Using VMware Discovery

VMware Discovery services

vmware®

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

https://docs.vmware.com/

The VMware Web site also provides the latest product updates.

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

Discovery Service

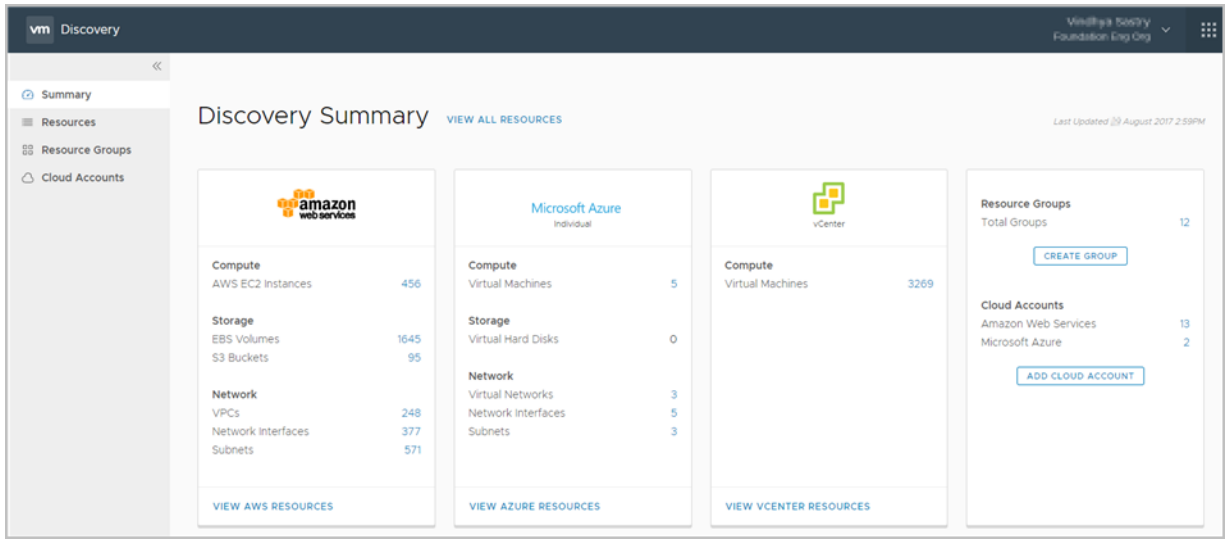
1

VMware Cloud services supports public cloud accounts, such as Amazon Web Services (AWS), Microsoft Azure, and also private cloud accounts, such as VMware vCenter Server.

The Discovery service is used to "discover" resources associated with public and private cloud accounts. Discovery allows a user to see specific information about cloud resources. These include:

- Cloud types
- Virtual machines
- Storage units
- IP addresses
- Network interfaces
- Subnets
- Virtual networks
- S3 buckets

Choose **Dashboard** to see a summary of your current cloud accounts and groups. From the Discovery Summary screen, you can add a new cloud account, create a new group, or view resources for a specific cloud account, such as AWS, Azure, or vCenter Server.



Choose **Resources** to view the resources in your VMware Cloud services account. You can use filtering to display specific resources, and use wildcards and operands to drill down further. For example, you can search for a specific kind of resource, like all virtual machines, or search for resources that contain a similar name or string.

Choose **Resource Groups** to see a list of your groups or to create a new group. Creating a group allows you to use filtering to define specific resources you can view again, then assign them a unique name. Next time you want to view those resources, you simply click on the name of the group. This is an easy way to view selected resources again and again.

Choose **Cloud Accounts** to see your public and private cloud accounts. To add a new public or private account, click **Add New**. To see more information about a specific account in your list, click the account name to display Account Details.

Adding an AWS Account 2

To add an AWS public cloud account in VMware Cloud services, you need your AWS security credentials (Access Key ID and Secret Access Key) and your S3 bucket name. You also need to set billing access and the correct permissions for IAM users in your account.

Amazon recommends specific best practices for setting up IAM users and security credentials. For more information on these recommendations, see https://media.amazonwebservices.com/AWS_Cloud_Best_Practices.pdf.

This chapter includes the following topics:

Overview

VMware Cloud services provides a sophisticated set of tools for managing and tracking the hardware and software resources in your AWS cloud account, and your billing data. Registering your AWS account with VMware Cloud services gives you the tools to maximize your resource usage and analyze your cloud expenses for the best returns.

You can register the following kinds of accounts with VMware Cloud services :

- Individual AWS account
- AWS Organization master account
- Member account (also known as a "linked" account, inside a AWS Organization master account)

An individual AWS account is set up with a single user. Billing is driven through a single S3 bucket and permissions can be set on any users you choose to add to the account.

For a large organization, such as a business, a better structure is an AWS Organization master account. An AWS Organization master account allows you to set up many individual member (linked) accounts, but consolidates your billing in a single S3 bucket. This gives your organization the flexibility it needs across departments and teams, while still allowing close control over your billing data.

Providing Access to Your VMware Cloud services Account

When you register your AWS public cloud account with VMware Cloud services, you establish a connection between the two accounts. This connection allows information about your AWS resources and billing to be shared, analyzed, and updated in real time inside VMware Cloud services.

To ensure a smooth connection, do the following in your AWS account before you register it with VMware Cloud services.

- Grant IAM users and roles access to your AWS billing information. Not doing this may cause the free flow of billing information to be blocked. See "Setting Up an Individual AWS Account," on page 11.
- Collect security credentials for your AWS account (Access Key ID and Secret Access Key). You need these credentials to validate the connection between your AWS account and VMware Cloud services. See "Collecting Your AWS Security Credentials," on page 10.
- Create an S3 bucket. The S3 bucket is used for billing in an individual account and for consolidated billing in an AWS Organization master account. See "Creating Amazon Security Credentials and an S3 Bucket," on page 11.
- Assign specific permissions to users, to allow them access to VMware Cloud services. In an AWS Organization master account, define policies that allow usage data from member accounts to be collected in VMware Cloud services. See "Setting Permissions in AWS," on page 12.

Entering Your AWS Cloud Credentials

The credentials you need for your AWS cloud account are your security credentials (Access Key ID and Secret Access Key) and the S3 Bucket name of your billing account. If you have these credentials with you, you can quickly get registered with VMware Cloud services by filling in the AWS Add New Account form.

