Get started

BlueXP setup and administration

NetApp
August 29, 2025

Table of Contents

Get started

Learn the basics

Learn about BlueXP

NetApp BlueXP provides your organization with a single control plane that helps you build, protect, and govern data across your on-premises and cloud environments. The BlueXP software as a service (SaaS) platform includes services that provide storage management, data mobility, data protection, and data analysis and control. Management capabilities are provided through a web-based console and APIs.

Features

BlueXP provides unified control of storage across your hybrid multicloud and integrated data services to protect, secure, and optimize data.

Unified control of storage from the BlueXP canvas

The *BlueXP canvas* lets you discover, deploy, and manage cloud and on-premises storage. The canvas centralizes storage management.

Supported cloud and on-premises storage

BlueXP enables you to manage the following types of storage from the BlueXP canvas:

Cloud storage solutions

- Amazon FSx for NetApp ONTAP
- Azure NetApp Files
- Cloud Volumes ONTAP
- Google Cloud NetApp Volumes

On-premises flash and object storage

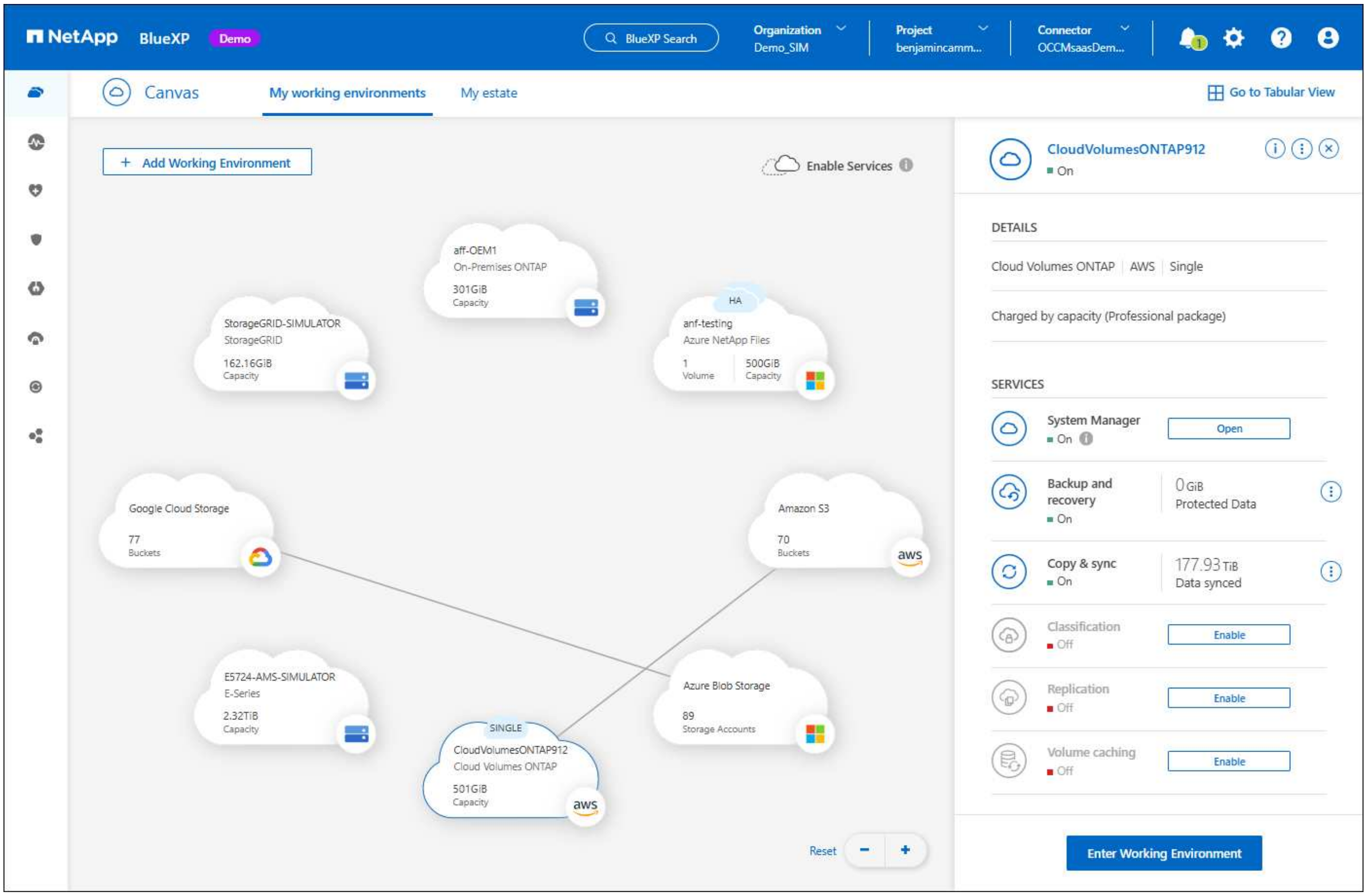
- E-Series systems
- ONTAP clusters
- StorageGRID systems

Cloud object storage

- Amazon S3 storage
- Azure Blob storage
- Google Cloud Storage

Storage management from working environments

On the BlueXP canvas, *working environments* represent discovered or deployed storage. You can select a *working environment* to integrate it with BlueXP data services or manage storage, such as adding volumes.



