Configure QRadar Integration with Umbrella Log Management and S3

Contents

Introduction

This document describes how to configure QRadar to ingest logs from an AWS S3 bucket for Umbrella log management..

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

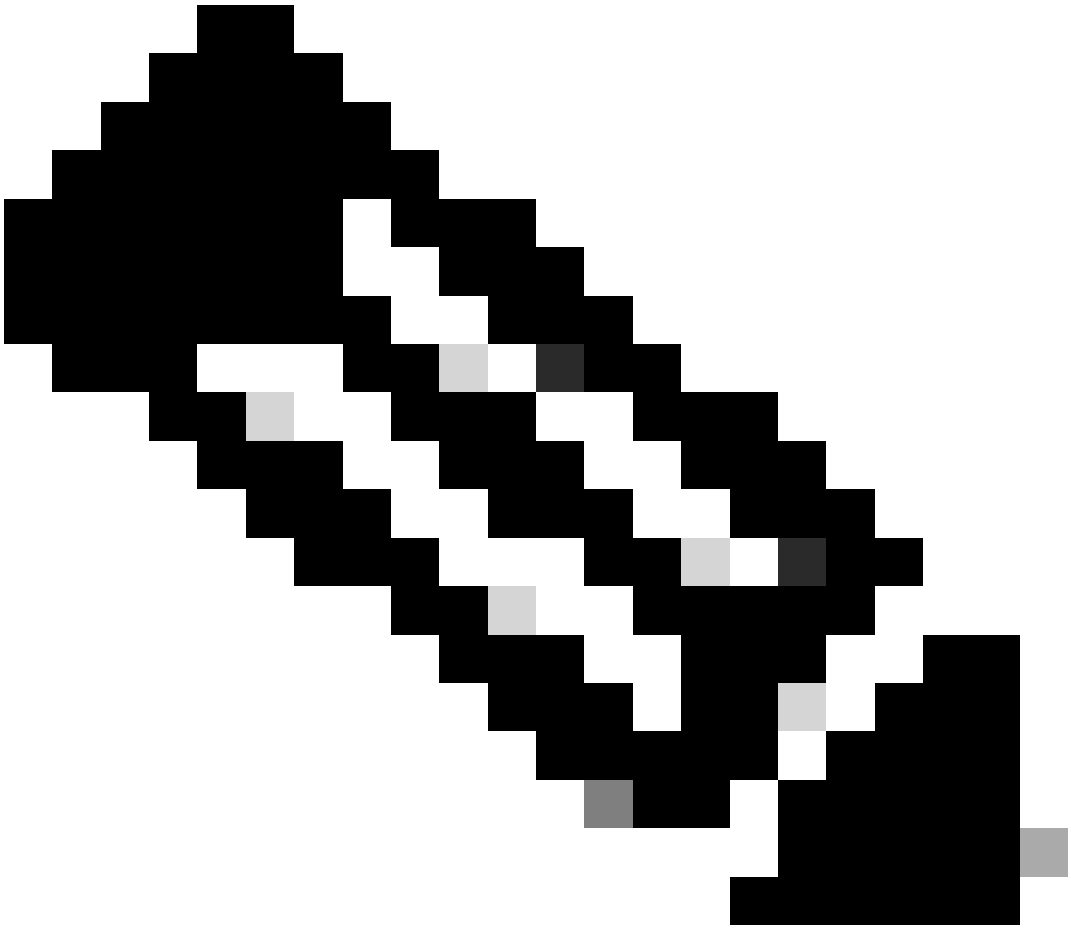
- This document assumes that your Amazon AWS S3 bucket has been configured in Umbrella (**Settings > Log Management**) and is showing green with recent logs having been uploaded. For more information on how to configure this feature, read this article: Download Logs from Umbrella Log Management in AWS S3
- Besides administrative rights to the QRadar appliance(s), the Amazon S3 configuration and Umbrella dashboard, these instructions assume that the QRadar administrator is familiar with creating LSX (Log source Extension) files.

Components Used

The information in this document is based on Cisco Umbrella.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Overview



> **Note**: The best method of configuring QRadar for use with Cisco Umbrella is through the Cisco Cloud Security App. Only proceed with this method if the app cannot be configured.