Your Security Credentials

The AWS security credentials you need are your 20-digit Access Key ID and its corresponding Secret Access Key. (You can find these in the .csv file you saved when you generated the credentials.)

The following are example credentials:

- Access Key ID: ASDFKWELN48205JHW0W03
- Secret Access Key: j51+LMwCMnPtna/v+ASDFQ7228copQQQ/i0reX11

If you don't have your Access Key ID and Secret Access Key in front of you, you can quickly get them from your AWS account. See "Collecting Your AWS Security Credentials," on page 10.

Your S3 Bucket Name

Your S3 Bucket name can be any name you choose. (For example, my-unique-s3-bucket.) It must meet only two standards :

- It must be unique to all accounts in the AWS namespace, not just your own account.
- It must meet DNS standards for naming. For example, it must be all lower case and separators must be dashes, not underscores.

If you don't have your S3 Bucket name in front of you, you can quickly get it from your AWS account. See "Collecting Your S3 Bucket Name," on page 10.

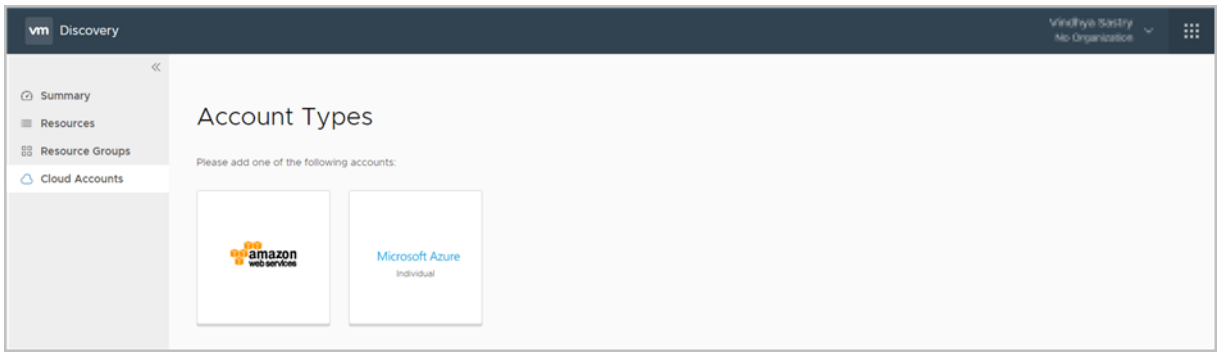
Fill In the AWS Add New Account Form

If you're ready to go with your AWS security credentials and S3 bucket name, go ahead and create your public cloud account in VMware Cloud services.

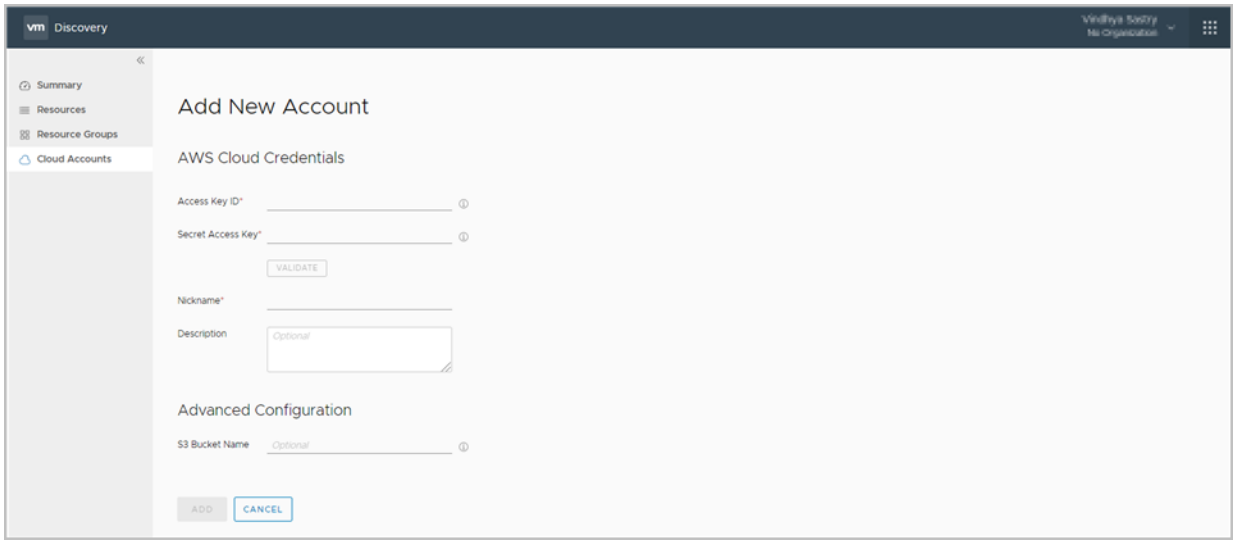
Procedure

1 Navigate to the VMware Cloud services Discovery page.

2 Select **Cloud Accounts**, click **Add New** and select **Amazon Web Services**.



3 Perform the following steps on the AWS Add New Account page:



a Enter your AWS Access Key ID and Secret Access Key.

b Click **Validate** to verify your security credentials.

c When your credentials have been validated, enter a **Nickname** and **Description** to help you identify this account.

d If you are setting up this account for individual or master organization account billing, enter the **S3 Bucket Name** you want to use for your billing reports.

e Click **Add**.

To add another AWS account to VMware Cloud services, click **Add Another Cloud**, or click **Next** to view the resources in your account.

Collecting Your AWS Security Credentials

If you don't have your AWS security credentials (Access Key ID and Secret Access Key) ready to go, here is how you can quickly get them from your AWS account.

To Get Your Security Credentials

Follow the steps below to create new security credentials. (AWS makes it easy to generate new security credentials and difficult to retrieve them if you don't already have them.)

Procedure

1 Log into your AWS console (https://console.aws.amazon.com). Navigate to **Services**, then select the **IAM** service.

2 On the Welcome to Identity and Access Management screen, select **Create Individual IAM Users**.

3 Click **Manage Users**. When the list of user names is displayed, click the name of the user whose credentials you want to generate. (Following AWS best practices, this should be an IAM user with Admin permissions.)

