∏ NetApp

Get started with private mode

Setup and administration

NetApp
September 19, 2023

Table of Contents

Get started with private mode

Getting started workflow (private mode)

Get started with BlueXP in private mode by preparing your environment and deploying the Connector.

Before you get started, you should have an understanding of BlueXP accounts, Connectors, and deployment modes.

1   **Prepare for deployment**

a. Prepare a dedicated Linux host that meets requirements for CPU, RAM, disk space, Docker Engine, and more.

b. Set up networking that provides access to the target networks.

c. For cloud deployments, set up permissions in your cloud provider so that you can associate those permissions with the Connector after you install the software.

2   **Deploy the Connector**

a. Install the Connector software on your own Linux host.

b. Set up BlueXP by opening a web browser and entering the Linux host's IP address.

c. For cloud deployments, provide BlueXP with the permissions that you previously set up.

Prepare for deployment in private mode

Prepare your environment before you deploy BlueXP in private mode. For example, you need to review host requirements, prepare networking, set up permissions, and more.

> ℹ️ If you want to use BlueXP in the AWS Secret Cloud or the AWS Top Secret Cloud, then you should follow separate instructions to get started in those environments. Learn how to get started with Cloud Volumes ONTAP in the AWS Secret Cloud or Top Secret Cloud

Step 1: Understand how private mode works

Before you get started, you should have an understanding of how BlueXP works in private mode.

For example, you should understand that you need to use the browser-based interface that is available locally from the BlueXP Connector that you need to install. You can't access BlueXP from the web-based console that's provided through the SaaS layer.

In addition, not all BlueXP services are available.

Learn how private mode works.

Step 2: Review installation options

In private mode, you can install the Connector on premises or in the cloud by manually installing the Connector on your own Linux host.

If you want to create a Cloud Volumes ONTAP system in Google Cloud, then the Connector must be running in Google Cloud—it can't be running on premises.

Step 3: Review host requirements

The Connector software must run on a host that meets specific operating system requirements, RAM requirements, port requirements, and so on.

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

AWS EC2 instance type

An instance type that meets the CPU and RAM requirements above. We recommend t3.xlarge.

Azure VM size

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

Google Cloud machine type

An instance type that meets the CPU and RAM requirements above. We recommend n2-standard-4.

The Connector is supported in Google Cloud on a VM instance with an OS that supports Shielded VM features

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

Step 4: Prepare networking for the Connector

Set up your networking so the Connector can manage resources and processes within your public cloud environment. Other than having a virtual network and subnet for the Connector, you'll need to ensure that the following requirements are met.

Connections to target networks

    The Connector must have a network connection to the location where you plan to manage storage. For example, the VPC or VNet where you plan to deploy Cloud Volumes ONTAP, or the data center where your on-premises ONTAP clusters reside.
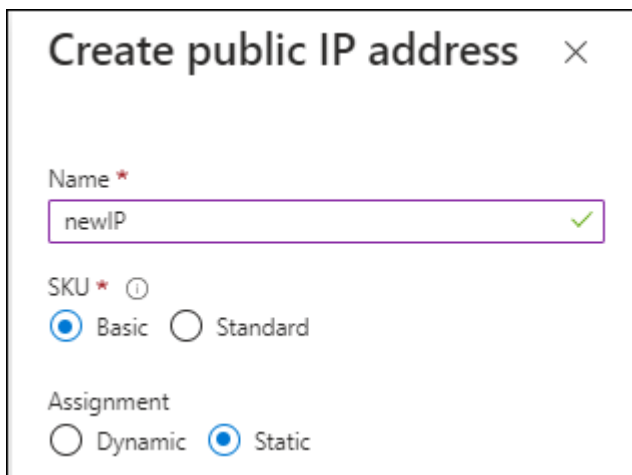
Endpoints for day-to-day operations

    The Connector contacts the following endpoints to manage resources and processes within your public cloud environment.

Endpoints	Purpose
AWS services (amazonaws.com): • CloudFormation • Elastic Compute Cloud (EC2) • Identity and Access Management (IAM) • Key Management Service (KMS) • Security Token Service (STS) • Simple Storage Service (S3)	To manage resources in AWS. The exact endpoint depends on the AWS region that you're using. Refer to AWS documentation for details
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.azure.microsoft.scloud https://login.microsoftonline.microsoft.scloud https://blob.core.microsoft.scloud https://core.microsoft.scloud	To manage resources in the Azure IL6 region.

