Cavirin Quick Start

Sizing Specifications

Sizing Specifications	
AWS Instance Type:	M5.xlarge (4 vCPUs, 16 GB memory)
GCP Instance Type:	n1-standard-4 (4 vCPUs, 16 GB memory)
Azure Instance Type:	Standard D4s v3 (4 vCPUs, 16 GB memory)
On-Prem:	4 vCPUs, 16 GB memory
Storage:	150 GB

Connectivity Requirements

From	To	Port	Protocol	Application/Purpose
Cavirin Platform's IP	Internet (Outbound)	Per the Network	HTTP/HTTPS	Any
Cavirin Platform's IP	Windows Target	5985/5986	HTTP/HTTPS	Windows RM Service/Scan
			ICMP (on-prem only)	Discovery
Cavirin Platform's IP	Linux Target	22	SSH	Assessment/Scan
			ICMP (on-prem only)	Discovery

Credentials for Accessing Clouds and On-prem Hosts

The Cavirin Platform must offer credentials to an organization's computing resources or clouds, so the organization can authenticate the Platform, as follows:

- Cavirin offers *cloud credentials* to gain access to cloud services and computing resources within the cloud. The Platform does not offer one credential to the organization's computing resources and a separate credential for cloud services.
- Cavirin offers *host credentials* to the on-prem resources.

You might have resources that are on-prem as well as in a cloud; you can specify multiple sets of credentials for any deployment, as needed.

AWS cloud credentials are configured in the AWS cloud and then copied to the Cavirin Platform. Choices for credentials are:

- *IAM Role*.
- An *Amazon Resource Name* (*ARN*) uniquely identifies an AWS resource. (AWS needs an ARN if a resource is to be specified unambiguously across all the AWS environment.) An ARN applies to IAM policies, Amazon Relational Database Service (Amazon RDS) tags, and API calls, for example.
- *Access Key and Secret Key* (*AKSK*).

Configuring IAM Role Credentials for an AWS Cloud

The screen for adding an AWS cloud account is divided as follows:

- At left, the steps performed on the Cavirin VM.
- At right, a description of steps performed in the cloud itself.
- Some values you enter in the cloud are also added to the Cavirin configuration.

NOTE: The steps in the following numbered list are the current version. Therefore, use the steps described below if the UI appears different.

1. Log into the AWS Console.
2. Click **Services**, then select **IAM**.
3. Select **Policies**, then click **Create Policy**.
4. Select **Create Your Own Policy**. (This policy will come from Cavirin's Platform.)
5. Click the **JSON** tab.
6. Here in the Platform's screen, copy the policy in one of two ways: Click the icon or click **Show Policy**, select-all, then copy.
7. In the AWS window for creating policies, paste the policy into the *Policy Document* area, then click **Review Policy**.
8. Create a name for the policy that AWS is about to get from the Cavirin Platform (for example, cavirin_iam) and then click **Create Policy**.
9. In the left pane (still AWS), select **Roles**, then click **Create new role**.
10. From Role Type, select **Amazon EC2** (allow EC2 instances to call AWS services on your behalf).
11. Search for the policy created in Steps 4 - 8. Select the policy, then click **Next Step**.
12. Set Role Name with your choice ('cavirin_trusted_role'), then click **Create Role**.
13. Click **Services**, then select the **EC2**.
14. Locate and select the EC2 instance where the Cavirin Platform resides.
15. Click **Actions** -> **Instance Settings**, then select **Attach/Replace the IAM Role**.
16. Select the Role you created in Step 12 in the dropdown.
17. Click **Validate** at the bottom of the screen. After validation, the button changes to *Save*.
18. Click **Save** now unless you plan to enable Monitoring, below. (After completing the steps for Monitoring, click **Save**.)

Addition of a cloud account ends with **Validate** and then **Save** (unless monitoring is planned). If your organization plans to enable monitoring, see "**Error! Reference source not found.**" before proceeding because of the alternate sequence. With monitoring, the final sequence is:

1. The user clicks **Validate**. After validation succeeds, the button changes to *Save*.
2. Complete the steps described in "How to Set Up Monitoring with AWS CloudTrail."
3. Click **Save.**

Configuring Amazon Resource Name Credentials for AWS

1. Log into the AWS account that you intend to evaluate AWS Console.
2. Click **Services**, and then select **IAM**.
3. Select **Policies**, and then click **Create Policy**.
4. Select **Create Your Own Policy**. (This policy will come from Cavirin's Platform.)
5. Select **Policies** and then click **Create Policy**.
6. Click the **JSON** tab.
7. In the Platform Platform's cloud account's screen, copy the policy in one of two ways: (1) Click the icon or (2) click **Show Policy**, select-all, and then copy it.
8. Paste the policy from Step 6 into the text area in the AWS policy creation window, then click **Create Policy**.
9. Type a name for the policy that you got from the Platform and pasted in Step 7.
10. In the left pane (still in AWS), select **Roles** and then click **Create new role**.
11. In Role Type, select **Role for cross-account Access**. Select **Provide access between your AWS account and a 3rd party AWS account**.

