Azure

Setup and administration

NetApp
August 11, 2023

Table of Contents

Azure . . . 1
- Quick start to create a Connector in Azure . . . 1
- Connector installation options in Azure . . . 2
- Set up Azure networking . . . 3
- Review Connector host requirements for Azure installs . . . 5
- Set up Azure permissions . . . 6
- Create a Connector in Azure . . . 22
- Provide Azure permissions to BlueXP . . . 28

Azure

Quick start to create a Connector in Azure

Create a Connector in Azure by choosing an installation option, setting up networking, preparing permissions, and more.

1 Understand your installation options

The standard way to create a Connector in Azure is directly from BlueXP, but you can also create it from the Azure Marketplace, or you can manually install the software on a pre-existing Linux host.

Learn more about your installation options.

2 Set up networking

Prepare the following for the Connector:

- A VNet and subnet
- A network connection to the networks where you're planning to create and manage working environments
- Outbound internet access to specific endpoints for day-to-day operations
- The IP address, credentials, and HTTPS certificate of a proxy server, if a proxy server is required for outbound internet

Learn more about networking requirements.

3 Review host requirements

If you want to manually install the Connector software on your own Linux host, then you should ensure that your host meets specific requirements. If you're creating the Connector from BlueXP or from the Azure Marketplace, then these requirements are taken care of for you because the software is deployed from an image.

The key requirements are as follows:

- A dedicated host running Ubuntu 22.04, CentOS 7.6 to 7.9, or RHEL 7.6 to 7.9
- 4 CPUs
- 14 GB of RAM
- Docker Engine 19.3.1 or later

Learn more about these host requirements.

4 Set up Azure permissions

Set up Azure permissions for the installation option that you're planning to use:

- **Install from BlueXP**: Create a custom role and then apply it to your Azure account or an Azure AD service principal. BlueXP authenticates with Azure and uses these permissions to create the Connector instance on your behalf.
- **Install from the Azure Marketplace**: Create a custom role that you can associate with the Connector VM instance or with an Azure AD service principal.
- **Manual install**: Create a custom role that you can associate with the Connector VM instance or with an Azure AD service principal.

Follow step-by-step instructions for each of these options.

Create the Connector

Create the Connector using one of the available installation options:

- **From BlueXP**: Select the Connector drop-down, select **Add Connector** and follow the prompts.
- **From the Azure Marketplace**: Go to the NetApp Connector VM page in the Azure Marketplace and follow the prompts to create the Connector VM.
- **Manual install**: Download the Connector software from the NetApp Support Site and run the installation script.

Follow step-by-step instructions for each of these options.

Provide BlueXP with permissions

If you created the Connector from the Azure Marketplace or manually installed the software, you need to provide BlueXP with the permissions that you previously set up.

Follow step-by-step instructions.

Connector installation options in Azure

There are a few different ways to create a Connector in Azure. Directly from BlueXP is the most common way. The installation option that you choose determines how you prepare for deployment.

The following installation options are available:

- Create the Connector directly from BlueXP (this is the standard option)

  This action launches a VM running Linux and the Connector software in a VNet of your choice.

- Create a Connector from the Azure Marketplace

  This action also launches a VM running Linux and the Connector software.

- Download and manually install the software on your own Linux host

The installation option that you choose impacts how you prepare for installation. This includes how you provide BlueXP with the required permissions that it needs to authenticate and manage resources in Azure.

Learn how to install the Connector in Azure.

Set up Azure networking

Set up your networking so the Connector can manage resources and processes within your hybrid cloud environment. For example, you need to ensure that connections are available to target networks and that outbound internet access is available.

VNet and subnet

When you create the Connector, you need to specify the VNet and subnet where the Connector should reside.

Azure region

If you use Cloud Volumes ONTAP, the Connector should be deployed in the same Azure region as the Cloud Volumes ONTAP systems that it manages, or in the Azure region pair for the Cloud Volumes ONTAP systems. This requirement ensures that an Azure Private Link connection is used between Cloud Volumes ONTAP and its associated storage accounts.

Learn how Cloud Volumes ONTAP uses an Azure Private Link

Connections to target networks

A Connector requires a network connection to the location where you're planning to create and manage working environments.

Outbound internet access

The network location where you deploy the Connector must have an outbound internet connection. Outbound internet access is also required from your web browser when deploying the Connector from the BlueXP console.

Endpoints contacted from the BlueXP console

As you use the BlueXP web-based console that's provided through the SaaS layer, it contacts several endpoints to complete data management tasks. This includes endpoints that are contacted to deploy the Connector from the BlueXP console.

View the list of endpoints contacted from the BlueXP console.

Endpoints contacted during manual installation

When you manually install the Connector on your own Linux host, the installer for the Connector requires access to the following URLs during the installation process:

- https://support.netapp.com
- https://mysupport.netapp.com
- https://cloudmanager.cloud.netapp.com/tenancy
- https://stream.cloudmanager.cloud.netapp.com
- https://production-artifacts.cloudmanager.cloud.netapp.com

- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

The host might try to update operating system packages during installation. The host can contact different mirroring sites for these OS packages.

Endpoints contacted from the Connector

The Connector requires outbound internet access to contact the following endpoints in order to manage resources and processes within your public cloud environment for day-to-day operations.

Endpoints	Purpose
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	To manage resources in Azure public regions.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	To manage resources in Azure China regions.
https://support.netapp.com	To obtain licensing information and to send AutoSupport messages to NetApp support.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://api.cloud.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com/userinfo	To provide SaaS features and services within BlueXP. Note that the Connector is currently contacting "cloudmanager.cloud.netapp.com" but it will start contacting "api.bluexp.netapp.com" in an upcoming release.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	To upgrade the Connector and its Docker components.

Proxy server

If your organization requires deployment of a proxy server for all outgoing internet traffic, obtain the following information about your HTTP or HTTPS proxy. You'll need to provide this information during installation.

- IP address
- Credentials
- HTTPS certificate

Ports

There's no incoming traffic to the Connector, unless you initiate it or if the Connector is used as a proxy to send AutoSupport messages from Cloud Volumes ONTAP to NetApp Support.

- HTTP (80) and HTTPS (443) provide access to the local UI, which you'll use in rare circumstances.
- SSH (22) is only needed if you need to connect to the host for troubleshooting.
- Inbound connections over port 3128 are required if you deploy Cloud Volumes ONTAP systems in a subnet where an outbound internet connection isn't available.

  If Cloud Volumes ONTAP systems don't have an outbound internet connection to send AutoSupport messages, BlueXP automatically configures those systems to use a proxy server that's included with the Connector. The only requirement is to ensure that the Connector's security group allows inbound connections over port 3128. You'll need to open this port after you deploy the Connector.

IP address limitation

There's a possible conflict with IP addresses in the 172 range. Learn more about this limitation.

Review Connector host requirements for Azure installs

The Connector software must run on a host that meets specific operating system requirements, RAM requirements, port requirements, and so on. If you plan to manually install the Connector, you should ensure that your host meets these requirements.

When you deploy the Connector from BlueXP or from the Azure Marketplace, the image includes the required OS and software components.

Dedicated host

The Connector is not supported on a host that is shared with other applications. The host must be a dedicated host.

Supported operating systems

- Ubuntu 22.04
- CentOS 7.6, 7.7, 7.8, and 7.9
- Red Hat Enterprise Linux 7.6, 7.7, 7.8, and 7.9

  The host must be registered with Red Hat Subscription Management. If it's not registered, the host can't access repositories to update required 3rd-party software during Connector installation.

  The Connector is supported on English-language versions of these operating systems.

Hypervisor

A bare metal or hosted hypervisor that is certified to run Ubuntu, CentOS, or Red Hat Enterprise Linux is required.

Red Hat Solution: Which hypervisors are certified to run Red Hat Enterprise Linux?

CPU

4 cores or 4 vCPUs

RAM

14 GB

Azure VM size

An instance type that meets the CPU and RAM requirements above. We recommend DS3 v2.