Endpoints	Purpose
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://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	To manage resources in Google Cloud.

Public IP address in Azure

If you want to use a public IP address with the Connector VM in Azure, the IP address must use a Basic SKU to ensure that BlueXP uses this public IP address.

If you use a Standard SKU IP address instead, then BlueXP uses the *private* IP address of the Connector, instead of the public IP. If the machine that you're using to access the BlueXP Console doesn't have access to that private IP address, then actions from the BlueXP Console will fail.

Azure documentation: Public IP SKU

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

With private mode, the only time that BlueXP sends outbound traffic is to your cloud provider in order to create a Cloud Volumes ONTAP system.

Ports

There's no incoming traffic to the Connector, unless you initiate it.

HTTP (80) and HTTPS (443) provide access to the BlueXP console. SSH (22) is only needed if you need to connect to the host for troubleshooting.

Step 5: Prepare cloud permissions

If you are planning to create Cloud Volumes ONTAP systems, then BlueXP requires permissions from your cloud provider. You need to set up permissions in your cloud provider and then associate those permission with the Connector instance after you install it.

To view the required steps, select the authentication option that you'd like to use for your cloud provider.

If you're going to install the Connector on premises, then you must provide permissions using AWS access keys or an Azure service principal. The other options are not supported.

AWS IAM role

Use an IAM role to provide the Connector with permissions. You'll need to manually attach the role to the EC2 instance for the Connector.

Steps

1. Log in to the AWS console and navigate to the IAM service.

2. Create a policy:

    a. Select **Policies > Create policy**.

    b. Select **JSON** and copy and paste the contents of the IAM policy for the Connector.

    c. Finish the remaining steps to create the policy.

3. Create an IAM role:

    a. Select **Roles > Create role**.

    b. Select **AWS service > EC2**.

    c. Add permissions by attaching the policy that you just created.

    d. Finish the remaining steps to create the role.

Result

You now have an IAM role for the Connector EC2 instance.

AWS access key

Set up permissions and an access key for an IAM user. You'll need to provide BlueXP with the AWS access key after you install the Connector and set up BlueXP.

Steps

1. Log in to the AWS console and navigate to the IAM service.

2. Create a policy:

    a. Select **Policies > Create policy**.

    b. Select **JSON** and copy and paste the contents of the IAM policy for the Connector.

    c. Finish the remaining steps to create the policy.

    Depending on the BlueXP services that you're planning to use, you might need to create a second policy.

    For standard regions, the permissions are spread across two policies. Two policies are required due to a maximum character size limit for managed policies in AWS. Learn more about IAM policies for the Connector.

3. Attach the policies to an IAM user.

    ◦ AWS Documentation: Creating IAM Roles

    ◦ AWS Documentation: Adding and Removing IAM Policies

4. Ensure that the user has an access key that you can add to BlueXP after you install the Connector.

Result

The account now has the required permissions.

Azure role

Create an Azure custom role with the required permissions. You'll assign this role to the Connector VM.