    - For *account ID*, provide the AWS *account ID* for the account where your Platform instance is running.
    - The range for *external ID* is 2 - 96 characters. Later, insert this ID to finish setup.
    - Clear the *Require MFA* box.

12. Click **Next Step**.
13. Search for and then select the policy created in Steps 4 - 8, then click **Next Step**.
14. Specify a *Role Name* for your choice, then click **Create Role**.
15. On the search box, find the *role name* typed in the preceding step and click it.
16. Copy the Role ARN value. Paste it in the ARN Role field in the Cavirin Platform.
17. Provide the *external ID* from Step 10.
18. Click **Validate** at the bottom of the Cavirin screen. After validation, the button changes to *Save*.
19. Click **Save** now unless you plan to enable Monitoring, below. (After completing the steps for Monitoring, then you click Save.)

Addition of a cloud account ends with **Validate** and then **Save** (unless monitoring is planned). If an organization plans to enable monitoring, see "**Error! Reference source not found.**" before proceeding because of the alternate sequence. With monitoring, the final sequence is:

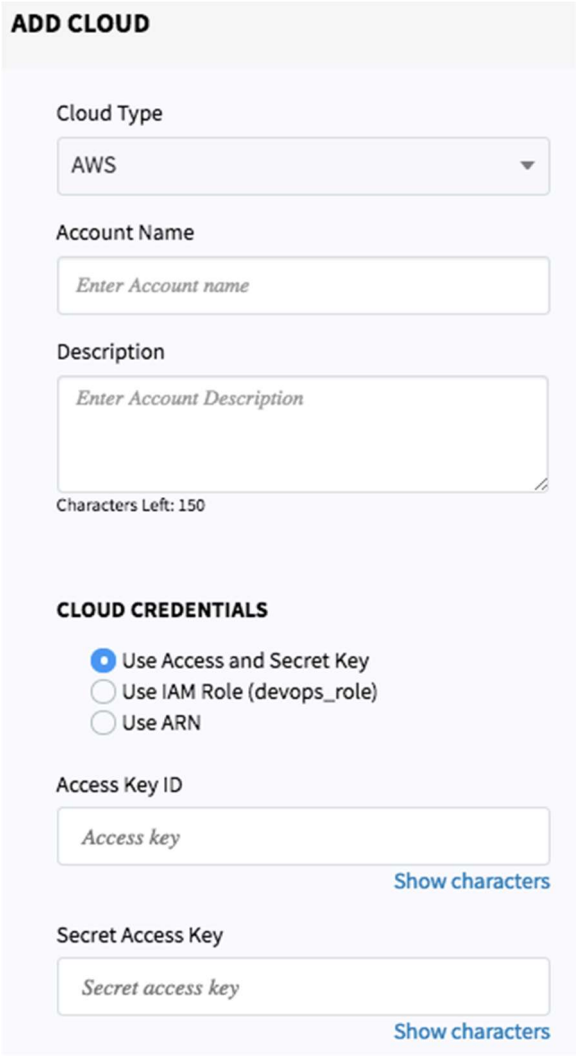
1. The user clicks **Validate**. After validation succeeds, the button changes to *Save*.
2. Complete the steps described in "How to Set Up Monitoring with AWS CloudTrail."
3. Click **Save**.

Configuring Access Key and Secret Key Credentials

It is assumed that the user has the Access Key ID and the Secret Access Key. The points to understand follow.

Addition of a cloud account ends with **Validate** and then **Save** (unless monitoring is planned). If an organization plans to enable monitoring, see "How to Set Up Monitoring with AWS CloudTrail" before proceeding because of the alternate sequence. With monitoring, the final sequence is:

1. The user clicks **Validate**. After validation succeeds, the button changes to *Save*.
2. Complete the steps described in "How to Set Up Monitoring with AWS CloudTrail."
3. Click **Save**.



Adding Credentials for Microsoft Azure

This section describes the steps for adding a Microsoft Azure account to the Cavirin Platform so that the Platform can assess it. The site of the configuration steps alternates between Cavirin's Add Cloud Account screen and the Azure Management Portal. The user who executes these steps should understand the organization's Azure presence.

NOTE: To complete the steps in Azure, the user must have the owner role in Azure.