4 On the Summary screen, select **Security credentials** and click Create access key. (If there are already two pairs of security credentials, delete one. AWS only allows two.)

5 From the Create Access Key screen, click **Show** to make note of the Secret Access Key. Download the **.csv** file.

6 Go back to VMware Cloud services and add the AWS security credentials into the AWS Add New Account form. See "Fill In the AWS Add New Account Form," on page 9.

Note: Once you have used your AWS security credentials to register your AWS account with VMware Cloud services, do *not* delete them in AWS. Your AWS security credentials are the identifier that allows the two products to share data in the cloud.

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

Collecting Your S3 Bucket Name

If your S3 bucket is already set up in your AWS account, it is easy to collect the S3 bucket name.

Procedure

1 Log into the AWS console (https://console.aws.amazon.com). Navigate to **Services**, then select the **S3** service.

2 This opens the Amazon S3 bucket page. Your existing S3 bucket name is displayed in the Bucket Name list.

When you find the name of your S3 bucket, enter it into the AWS Add New Account form. See "Fill In the AWS Add New Account Form," on page 9.

For more information on Amazon S3 buckets, see http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/billing-reports.html.

Setting Up an Individual AWS Account

The following instructions walk you through basic setup in your AWS account. You should have done these things already, so you are ready to go with VMware Cloud services. However, if you need more complete instructions, you can get them here.

Prerequisites

You do not need to create an S3 bucket and set up billing for the resources in your AWS account to be listed in the Discovery service. However, if you plan to capture billing data in your AWS account, configure your IAM user setting first.

Procedure

1 Login to your Amazon account console at https://console.aws.amazon.com.

2 Go to the name of your AWS account in the top right of the console and select **My Account**.

3 Scroll down until you see **IAM User and Role Access to Billing Information**.

4 Click **Edit**. Then select **Activate IAM Access** and click **Update**.

Once you've set this option in your account, it remains turned on and you don't need to do it again.

Creating Amazon Security Credentials and an S3 Bucket

If you need to create an S3 bucket for billing in your AWS account, this is how you do it. Once an S3 bucket is setup in AWS, you can carry your billing data over into VMware Cloud services.

Prerequisites

The process for creating new AWS security credentials (Access Key ID and Secret Access Key) is same as collecting your credentials. For more information, see "Collecting Your AWS Security Credentials," on page 10.

To create a new S3 Bucket:

Procedure

1 Log into the AWS console (https://console.aws.amazon.com). Navigate to **Services**, then select the **S3** service.

2 This opens the Amazon S3 bucket page.

3 Select **Create Bucket**.

4 Enter a valid DNS-compliant bucket name and click **Create**. (Amazon has specific rules for creating a valid bucket name. For more information on DNS naming requirements, see http://docs.aws.amazon.com/AmazonS3/latest/dev//BucketRestrictions.html#bucketnamingrules.)

   This creates the S3 bucket name you have defined. Click **Next** to continue.

5 Click on your account name from the top menu and select **My Account**.

   The Billing Management Console opens in a new tab.

6 Click **Preferences** in the left hand column and perform the following steps:

   a Select the **Receive Billing Reports** option.

   b Click the **Sample Policy** link, and copy the policy content to the clipboard.

   c Click **Close**.

7 Navigate back to the S3 management console by clicking **Services > S3** in the Amazon menu.

8 Select the name of the bucket you created and perform the following on the S3 Management Console.

   a Click the **Permissions** tab and then click the **Bucket Policy** tab.

   b Paste the sample policy text you copied to the clipboard into the Bucket Policy Editor.

   c Click **Save**.

9 Return to the Billing Management Console by clicking on your account name and selecting **My Account > Preferences** window, and perform the following:

   a Click **Verify**. You see the Valid Bucket message.

   b Under **Report**, select **Detailed billing report with resources and tags**.

   c Click **Save Preferences**.

For more information on working with Amazon S3 buckets, see http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/billing-reports.html.

Setting Permissions in AWS

To ensure correct access to VMware Cloud services for users in your AWS account, you must assign them specific permissions.

The following are the minimum AWS permissions needed to work correctly with VMware Cloud services. You assign these permissions to users in an individual account and in a master organization account.

- **AmazonEC2ReadOnlyAccess** - Allows a user to collect data on Amazon Elastic Block Store (EBS) blocks and computes
- **AmazonS3ReadOnlyAccess** - Allows a user to collect data on S3 buckets
- **AmazonVPCReadOnlyAccess** - Allows a user to collect data on a Virtual Private Cloud (VPC)
- **CloudWatchLogsReadOnlyAccess** - Allows a user to collect metrics from AWS

For more information on permissions in AWS, see http://docs.aws.amazon.com/organizations/latest/userguide/orgs_permissions_overview.html.

Setting Up a Master Organization Account

In a large organization, such as a business, there can be good reasons to have independent AWS accounts, to better track projects across business units. However, bills and accounting reports may still need to be consolidated in one place. To solve this problem, AWS created Master Organization accounts.

There are two ways to set up member accounts (also known as linked accounts) in a master organization account:

- Create a new member account inside your master account. Each new member account can have its own users, groups, resources, and permissions, but the billing for it is consolidated in the S3 bucket of the master organization account.
- Invite an already existing, independent AWS account into your master organization account. Upon acceptance of the invitation, the billing for the invited account is consolidated into the S3 bucket of the master organization account.

AWS allows you to have up to 20 member accounts. For more information on how master organization accounts can be set up, see http://docs.aws.amazon.com/organizations/latest/userguide/orgs_getting-started_concepts.html.

If you want the resources in your member accounts (for example, virtual machines, data storage, CPU processing, network routing, and more) to be listed in the Discovery Service, you must add each member account individually to VMware Cloud services. This means you must:

- Generate unique security credentials (Access Key ID and Secret Access Key) for each member account. See "Collecting Your AWS Security Credentials," on page 10.
- Add the unique security credentials for each member account to VMware Cloud services using the AWS Add New Account form. See "Fill In the AWS Add New Account Form," on page 9.
- Set **IAM User Access to Billing Information** in the IAM Management console. For more information, see "Setting Up an Individual AWS Account," on page 11.