Disk space in /opt

100 GiB of space must be available

Disk space in /var

20 GiB of space must be available

Docker Engine

Docker Engine version 19.3.1 or later is required on the host before you install the Connector. View installation instructions

Set up Azure permissions

Set up permissions in Azure so that you can deploy the Connector with the permissions that it needs to manage your data and storage infrastructure. How you set up permissions depends on the installation option that you're planning to use.

You can choose from the following installation options:

- **Install from BlueXP**: Set up permissions that enable BlueXP to authenticate with Azure and deploy the VM. BlueXP automatically sets up permissions for the Connector VM during deployment.

  View step-by-step instructions.

- **Install from the Azure Marketplace**: Set up an Azure custom role to associate with the Connector VM or with an Azure AD service principal.

  View step-by-step instructions.

- **Manual install**: Set up an Azure custom role to associate with the Connector VM or with an Azure AD service principal.

  View step-by-step instructions.

Set up permissions to create the Connector from BlueXP

To create a Connector from BlueXP, you need to provide BlueXP with a login that has the required permissions to create the Connector VM in Azure. You have two options:

1. Sign in with your Microsoft account when prompted. This account must have specific Azure permissions. This is the default option.
2. Provide details about an Azure AD service principal. This service principal also requires specific permissions.

With both options, the first step is create a custom role.

Create a custom role

Create a custom role that you can assign to your Azure account or to a service principal.

Note that you can create an Azure custom role using the Azure portal, Azure PowerShell, Azure CLI, or REST API. The following steps show how to create the role using the Azure CLI. If you would prefer to use a different method, refer to Azure documentation

Steps

1. Copy the required permissions for a new custom role in Azure and save them in a JSON file.

This policy contains only the permissions needed to launch the Connector VM in Azure from BlueXP. Don't use this policy for other situations. When BlueXP creates the Connector, it applies a new set of permissions to the Connector VM that enables the Connector to manage the resources in your public cloud environment.

```
{
    "Name": "Azure SetupAsService",
    "Actions": [
        "Microsoft.Compute/disks/delete",
        "Microsoft.Compute/disks/read",
        "Microsoft.Compute/disks/write",
        "Microsoft.Compute/locations/operations/read",
        "Microsoft.Compute/operations/read",
        "Microsoft.Compute/virtualMachines/instanceView/read",
        "Microsoft.Compute/virtualMachines/read",
        "Microsoft.Compute/virtualMachines/write",
        "Microsoft.Compute/virtualMachines/delete",
        "Microsoft.Compute/virtualMachines/extensions/write",
        "Microsoft.Compute/virtualMachines/extensions/read",
        "Microsoft.Compute/availabilitySets/read",
        "Microsoft.Network/locations/operationResults/read",
        "Microsoft.Network/locations/operations/read",
        "Microsoft.Network/networkInterfaces/join/action",
        "Microsoft.Network/networkInterfaces/read",
        "Microsoft.Network/networkInterfaces/write",
        "Microsoft.Network/networkInterfaces/delete",
        "Microsoft.Network/networkSecurityGroups/join/action",
        "Microsoft.Network/networkSecurityGroups/read",
        "Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
        "Microsoft.Network/virtualNetworks/read",
        "Microsoft.Network/virtualNetworks/subnets/join/action",
        "Microsoft.Network/virtualNetworks/subnets/read",
```

```
"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
        "Microsoft.Network/virtualNetworks/virtualMachines/read",
        "Microsoft.Network/publicIPAddresses/write",
        "Microsoft.Network/publicIPAddresses/read",
        "Microsoft.Network/publicIPAddresses/delete",
        "Microsoft.Network/networkSecurityGroups/securityRules/read",
        "Microsoft.Network/networkSecurityGroups/securityRules/write",
        "Microsoft.Network/networkSecurityGroups/securityRules/delete",
        "Microsoft.Network/publicIPAddresses/join/action",

"Microsoft.Network/locations/virtualNetworkAvailableEndpointServices/rea
d",
        "Microsoft.Network/networkInterfaces/ipConfigurations/read",
        "Microsoft.Resources/deployments/operations/read",
        "Microsoft.Resources/deployments/read",
        "Microsoft.Resources/deployments/delete",
        "Microsoft.Resources/deployments/cancel/action",
        "Microsoft.Resources/deployments/validate/action",
        "Microsoft.Resources/resources/read",
        "Microsoft.Resources/subscriptions/operationresults/read",
        "Microsoft.Resources/subscriptions/resourceGroups/delete",
        "Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
        "Microsoft.Resources/subscriptions/resourceGroups/write",
        "Microsoft.Authorization/roleDefinitions/write",
        "Microsoft.Authorization/roleAssignments/write",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreem
ents/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreem
ents/write",
        "Microsoft.Network/networkSecurityGroups/delete",
        "Microsoft.Storage/storageAccounts/delete",
        "Microsoft.Storage/storageAccounts/write",
        "Microsoft.Resources/deployments/write",
        "Microsoft.Resources/deployments/operationStatuses/read",
        "Microsoft.Authorization/roleAssignments/read"
    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "Azure SetupAsService",
    "IsCustom": "true"
}
```