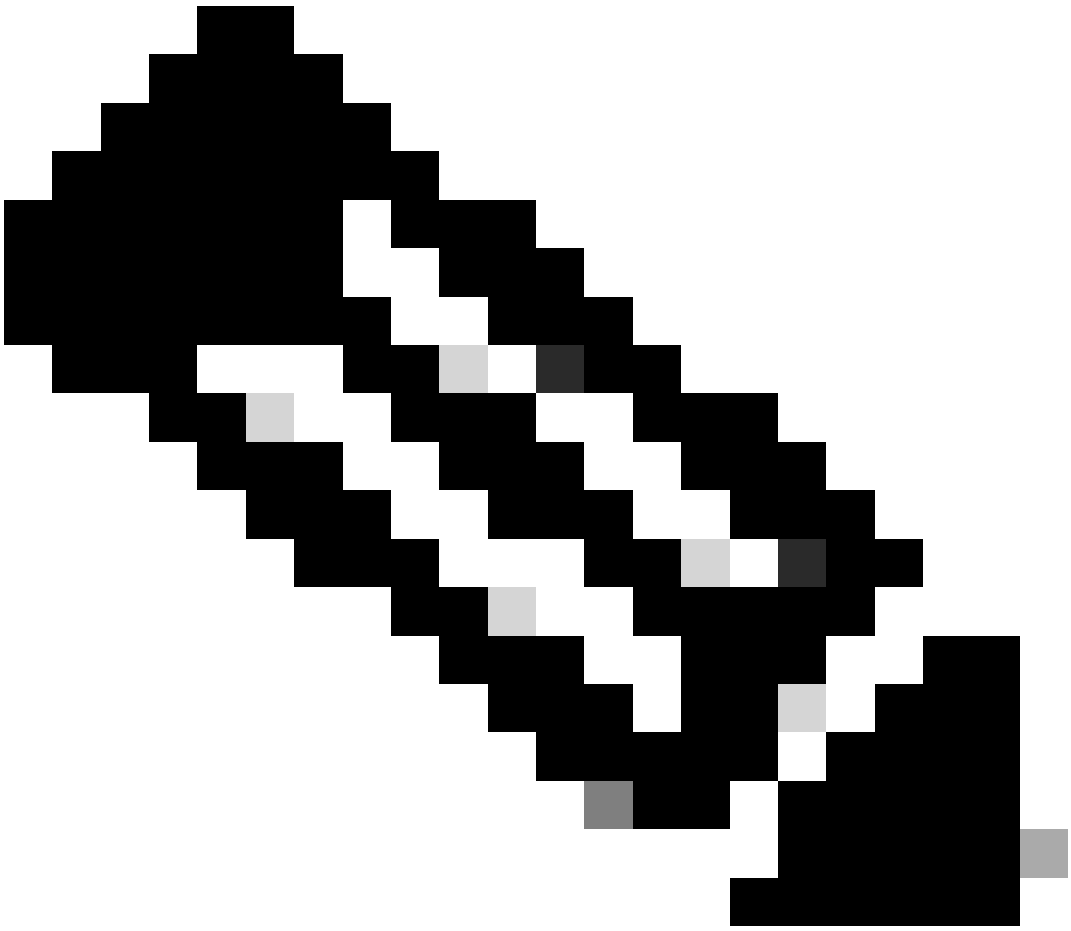
QRadar from IBM is a popular SIEM for log analysis. It provides a powerful interface for analyzing large chunks of data, such as the logs provided by Cisco Umbrella for your organization's DNS traffic.

This article outlines the how to get QRadar set up and running so that it is able to pull the logs from your S3 bucket and consume them. There are two main stages:

- Configure your AWS S3 Security Credentials to allow QRadar access to the logs.
- Configure QRadar itself to point at your bucket.

If you are using the Cisco-managed S3 bucket, please use these instructions in the article Download Logs