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. Enable a system-assigned managed identity on the VM where you plan to install the Connector 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.
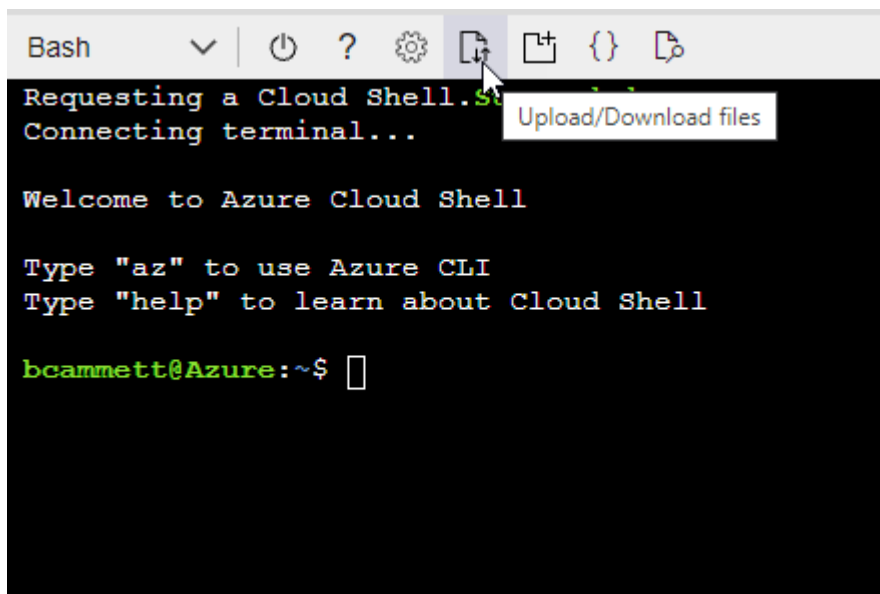
    c. Use the Azure CLI to create the custom role:

```
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.

Azure service principal

Create and set up a service principal in Azure Active Directory and obtain the Azure credentials that BlueXP needs. You'll need to provide BlueXP with these credentials after you install the Connector and set up BlueXP.

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.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

DESCRIPTION	EXPIRES	VALUE	Copy to clipboard
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA	

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.

Google Cloud service account

Create a role and apply it to a service account that you'll use for the Connector VM instance.

Steps

1. Create a custom role in Google Cloud:

   a. Create a YAML file that includes the permissions defined in the Connector policy for Google Cloud.

   b. From Google Cloud, activate cloud shell.

   c. Upload the YAML file that includes the required permissions for the Connector.

   d. Create a custom role by using the `gcloud iam roles create` command.

   The following example creates a role named "connector" at the project level:

   ```
   gcloud iam roles create connector --project=myproject
   --file=connector.yaml
   ```

   Google Cloud docs: Creating and managing custom roles

2. Create a service account in Google Cloud:

   a. From the IAM & Admin service, select **Service Accounts > Create Service Account**.

   b. Enter service account details and select **Create and Continue**.

   c. Select the role that you just created.

   d. Finish the remaining steps to create the role.

   Google Cloud docs: Creating a service account

Result

You now have a service account that you can assign to the Connector VM instance.

Step 6: Enable Google Cloud APIs

Several APIs are required to deploy Cloud Volumes ONTAP in Google Cloud.

Step

1. Enable the following Google Cloud APIs in your project

    ◦ Cloud Deployment Manager V2 API

    ◦ Cloud Logging API

    ◦ Cloud Resource Manager API

    ◦ Compute Engine API

    ◦ Identity and Access Management (IAM) API

    ◦ Cloud Key Management Service (KMS) API

    (Required only if you are planning to use BlueXP backup and recovery with customer-managed encryption keys (CMEK))

Deploy the Connector in private mode

Deploy the Connector in private mode so that you can use BlueXP with no outbound connectivity to the BlueXP SaaS layer. To get started, install the Connector, set up BlueXP by accessing the user interface that's running on the Connector, and then provide the cloud permissions that you previously set up.

Step 1: Install the Connector

Download the product installer from the NetApp Support Site and then manually install the Connector on your own Linux host.

If you want to use BlueXP in the AWS Secret Cloud or the AWS Top Secret Cloud, then you should follow separate instructions to get started in those environments. Learn how to get started with Cloud Volumes ONTAP in the AWS Secret Cloud or Top Secret Cloud

Required privileges

Root privileges are required to install the Connector.

Steps

1. Verify that docker is enabled and running.

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

2. Download the Connector software from the NetApp Support Site

   Be sure to download the installer for restricted networks without internet access.

3. Copy the installer to the Linux host.

4. Assign permissions to run the script.

```
chmod +x /path/cloud-manager-connector-offline-<version>
```

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

5. Run the installation script:

```
sudo /path/cloud-manager-connector-offline-<version>
```

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

Result

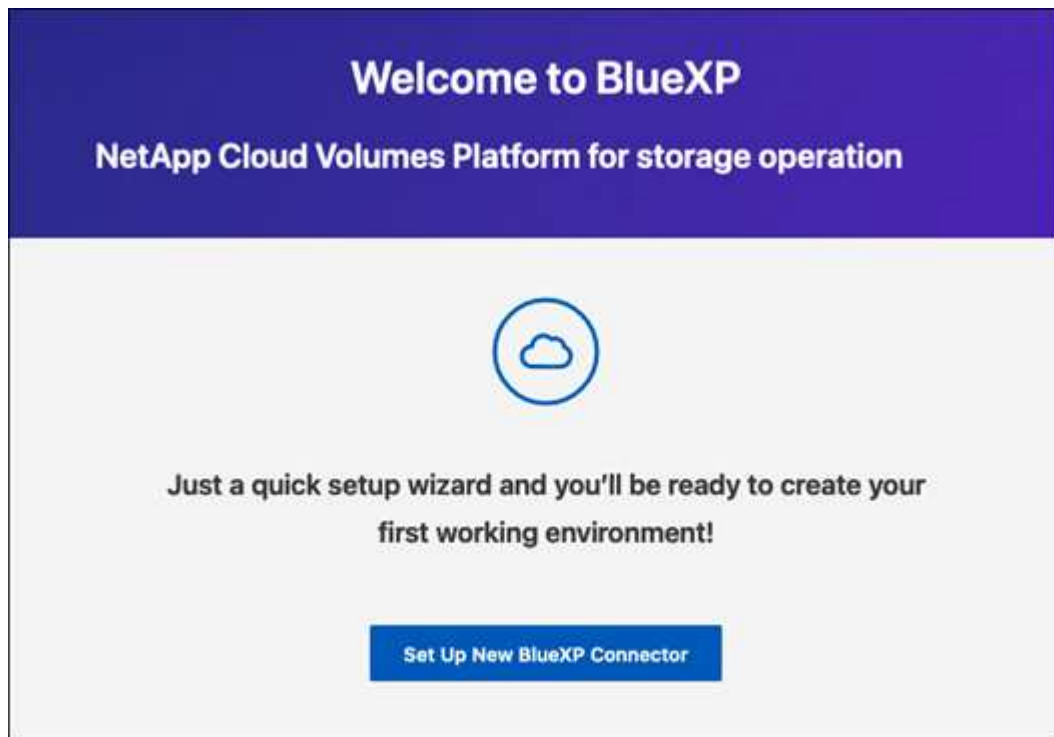The Connector software is installed. You can now set up BlueXP.

Step 2: Set up BlueXP

When you access the BlueXP console for the first time, you'll be prompted to set up BlueXP.

Steps

1. Open a web browser and enter https://*ipaddress* where *ipaddress* is the IP address of the Linux host where you installed the Connector.

   You should see the following screen.

2. Select **Set Up New BlueXP Connector** and follow the prompts to set up the system.
   ◦ **System Details**: Enter a name for the Connector and your company name.

◦ **Create an Admin User**: Create the admin user for the system.

This user account runs locally on the system. There's no connection to the auth0 service available through BlueXP.

◦ **Review**: Review the details, accept the license agreement, and then select **Set Up**.

3. Log in to BlueXP using the admin user that you just created.

Result

The Connector is now installed and set up.

When new versions of the Connector software are available, they'll be posted to the NetApp Support Site. Learn how to upgrade the Connector.

What's next?

Provide BlueXP with the permissions that you previously set up.

Step 3: Provide permissions to BlueXP

If you want to create Cloud Volumes ONTAP working environments, you'll need to provide BlueXP with the cloud permissions that you previously set up.

Learn how to prepare cloud permissions.

AWS IAM role

Attach the IAM role that you previously created to the Connector EC2 instance.

Steps

1. Go to the Amazon EC2 console.

2. Select **Instances**.

3. Select the Connector instance.

4. Select **Actions > Security > Modify IAM role**.

5. Select the IAM role and select **Update IAM role**.

Result

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

AWS access key

Provide BlueXP with the AWS access key for an IAM user that has the required permissions.

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 **Amazon Web Services > Connector**.

   b. **Define Credentials**: Enter an AWS access key and secret key.

   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 AWS on your behalf.

Azure 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.

Azure service principal

Provide BlueXP with the credentials for the Azure service principal that you previously setup.

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.

Google Cloud service account

Associate the service account with the Connector VM.

Steps

1. Go to the Google Cloud portal and assign the service account to the Connector VM instance.

   Google Cloud documentation: Changing the service account and access scopes for an instance

2. If you want to manage resources in other projects, grant access by adding the service account with the BlueXP role to that project. You'll need to repeat this step for each project.

> **Result**
>
> BlueXP now has the permissions that it needs to perform actions in Google Cloud on your behalf.

What you can do next (private mode)

After you get up and running with BlueXP in private mode, you can start using the BlueXP services that are supported with private mode.

For help, refer to the following documentation:

- Create Cloud Volumes ONTAP systems
- Discover on-premises ONTAP clusters
- Replicate data
- Scan on-prem ONTAP volume data using BlueXP classification
- Back up on-prem ONTAP volume data to StorageGRID using BlueXP backup and recovery

Related link

BlueXP deployment modes