Creating a Master Organization Account

If you have an AWS individual account with an S3 bucket, you can use it as the starting point for creating your AWS Master Organization account.

Prerequisites

Do the following to make it easy to set up multiple member accounts in your master organization account:

- Make a list of the teams in your company that need their own member accounts.
- Decide the owner for each new member account. Collect basic information, such as the owners email address, which can be used as the login identifier for the new account.
- If you haven't already done so, set the **IAM User and Role Access to Billing Information** setting in your AWS account. See "Setting Up an Individual AWS Account," on page 11.

For more information on AWS Organization master accounts, see http://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_create.html.

Procedure

1. Go to the AWS Organizations console at https://console.aws.amazon.com/organizations.
2. Login using the account credentials for your individual account.
3. Click **Create Organization**.
4. Select **Enable All Features** and click **Create organization**.

   This displays the newly created AWS Organization master account. It contains useful information, including the owner's email address and the Account ID.

Adding a New Member Account

The big advantage of creating a new member account inside your master organization account is to consolidate billing for all member accounts in one place, your master S3 bucket.

Prerequisites

You must have a AWS Organization master account set up.

Procedure

1. Go to the AWS Organizations console at https://console.aws.amazon.com/organizations.
2. Login using the credentials for the master organization account.
3. On the AWS Organizations page, click **Add Account**.

4 Select **Create Account**. Enter the required details and click **Create**.

The owner of the AWS Organization master account (listed under Account Name) has administrator privileges for all new member accounts. The owner of the new member account (listed under Email) has administrator privileges only for the new member account.

Setting a Password for a New Member Account

Before the new member account can be used, the owner of the new member account must set a password for it.

Procedure

1 Go to the AWS IAM console at https://console.aws.amazon.com/iam.

2 Do the following:

a Type in the new owner's email address.

b Select the **I am a new user** option.

c Click the **Forgot your password?** link.

3 In the Password Assistance form, enter the owner's email address and security characters, and click **Continue**.

4 Check your email for a message instructing you how to reset the password on your account and click the password reset link.

5 On the Amazon Password Assistance page, create a new password for the new member account and click **Save changes**.

6 Go to the AWS IAM console (https://console.aws.amazon.com/iam) and perform the following:

a Enter your new member account email address.

b Select the **I am a returning user and my password is** option.

c Enter the new password.

d Click **Sign in using our secure server**.

All billing charges for the new member account are consolidated in the AWS Organization master S3 bucket.

You can create a new member account by inviting an existing AWS account into your master organization account. For information on how to do this, see http://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_accounts_invites.html.

Setting a Policy for a New Member Account

In order for the resources in a new member account to be correctly inventoried in VMware Cloud services, you must assign the following JSON policy to each of the new member accounts you add to your AWS Organization master account.

Prerequisites

Once you've assigned this JSON policy to a new member account, you must enter the AWS security credentials for that account into the AWS Add New Account form.

Since the billing for all new member accounts are consolidated in the S3 bucket you set up when you created the AWS Organization master account, you only need to enter the security credentials for each new member account, not the S3 bucket name. For more information on how to add the new Member account security credentials to VMware Cloud services, see "Fill In the AWS Add New Account Form," on page 9.

Procedure

1 Log into the AWS console (https://console.aws.amazon.com) and select the IAM service.

2 On the Welcome to Identity and Access Management screen and select **Policies**, then **Create policy**.

3 On the Create Policy page, select **Create Your Own Policy**.

4 On the Review Policy page, copy or enter the following JSON policy into the blank **Policy Document**.

```
{
            "Version": "2012-10-17",
            "Statement": [
            {
            "Effect": "Allow",
            "Action": [
            "iam:ListAccountAliases"
               ],
            "Resource": [
             "*"
            ]
            },
            {
            "Effect": "Allow",
            "Action": [
            "ec2:Describe*"
            ],
            "Resource": "*"
            },
            {
            "Action": [
            "logs:Describe*",
            "logs:Get*",
            "logs:TestMetricFilter",
               "logs:FilterLogEvents"
            ],
               "Effect": "Allow",
            "Resource": "*"
            }
            ]
            }
```

5 Enter a **Policy Name** and an optional **Description**. Click **Create Policy**.

6 In the IAM console, select **Roles**. Click **Create new role**.

7 On the Select role type screen, select **Amazon EC2**.

8 On the Attach Policy screen, enter the policy name in the search box.

9 Select the Policy name and click **Next step**.

10 On the Set role name and review page, enter a **Role Name** and click **Create role**. This adds the new role to your list of roles.

11 On the AWS console, select **Users**, then **Add user**.

12 Enter a **User name**. Select **Access type** and **Programmatic Access**. This allows you to create an Access Key ID and Secret Access Key for your account. Click **Next: Permissions**.

13 On the Set permissions page, select **Attach existing policies directly**.

14 Search for the name of the policy you want to attach. Select the **Policy name** and click **Next: Review**.

15 When you have reviewed the user and policy you have assigned, click **Create user**.

16 You see the Success form and the **Access Key ID** and **Secret Access Key** for the user you created. Click **Download .csv** to save these security credentials to a file. Once you click Close on this screen, you are not able to display your Secret Access Key again.

17 Copy the **Access Key ID** and **Secret Access Key** into the Discovery service Add New Account form to register the new member account withVMware Cloud services. See "Fill In the AWS Add New Account Form," on page 9.

Once you're registered the new member account with VMware Cloud services, you've enabled the Discovery service to find, sort, filter, group, and display the resources you create in this new account.

Note: Do this procedure once for each new member account you create in your AWS Organization master account. This applies to both member and invited accounts.

Adding an Azure Account 3

VMware Cloud services supports two kinds of Azure public cloud accounts. An individual account contains inventory data with minimal resources and billing. An Enterprise account contains inventory data with extensive resources and billing.

An individual Azure account is set up through the Discovery service, as there is little need to generate or display billing information. An Azure Enterprise account is set up through the Cost Insight service, as billing and cost data are important features of this kind of account.

This chapter includes the following topics:

Before You Begin

Before you begin working with VMware Cloud services, you need to know several important IDs and keys. Security details are generated in your Azure account when it is configured.