CloudVolumesONTAP912
On

DETAILS

Cloud Volumes ONTAP | AWS | Single

Charged by capacity (Professional package)

SERVICES

System Manager On		Open
Backup and recovery On	0 GiB Protected Data	
Copy & sync On	177.93 TiB Data synced	
Classification Off		Enable
Replication Off		Enable
Volume caching Off		Enable

Enter Working Environment

Integrated services to protect, secure, and optimize data

BlueXP includes data services to secure and maintain data availability across storage.

BlueXP alerts

View issues related to capacity, availability, performance, protection, and security in your ONTAP environment.

BlueXP automation catalog

Use scripted solutions to automate the deployment and integration of NetApp products and services.

BlueXP backup and recovery

Back up and restore cloud and on-premises data.

BlueXP classification

Get your application data and cloud environments privacy ready.

BlueXP copy and sync

Sync data between on-premisesand cloud data stores.

BlueXP digital advisor

Use predictive analytics and proactive support to optimize your data infrastructure.

BlueXP digital wallet

Manage and monitor your licenses and subscriptions.

BlueXP disaster recovery

Protect on-premises VMware workloads using VMware Cloud on Amazon FSx for ONTAP as a disaster recovery site.

BlueXP economic efficiency

Identify clusters with current or forecasted low capacity and implement data tiering or additional capacity recommendations.

BlueXP ransomware protection

Detect anomalies that might result in ransomware attacks. Protect and recover workloads.

BlueXP replication

Replicate data between storage systems to support backup and disaster recovery.

BlueXP software updates

Automate the assessment, planning, and execution of ONTAP upgrades.

BlueXP sustainability dashboard

Analyze the sustainability of your storage systems.

BlueXP tiering

Extend your on-premises ONTAP storage to the cloud.

BlueXP volume caching

Create a writable cache volume to speed up access to data or offload traffic from heavily accessed volumes.

BlueXP workload factory

Design, set up, and operate key workloads using Amazon FSx for NetApp ONTAP.

Learn more about BlueXP and the available data services

Supported cloud providers

BlueXP enables you to manage cloud storage and use cloud services in Amazon Web Services, Microsoft Azure, and Google Cloud.

Cost

Pricing for BlueXP depends on the services that you use.
Learn about BlueXP pricing

How BlueXP works

BlueXP includes a web-based console that’s provided through the SaaS layer, a resource and access management system, Connectors that manage working environments and enable BlueXP cloud services, and different deployment modes to meet your business requirements.

Software-as-a-service

BlueXP is accessible through a web-based console and APIs. This SaaS experience enables you to automatically access the latest features as they’re released and to easily switch between your BlueXP organizations, projects, and Connectors.

BlueXP identity and access management (IAM)

BlueXP identity and access management (IAM) is a resource and access management model that provides granular management of resources and permissions:

- A top-level *organization* enables you to manage access across your various *projects*
- *Folders* enable you to group related projects together
- Resource management enables you to associate a resource with one or more folders or projects
- Access management enables you to assign a role to members at different levels of the organization hierarchy

BlueXP IAM is supported when using BlueXP in standard or restricted mode. If you're using BlueXP in private mode, then you use a BlueXP *account* to manage workspaces, users, and resources.

- Learn more about BlueXP IAM

Connectors

You don't need a Connector to get started with BlueXP, but you'll need to create a Connector to unlock all BlueXP features and services. A Connector enables you to manage resources and processes across your on-premises and cloud environments. You need it to manage working environments (for example, Cloud Volumes ONTAP) and to use many BlueXP services.

Learn more about Connectors.

Deployment modes

BlueXP offers three deployment modes. *Standard mode* leverages the BlueXP software as a service (SaaS) layer to provide full functionality. If your environment has security and connectivity restrictions, *restricted mode* and *private mode* limit outbound connectivity to the BlueXP SaaS layer.

Learn more about BlueXP deployment modes.

SOC 2 Type 2 certification

An independent certified public accountant firm and services auditor examined BlueXP and affirmed that BlueXP achieved SOC 2 Type 2 reports based on the applicable Trust Services criteria.

View NetApp's SOC 2 reports

Learn about BlueXP Connectors

A *Connector* is NetApp software running in your cloud network or on-premises network. It's used to connect BlueXP's services to your storage environments.

What you can do without a Connector

A Connector isn't required to get started with BlueXP. You can use several features and services within BlueXP without ever creating a Connector.