1. Type a name for the Azure account the Platform uses locally. (It does not need to match the account name entered in the Azure UI.)
2. Type a description, as needed.
3. Log into the Azure Management Portal.
4. Go to Azure Active Directory. (A frequent Azure user easily finds this in the blade at left, but a new Azure user will have to search for it.) Click **Properties**.
5. **Copy** the directory ID.
6. In Cavirin, paste the directory ID value into the Tenant ID.
7. In the Azure Active Directory navigation blade, click App registrations, then click **New application registration**.
8. Type a name for the Cavirin application in the Name box.
9. In the Application Type dropdown, select **Web app/API**.
10. For a sign-on URL, type any valid URL. (Cavirin ignores this URL, but Azure requires a URL.) The **Create** button now appears at the bottom of the screen.
11. Click **Create**. Azure begins generating the application ID (but does not display it in this blade).
12. In the App registrations list, find the generated application ID, click on it, and **copy** it.
13. In Cavirin, paste the application ID in the Application ID box.
14. In Azure (where the same window is open), select the **Settings** blade at right and then select **Keys** near the top of the blade.
15. Specify a key description and a duration (expiration) for the key.
16. Click Save at the top of the blade. Azure now generates the key and displays it.
17. Record the value of the key and safely store it.
    WARNING: Record the key (before next step) because you can't retrieve it later.
18. **Copy** the key and paste it the Cavirin Application Key.
19. In Azure, in the blade at left, click Subscriptions; copy the subscription ID.
20. Paste this subscription ID into the Cavirin UI's Subscription ID box.
21. In Azure, again locate the subscription; click on it to open a configuration blade at right.
22. Select Access control (IAM) in the menu. The Add button appears (if you have an owner role).
23. Click Add. The blade for role configuration opens at right. In the Role dropdown at upper-right, select Reader.
24. In the Select box, start typing the name of the Cavirin application (from Step 9). When auto-complete displays the app name, click it.
25. Click Save. This completes the tasks in the Azure management portal.
26. Click the Validate button at the bottom of the screen (not shown in next figure). After successful validation, the button changes to Save (also not shown).
27. Click Save. This completes the addition of the Azure cloud account.

Adding Credentials for Google Cloud

This section describes the steps for adding a Google Cloud account so that Cavirin can assess it. The site of configuration activity alternates between the Cavirin Add Cloud Account screen and the Google Cloud Console. The person that executes these steps should understand the organization's Google Cloud presence.

A cloud credential for Google Cloud is a key in JSON format. A description for importing each type of key is included.

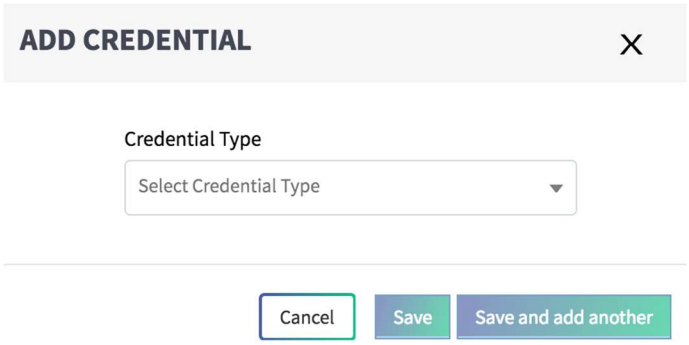
Obtaining Credentials

1. Type a name for the Google account for the Platform to use locally. (It does not need to match the account name entered in Google Cloud.)
2. Type a description, as needed.
   In the Cloud Credentials area, select JSON.
3. Log into the organization's Google Cloud Console. https://cloud.google.com
4. Select the name of a project at the top of the screen; click Open.
5. In the upper-left corner, click the list icon (for Products and Services) to open a navigation pane.
6. Click APIs and services and select Dashboard (default). (You can bypass the dashboard by selecting).
7. Click Enable APIs and Services. You will use a search box to locate and enable two APIs (they might already be enabled).
8. In the Enable APIs and Service search box, type Google Compute Engine API to start searching for it. After finding it, click on the API.
9. Click Enable if this button is visible (otherwise, the API is already enabled).
10. In the same search box, type Google Cloud Resource Manager API. After finding it, click on this API. Click Enable if visible (otherwise, it is already enabled).
11. Again, in APIs and Services, locate and click Credentials (in the menu at left).
12. Click Create Credentials, and then select Service account key.
13. In the Service account dropdown, choose New service account (near bottom of the list).
14. Type a name for the service account (for example, "Cavirin").
15. Access the Role dropdown and select the Viewer role.
16. For Key type, select JSON.
17. Click Create. Google creates and downloads a key to your local system.
18. (This and the remaining steps are in the Cavirin system.) In the Select JSON box, Browse to and select the JSON file (downloaded with preceding step); click Open.
19. At the bottom of the screen for a new account, click. After validation succeeds, the button changes to Save. Click Save.