For an individual Azure account, you need the following IDs and keys:

- **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 an Azure Enterprise Agreement (EA) account, you need the following IDs and keys:

- **Enrollment ID** - Indicates the master account used for Enterprise billing.
- **API Access Key** - Allows access to the Azure Billing API.

Setting Up an Individual Azure Account

You set up your individual Azure account first, then add your account to VMware Cloud services .

Prerequisites

Ensure that you have an Azure Individual account.

Procedure

1 Navigate to the Microsoft Azure portal at https://account.azure.com/Home/Index.

2 Click **Account Center** and click the name of your Azure individual account.

You see the details of your subscription.

3 To see the services and resources you've set up in your Azure individual account, click **Portal**.

Login to see your account information and your current subscriptions on the dashboard. For more information about your Azure individual account, see https://azure.microsoft.com/en-us/overview/what-is-azure.

Collect Your Individual Azure Account Information

Before you add your individual Azure account to VMware Cloud services, it's a good idea to collect the security credentials and account information you need first.

VMware Cloud services sets the scope of an individual Azure account on an application-by-application basis. So, 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.

Once you've ensured that your individual Azure account is correctly set up, here's what you do to collect the security credentials and other information you need to register it with VMware Cloud services.

Prerequisites

Procedure

1 Open the Azure Billing page (https://account.azure.com) on the Azure portal, and make a note of your **Subscription ID**.

Subscription ID is a combination of 32 alphanumeric characters that looks like *5c0ta9a0c-8r51-4aa8-af76-xxxxxxxxxx*.

2 Perform the following steps to find your **Tenant ID**.

a In the upper right of your Azure portal (https://portal.azure.com), click the **Help** icon.

b Click **Show diagnostics**.

This downloads the PortalDiagnostics JSON file.

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 Azure account portal, select **Azure Active Directory**.

b Click **App Registrations.** You see a list of registered applications.

c Look for your application in the list. The Client Application ID is in the right hand column.

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

a Click on the name of your application in the Display Name column.

You see the details 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**.

You see the value of the Client Application Secret Key.

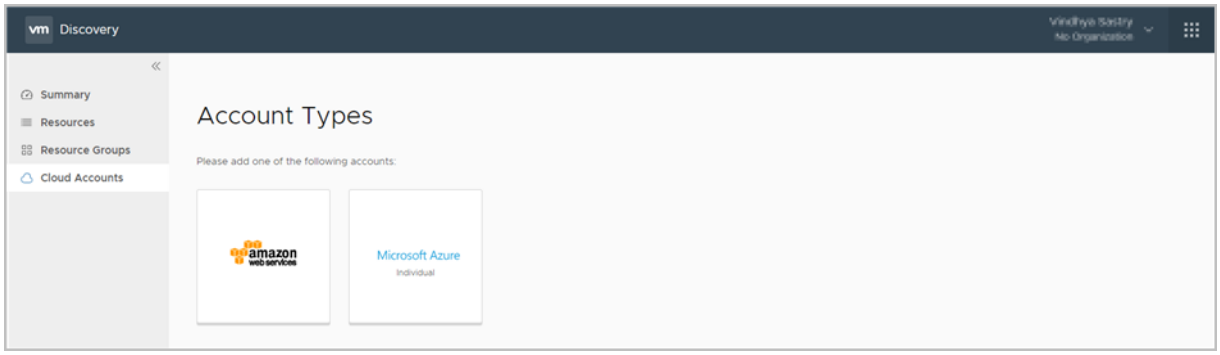
Fill In the Individual Azure Add New Account Form

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

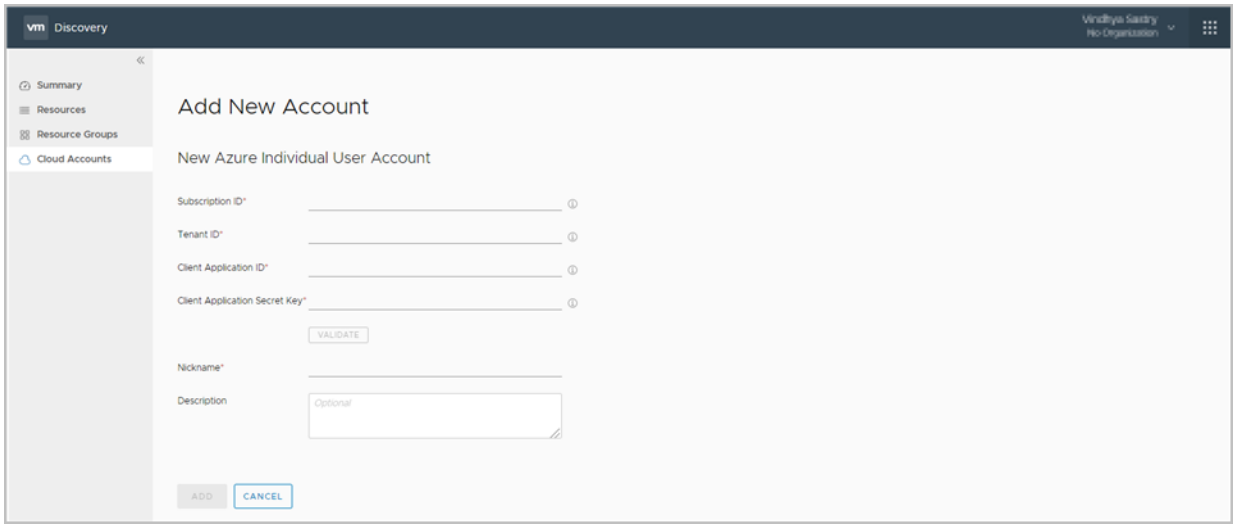
Procedure

1 Navigate to the VMware Cloud services Discovery page.

2 Select **Cloud Accounts**, click **Add New** and select **Microsoft Azure**.



3 Click **Add New** and select **Microsoft Azure** to display the Add New Account screen.



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

b Enter a nickname and a description for your account, and click **Add**.

Your new individual Azure account is displayed in the Discovery Accounts screen. To display details about your account, click the name of the account in the Accounts list. To see the resources in your account and use filtering to display specific resources, click **Resources** in the left column.