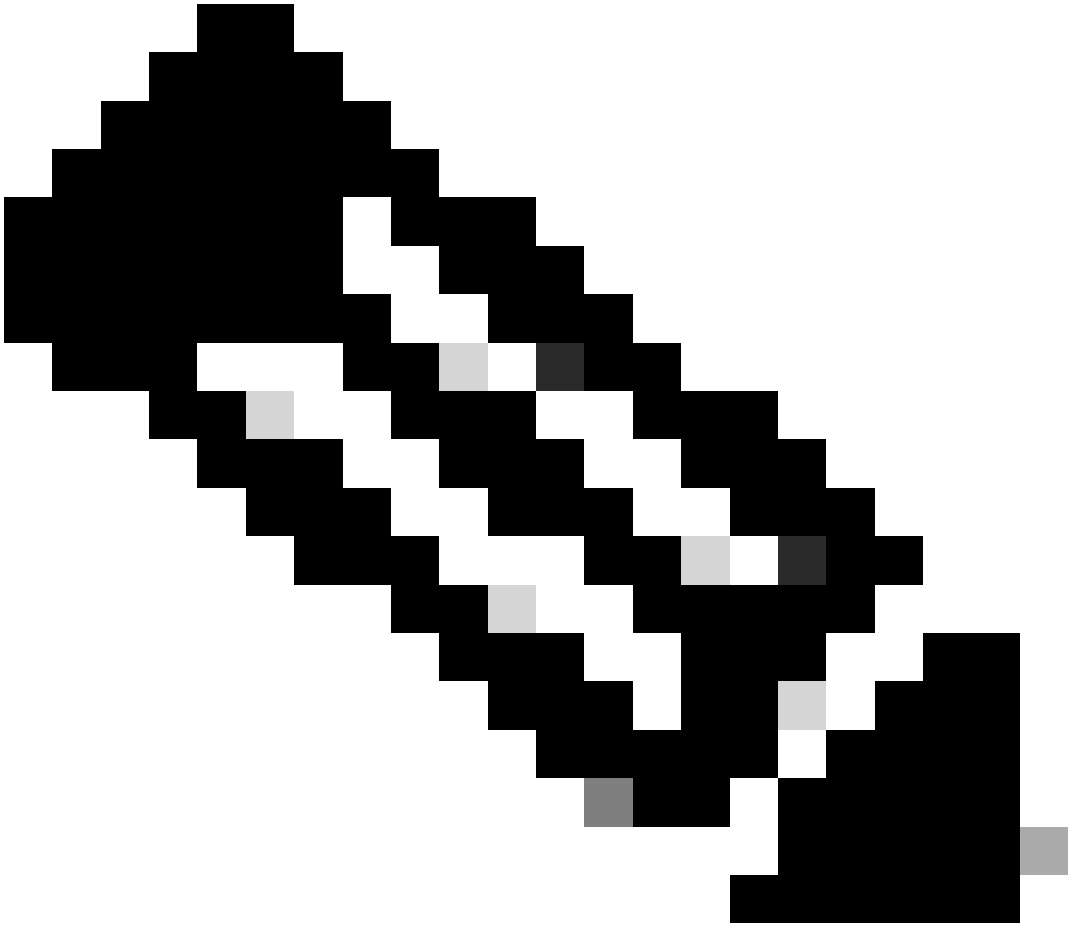
from Umbrella Log Management Using the AWS CLI.



Note: This integration has been tested with both customer managed S3 buckets and Cisco managed S3 buckets. The information discussed in this article is current as of this writing (October 2019). It can change based on the way QRadar and AWS Services interface. This document is a living document. If you have feedback or have found tricks or hints that could help other customers, please contact Cisco Umbrella Support.

Support for QRadar must come from IBM, as Cisco is unable to directly support third-party hardware or software. For any issues connecting your Umbrella dashboard to your S3 bucket, Cisco Umbrella can provide support. Much of the information found in this article can also be found on the IBM website.

Stage 1: Configuring Your Security Credentials in AWS



Note: These steps are the same as those outlined in the article describing how to configure a tool to download the logs from your bucket (Download Logs from Umbrella Log Management in AWS S3). If you have already performed those steps, you can skip to stage 2, although you later need the security credentials from your IAM user to authenticate QRadar to your bucket.

Step 1

1. Add an access key to your Amazon Web Services account to allow for remote access to your local tool and give the ability to upload, download and modify files in S3:

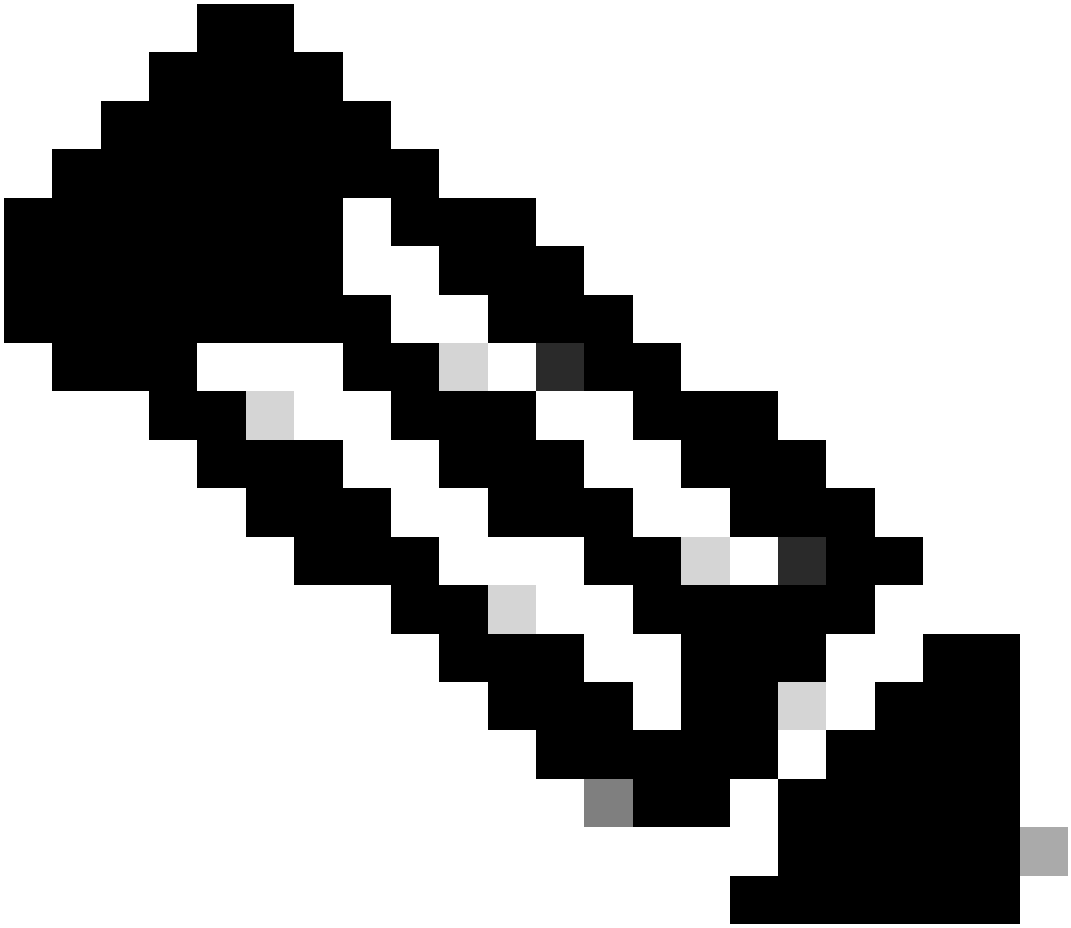
1. Log in to AWS.
2. Select your account name in the upper-right hand corner.
3. In the drop-down, select **Security Credentials**.

2. You are then prompted to use Amazon Best Practices and create an **AWS Identity and Access Management** (IAM) user. In essence, an IAM user ensures that the account that s3cmd uses to access your bucket is not the master account (for example, your account) for your entire S3 configuration. By creating individual IAM users for people accessing your account, you can give each IAM user a unique set of security credentials. You can also grant different permissions to each IAM user. If necessary, you can

change or revoke an IAM user's permissions at any time. For more information on IAM users and AWS best practices, read the AWS documentation.

Step 2

1. Select **Get Started with IAM Users** to create an IAM user to access your S3 bucket You are then taken to a screen where you can create an IAM User.
2. Select **New Users**, then complete the fields.



Note: The user account cannot contain spaces.

---

3. After creating the user account, you are then given only one opportunity to grab two critical pieces of information containing your Amazon User Security Credentials. Umbrella highly suggests that you download these using the button in the lower right to back them up. They are not available after this stage in the setup. Ensure you make a note of both your **Access Key ID** and **Secret Access Key** since they are required in a later step.

Step 3

Next, add a policy for your IAM user so they have access to your S3 bucket:

1. Select the user that just created, then scroll down through the users' properties until you see the **Attach Policy** button.