2. Modify the JSON by adding your Azure subscription ID to the assignable scope.

   Example

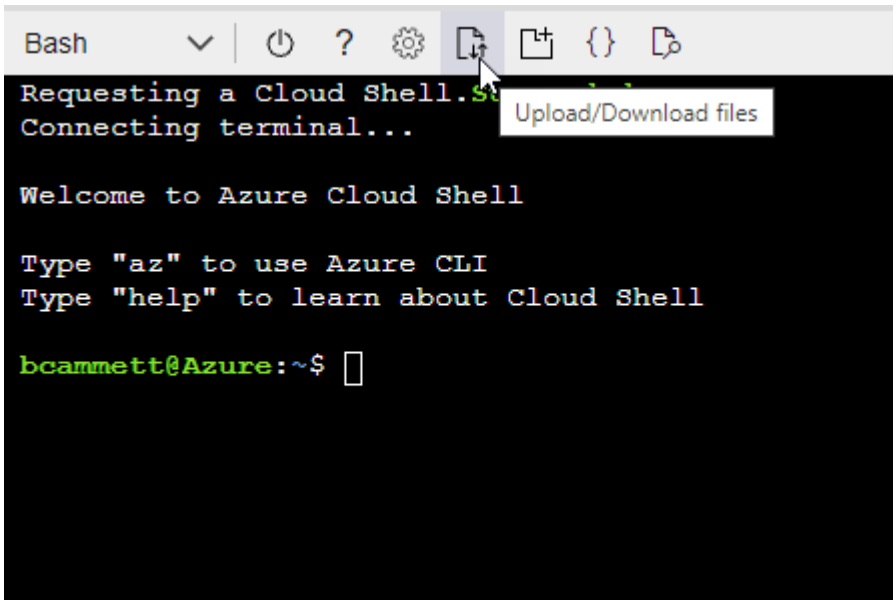
   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"
   ],
   ```

3. Use the JSON file to create a custom role in Azure.

   The following steps describe how to create the role by using Bash in Azure Cloud Shell.

   a. Start Azure Cloud Shell and choose the Bash environment.

   b. Upload the JSON file.

   c. Enter the following Azure CLI command:

   ```
   az role definition create --role-definition
   Policy_for_Setup_As_Service_Azure.json
   ```

   You should now have a custom role called *Azure SetupAsService*. You can now apply this custom role to your user account or to a service principal.

Set up an authentication method

To deploy the BlueXP Connector, BlueXP needs to authenticate with Azure. You can choose between two Azure authentication methods.

Azure user account

Assign the custom role to the user who will deploy the Connector from BlueXP.

Steps

1. In the Azure portal, open the **Subscriptions** service and select the user's subscription.
2. Select **Access control (IAM)**.
3. Select **Add** > **Add role assignment** and then add the permissions:
   a. Select the **Azure SetupAsService** role and select **Next**.

   > Azure SetupAsService is the default name provided in the Connector deployment policy for Azure. If you chose a different name for the role, then select that name instead.

   b. Keep **User, group, or service principal** selected.
   c. Select **Select members**, choose your user account, and select **Select**.
   d. Select **Next**.
   e. Select **Review + assign**.

Result

The Azure user now has the permissions required to deploy the Connector from BlueXP.

Service principal

Rather than logging in with your Azure account, you can provide BlueXP with the credentials for an Azure service principal that has the required permissions.

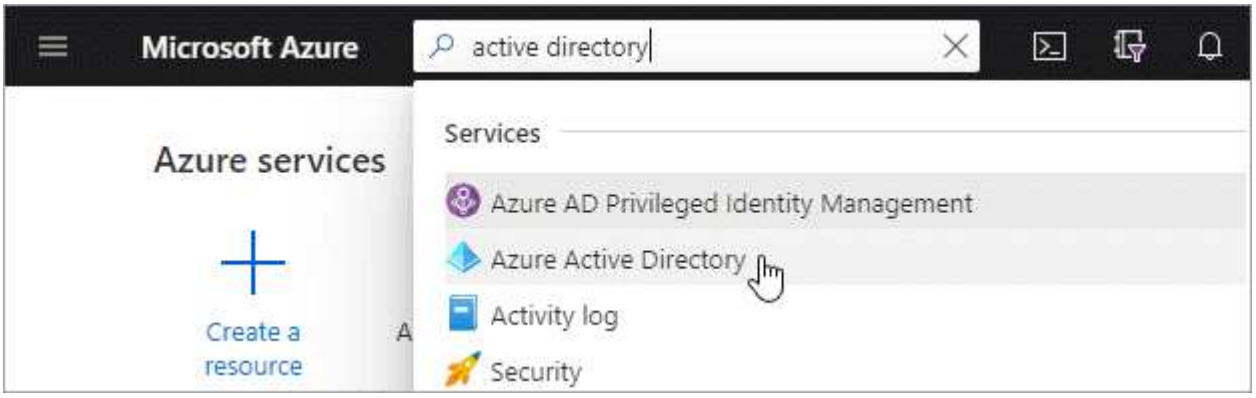
Create and set up a service principal in Azure Active Directory and obtain the Azure credentials that BlueXP needs.

Create an Azure Active Directory application for role-based access control

1. Ensure that you have permissions in Azure to create an Active Directory application and to assign the application to a role.

   For details, refer to Microsoft Azure Documentation: Required permissions

2. From the Azure portal, open the **Azure Active Directory** service.



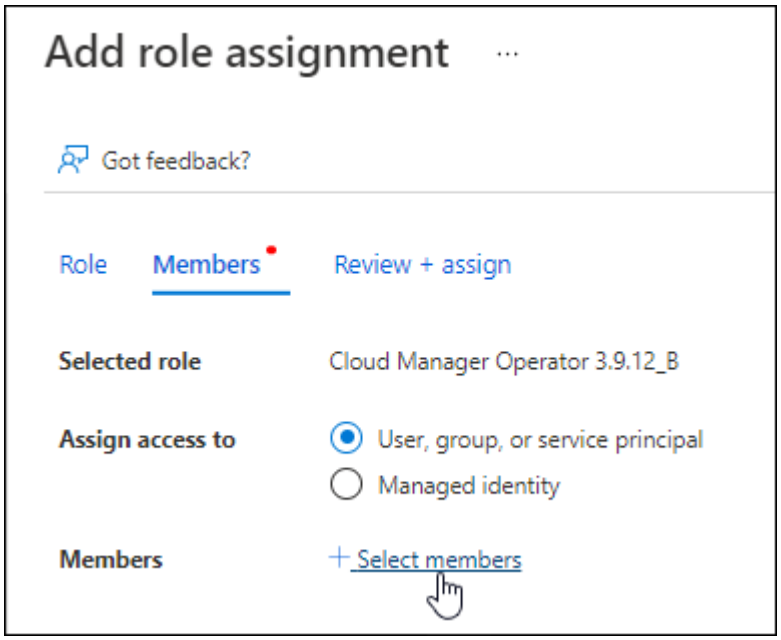
3. In the menu, select **App registrations**.

4. Select **New registration**.
5. Specify details about the application:
   - **Name**: Enter a name for the application.
   - **Account type**: Select an account type (any will work with BlueXP).
   - **Redirect URI**: You can leave this field blank.
6. Select **Register**.

   You've created the AD application and service principal.

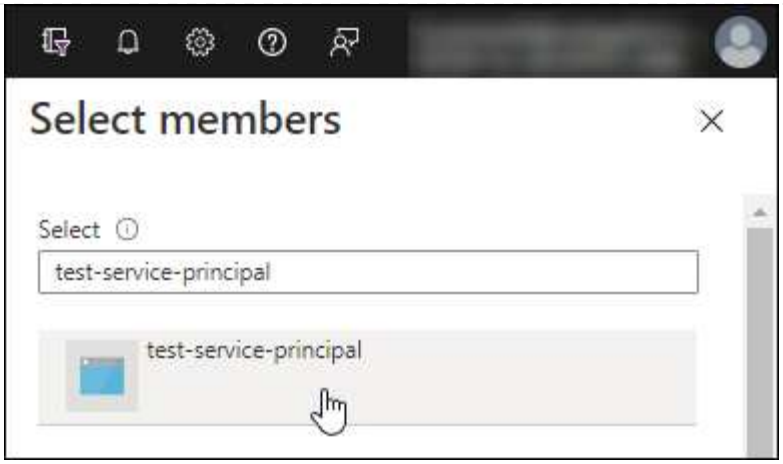
Assign the custom role to the application

1. From the Azure portal, open the **Subscriptions** service.
2. Select the subscription.
3. Select **Access control (IAM) > Add > Add role assignment**.
4. In the **Role** tab, select the **BlueXP Operator** role and select **Next**.
5. In the **Members** tab, complete the following steps:
   a. Keep **User, group, or service principal** selected.
   b. Select **Select members**.



   c. Search for the name of the application.

      Here's an example:



d. Select the application and select **Select**.

e. Select **Next**.

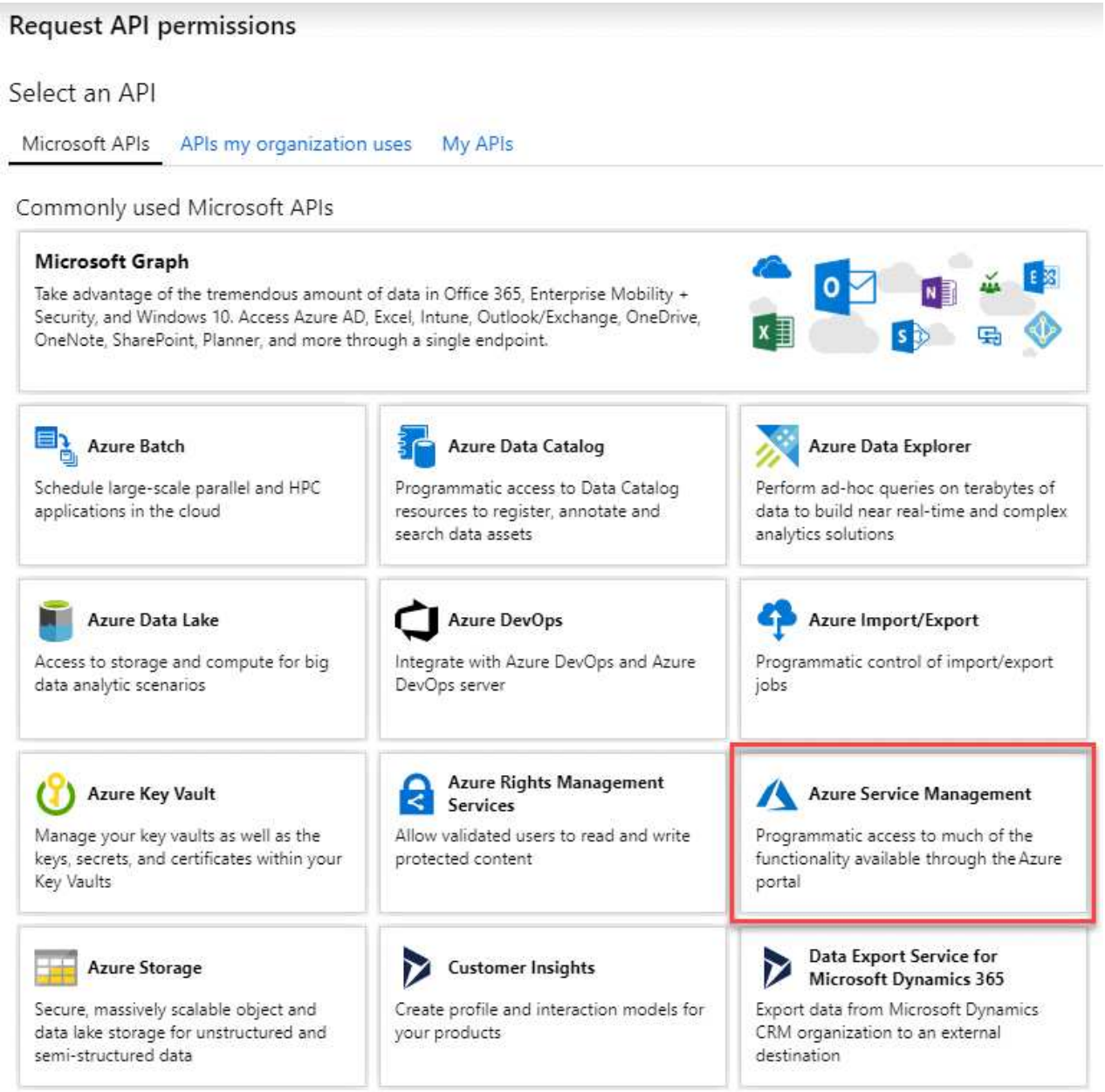
6. Select **Review + assign**.