You can use the following BlueXP features and services without a Connector:

- Amazon FSx for NetApp ONTAP

Some actions require a Connector or a BlueXP workload factory link. Learn which actions require a Connector or link

- Automation catalog
- Azure NetApp Files

  While a Connector isn’t required to set up and manage Azure NetApp Files, a Connector is required if you want to use BlueXP classification to scan Azure NetApp Files data.

- Cloud Volumes Service for Google Cloud
- Copy and sync
- Digital advisor
- Digital wallet (licenses only, subscription monitoring requires a Connector)

  In almost all cases, you can add a license to the digital wallet without a Connector.

  The only time that a Connector is required to add a license to the digital wallet is for Cloud Volumes ONTAP *node-based* licenses. A Connector is required in this case because the data is taken from the licenses installed on Cloud Volumes ONTAP systems.

- Direct discovery of on-premises ONTAP clusters

  While a Connector isn’t required for direct discovery of an on-premises ONTAP cluster, a Connector is required if you want to take advantage of additional BlueXP features.

  Learn more about discovery and management options for on-premises ONTAP clusters

- Software updates
- Sustainability
- Workload factory

When a Connector is required

When you use BlueXP in standard mode, a Connector is required for the following features and services in BlueXP:

- Alerts
- Amazon FSx for ONTAP management features
- Amazon S3 storage
- Azure Blob storage
- Backup and recovery
- Classification
- Cloud Volumes ONTAP
- Disaster recovery
- E-Series systems
- Economic efficiency [1]
- Google Cloud Storage buckets

- On-premises ONTAP cluster integration with BlueXP data services
- Ransomware protection
- StorageGRID systems
- Tiering
- Volume caching

[1] While you can access these services without a Connector, a Connector is required to initiate actions from the services.

A Connector is required to use BlueXP in restricted mode or private mode.

Connectors must be operational at all times

Connectors are a fundamental part of the BlueXP service architecture. It's your responsibility to ensure that relevant Connectors are up, operational, and accessible at all times. While the service is designed to overcome short outages of Connector availability, you must take immediate action when required to remedy infrastructure failures.

This documentation is governed by the EULA. If the product is not operated in accordance with the documentation, the functionality and operation of the product, as well as your rights under the EULA, might be adversely impacted.

Supported locations

A Connector is supported in the following locations:

- Amazon Web Services
- Microsoft Azure

  A Connector in Azure 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

- Google Cloud

  If you want to use BlueXP services with Google Cloud, then you must use a Connector that's running in Google Cloud.

- On your premises

Communication with cloud providers

The Connector uses TLS 1.3 for all communication to AWS, Azure, and Google Cloud.

Restricted mode and private mode

To use BlueXP in restricted mode or private mode, you get started with BlueXP by installing the Connector and then accessing the user interface that's running locally on the Connector.

Learn about BlueXP deployment modes.

How to install a Connector

You can install a Connector directly from BlueXP, from your cloud provider's marketplace, or by manually installing the software on your own Linux host. How you get started depends on whether you're using BlueXP in standard mode, restricted mode, or private mode.

- Learn about BlueXP deployment modes
- Get started with BlueXP in standard mode
- Get started with BlueXP in restricted mode
- Get started with BlueXP in private mode

Permissions

Specific permissions are needed to create the Connector directly from BlueXP and another set of permissions are needed for the Connector instance itself. If you create the Connector in AWS or Azure directly from BlueXP, then BlueXP creates the Connector with the permissions that it needs.

When using BlueXP in standard mode, how you provide permissions depends on how you plan to create the Connector.

To learn how to set up permissions, refer to the following:

- Standard mode
  - Connector installation options in AWS
  - Connector installation options in Azure
  - Connector installation options in Google Cloud
  - Set up cloud permissions for on-premises deployments
- Set up permissions for restricted mode
- Set up permissions for private mode

To view the exact permissions that the Connector needs for day-to-day operations, refer to the following pages:

- Learn how the Connector uses AWS permissions
- Learn how the Connector uses Azure permissions
- Learn how the Connector uses Google Cloud permissions

It's your responsibility to update the Connector policies as new permissions are added in subsequent releases. If new permissions are required, they will be listed in the release notes.

Connector upgrades

We typically update the Connector software each month to introduce new features and to provide stability improvements. While most of the services and features in the BlueXP platform are offered through SaaS-based software, a few features are dependent on the version of the Connector. That includes Cloud Volumes ONTAP management, on-premisesONTAP cluster management, settings, and help.

When you use BlueXP in standard mode or restricted mode, the Connector automatically updates its software to the latest version, as long as it has outbound internet access to obtain the software update. If you're using BlueXP in private mode, then you'll need to manually upgrade the Connector.

Learn how to manually upgrade the Connector software when using private mode.

Operating system and VM maintenance

Maintaining the operating system on the Connector host is your (customer's) responsibility. For example, you (customer) should apply security updates to the operating system on the Connector host by following your company's standard procedures for operating system distribution.