2. Select **Attach Policy,** then enter "s3" in the policy type filter. This shows two results:

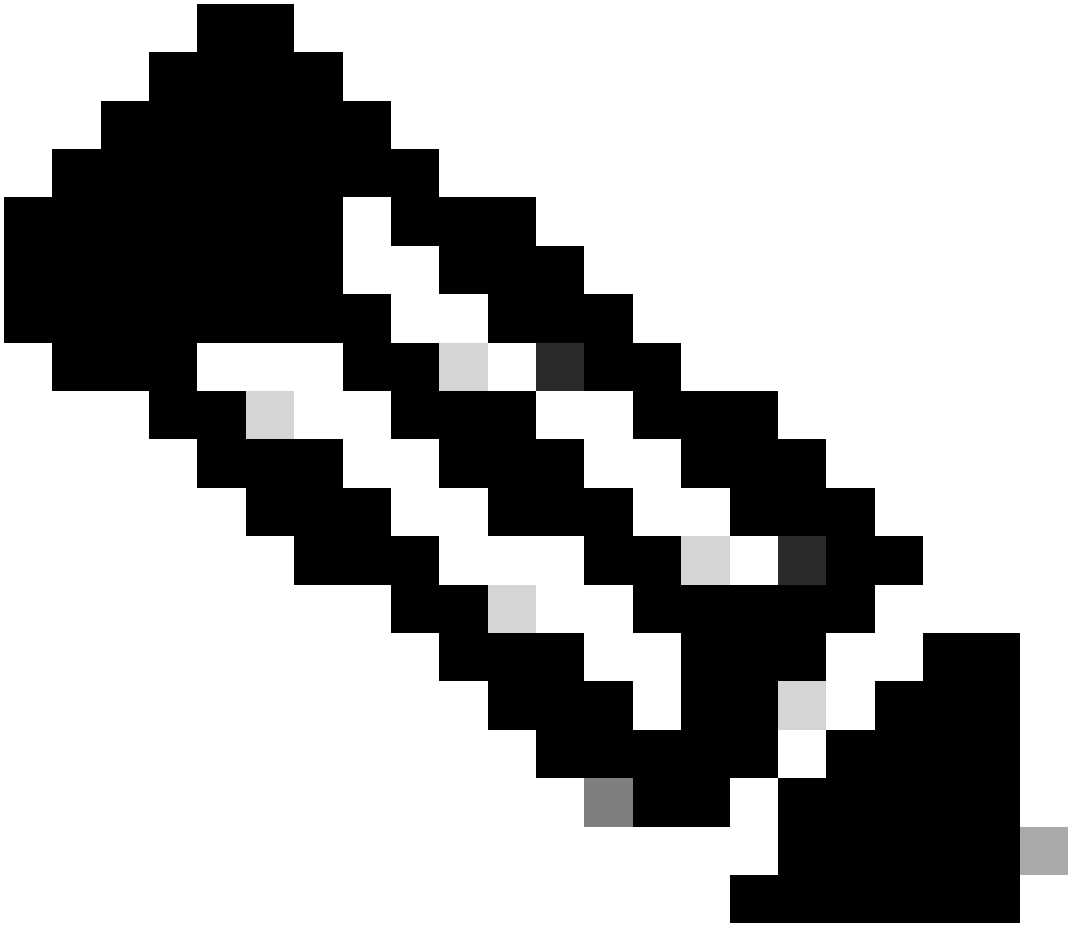
- AmazonS3FullAccess
- AmazonS3ReadOnlyAccess

3. Select **AmazonS3FullAccess**, and then select **Attach Policy** in the lower right corner.

Stage 2: Setting Up QRadar to Pull DNS Log Data from Your S3 bucket

QRadar makes use of the AWS CloudTrail service, which is a web service that records AWS API calls for your account and delivers log files to you.

Prior to QRadar accessing Amazon S3, complete this procedure from IBM to get the Amazon server certificate. This part is difficult, so please ensure that you complete the instructions exactly.



Note: In testing, you **must** use the Firefox browser in order to get this to work as expected.

To get the Amazon server certificate, you must move the certificate in DER format to the proper QRadar appliance. The QRadar appliance that requires the certificate is the appliance assigned in the **Target Event Collector** field in the Amazon AWS CloudTrail log source.