Setting Up an Azure Enterprise Account

A Microsoft Azure Enterprise Agreement (EA) account is intended for a large organization with many resources, such as hardware, applications, virtual machines, storage, network interfaces, subnets, billing, and more.

Microsoft Azure EA allows you to set up resources and billing across a wide variety of departments, subscriptions, accounts, and administrative roles. To effectively manage your Microsoft EA account in VMware Cloud services, you must be an Enterprise Administrator and understand the Azure EA ecosystem. As an Azure Enterprise Administrator, you login using the Azure Enterprise Account portal, https://ea.azure.com.

To manage accounts and subscriptions, you login using the Microsoft Azure portal, https://account.azure.com

For a detailed overview of Microsoft Azure EA, see https://docs.microsoft.com/en-us/azure/fundamentals-introduction-to-azure

For detailed information about Microsoft Azure EA, including deploying virtual machines, developing applications, managing databases, and using Microsoft tools, see the Azure documentation at https://docs.microsoft.com/en-us/azure.

Collect Your Azure Enterprise Account Details

Your Azure Enterprise account provides two credentials. You need these credentials to set up your account in VMware Cloud services.

Prerequisites

You need the following Azure Enterprise account credentials:

- **Enrollment ID** - The master account number used for all of your Azure Enterprise billing. (Called the Enrollment Number in Azure Enterprise.)
- **API Access Key** - Grants access to the Azure Billing API.

The Enrollment ID and API Access Key are available only to your account's Enterprise Administrator. The Enterprise Administrator is the top-level administrator of your Azure Enterprise account.

Procedure

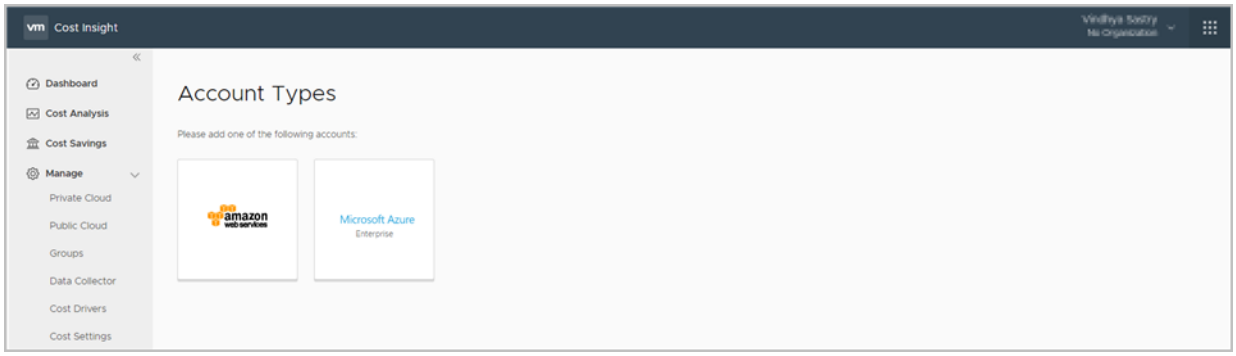
1. Login to your Azure Enterprise account at https://ea.azure.com.
2. Obtain your Enrollment ID (Enrollment Number).
   a. Click the **Enrollment** tab, then click **Manage**.
   b. Locate the Enrollment Number in the list of enrollment details.
   c. Copy the Enrollment Number and save it for later use.
3. Obtain your 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** field to generate the API Access Key.
   e. Copy and paste the entire API Access Key string (it is very long) into a text file and save it for later use.

Fill In the Azure Enterprise Add New Account Form

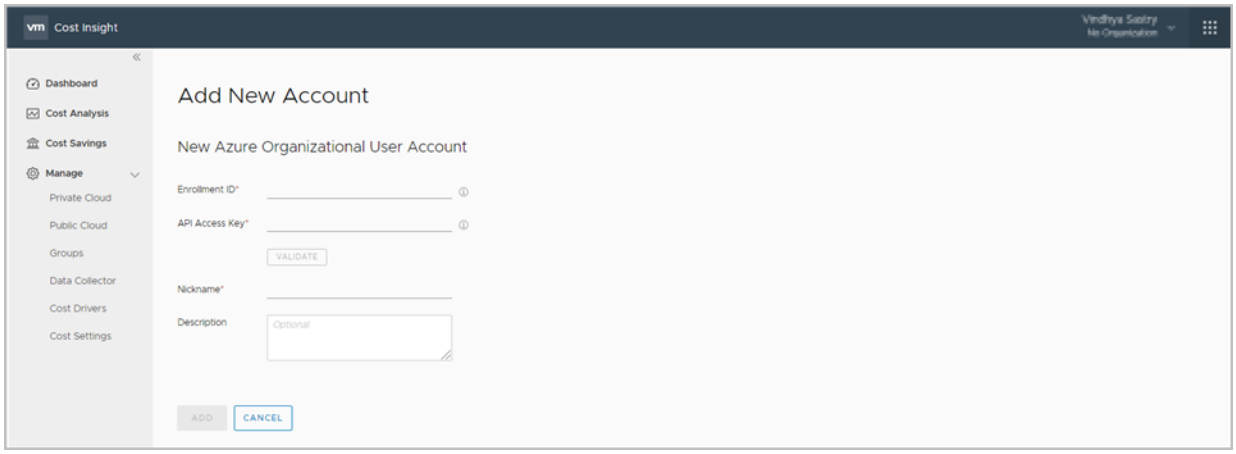
To add a new Azure Enterprise account, navigate to the Cost Insight service. To find the Cost Insight service from the Discovery service, click the box in the upper right of the Discovery screen.

Procedure

1 Navigate to the Cost Insight service and expand **Manage > Public Cloud**.



2 Click **Add New** and select **Microsoft Azure** to display the Add New Account form.



a Enter the required information and click **Validate**.

b Enter a nickname and a description for your account and click **Add**.

Your new Azure Enterprise account is registered in the Cost Insight service. To display details about your new account, click the name of the account in the Accounts screen.

Set Up Billing for an Azure Enterprise Account

The billing structure in a Microsoft Azure Enterprise account can vary from company to company, depending on the size of the organization, the number of departments it creates, the number of subscriptions assigned to each department, and other factors. Azure Enterprise makes it possible to consolidate all your billing in one place, giving your company fine-grained control over it's incoming and outgoing expenses.

