Using VMware Discovery

VMware Discovery

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

1 Using VMware Discovery

Welcome to the Using VMware Discovery documentation. Use the navigation on the left to browse through the documentation.

We provide step by step instructions on how to create public cloud accounts such as AWS and Azure, and private cloud accounts such as vCenter.

Working with AWS Accounts in VMware Cloud Services

2

When you add an AWS public cloud account to VMware Cloud services, you establish a connection that allows information about your AWS resources and billing to be shared, analyzed, and updated in VMware Cloud services.

The AWS accounts you create in VMware Discovery can be opened in other VMware Cloud services such as VMware Cost Insight and VMware Network Insight. If you are working with VMware Cost Insight, and you want to view billing information, you must add both an AWS master account and an AWS linked account. VMware Cloud services collect cost information from the master account, and inventory information from the linked accounts.

You can add two types of AWS accounts in VMware Discovery.

What Kind of AWS Account	What should I Know
AWS account set up with an IAM role	Adding an AWS account that has been set up with an IAM role provides additional security for your organization. Before you set up this type of AWS public cloud account in Discovery, you create an IAM role in AWS. When you create this role in AWS, you input a policy, an account ID, and an external ID which are provided by VMware Discovery. The external ID is a unique ID which means that the account is organization-specific. You can use the account for all the services in your organization, but not for services in another organization. This provides additional security for your organization. To set up this type of AWS public cloud account in VMware Discovery, you need the Amazon Resource Name (ARN) of the IAM role. An ARN is a unique identifier for an individual AWS resource. To create an IAM role in AWS and obtain the required ARN, see How Do I Obtain an ARN.
AWS account set up with an IAM user	To set up an AWS public cloud account in VMware Discovery you need your access key ID and your secret access key. Both of these credentials were created when you set up the account in AWS. If you have forgotten your credentials, you can create them again. SeeHow Do I Create AWS Security Credentials.

This chapter includes the following topics:

Add an AWS Account with an IAM Role

Adding an AWS account that has been set up with an IAM role provides additional security for your organization.

For more information about setting up AWS accounts with an IAM role, see Chapter 2 Working with AWS Accounts in VMware Cloud Services.

Prerequisites

You need the role ARN you collected when you set up an IAM role in AWS. See, How Do I Obtain an ARN.

Procedure

1. Select **Manage > Cloud Accounts**.
2. Click **Add New**, and select **Amazon Web Services**.
3. Select **Add a single account**, and click **Next**.
4. Click **Next**.
5. Copy the role ARN into the **ARN** text box.

   If you do not have a role ARN, refer to the link in the prerequisite above to see how to obtain one.
6. Enter a name for the account.
7. Add more owners to the account by clicking **+** and selecting an owner from the displayed list.
8. Enter a tag. You use tags to group the cloud accounts. You can search for these groups using the tag.

   Custom tag pairs, denoted with the notation key=value. Multiple values might be set to the same key using a comma within the values (like key=value1,value2). Multiple tag pairs might be semicolon-delimited within the column to indicate multiple (like key1=value1;key2=value2).
9. Click **Save**.

Add Multiple AWS Accounts with an IAM Role

You can add multiple AWS accounts by importing a CSV file that contains the required account information.

In this step, we show you how to create a CSV file and enter the information VMware Discovery requires to import multiple AWS accounts simultaneously. Then, we show you how to import the CSV file into VMware Discovery to upload these accounts.

For more information about setting up AWS accounts with an IAM role, see Chapter 2 Working with AWS Accounts in VMware Cloud Services.

Prerequisites

You need the role ARNs you obtained when you set up the IAM roles in AWS. See, How Do I Obtain an ARN.

Procedure

1 Open Microsoft Excel and create a file.

a In each column, enter the data in the order in which it appears below. You can enter multiple roles from any number of AWS accounts, or multiple roles from a single account.

A typical entry might look something like this ABIAJAKUWJS5YCEVW23M;WUZmEwDB3ysbGJsw9Zhy0MIRdp8G+u02jzSTOPyd,My AWS US-East,My AWS Account for US-East region,my@company.com,dept=eng.