Before You Begin

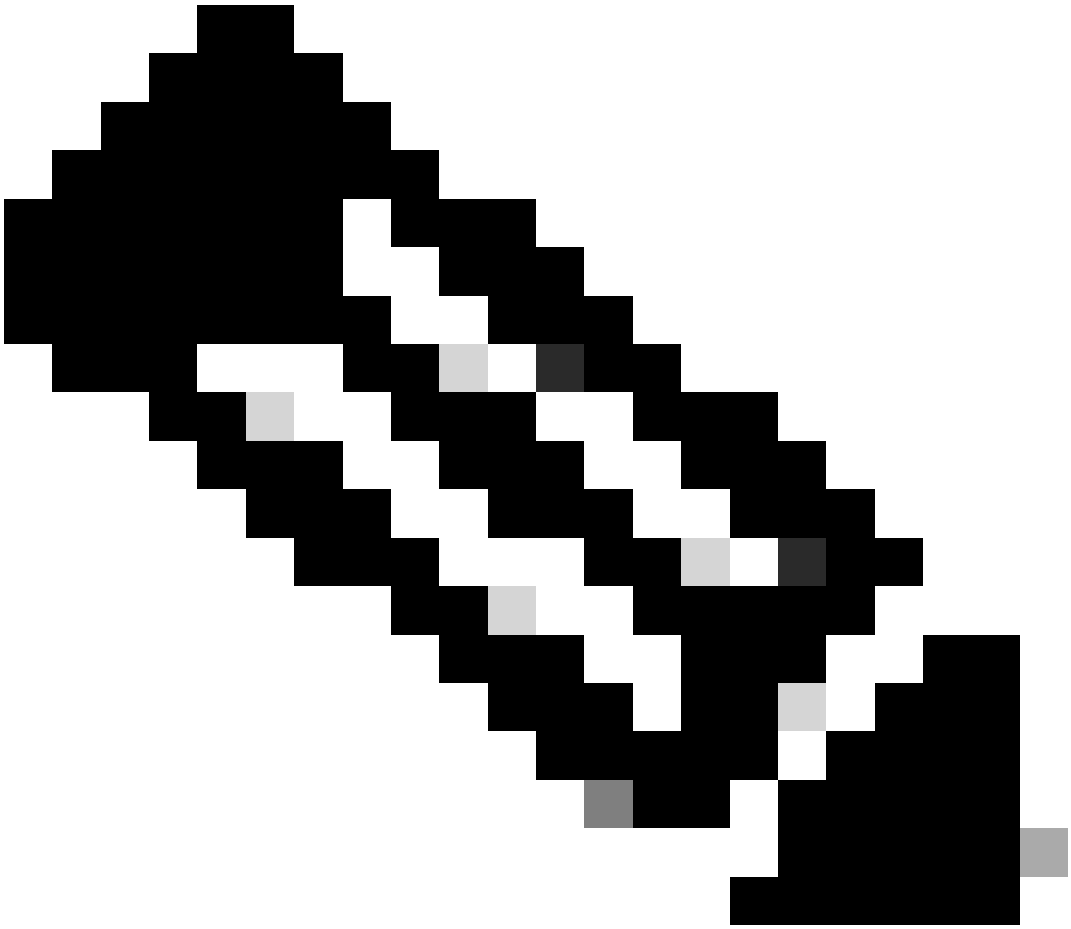
- The certificate must be in .DER format.
- The extension .DER is case sensitive and must be uppercase.
- If the certificate is exported in lowercase, then the log source can experience event collection issues.

Initial Steps

1. Access your AWS CloudTrail S3 bucket: `https://<bucketname>.s3.amazonaws.com`

2. Use Firefox to export the SSL certificate from AWS as a (.DER) certificate. Firefox can create the required certificate with the .DER extension:

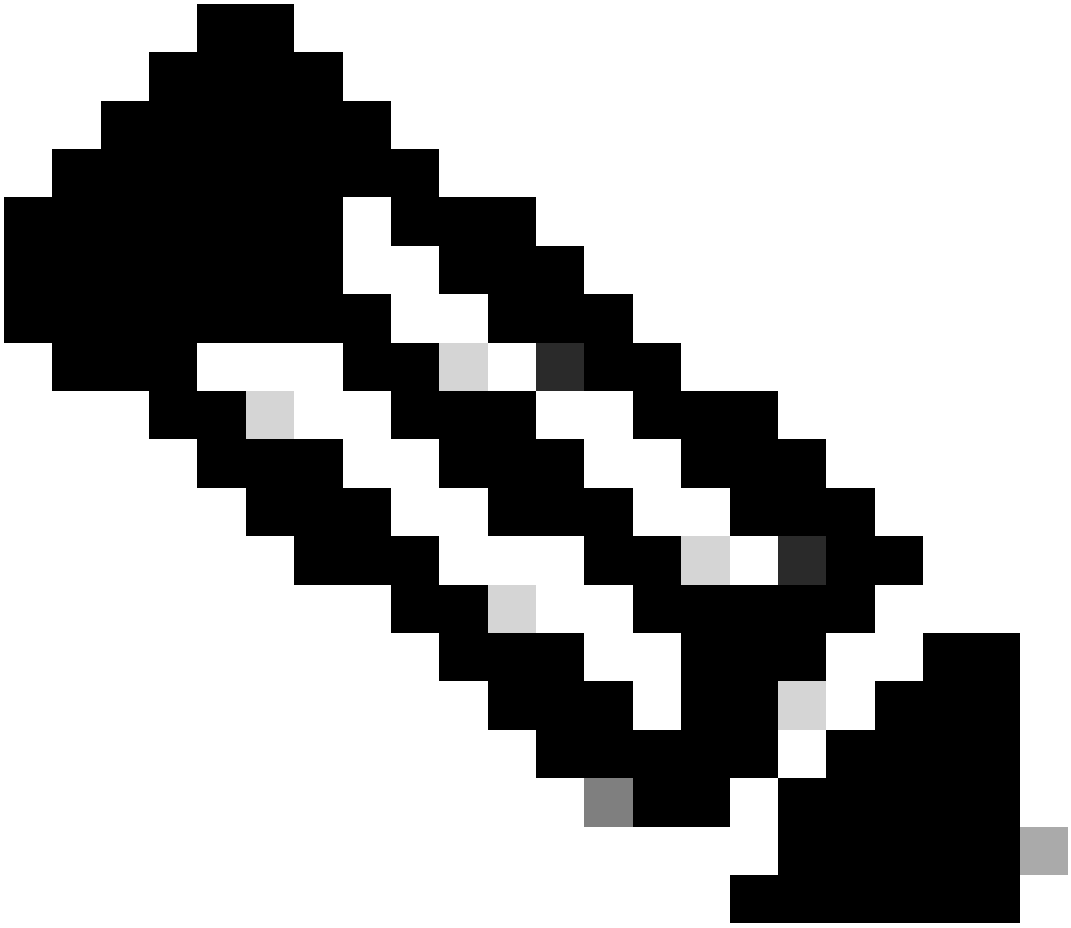
1. Select the **Site Identity** icon (the lock icon in the address bar).
2. Select **More Information > View Certificate** and select the Details tab.
3. Select **Export** to export in the certificate .DER format.