Prerequisites

This section provides an overview of how you set up your Azure Enterprise account. Ensure that your Active Directory and Azure Enterprise accounts are correctly set up together. If they are, your billing and account information migrate seamlessly into VMware Cloud services.

Procedure

1. When your organization signs the Enterprise Account Agreement with Microsoft, the first thing you do is create an Enterprise Administrator.
   a. The Enterprise Administrator has permission to control everything in your Azure Enterprise account. This includes having access to your Enrollment ID.
   b. The Enterprise Administrator is the main point of contact in your organization for billing transactions and all other correspondence with Microsoft about your account.
   c. The Enterprise Administrator logs in to your Azure account at https://ea.azure.com.
   d. The Enterprise Administrator defines access to the other primary elements of your account: Departments, Accounts, and Subscriptions.
   e. To make managing Azure Enterprise easier, the Enterprise Administrator can create other Enterprise Administrators, with the same level of permissions and access to the account.
2. The Enterprise Administrator creates one (or more) departments to match the needs of your organization's business structure.
   a. There can be many independent departments inside your organization, each with its own structure, organization, and flow. Marketing, Finance, Sales, and Engineering are just a few of the possible departments your Enterprise Administrator can create.
3. The Enterprise Administrator creates one (or more) department administrators for each department.
   a. The Department Administrator has full permissions to create accounts in the department, set up cost centers, and view monthly usage and billing charges, but cannot access equivalent details about any other department.
4. The Department Administrator creates one (or more) accounts for each department and assigns an Account Owner to each account.
   a. The Account Owner keeps track of the account, including creating and managing subscriptions, updating and managing account details, and monitoring billing in any cost centers associated with the account.
   b. The Account Owner logs in to their Azure account at https://account.azure.com
5. The Enterprise Administrator gives the Account Owner access to the cost data for the department account.
   a. Access to the cost data for the department can only be granted by the Enterprise Administrator, who manages the cost data for the entire Azure Enterprise account.

6 The Account Owner creates one (or more) subscriptions in the department account to allocate and manage the department's resources and expenses.

   a Subscriptions are flexible and can be set up in multiple ways. There are no limits on the number of subscriptions that can be created to manage resources in an account. For example, every application - and all the teams creating it - can be linked to a single subscription in an engineering account. Or each development team working on an application can be linked to its own subscription instead.

   b The Account owner controls access to the billing information in the account subscriptions using role-based access. See https://docs.microsoft.com/en-us/azure/billing/billing-manage-access

   c The Account Owner can create as many subscriptions as needed, depending upon the needs, resources, and functions assigned to the account. For example, if an account includes a multinational engineering team with developers in several countries, there could be multiple subscriptions. In a smaller local company, there may be only a few.

   d Subscriptions can be created inside other subscriptions, to further allocate and manage resources, expenses, and personnel.

   e Billing associated with a specific subscription can be managed and tracked. Billing and expenses can be rolled up into a parent subscription, and then into the account itself using Cost Centers set up by the Account Owner.

   f The Account Owner creates, revises, updates, and removes subscriptions from the account as needed.

7 Additional granularity can be achieved by assigning tags to the cost and expense resources in your subscriptions and accounts. This tagging is used to monitor, collect, and manage expenses on specific resources.

   a For more information on using tagging with Microsoft Azure Enterprise resources, see https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags

   b Once granularity is set up at the lowest level of your Azure Enterprise account, the flow of billing information inside your Azure Enterprise account carries smoothly into VMware Cloud services.

For additional information on how to set up and manage billing in your Azure Enterprise account, see https://docs.microsoft.com/en-us/azure/billing/billing-getting-started.

Adding Account Resources to VMware Cloud Services

The top-level administrator in your Azure Enterprise account can create accounts at lower levels of your organization. Each of these accounts can have one or more subscriptions inside it. In order for the resources in each account (and the resources of its subscriptions) to be correctly inventoried in VMware Cloud services, each account must follow the procedure in this section.

To properly ensure that the resources of each subscription inside your account are inventoried correctly in VMware Cloud services, you must do the following.

Prerequisites

When an account is set up in Azure Enterprise, an account owner is assigned to it. The account owner becomes the administrator for that account. Like an individual account in Azure, an account set up inside Azure Enterprise gets a set of credentials that identify the account:

- **Subscription ID** - Grants access to your Azure subscriptions.
- **Tenant ID** - The authorization endpoint for the application you create in your account.

The administrator for an account can create subscriptions inside it. Each subscription acts like an individual account inside the account. But, each subscription does not get its own credentials. It uses the same credentials as the account where it is set up.

Procedure

1 The administrator of the account that contains the subscriptions must set permissions on the subscriptions so their resource data can be collected.

2 The best way to collect the data from the subscriptions is to write an application that collects this data. This is no different than writing an application inside an individual Azure account.

3 Azure assigns the following identifiers to the application you write for your subscriptions:

- **Client Application ID** - Identifies the application to Microsoft Active Directory.
- **Client Application Secret Key** - The unique secret key generated to pair with your Client Application ID.

4 Enter the four identifiers for your account and application into the Add New Account form of the Discovery service. For information on how to collect the identifiers, see "Collect Your Azure Enterprise Account Details," on page 20. For information on how to enter the identifiers into the Add New Account form, see "Fill In the Azure Enterprise Add New Account Form," on page 21.

5 Do steps 1-4 for every new account you create in your Azure Enterprise account. If you do not register each new account and its subscriptions with VMware Cloud services, the resources for the account are not listed in the Discovery service.

Adding a vCenter Account 4

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

Verify that your vCenter Server meets these requirements:

- Must be version 5.5 or later
- Must have 2GB RAM and 10 GB of storage available.

This chapter includes the following topics:

Before You Begin

Setting up a vCenter Server private cloud account requires you to collect specific information about your account.

Before you begin setting up a vCenter Server private cloud account, do the following:

- Verify that your vCenter Server 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 inside VMware Cloud services.

If your vCenter Server private network does not use DHCP, you must gather the following 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 complete the configuration process.

- Default Gateway
- Domain Name
- Domain Name Servers
- Domain Search Path
- Network IP Address

- Network 1 Netmask

Deploy a Data Collector for vCenter Private Cloud

The first time you try to add a private cloud account in the Cost Insight service, VMware Cloud services prompts you to add a data collector.

