Salesforce Security Monitoring

Contents

Salesforce Security Monitoring

The IBM® Security QRadar® DSM for Salesforce Security Monitoring can collect event logs from your Salesforce console by using a RESTful API in the cloud.

The following table identifies the specifications for the Salesforce Security Salesforce Security Monitoring DSM:

Table 1-1. Salesforce Security Salesforce Security Monitoring DSM specifications

Specification	Value
Manufacturer	Salesforce
DSM	Salesforce Security Monitoring
RPM file name	DSM-SalesforceSecurityMonitoring-QRadar_Version-Build_Number.noarch.rpm
Protocol	Salesforce REST API Protocol
QRadar recorded events	Login History, Account History, Case History, Entitlement History, Service Contract History, Contract Line Item History, Contract History, Contact History, Lead History, Opportunity History, Solution History
Automatically discovered	No
Includes identity	Yes
More information	Salesforce website (http://www.salesforce.com/)

Salesforce Security Monitoring DSM integration process

To integrate Salesforce Security Monitoring DSM with QRadar, use the following procedures:

1. If automatic updates are not enabled, download and install the most recent versions of the following RPMs on your QRadar Console.
   - DSMCommon RPM
   - SalesforceRESTAPI Protocol RPM
   - Salesforce Security Monitoring RPM
2. Configure the Salesforce Security Monitoring server to communicate with QRadar.
3. Obtain and install a certificate to enable communication between Salesforce Security Monitoring and QRadar. The certificate must be in the /opt/QRadar/conf/trusted_certificates/ folder and be in .DER format.
4. For each instance of Salesforce Security Monitoring, create a log source on the QRadar Console.

Configuring the Salesforce Security Monitoring server to communicate with QRadar

To allow QRadar communication, you need to configure Connected App on the Salesforce console and collect information that the Connected App generates. This information is required for when you configure the QRadar log source.

Before you begin

If the RESTful API is not enabled on your Salesforce server, contact Salesforce support.

Procedure

1. Log in to your Salesforce Security Monitoring server.
2. From the **Setup** menu, click **Create > Apps > New**.
3. Type the name of your application.
4. Type the contact email information.
5. Select **Enable OAuth Settings**.
6. From the **Selected OAuth Scopes** list, select **Full Access**.
7. In the **Info URL** field, type a URL where the user can go for more information about your application.
8. Configure the remaining optional parameters.
9. Click **Save**.

What to do next

The Connected App generates the information that is required for when you to configure a log source on QRadar. Record the following information:

Consumer Key

Use the **Consumer Key** value to configure the **Client ID** parameter for the QRadar log source.

Consumer Secret

You can click the link to reveal the consumer secret. Use the **Consumer Secret** value to configure the **Secret ID** parameter for the QRadar log source.

Important: The **Consumer Secret** value is confidential. Do not store the consumer secret as plain text.

Security token

A security token is sent by email to the email address that you configured as the contact email.

Configuring a Salesforce Security Monitoring log source in QRadar

To collect Salesforce Security Monitoring events, configure a log source in QRadar.

Before you begin

When you configured a Connected App on the Salesforce Security Monitoring server, the following information was generated:

- Consumer Key

- Consumer Secret
- Security token

This information is required to configure a Salesforce Security Monitoring log source in QRadar.

Ensure that the trusted certificate from the Salesforce Security Monitoring instance is copied to the `/opt/QRadar/conf/trusted_certificates/` folder in .DER format on QRadar system.

Procedure

1. Log in toQRadar.
2. Click the **Admin** tab.
3. In the navigation menu, click **Data Sources**.
4. Click the **Log Sources** icon.
5. Click **Add**.
6. From the **Log Source Type** list, select **Salesforce Security Monitoring**.
7. From the **Protocol Configuration** list, select **Salesforce Rest API**.
8. Configure the following Salesforce Security Monitoring parameters:

Parameter	Description
Login URL	The URL of the Salesforce security console.
Username	The user name of the Salesforce security console.
Security Token	The security token that was sent to the email address configured as the contact email for the Connected App on the Salesforce security console.
Client ID	The Consumer Key that was generated when you configured the Connected App on the Salesforce security console.
Secret ID	The Consumer Secret that was generated when you configured the Connected App on the Salesforce security console.

9. Configure the remaining parameters.
10. Click **Save**.
11. On the Admin tab, click **Deploy Changes**.