Note: The .DER extension is case sensitive and must be uppercase.

---

3. Copy the .DER certificate to the **/opt/QRadar/conf/trusted_certificates** directory of the QRadar appliance that manages the Amazon AWS CloudTrail log source. You can use WinSCP to copy it.



Note: The QRadar appliance that manages the log source is identified by the **Target Event Collect** field in the Amazon AWS CloudTrail log source. The QRadar appliance that manages the Amazon AWS CloudTrail log source must have a copy of the .DER certificate in **/opt/QRadar/conf/trusted_certificates**.

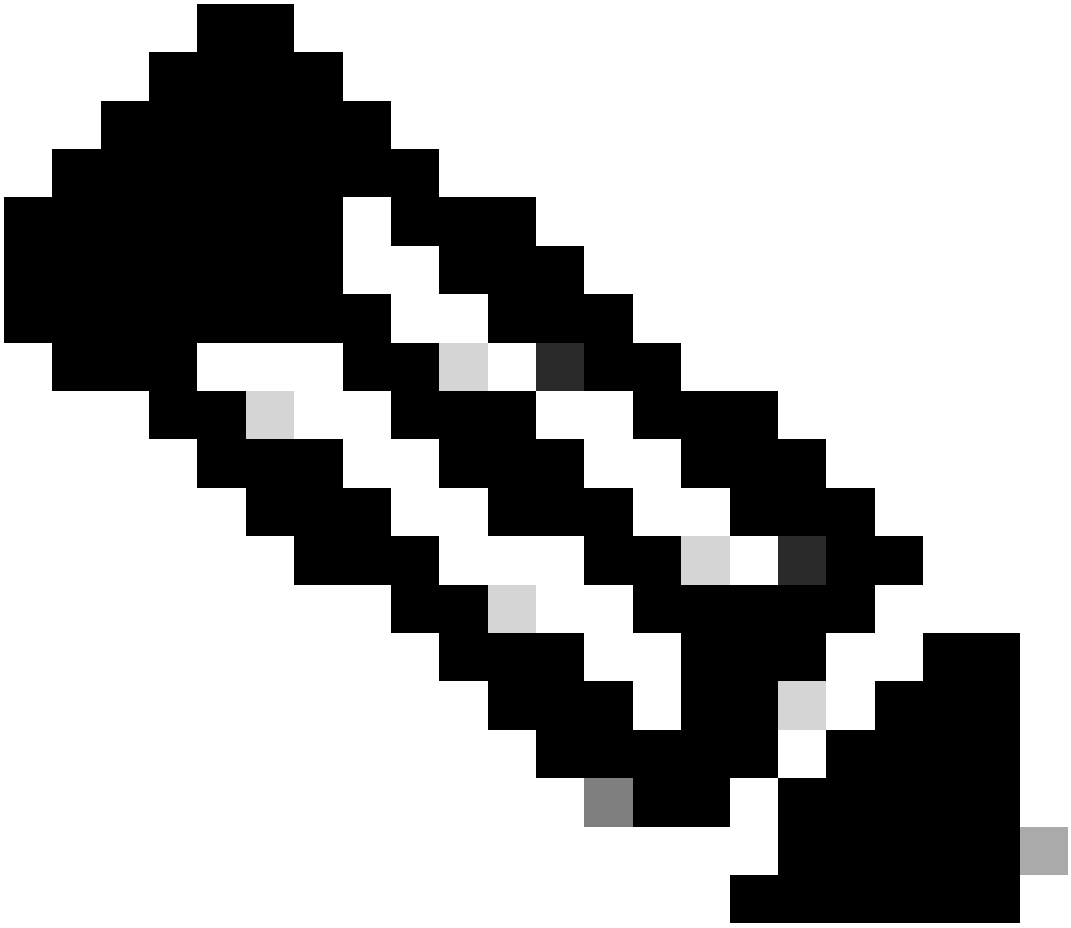
4. Log in to the QRadar user interface as an Administrative user.