Note that you (customer) don't need to stop any services on the Connector host when applying minor security updates.

If you (customer) need to stop and then start the Connector VM, you should do so from your cloud provider's console or by using the standard procedures for on-premises management.

Be aware that the Connector must be operational at all times.

Multiple working environments and Connectors

A Connector can manage multiple working environments in BlueXP. The maximum number of working environments that a single Connector should manage varies. It depends on the type of working environments, the number of volumes, the amount of capacity being managed, and the number of users.

If you have a large-scale deployment, work with your NetApp representative to size your environment. If you experience any issues along the way, reach out to us by using the in-product chat.

In some cases, you might only need one Connector, but you might find yourself needing two or more Connectors.

Here are a few examples:

- You have a multicloud environment (for example, AWS and Azure) and you prefer to have one Connector in AWS and another in Azure. Each manages the Cloud Volumes ONTAP systems running in those environments.
- A service provider might use one BlueXP organization to provide services for their customers, while using another organization to provide disaster recovery for one of their business units. Each organization would have separate Connectors.

Learn about BlueXP deployment modes

BlueXP offers *deployment modes* that enable you to meet your business and security requirements. *Standard mode* leverages a software as a service (SaaS) layer to provide full functionality, while *restricted mode* and *private mode* are available for organizations that have connectivity restrictions.

While BlueXP inhibits the flow of traffic, communication, and data when using restricted mode or private mode, it's your responsibility to ensure that your environment (on-premises and in the cloud) is in compliance with the required regulations for your business.

Overview

Each deployment mode differs in outbound connectivity, location, installation, authentication, data services, and charging methods.

Standard mode

You use a SaaS service from the web-based console. Depending on the data services and features that you plan to use, a BlueXP admin creates one or more Connectors to manage data within your hybrid cloud environment.

This mode uses encrypted data transmission over the public internet.

Restricted mode

You install a BlueXP Connector in the cloud (in a government, sovereign, or commercial region), and it has limited outbound connectivity to the BlueXP SaaS layer.

This mode is typically used by state and local governments and regulated companies.

Learn more about outbound connectivity to the SaaS layer.

Private mode

You install a BlueXP Connector on-premises or in the cloud (in a secure region, sovereign cloud region, or commercial region) and has *no* connectivity to the BlueXP SaaS layer. Users access the BlueXP console provided by the Connector locally, not the SaaS layer.

A secure region includes AWS Secret Cloud, AWS Top Secret Cloud, and Azure IL6

The following table provides a comparison of these modes.

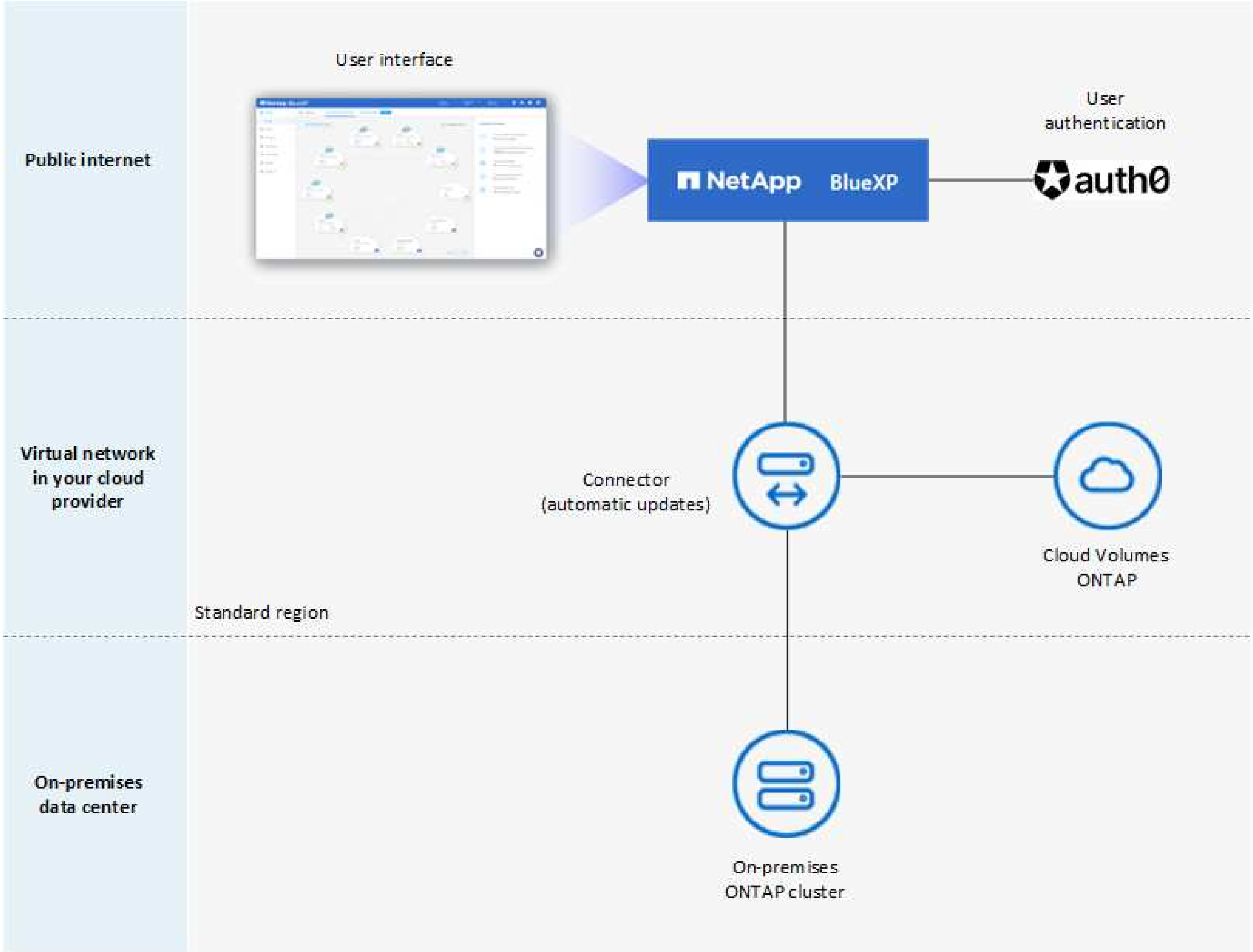
	Standard mode	Restricted mode	Private mode
Connection required to BlueXP SaaS layer?	Yes	Outbound only	No
Connection required to your cloud provider?	Yes	Yes, within the region	Yes, within the region (if using Cloud Volumes ONTAP)
Connector installation	From BlueXP, cloud marketplace, or manual install	Cloud marketplace or manual install	Manual install
Connector upgrades	Automatic upgrades of NetApp Connector software	Automatic upgrades of NetApp Connector software	Manual upgrade required
UI access	From the BlueXP SaaS layer	Locally from the Connector VM	Locally from the Connector VM
API endpoint	The BlueXP SaaS layer	The Connector	The Connector
Authentication	Through SaaS using auth0, NSS login, or identity federation	Through SaaS using auth0 or identity federation	Local user authentication
Multi-factor authentication	Available for local users	Not available	Not available
Storage and data services	All are supported	Many are supported	Several are supported