Type of information	Description
Identifier	The role ARN of the account. You can find this by clicking the role in AWS and viewing the summary. For example: arn:aws:iam::071111117054:role/bulk-import-account
Nickname	The name of the account, for example Discovery AWS Account.
Description	A description so that you can easily identify the account. For example, My AWS US-East, My AWS Account for US-East region
Owners	One or more owners of the account. Enter this information in the form of a set of semicolon-delimited email addresses that authorize who might manage this cloud account. You can only add users that are in your organization. For example, my@company.com;abc@company.com
Tags	Custom tag pairs, denoted with the notation key=value. Multiple values might be set to the same key using a comma within the values (like key=value1,value2). Multiple tag pairs might be semicolon-delimited within the column to indicate multiple (like key1=value1;key2=value2). For example, ■ key=value ■ key=value1,value2 ■ key1=value1;key2=value2 ■ k1=v1,v2;k2=v3 For example, dept=eng;team=alpha Use tags to group the cloud accounts. You can search for these groups using the tag.

b Save the file in CSV format.

2 Import the file into VMware Discovery:

a Select **Manage > Cloud Accounts**.

b Click **Add New**, and select **Amazon Web Services**.

c Select **Add multiple accounts**, and click **Next**.

d Click **Next**.

e On the Import Accounts page, click **Browse** and locate the CSV file.

f Click **Import**.

The file is uploaded.

You can view the imported accounts on the Accounts page. You are notified if there are issues with any of the accounts. To fix any issues, click **View Details**, and follow the instructions.

How Do I Obtain an ARN

An Amazon Resource Name (ARN) is a unique identifier for an individual AWS resource. You need an ARN to set up an AWS account with an IAM user in VMware Discovery.

During this procedure, you work with both VMware Discovery and AWS simultaneously to create a policy and a new IAM role in AWS. You might find it easier to follow the procedure if you open VMware Discovery and AWS in two different tabs of the same browser. This way you can switch between the two applications and copy the required values from one application to another.

Procedure

1 Create a policy to attach to the IAM role in AWS.

a Log in to the AWS Console as a user with permissions to create an IAM role.

b Select **Services > IAM**.

c Select **Policies** and click **Create Policy**.

d Click the **JSON** tab.

e In VMware Discovery, click **Copy** underneath the policy.

f In AWS, copy the policy into the space provided in the **JSON** tab.

g Click **Review Policy**, and enter a name.

h Click **Create Policy**.

2 Create an IAM role in AWS.

a Select **Roles** from the menu on the left, and click **Create role**.

b Click **Another AWS account**.

c In VMware Discovery, click **Copy** next to the Account ID.

d In AWS, copy the Account ID into the Account ID text box.

e In VMware Discovery, click **Copy** next to the External ID.

f In AWS, select the check box next to Require external ID, copy in the external ID, and click **Next: Permissions**.

g Search for the policy you created, select the check box next to the policy, and click **Next: Review**.

h On the Create role page, enter a name and a description for the role, and click **Create Role**.

3 Copy the role ARN to the clipboard.

a Click the role, and view the summary information. The role ARN is displayed at the top of the summary.

b Copy the role ARN to the clipboard.

Add an AWS Account with an IAM User

If you have access to your AWS security credentials, you can create your public cloud account in VMware Cloud services.

Prerequisites

Make sure that the following permissions have been set in your AWS account to ensure that the account works correctly with VMware Cloud services.

- AmazonEC2ReadOnlyAccess, to collect data on Amazon Elastic Block Store (EBS) blocks and computes.
- AmazonVPCReadOnlyAccess, to collect data on a Virtual Private Cloud (VPC)
- CloudWatchLogsReadOnlyAccess, to collect metrics from AWS

Make sure that you have your AWS security credentials available. AWS security credentials consist of the access key ID and secret key associated with your AWS account. If you did not make a note of these credentials when you set up your account, you can create new credentials. See How Do I Create AWS Security Credentials

Procedure

1 Sign in to VMware Discovery.

- If you are adding a cloud account for the first time, the list of cloud account types that you can create is displayed.
- If you have already added a cloud account, select **Manage > Cloud Accounts**, and click **Add New**.

2 Select **Amazon Web Services**.

3 Select **IAM User**, and click **Next**.

4 Enter your access key ID and your secret access key, and click validate to verify your credentials.

5 To help you identify this account, enter a nickname, and click **Add**.

You can view a summary of the account resources on the Summary page.

6 To edit the account, click **Manage > Cloud Account**, and click the account nickname.

How Do I Create AWS Security Credentials

You create AWS security credentials when you set up your AWS account with an IAM user in AWS. You need these security credentials to set up your AWS account in VMware Discovery.