   The service principal now has the required Azure permissions to deploy the Connector.

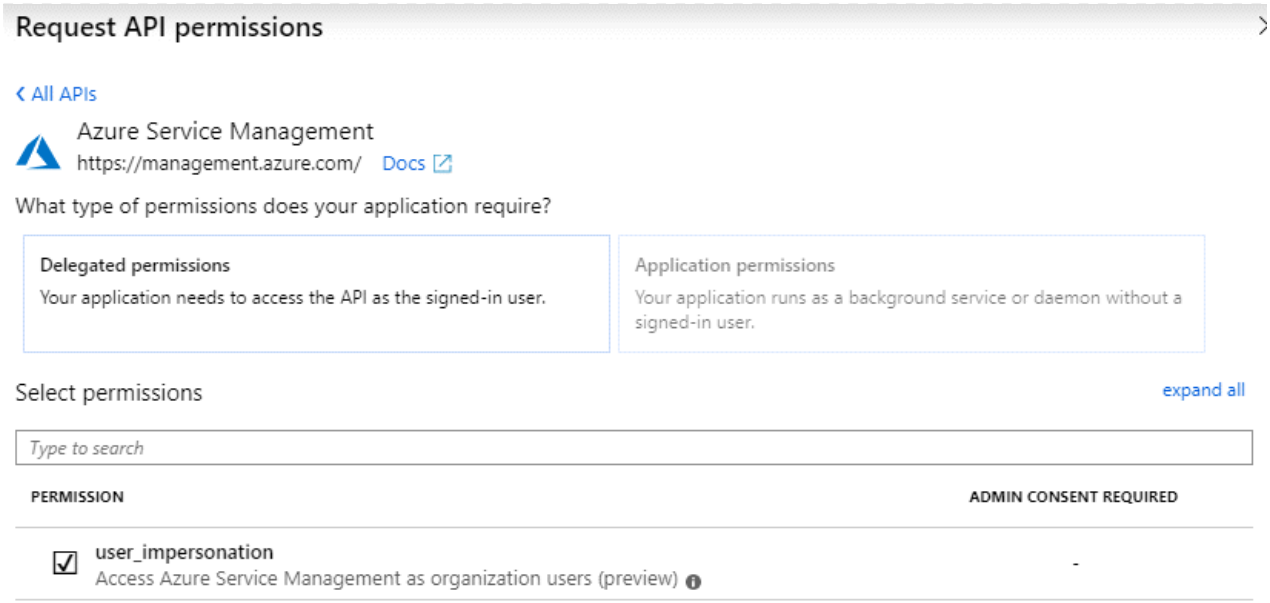
   If you want to manage resources in multiple Azure subscriptions, then you must bind the service principal to each of those subscriptions. For example, BlueXP enables you to select the subscription that you want to use when deploying Cloud Volumes ONTAP.

Add Windows Azure Service Management API permissions

1. In the **Azure Active Directory** service, select **App registrations** and select the application.
2. Select **API permissions > Add a permission**.
3. Under **Microsoft APIs**, select **Azure Service Management**.

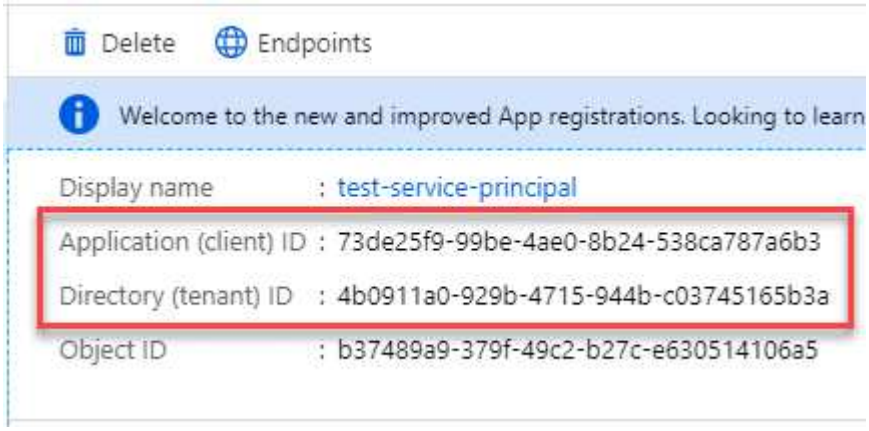


4. Select **Access Azure Service Management as organization users** and then select **Add permissions**.



Get the application ID and directory ID for the application

1. In the **Azure Active Directory** service, select **App registrations** and select the application.
2. Copy the **Application (client) ID** and the **Directory (tenant) ID**.



When you add the Azure account to BlueXP, you need to provide the application (client) ID and the directory (tenant) ID for the application. BlueXP uses the IDs to programmatically sign in.

Create a client secret

1. Open the **Azure Active Directory** service.
2. Select **App registrations** and select your application.
3. Select **Certificates & secrets > New client secret**.
4. Provide a description of the secret and a duration.
5. Select **Add**.
6. Copy the value of the client secret.

You now have a client secret that BlueXP can use it to authenticate with Azure AD.

Result

Your service principal is now setup and you should have copied the application (client) ID, the directory (tenant) ID, and the value of the client secret. You need to enter this information in BlueXP when you create the Connector.

Set up permissions to assign after Azure Marketplace deployment or manual installation

If you deploy the Connector from the Azure Marketplace or if you manually install the Connector software on your own Linux host, you can provide permissions in the following ways:

- Option 1: Assign a custom role to the Azure VM using a system-assigned managed identity.
- Option 2: Provide BlueXP with the credentials for an Azure service principal that has the required permissions.

Custom role

Note that you can create an Azure custom role using the Azure portal, Azure PowerShell, Azure CLI, or REST API. The following steps show how to create the role using the Azure CLI. If you would prefer to use a different method, refer to Azure documentation

Steps

1. If you're planning to manually install the software on your own host, enable a system-assigned managed identity on the VM so that you can provide the required Azure permissions through a custom role.

   Microsoft Azure documentation: Configure managed identities for Azure resources on a VM using the Azure portal

2. Copy the contents of the custom role permissions for the Connector and save them in a JSON file.
3. Modify the JSON file by adding Azure subscription IDs to the assignable scope.

   You should add the ID for each Azure subscription that you want to use with BlueXP.

   Example

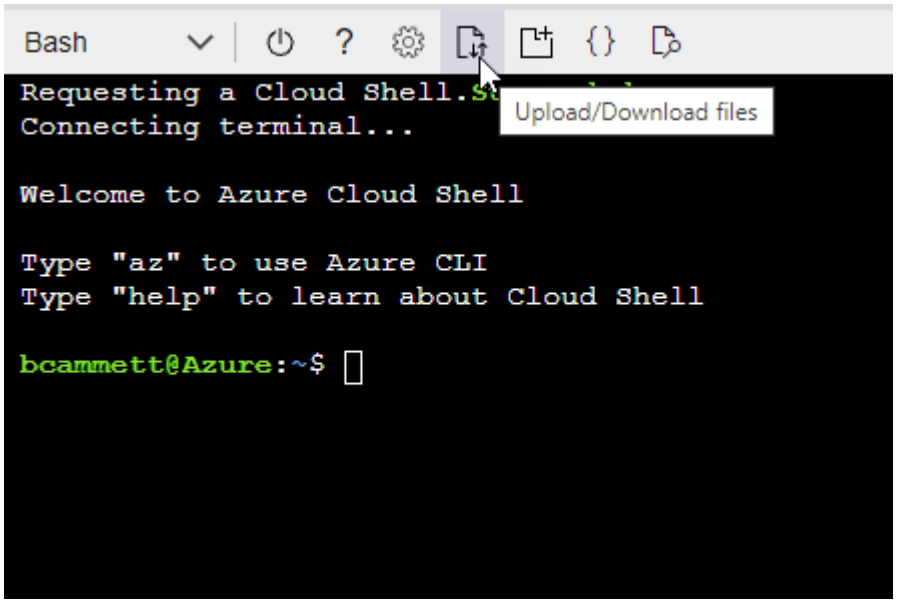
   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ```

4. Use the JSON file to create a custom role in Azure.

   The following steps describe how to create the role by using Bash in Azure Cloud Shell.

   a. Start Azure Cloud Shell and choose the Bash environment.

   b. Upload the JSON file.



c. Use the Azure CLI to create the custom role:

```
az role definition create --role-definition Connector_Policy.json
```

Result

You should now have a custom role called BlueXP Operator that you can assign to the Connector virtual machine.

Learn how to provide these permissions to BlueXP.

Service principal

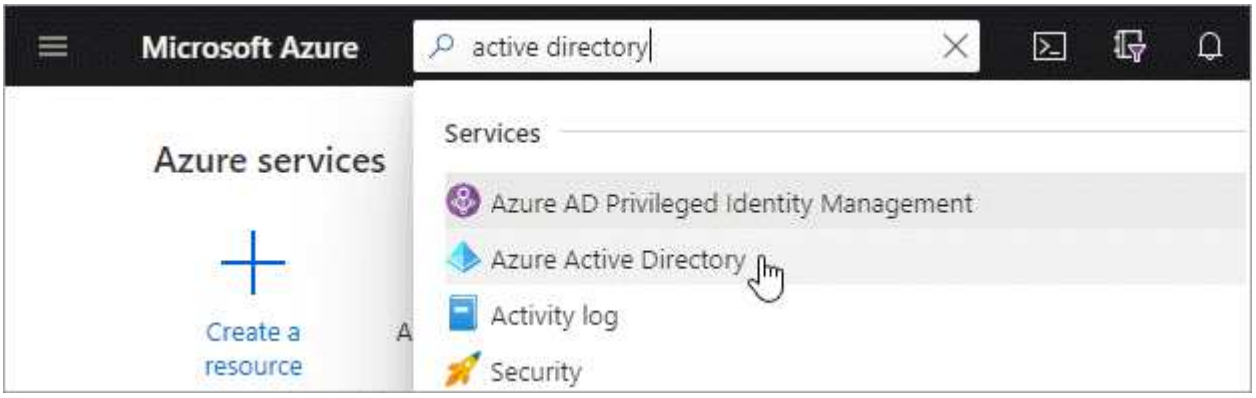
Create and set up a service principal in Azure Active Directory and obtain the Azure credentials that BlueXP needs.

Create an Azure Active Directory application for role-based access control

1. Ensure that you have permissions in Azure to create an Active Directory application and to assign the application to a role.

   For details, refer to Microsoft Azure Documentation: Required permissions

2. From the Azure portal, open the **Azure Active Directory** service.



3. In the menu, select **App registrations**.
4. Select **New registration**.
5. Specify details about the application:
   - **Name**: Enter a name for the application.
   - **Account type**: Select an account type (any will work with BlueXP).
   - **Redirect URI**: You can leave this field blank.
6. Select **Register**.

   You've created the AD application and service principal.

Assign the application to a role

1. Create a custom role:

   Note that you can create an Azure custom role using the Azure portal, Azure PowerShell, Azure CLI,

or REST API. The following steps show how to create the role using the Azure CLI. If you would prefer to use a different method, refer to Azure documentation

a. Copy the contents of the custom role permissions for the Connector and save them in a JSON file.

b. Modify the JSON file by adding Azure subscription IDs to the assignable scope.

You should add the ID for each Azure subscription from which users will create Cloud Volumes ONTAP systems.

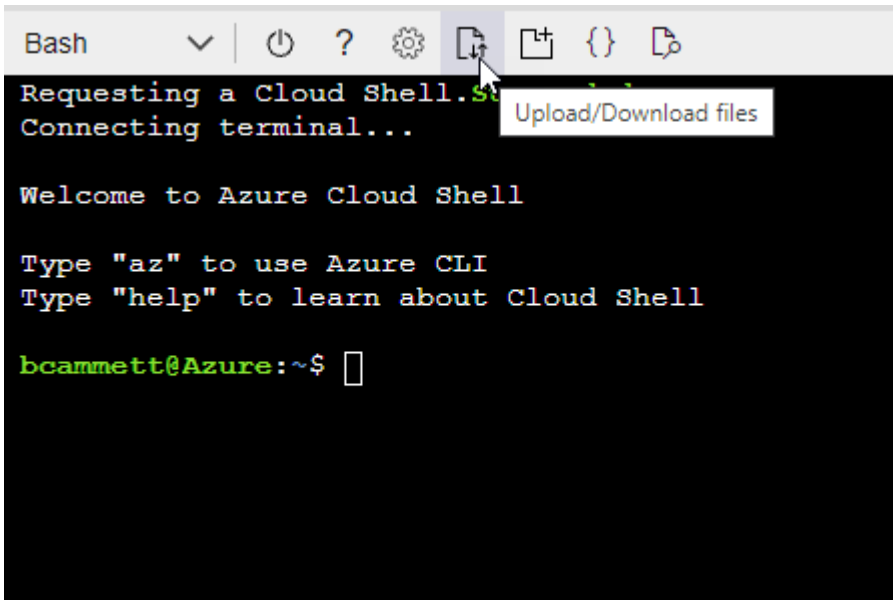
Example