	Standard mode	Restricted mode	Private mode
Data service licensing options	Marketplace subscriptions and BYOL	Marketplace subscriptions and BYOL	BYOL

Read through the following sections to learn more about these modes, including which BlueXP features and services are supported.

Standard mode

The following image is an example of a standard mode deployment.



BlueXP works as follows in standard mode:

Outbound communication

Connectivity is required from the Connector to the BlueXP SaaS layer, to your cloud provider's publicly available resources, and to other essential components for day-to-day operations.

- Endpoints that the Connector contacts in AWS
- Endpoints that the Connector contacts in Azure

- Endpoints that the Connector contacts in Google Cloud

Supported location for the Connector

In standard mode, the Connector is supported in the cloud or on your premises.

Connector installation

You can install the Connector using the BlueXP setup wizard, AWS or Azure Marketplace, the Google Cloud SDK, or a manual installer on a Linux host in your data center or cloud.

Connector upgrades

BlueXP provides automated upgrades of the Connector software with monthly updates.

User interface access

The user interface is accessible from the web-based console that's provided through the SaaS layer.

API endpoint

API calls are made to the following endpoint:
https://cloudmanager.cloud.netapp.com

Authentication

BlueXP provides authentication with auth0 or NetApp Support Site (NSS) logins. Identity federation is available.

Supported BlueXP services

All BlueXP services are available to users.

Supported licensing options

Marketplace subscriptions and BYOL are supported with standard mode; however, the supported licensing options depends on which BlueXP service you are using. Review the documentation for each service to learn more about the available licensing options.