AWS security credentials consist of the access key ID and secret key associated with your AWS account. If you did not make a note of these credentials when you set up your account, you can create new credentials.

For more information on AWS security credentials, see http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html.

Procedure

1. Sign in to your AWS account at https://console.aws.amazon.com.
2. Click **Services > IAM**.
3. Select **Create Individual IAM Users**.
4. Click **Manage Users** and select a user with administrative permissions whose credentials you want to generate.
5. Select **Security credentials** and click **Create access key**.

   If there are already two pairs of security credentials, delete one. AWS only allows two.
6. Download the CSV file that contains your credentials, or click **Show** to display the secret access key and copy the credentials.

   Do not delete these security credentials in AWS. They are the identifier that allows AWS and VMware Cloud services to share data.

Working with Azure Accounts in VMware Cloud Services

3

You can add two kinds of Azure public cloud accounts in VMware Cloud services. An individual account which contains inventory data with minimal resources and billing, and an Enterprise account which contains inventory data with extensive resources and billing.

You add an Azure account with VMware Discovery because you do not need to generate or display billing information. You set up an Azure Enterprise account with VMware Cost Insight because billing and cost data is important features of this kind of account.

This chapter includes the following topics:

How Do I Add an Azure Account

You add an Azure account to VMware Cloud services with VMware Discovery because you do not need to generate or display billing information.

Before you add your Azure account, refer to this check list to identify the tasks you must perform to set up your account before you add it to VMware Cloud services.

To	Do this
☑ Make sure that your account has been set up correctly.	VMware Cloud services set the scope of an Azure account on an application-by-application basis. Your account must be set up with a Microsoft Active Directory application and have the required permissions set for it. For more information, see https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-create-service-principal-portal. You can check your account at https://account.azure.com/Home/Index. To view the details of your subscription, click **Account Center** and select the name of your Azure individual account. To see the services and resources set up in your account, click **Portal**.
☑ Collect Keys and IDs	To add your Azure account to VMware Cloud services, you need the following keys and IDs. ■ Subscription ID. Allows you access to your Azure subscriptions. ■ Client Application ID. Provides access to Microsoft Active Directory in your Azure individual account. ■ Client Application Secret Key. The unique secret key generated to pair with your Client Application ID. ■ Tenant ID. The authorization endpoint for the Active Directory applications you create in your Azure account. For information about how to collect these keys and IDs, see Locate Your Azure Account Credentials.
☑ Add your Azure account to VMware Cloud services.	Establish a connection between your Azure account and VMware Cloud services. See, Add an Azure Account.

Locate Your Azure Account Credentials

You need the security credentials associated with your Azure account to add the account to VMware Cloud service. These include your Subscription ID, Tenant ID, Client Application ID, and Client Application Secret Key. You can locate these credentials in your Azure account.

Procedure

1 Sign in to your Azure account at https://account.azure.com, open the Billing page, and make a note of your Subscription ID.

The Subscription ID is a combination of 32 alphanumeric characters.

2 Perform the following steps to locate your Tenant ID.

a In the upper right of the Azure portal, click the **Help** icon.

b Click **Show diagnostics**.

The PortalDiagnostics JSON file is downloaded.

c Open the JSON file and scan for the tenants block to find the 32-digit Tenant ID.

3 Perform the following steps to find your Client Application ID.

   a On the navigation bar of the Azure account portal, select **Azure Active Directory**.

   b Click **App Registrations**.

   c Look for your application in the list of registered applications. The Client Application ID is located in the right column.

4 Perform the following to generate a Client Application Secret Key.

   a In the Display Name column, click the name of your application.

   b Click **All settings**.

   c On the Settings page, select **Keys** under the API Access section.

   d Enter a description and an expiration for your application.

   e Click **Save**.

   The value of the Client Application Secret Key is displayed.

Add an Azure Account

When you add your individual Azure account to VMware Cloud services, you can view its resources in VMware Discovery.

Procedure

1 Access VMware Discovery.

   - If you are adding a cloud account for the first time, the list of account types you can add is displayed.
   - If you have already added a cloud account, select **Manage > Cloud Accounts**, and click **Add New**.

2 Select **Microsoft Azure**.

3 Enter the security credentials and application information for your Azure account, and click **Validate**.

4 To help you identify this account, enter a nickname, and click **Add**.

   To see the resources in your account and use filtering to display specific resources, click **Resources** in the left column.