```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
"/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
"/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

c. Use the JSON file to create a custom role in Azure.

The following steps describe how to create the role by using Bash in Azure Cloud Shell.

- Start Azure Cloud Shell and choose the Bash environment.
- Upload the JSON file.

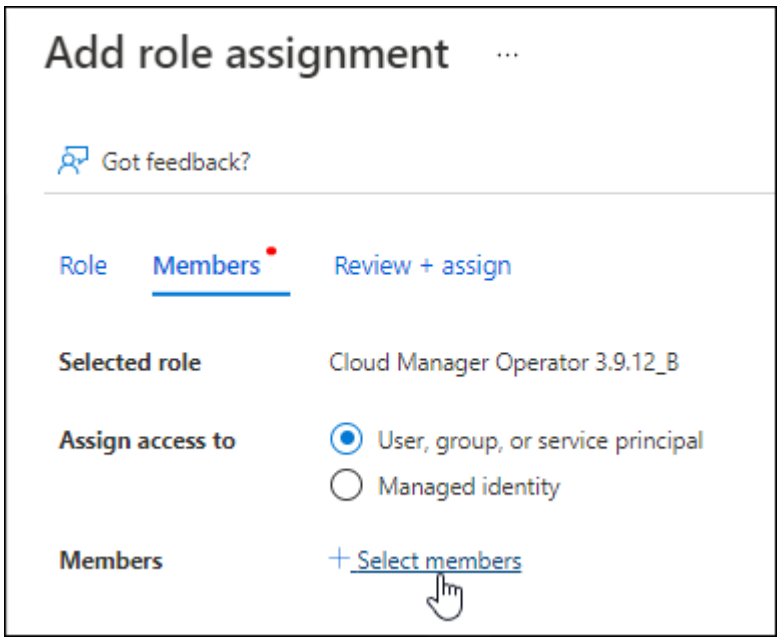


- Use the Azure CLI to create the custom role:

```
az role definition create --role-definition
Connector_Policy.json
```

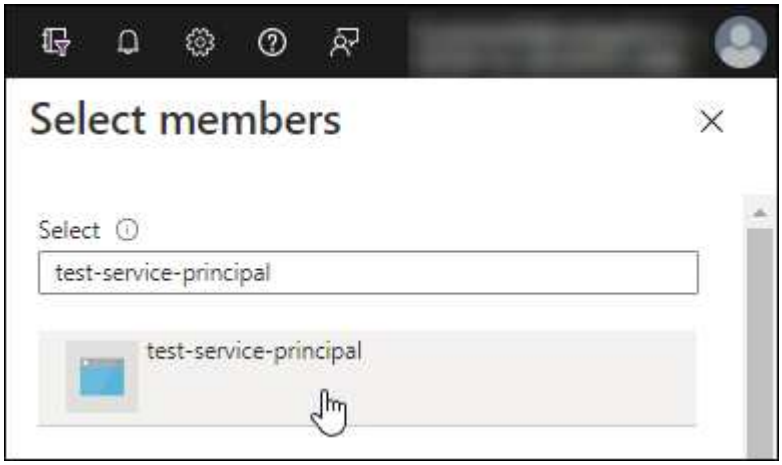
You should now have a custom role called BlueXP Operator that you can assign to the Connector virtual machine.

2. Assign the application to the role:
    a. From the Azure portal, open the **Subscriptions** service.
    b. Select the subscription.
    c. Select **Access control (IAM) > Add > Add role assignment**.
    d. In the **Role** tab, select the **BlueXP Operator** role and select **Next**.
    e. In the **Members** tab, complete the following steps:
        - Keep **User, group, or service principal** selected.
        - Select **Select members**.



        - Search for the name of the application.

          Here's an example:



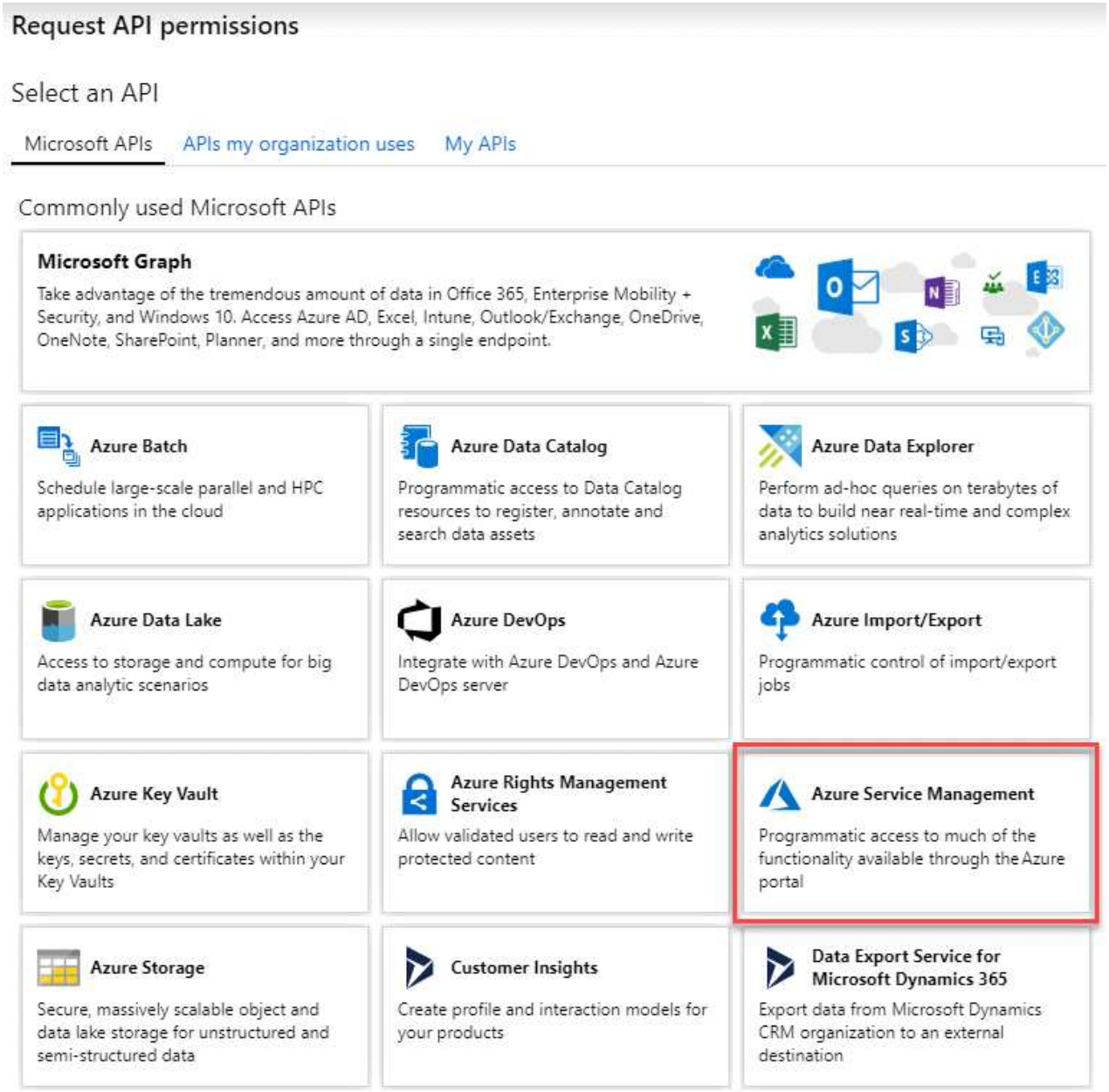
        - Select the application and select **Select**.
        - Select **Next**.
    f. Select **Review + assign**.

The service principal now has the required Azure permissions to deploy the Connector.