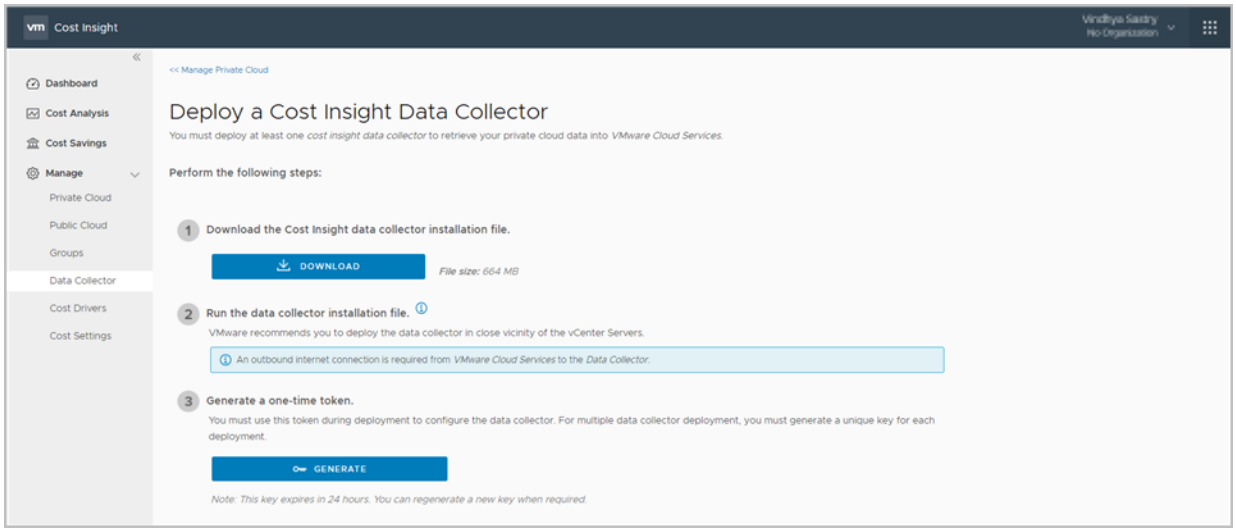
You can deploy as many data collectors as you want, one for each vCenter Server. To link your vCenter Servers into the same private cloud and gather information from them all, give each vCenter Server the same private cloud name in the Add/Edit vCenter form.

Do the following procedure to download the data collector .OVA file and deploy it to your private vCenter account.

Procedure

1 Log in to the Cost Insight service.

2 Expand **Manage** and select **Data Collector**.



3 Click **vCenter**. This displays the Setup a Data Collector Virtual Appliance screen. (Leave this screen open, you need it later.)

4 Click **Download** in Step 1 of the Data Collector form to obtain the data collector .OVA file.

Note: The data collector is different for the Network Insight service.

5 Navigate to your VMware vSphere Web Client data center and click on the name of your vCenter cluster. In the drop down menu, select **Deploy OVF Template**.

6 This displays the Deploy OVF Template form. The steps to the left guide you through deployment of your data collector.

a Click **Select template**, then the **URL** radio button. Paste in the path to the .OVA data collector file you downloaded. (If you have already installed a data collector to your vCenter and are reinstalling it, click Local file.) Click **Next**.

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. Click **Next**.

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

d Review the details of your data collector deployment. Notice the **Size on disk** field. 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 to accept your OVA file. Click **Next**.

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

h Click **Customize template** and fill in the form with the required information. Do not click Next.

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

i Return toVMware Cloud services and collect the token key provided by the Discovery service 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** field. Do not click Next.

k Click the **Networking Properties** drop down. This displays a number of network settings. If you use DHCP in your vCenter network, do **not** fill out any of these fields. Leave them blank. If you do not use DHCP, then you need to provide a setting for each of these fields. When you have filled out - or left blank - the Networking Properties field, click **Next**.

l Click **Ready to complete** and review your configuration data. Click Back to revise or click **Finish**.

Clicking Finish installs the data collector into your vSphere Web Client.

7 Return to the vSphere Web Client to run the data collector. Once 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.

8 If not already running when you return to your vSphere Web Client, click the **green arrow** at the top of your screen to start it.

9 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**.

10 Return to the VMware Cloud services **Set Up a Data Collector Virtual Appliance** form. Wait for a connection to be made between your vSphere Web Client andVMware Cloud services . (This may take several minutes.) When the connection has been made successfully, you see the **Next** button at the bottom of the screen become active. Click **Next**.

Fill In the Add a New vCenter Account Form

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

Procedure

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

2 Enter the name you want to use for your private cloud.

You can group any number of vCenter Servers together into one private cloud by giving each vCenter Server the same private cloud name.

3 Enter the name of your vCenter Server.

   You cannot change the name later.

4 Enter the fully-qualified domain name (FQDN) or IP address of the vCenter Server in your private LAN.

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

6 Click **Add**.

   Once it is installed in VMware Cloud services, click the name of the account in the list of your Resources and make the desired changes.

Editing a vCenter Server

Once you've created a vCenter Server private cloud account, you can easily edit its details. To edit a vCenter Server private cloud account, do the following.

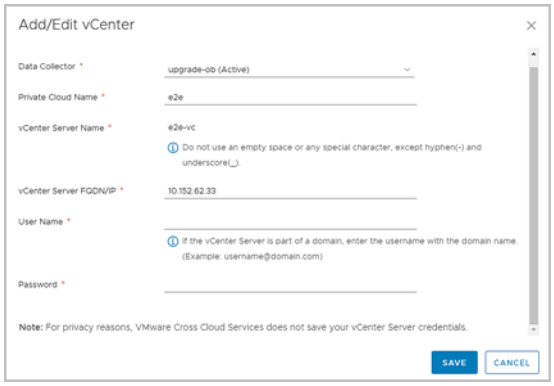
Procedure

1 Switch to the Cost Insight service.

2 Click **Manage > Private Cloud**.

3 Click the edit icon next to the vCenter Server details that you want to modify.

4 In the Add/Edit vCenter form, modify the required details and click **Save**.



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 the 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**.