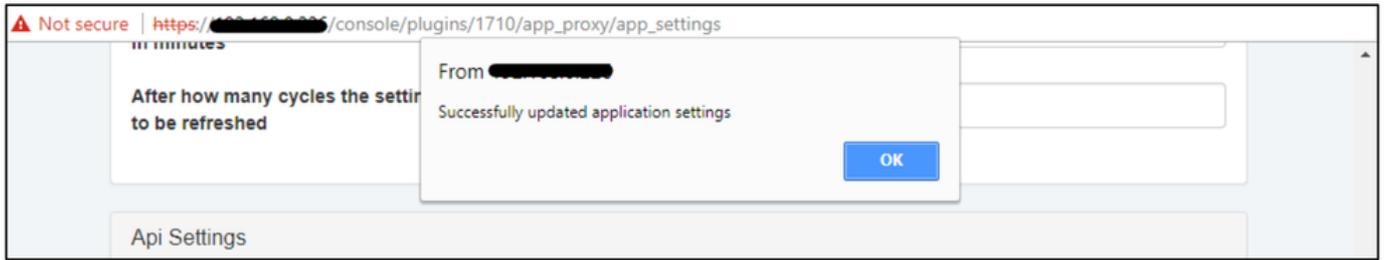
Cisco Enforce CustomerKey

Cisco Cloudlock Base URL

Cisco Cloudlock API token

360072703611

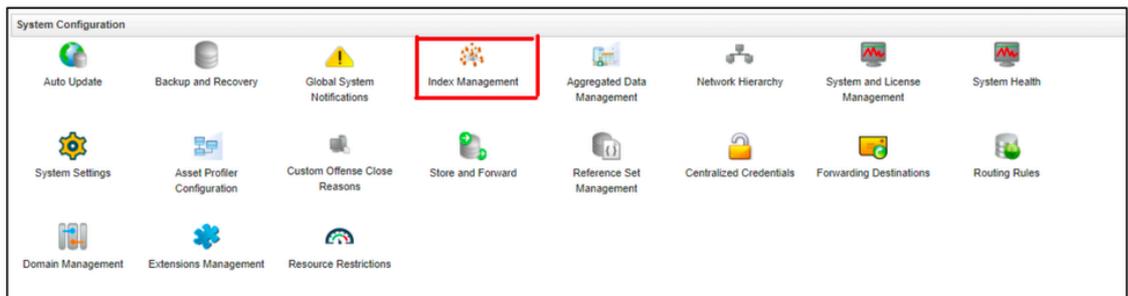
Une fenêtre contextuelle indique que les paramètres de l'application ont été correctement mis à jour.



360071986151

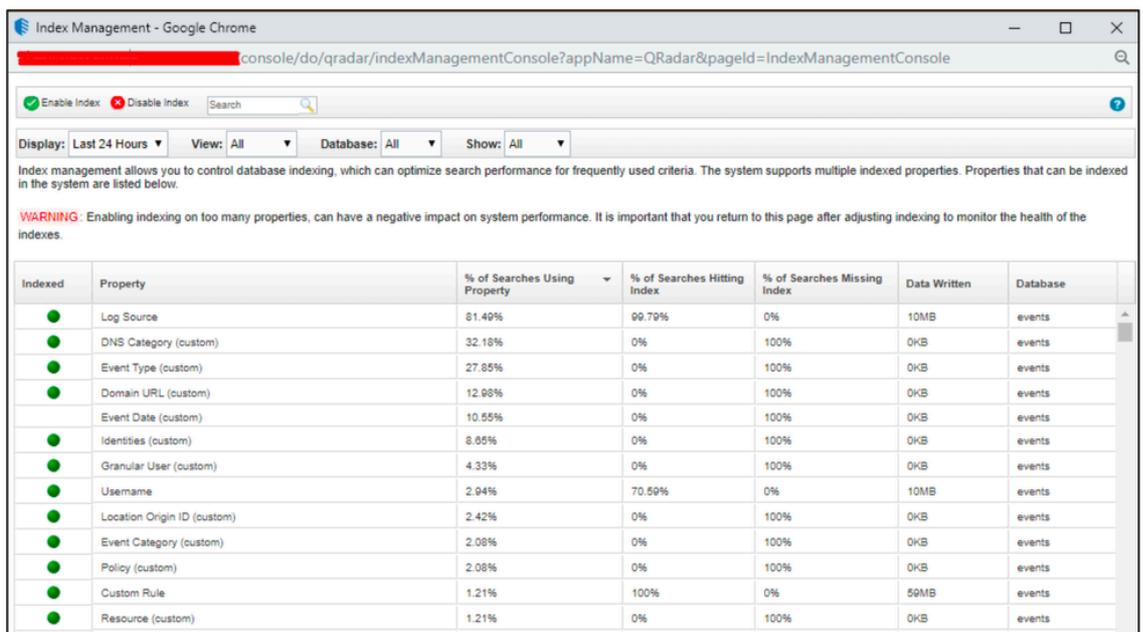
Indexation dans QRadar

1. Accédez à l'onglet Admin, puis cliquez sur Index Management.



360071780112

2. Indexer les CEP emballés avec l'application.



Index management allows you to control database indexing, which can optimize search performance for frequently used criteria. The system supports multiple indexed properties. Properties that can be indexed in the system are listed below.

WARNING: Enabling indexing on too many properties, can have a negative impact on system performance. It is important that you return to this page after adjusting indexing to monitor the health of the indexes.

Indexed	Property	% of Searches Using Property	% of Searches Hitting Index	% of Searches Missing Index	Data Written	Database
●	Log Source	81.49%	99.79%	0%	10MB	events
●	DNS Category (custom)	32.18%	0%	100%	0KB	events
●	Event Type (custom)	27.85%	0%	100%	0KB	events
●	Domain URL (custom)	12.98%	0%	100%	0KB	events
●	Event Date (custom)	10.55%	0%	100%	0KB	events
●	Identities (custom)	8.85%	0%	100%	0KB	events
●	Granular User (custom)	4.33%	0%	100%	0KB	events
●	Username	2.94%	70.59%	0%	10MB	events
●	Location Origin ID (custom)	2.42%	0%	100%	0KB	events
●	Event Category (custom)	2.08%	0%	100%	0KB	events
●	Policy (custom)	2.08%	0%	100%	0KB	events
●	Custom Rule	1.21%	100%	0%	59MB	events
●	Resource (custom)	1.21%	0%	100%	0KB	events

360071988811

Voici les CEP recommandés à indexer :

1. Source du journal
2. Catégorie DNS
3. Type d'événement
4. URL du domaine
5. Identités
6. Utilisateur granulaire
7. Nom d'utilisateur
8. ID origine emplacement
9. Catégorie d'événement
10. Policy (politique)
11. Ressource

Vous êtes maintenant prêt à utiliser QRadar pour commencer à surveiller les activités de Cisco Umbrella, Investigate et CloudLock. Pour plus d'instructions sur la navigation dans QRadar, cliquez ici : [Navigation dans l'application de sécurité cloud Cisco.](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.