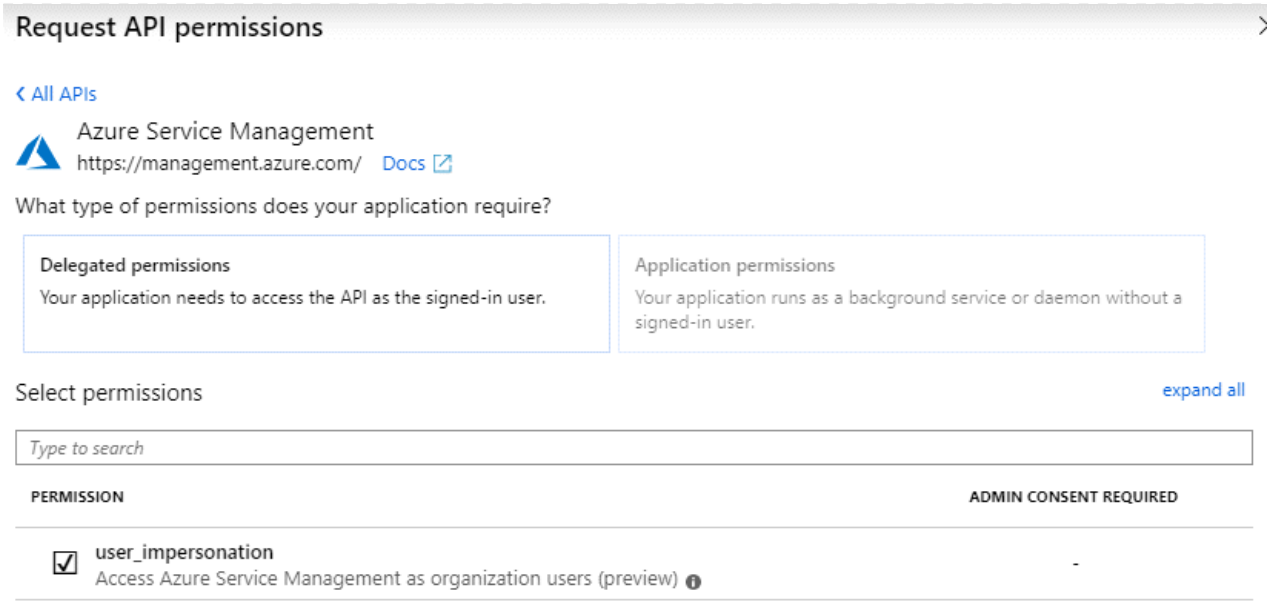
If you want to deploy Cloud Volumes ONTAP from multiple Azure subscriptions, then you must bind the service principal to each of those subscriptions. BlueXP enables you to select the subscription that you want to use when deploying Cloud Volumes ONTAP.

Add Windows Azure Service Management API permissions

1. In the **Azure Active Directory** service, select **App registrations** and select the application.
2. Select **API permissions > Add a permission**.
3. Under **Microsoft APIs**, select **Azure Service Management**.

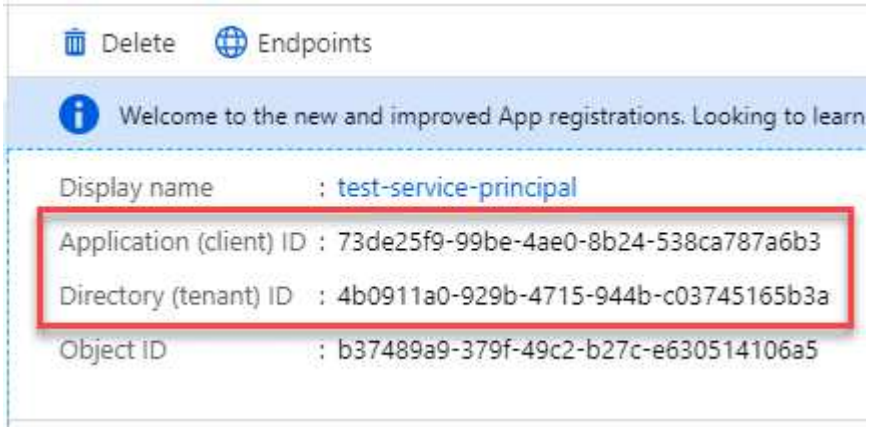


4. Select **Access Azure Service Management as organization users** and then select **Add permissions**.



Get the application ID and directory ID for the application

1. In the **Azure Active Directory** service, select **App registrations** and select the application.
2. Copy the **Application (client) ID** and the **Directory (tenant) ID**.



When you add the Azure account to BlueXP, you need to provide the application (client) ID and the directory (tenant) ID for the application. BlueXP uses the IDs to programmatically sign in.

Create a client secret

1. Open the **Azure Active Directory** service.
2. Select **App registrations** and select your application.
3. Select **Certificates & secrets > New client secret**.
4. Provide a description of the secret and a duration.
5. Select **Add**.
6. Copy the value of the client secret.

You now have a client secret that BlueXP can use it to authenticate with Azure AD.

Result

Your service principal is now setup and you should have copied the application (client) ID, the directory (tenant) ID, and the value of the client secret. You need to enter this information in BlueXP when you add an Azure account.

Learn how to provide these permissions to BlueXP.

Create a Connector in Azure

Create a Connector directly from the BlueXP web-based console, from the Azure Marketplace, or by installing the software on your own Linux host.

BlueXP

Before you begin

You should have the following:

- An Azure subscription.
- A VNet and subnet in your Azure region of choice.
- Details about a proxy server, if your organization requires a proxy for all outgoing internet traffic:
  - IP address
  - Credentials
  - HTTPS certificate
- An SSH public key, if you want to use that authentication method for the Connector virtual machine. The other option for the authentication method is to use a password.

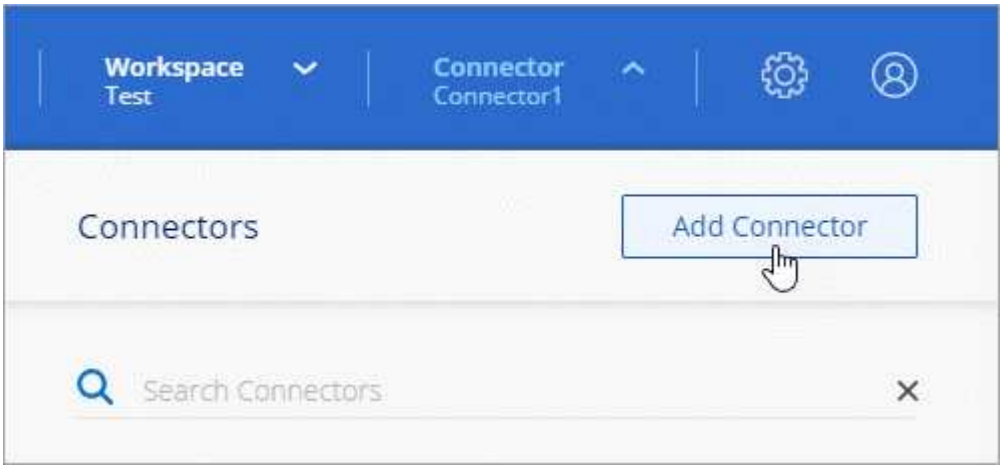
  Learn about connecting to a Linux VM in Azure

- If you don't want BlueXP to automatically create an Azure role for the Connector, then you'll need to create your own using the policy on this page.

  These permissions are for the Connector instance itself. It's a different set of permissions than what you previously set up to simply deploy the Connector.

Steps

1. If you're creating your first Working Environment, select **Add Working Environment** and follow the prompts. Otherwise, select the **Connector** drop-down and select **Add Connector**.



2. Choose **Microsoft Azure** as your cloud provider.
3. On the **Deploying a Connector** page:

   a. Under **Authentication**, select the authentication option that matches how you set up Azure permissions:

      - Select **Azure user account** to log in to your Microsoft account, which should have the required permissions.

        The form is owned and hosted by Microsoft. Your credentials are not provided to NetApp.

If you're already logged in to an Azure account, then BlueXP will automatically use that account. If you have multiple accounts, then you might need to log out first to ensure that you're using the right account.

- Select **Active Directory service principal** to enter information about the Azure Active Directory service principal that grants the required permissions:
  - Application (client) ID
  - Directory (tenant) ID
  - Client Secret

Learn how to obtain these values for a service principal.

4. Follow the steps in the wizard to create the Connector:
   - **VM Authentication**: Choose an Azure subscription, a location, a new resource group or an existing resource group, and then choose an authentication method for the Connector virtual machine that you're creating.