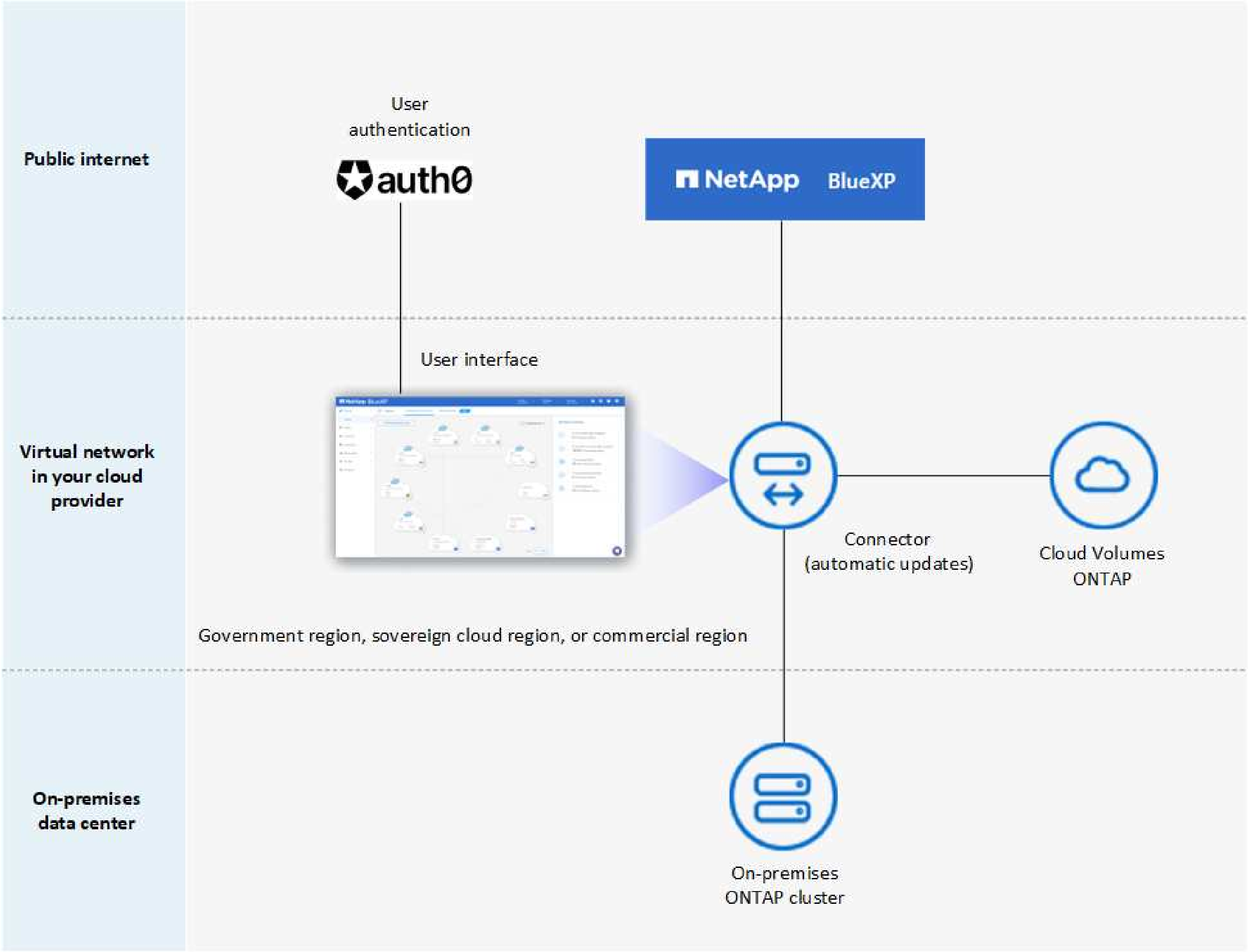
How to get started with standard mode

Go to the BlueXP web-based console and sign up.

Learn how to get started with standard mode.

Restricted mode

The following image is an example of a restricted mode deployment.


Public internet
Virtual network in your cloud provider
On-premises data center
User authentication
auth0
NetApp BlueXP
User interface
Connector (automatic updates)
Cloud Volumes ONTAP
Government region, sovereign cloud region, or commercial region
On-premises ONTAP cluster

BlueXP works as follows in restricted mode:

Outbound communication

The Connector requires outbound connectivity to the BlueXP SaaS layer for data services, software upgrades, authentication, and metadata transmission.

The BlueXP SaaS layer does not initiate communication to the Connector. All communication is initiated by the Connector, which can pull or push data from or to the SaaS layer as required.

A connection is also required to cloud provider resources from within the region.

Supported location for the Connector

In restricted mode, the Connector is supported in the cloud: in a government region, sovereign region, or commercial region.

Connector installation

Connector installation is possible from the AWS or Azure Marketplace or a manual installation on your own Linux host.

Connector upgrades

BlueXP provides automated upgrades of the Connector software with monthly updates.

User interface access

The user interface is accessible from the Connector virtual machine that's deployed in your cloud region.

API endpoint

API calls are made to the Connector virtual machine.

Authentication

Authentication is provided through BlueXP's cloud service using auth0. Identity federation is also available.

Supported BlueXP services

BlueXP supports the following storage and data services with restricted mode:

Supported services	Notes
Azure NetApp Files	Full support
Backup and recovery	Supported in Government regions and commercial regions with restricted mode. Not supported in sovereign regions with restricted mode. In restricted mode, BlueXP backup and recovery supports back up and restore of ONTAP volume data only. View the list of supported backup destinations for ONTAP data In restricted mode, BlueXP backup and recovery supports back up and restore of ONTAP volume data only. View the list of supported backup destinations for ONTAP data Back up and restore of application data and virtual machine data is not supported.
Classification	Supported in Government regions with restricted mode. Not supported in commercial regions or in sovereign regions with restricted mode.
Cloud Volumes ONTAP	Full support
Digital wallet	You can use the digital wallet with the supported licensing options listed below for restricted mode.
On-premises ONTAP clusters	Discovery with a Connector and discovery without a Connector (direct discovery) are both supported. When you discover an on-premisescluster with a Connector, the Advanced view (System Manager) is not supported.
Replication	Supported in Government regions with restricted mode. Not supported in commercial regions or in sovereign regions with restricted mode.