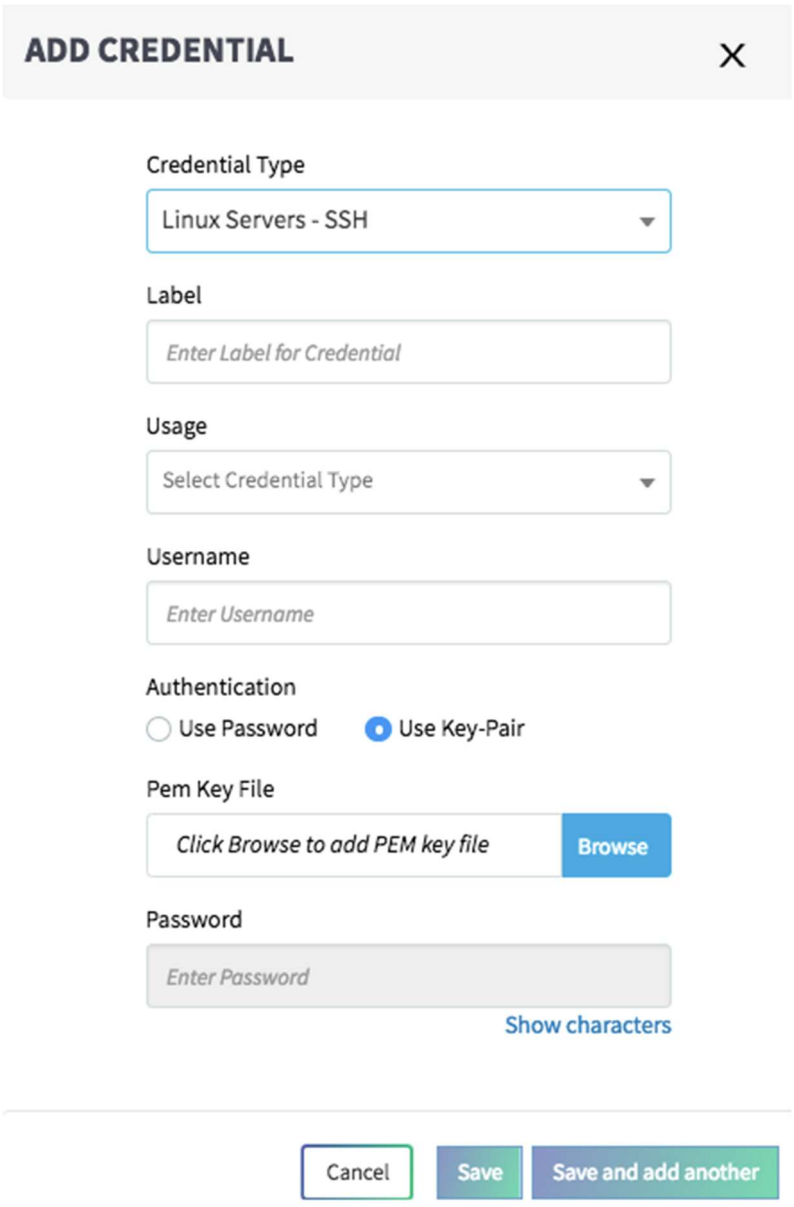
Creating Host Credentials

To specify a set of host credentials (Group Admin role):

1. Navigate to **Protect** > **Host Credentials**.
2. Click **Add** in the upper-left corner of the Host Credentials screen. The following pop-up window opens:



3. In the *Credential Type* dropdown, select **Docker Image**, **Linux Servers - SSH**, or **Windows Administrator**. The specifications are straight forward. The main thing to note is that *label* is the name you assign to a credential set. The next step is for the Linux credentials. It is slightly more complicated than the Windows or Docker credential, and this example suffices for Windows and Cloud host credentials.
4. Select **Linux Servers**. For the credential type. The next figure shows the configuration popup and the default authentication method as PEM-key.
5. Type a meaningful name for this credential set in the Label box.
6. Choose a usage of *Global* or *Restricted*. Global means the Platform offers this credential to all hosts in the on-prem environment. Restricted means this credential is offered to hosts in a specific group of computing resources.
7. For Authentication, choose one of the following:
    a. With Use Key-Pair, click **Browse** to locate and select the PEM key file.
    b. With Use Password marked, type a password.
8. Select **Save** if done or **Save and add another** for another Linux credential set.


ADD CREDENTIAL
Credential Type
Linux Servers - SSH
Label
Enter Label for Credential
Usage
Select Credential Type
Username
Enter Username
Authentication
Use Password
Use Key-Pair
Pem Key File
Click Browse to add PEM key file
Browse
Password
Enter Password
Show characters
Cancel
Save
Save and add another