5. Select the **Admin** tab.

6. Select the **Log Sources** icon.

7. Select the **Amazon AWS CloudTrail** log source.

8. From the navigation menu, select **Enable/Disable** to disable and then re-enable the Amazon AWS CloudTrail log source.



Note: When an administrator forces the log source from disabled to enabled, this allows the protocol to connect to the Amazon AWS bucket as defined in the log source. A certificate check then takes place as part of the first communication.

9. If you continue to have issues, verify that the Log Source Identifier field contains the correct Amazon AWS bucket name and that the Remote Directory path is correct in the log source configuration.

Finalize the QRadar Configuration

1. In QRadar ensure that all of your protocols, DSMs, and other information are up to date. Select the **LogFileProtocol** with these configurations (your frequency, Start Time, Recurrence, and other information can be different).

2. In the **Log Sources** tab, enter a **Log Source Name** and a **Log Source Description**. These can be whatever you like.

3. Enter your **S3 Bucket Name,** your **AWS Access Key,** your **AWS Secret Key**, and the **Remote Directory** (likely dnslogs but depends on your setup). Adding a Log Source Identifier like the year can help filter so only logs with "2019" in them are pulled.

4. Create an LSX (Log Source eXtension) that can parse the Cisco Umbrella events. (This is what it looks like after the import into QRadar.) More information about how exactly to create LSX can be found on the IBM website. This is just an example. The data you want to pull from the logs vary depending on the use case.

5. Double-check that your AWS Access Key and AWS Secret Key are copied successfully and pasted into the Log Source Configuration.

6. Select the GZIP Processor and an Event Generator of RegEx Based Multiline. The easiest way to get one event per line is by using a start pattern RegEx of:

```
("\d{4}-\d{2}-\d{2}\s\d{2}:\d{2}:\d{2}",")
```

Make sure you select your Log Source Extension and Use Condition, then save the log source.

7. Perform a Full Deploy in QRadar.

Your log source then use RestAPI to connect to your bucket with the credentials and keys that you provided and begin pulling events.

Additional Information

Enable Bucket Logging

To enable bucket logging, read the AWS documentation and complete the procedures outlined. By default, logging is disabled. Once enabled, a new folder called /logs resides in your bucket root to show you the information of GETS, PUTS, and DELETES.

Managing the Log Cycle

When you are using S3, you can manage the lifecycle of the data within the bucket to extend the duration of time you want to retain logs for. Depending on the purpose of what you are using the external log management for, the duration can be very short or very long. For instance, you can wish to simply download the logs from the S3 bucket after 24 hours and store them offline, or retain the logs indefinitely in the cloud.

By default, Amazon stores the data in a bucket indefinitely, but unlimited storage does raise the cost of maintaining the bucket. For more information on S3 lifecycles, please read the AWS documentation.

To configure the lifecycle of your bucket:

1. Select **Properties > Lifecycle**.

2. Select **Add a Rule**, then **Apply the Rule** to the whole bucket (or a subfolder if you configured it as such).

3. Select an Action on Objects, such as **Delete** or **Archive**, then select the time period and whether you want to use Glacier storage to help reduce your Amazon costs. (Glacier is "cold" offline storage, which, while slower to access, is much less expensive.)

If you prefer to manage logs in another method (for example, on your internal backup solution), you can simply download the logs from S3 and preserve them in another way.