Supported licensing options

The following licensing options are supported with restricted mode:

- Marketplace subscriptions (hourly and annual contracts)

  Note the following:

  - For Cloud Volumes ONTAP, only capacity-based licensing is supported.
  - In Azure, annual contracts are not supported with government regions.

- BYOL

  For Cloud Volumes ONTAP, both capacity-based licensing and node-based licensing are supported with BYOL.

How to get started with restricted mode

You need to enable restricted mode when you create your BlueXP account.

If you don't have an organization yet, you are prompted to create your organization and enable restricted mode when you log in to BlueXP for the first time from a Connector that you manually installed or that you created from your cloud provider's marketplace.

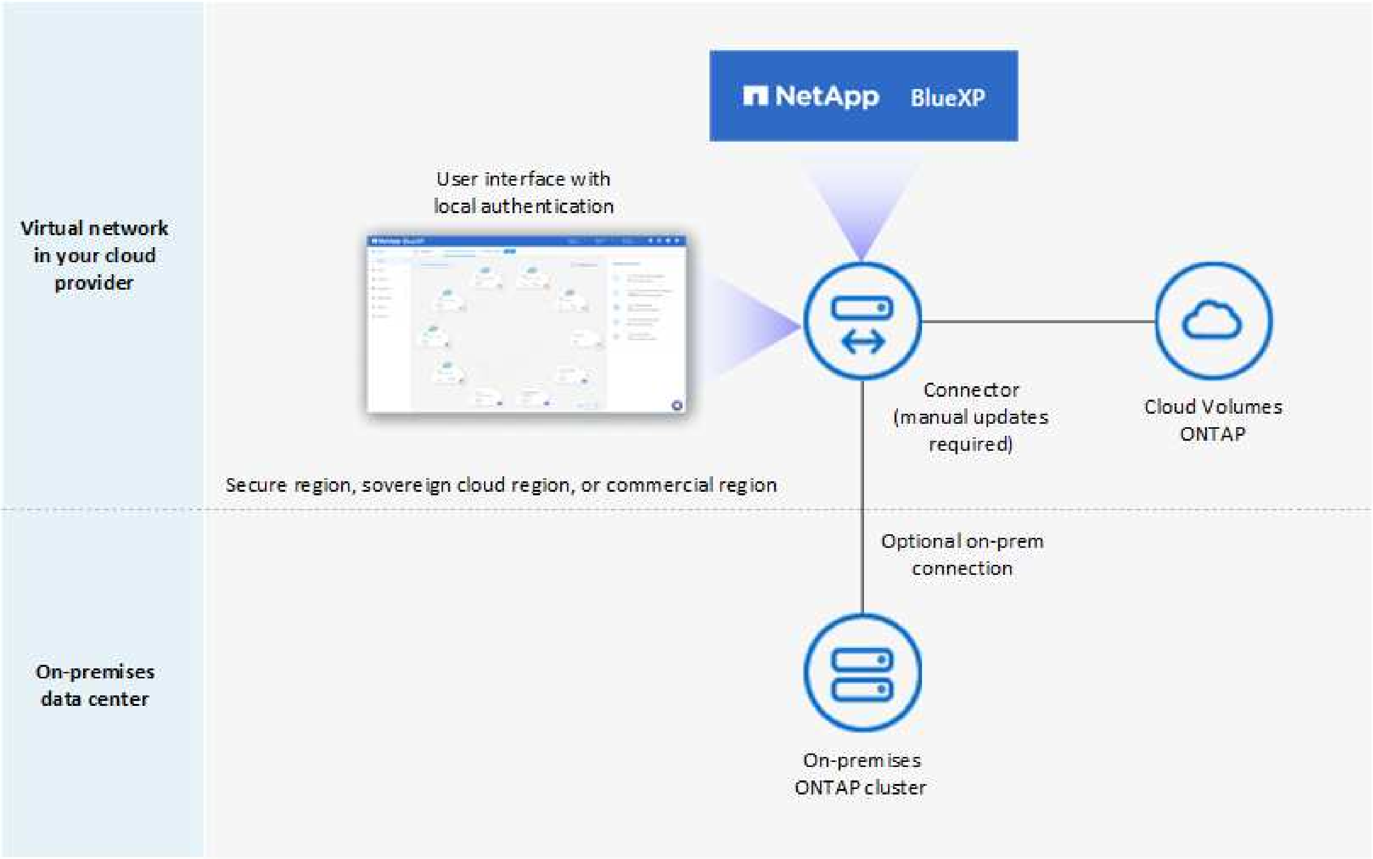
Note that you can't change the restricted mode setting after BlueXP creates the organization. You can't enable restricted mode later and you can't disable it later.