     The authentication method for the virtual machine can be a password or an SSH public key.

     Learn about connecting to a Linux VM in Azure

   - **Details**: Enter a name for the instance, specify tags, and choose whether you want BlueXP to create a new role that has the required permissions, or if you want to select an existing role that you set up with the required permissions.

     Note that you can choose the Azure subscriptions associated with this role. Each subscription that you choose provides the Connector permissions to manage resources in that subscription (for example, Cloud Volumes ONTAP).

   - **Network**: Choose a VNet and subnet, whether to enable a public IP address, and optionally specify a proxy configuration.
   - **Security Group**: Choose whether to create a new security group or whether to select an existing security group that allows the required inbound and outbound rules.

     View security group rules for Azure.

   - **Review**: Review your selections to verify that your set up is correct.
5. Select **Add**.

   The virtual machine should be ready in about 7 minutes. You should stay on the page until the process is complete.

Result

After the process is complete, the Connector is available for use from BlueXP.

Azure Marketplace

Steps

1. Go to the NetApp Connector VM page in the Azure Marketplace.

   Azure Marketplace page for commercial regions

2. Select **Get it now** and then select **Continue**.
3. From the Azure portal, select **Create** and follow the steps to configure the virtual machine.

   Note the following as you configure the VM:

   - **VM size**: Choose a VM size that meets CPU and RAM requirements. We recommend DS3 v2.
   - **Disks**: The Connector can perform optimally with either HDD or SSD disks.
   - **Network security group**: The Connector requires inbound connections using SSH, HTTP, and HTTPS.

     View security group rules for Azure.

   - **Identity**: Under **Management**, select **Enable system assigned managed identity**.

     This setting is important because a managed identity allows the Connector virtual machine to identify itself to Azure Active Directory without providing any credentials. Learn more about managed identities for Azure resources.

4. On the **Review + create** page, review your selections and select **Create** to start the deployment.

   Azure deploys the virtual machine with the specified settings. The virtual machine and Connector software should be running in approximately five minutes.

5. Open a web browser from a host that has a connection to the Connector virtual machine and enter the following URL:

   https://*ipaddress*

6. After you log in, set up the Connector:
   a. Specify the BlueXP account to associate with the Connector.
   b. Enter a name for the system.
   c. Under **Are you running in a secured environment?** keep restricted mode disabled.

      You should keep restricted mode disabled because these steps describe how to use BlueXP in standard mode. You should enable restricted mode only if you have a secure environment and want to disconnect this account from BlueXP backend services. If that's the case, follow steps to get started with BlueXP in restricted mode.

   d. Select **Let's start**.

The Connector is now installed and is set up with your BlueXP account.

What's next?

Provide BlueXP with the permissions that you previously setup.

Manual install

Before you begin

You should have the following:

- Root privileges to install the Connector.
- Details about a proxy server, if a proxy is required for internet access from the Connector.

You have the option to configure a proxy server after installation but doing so requires restarting the Connector.

- A CA-signed certificate, if the proxy server uses HTTPS or if the proxy is an intercepting proxy.
- A managed identity enabled on the VM in Azure so that you can provide the required Azure permissions through a custom role.

  Microsoft Azure documentation: Configure managed identities for Azure resources on a VM using the Azure portal

About this task

The installer that is available on the NetApp Support Site might be an earlier version. After installation, the Connector automatically updates itself if a new version is available.

Steps

1. Verify that docker is enabled and running.

   ```
   sudo systemctl enable docker && sudo systemctl start docker
   ```

2. If the *http_proxy* or *https_proxy* system variables are set on the host, remove them:

   ```
   unset http_proxy
   unset https_proxy
   ```

   If you don't remove these system variables, the installation will fail.

3. Download the Connector software from the NetApp Support Site, and then copy it to the Linux host.

   You should download the "online" Connector installer that's meant for use in your network or in the cloud. A separate "offline" installer is available for the Connector, but it's only supported with private mode deployments.

4. Assign permissions to run the script.

   ```
   chmod +x OnCommandCloudManager-<version>
   ```

   Where <version> is the version of the Connector that you downloaded.

5. Run the installation script.

   ```
    ./OnCommandCloudManager-<version> --proxy <HTTP or HTTPS proxy
   server> --cacert <path and file name of a CA-signed certificate>
   ```

   The --proxy and --cacert parameters are optional. If you have a proxy server, you will need to enter the parameter(s) as shown. The installer doesn't prompt you to provide information about a proxy.

Here's an example of the command using both optional parameters:

```
 ./OnCommandCloudManager-V3.9.26 --proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

--proxy configures the Connector to use an HTTP or HTTPS proxy server using one of the following formats:

- http://address:port
- http://username:password@address:port
- https://address:port
- https://username:password@address:port

  The user must be a local user. Domain users are not supported.

--cacert specifies a CA-signed certificate to use for HTTPS access between the Connector and the proxy server. This parameter is required only if you specify an HTTPS proxy server or if the proxy is an intercepting proxy.

6. Wait for the installation to complete.

   At the end of the installation, the Connector service (occm) restarts twice if you specified a proxy server.

7. Open a web browser from a host that has a connection to the Connector virtual machine and enter the following URL:

   https://*ipaddress*

8. After you log in, set up the Connector:
   a. Specify the BlueXP account to associate with the Connector.
   b. Enter a name for the system.
   c. Under **Are you running in a secured environment?** keep restricted mode disabled.

      You should keep restricted mode disabled because these steps describe how to use BlueXP in standard mode. You should enable restricted mode only if you have a secure environment and want to disconnect this account from BlueXP backend services. If that's the case, follow steps to get started with BlueXP in restricted mode.

   d. Select **Let's start**.

Result

The Connector is now installed and is set up with your BlueXP account.

What's next?

Provide BlueXP with the permissions that you previously setup.

Provide Azure permissions to BlueXP

If you created the Connector from the Azure Marketplace or manually installed the software, you need to provide BlueXP with the permissions that you previously set up. Providing the permissions enables BlueXP to manage your data and storage infrastructure in Azure.

Learn how to set up these permissions.

These steps don’t apply if you deployed the Connector directly from BlueXP because BlueXP assigns the required permissions during deployment.

Custom role

Go to the Azure portal and assign the Azure custom role to the Connector virtual machine for one or more subscriptions.

Steps

1. From the Azure Portal, open the **Subscriptions** service and select your subscription.
2. Select **Access control (IAM)** > **Add** > **Add role assignment**.
3. In the **Role** tab, select the **BlueXP Operator** role and select **Next**.

   BlueXP Operator is the default name provided in the BlueXP policy. If you chose a different name for the role, then select that name instead.

4. In the **Members** tab, complete the following steps:
   a. Assign access to a **Managed identity**.
   b. Select **Select members**, select the subscription in which the Connector virtual machine was created, choose **Virtual machine**, and then select the Connector virtual machine.
   c. Select **Select**.
   d. Select **Next**.
   e. Select **Review + assign**.
   f. If you want to manage resources in additional Azure subscriptions, switch to that subscription and then repeat these steps.

Result

BlueXP now has the permissions that it needs to perform actions in Azure on your behalf.

What's next?

Go to the BlueXP console to start using the Connector with BlueXP.

Service principal

Steps

1. In the upper right of the BlueXP console, select the Settings icon, and select **Credentials**.

2. Select **Add Credentials** and follow the steps in the wizard.
   a. **Credentials Location**: Select **Microsoft Azure > Connector**.
   b. **Define Credentials**: Enter information about the Azure Active Directory service principal that grants the required permissions:
      - Application (client) ID
      - Directory (tenant) ID
      - Client Secret
   c. **Marketplace Subscription**: Associate a Marketplace subscription with these credentials by

subscribing now or by selecting an existing subscription.

d. **Review**: Confirm the details about the new credentials and select **Add**.

Result

BlueXP now has the permissions that it needs to perform actions in Azure on your behalf.

Copyright information

Trademark information