You can view Azure resources on the Summary page. To edit the account, click **Manage > Cloud Account**, and click the account nickname.

How Do I Add an Azure Enterprise Account

You add an Azure Enterprise account to VMware Cloud services with VMware Cost Insight so that you can view billing and cost data.

Refer to this check list to identify the tasks you must perform to set up your Azure account and collect the required credentials before you add it to VMware Cloud services.

To	Do this
☑ Make sure that your account has been set up correctly.	VMware Cloud services set the scope of an Azure account on an application-by-application basis. Your account must be set up with a Microsoft Active Directory application and have the required permissions set for it. For more information, see https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-create-service-principal-portal. You can check your account at https://account.azure.com/Home/Index. To view the details of your subscription, click **Account Center** and select the name of your Azure individual account. To see the services and resources set up in your account, click **Portal**.
☑ Collect Keys and IDs	To add your Azure EA account to VMware Cloud services, you need the following keys and IDs. ■ Enrollment ID. Indicates the master account used for Enterprise billing. ■ API Access Key. Allows access to the Azure Billing API. For information about how to collect these keys and IDs, see, Locate Azure Enterprise Credentials.
☑ Add your Azure Enterprise account to VMware Cloud services.	Establish a connection between your Azure account and VMware Cloud services. See, Add an Azure Enterprise Account.

Locate Azure Enterprise Credentials

You need the Enrollment ID and API access key associated with your Azure Enterprise account to add the account to VMware Cloud service. You can locate these credentials in your Azure Enterprise account.

The Enrollment ID and API access key are available only to your account's enterprise administrator, the top-level administrator of your Azure Enterprise account.

Procedure

1 Log in to your Azure Enterprise account at https://ea.azure.com.

2 Locate your Enrollment ID.

   a Click the **Enrollment** tab, then click **Manage**.

   b Locate the Enrollment Number in the list of enrollment details.

   c Copy the Enrollment Number and save it for later use.

3 Generate an API access key.

   a Under the **Enrollment** tab, click **Reports**.

   b Click **Download Usage**.

   c Click **API Access Key**.

d Click the key icon in the **Primary Key** text box to generate the API access key.

e Copy the entire API access key string into a text file, and save the file.

Add an Azure Enterprise Account

You add an Azure Enterprise account in VMware Cost Insight.

Prerequisites

Make sure that your Azure Enterprise account has been set up correctly, and you have your Enrollment ID and API access key available. See How Do I Add an Azure Enterprise Account.

Procedure

1. In VMware Cost Insight, click **Manage > Cloud Accounts**, and click **Add New**.
2. Click **Microsoft Azure**.
3. Enter your credentials for your Azure Enterprise account, and click **Validate**.
4. To help you identify this account, enter a nickname, and click **Add**.

Working with vCenter Accounts in VMware Cloud Services

4

You can add one or more vCenter private cloud accounts, each of which contains one or more vCenter Servers to VMware Cloud services. These accounts allow you to retrieve information about your infrastructure inventory.

Before you add your account, refer to this check list to ensure that your vCenter environment is set up correctly, and that you have collected the security credentials required to add the account to VMware Cloud services.

Do this	
☑ Verify that your vCenter Server meets certain requirements.	■ Must be version 5.5 or later ■ Must have 4 vCPU, 8 GB RAM, and 80 GB of storage available. ■ Has outbound Internet access without any corporate firewall blocks. For example, on port 443, HTTPS.
☑ Verify that the vSphere Web Client is installed in your environment.	
☑ Create an administrative user with the correct permissions to access your vCenter Server private cloud account from VMware Cloud services.	
☑ If your vCenter Server private network does not use DHCP, you must gather certain information before you deploy a data collector and set up your private cloud account with VMware Cloud services.	Without this information, VMware's network cannot connect with your network to finish the configuration process. ■ Default Gateway ■ Domain Name ■ Domain Name Servers ■ Domain Search Path ■ Network IP Address ■ Network 1 Netmask

Do this	

☑ Ensure you have the vCenter user role and privileges correctly configured.	The role should be a vCenter server read-only role, with the following privileges selected:
	■ Profile-driven storage
	  ■ Profile-driven storage update
	  ■ Profile-driven storage view
	■ Storage views
	  ■ Configure service
	  ■ View

☑ Download and deploy a data collector	The first time you add a private cloud account to VMware Cloud services, you are prompted to add a data collector. For more information, see Deploy a Data Collector for a vCenter Server Cloud Account.

This chapter includes the following topics:

Deploy a Data Collector for a vCenter Server Cloud Account

The first time you add a private cloud account, VMware Discovery prompts you to add a data collector.

You can deploy as many data collectors as you want, one for each vCenter Server. To link your vCenter Servers to the same private cloud and gather information from them all, give each vCenter Server the same private cloud name.

You can also deploy a data collector in VMware Cost Insight and VMware Network Insight. The data collector that you download for use in VMware Network Insight is different from the data collector you deploy in VMware Cost Insight and VMware Discovery.

Procedure

1. Sign in to VMware Discovery and click **Manage > Data Collectors**.

   You can also perform this step in VMware Cost Insight.
2. Click **Add New**.
3. Click **Download**.
4. Navigate to your vSphere Web Client data center, click the name of your vCenter cluster, and select **Deploy OVF Template**.

5 In the Deploy OVF Template form, perform the following actions.

   a Click **Select template**, then **URL**. Paste in the path to the OVA data collector file you downloaded. Click **Next**.

      If you have already installed a data collector to your vCenter and are reinstalling it, click **Local file** and then **Next**.

      If you see a warning message that informs you that the specified Photon operating system is not support, click **Yes** and proceed.

   b Click **Select name and location**, then enter the name of your OVA file. Select the cluster where you want to install the data collector, and click **Next**.

   c Click **Select a resource** and the cluster where you want to run the data collector, and then click **Next**.

   d Review the details of your data collector deployment. Notice the **Size on disk** text box. The location where you deploy the data collector in the following steps must have enough space available. Click **Next**.

   e **Accept** the License Agreement. Click **Next**.

   f Click **Select storage** and select a datastore from the list with enough free space for the OVA file. Click **Next**.

   g Click **Select networks** and select a destination network, and then click **Next**.

   h Click **Customize template** and enter the required information. Do not click **Next**.

      - For **Name of the Remote Data Collector**, use the name of the OVA file.
      - For **Root User Password**, choose a unique password. It does not need to match the vCenter password.

   i Return to VMware Cloud services and collect the token key provided by VMware Discovery on the Setup a Data Collector Virtual Appliance form. Click **Copy** to copy the key.

   j When you see the Copied message, return to the vCenter **Customize template** form and paste the token key into the **VMware Cloud Services One-Time Token** text box. Do not click **Next**.

   k Click **Networking Properties**. If you use DHCP in your vCenter network, do not enter any information. If you do not use DHCP, then you must provide information for each setting. Click **Next**.

   l Click **Ready to complete** and review your configuration data. Click **Finish**.

      The data collector is installed into your vSphere Web Client.

6 Return to the vSphere Web Client to run the data collector.

   When you run the OVA file in the vSphere Web Client, the data collector works with the vCenter Server to push data to the VMware Cloud services.

7 If the data collector is not running when you return to your vSphere Web Client, click the **green arrow** at the top of your page.

8 To verify that your data collector is running, look under the **VMs** tab at the list of your virtual machines to ensure it is **Powered On**.

9 In VMware Discovery, wait for a connection to be made with your vSphere Web Client, and click **Next**.

It might take several minutes until a connection is made.

10 To upgrade an existing data collector, you must reboot the remote data collector VA.

Delete a Data Collector

If you no longer need a data collector and want to free up space, you can delete it from the vCenter Server.

Procedure

1 Log in to the vCenter Server as an administrator.

2 Navigate to the data collector that you have deployed.

3 Right-click the data collector virtual machine and select **All vCenter Actions > Delete from Disk**.

4 Click **OK**.

Add a vCenter Account

When you have deployed a data collector, you can add one or more private cloud accounts in VMware Cloud services.

Procedure

1 Sign in to VMware Discovery.

- If you are adding a cloud account for the first time, the list of cloud account types is displayed.
- If you have already added a cloud account, select **Manage > Cloud Accounts**, and click **Add New**.

2 Click **vCenter**.

3 Select the name of the data collector you deployed to the vCenter Server.

4 Enter the fully qualified domain name for your vCenter Server.

5 Enter the user name and password you used to access the vCenter Server.

6 To help you identify this account, enter a nickname, and then click **Add**.

You can view vCenter resources on the Summary page.

7 To edit the account, click **Manage > Cloud Accounts** and click the account nickname.