- Learn how to get started with restricted mode.

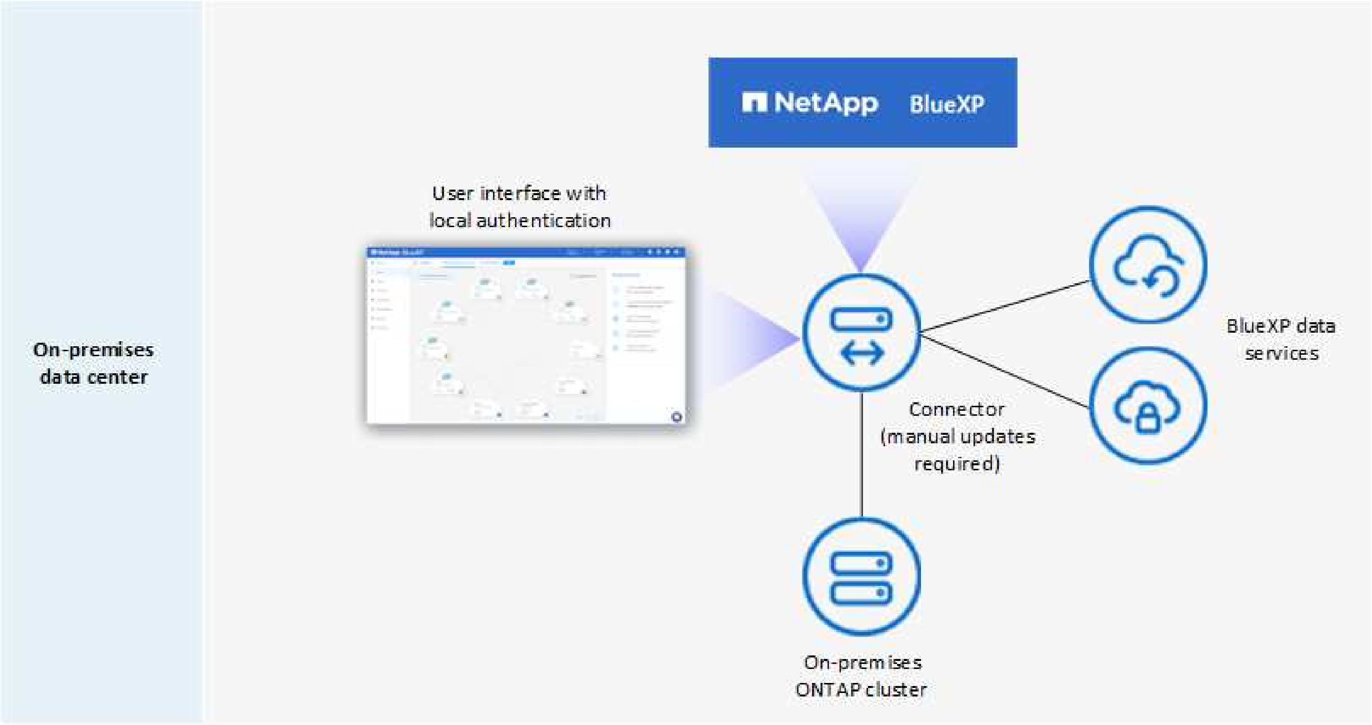
Private mode

In private mode, you can install a Connector either on-premises or in the cloud and then use BlueXP to manage data across your hybrid cloud. There is no connectivity to the BlueXP SaaS layer.

The following image shows an example of a private mode deployment where the Connector is installed in the cloud and manages both Cloud Volumes ONTAP and an on-premises ONTAP cluster.


NetApp BlueXP
Virtual network in your cloud provider
User interface with local authentication
Connector (manual updates required)
Cloud Volumes ONTAP
Secure region, sovereign cloud region, or commercial region
Optional on-prem connection
On-premises data center
On-premises ONTAP cluster

Meanwhile, the second image shows an example of a private mode deployment where the Connector is installed on-premises, manages an on-premises ONTAP cluster, and provides access to supported BlueXP data services.


On-premises data center
NetApp BlueXP
User interface with local authentication
BlueXP data services
Connector (manual updates required)
On-premises ONTAP cluster

BlueXP works as follows in private mode:

Outbound communication

No outbound connectivity is required to the BlueXP SaaS layer. All packages, dependencies, and essential components are packaged with the Connector and served from the local machine. Connectivity to your cloud provider's publicly available resources is required only if you are deploying Cloud Volumes ONTAP.

Supported location for the Connector

In private mode, the Connector is supported in the cloud or on-premises.

Connector installation

Manual installations of the Connector are supported on your own Linux host in the cloud or on-premises.

Connector upgrades

You need to upgrade the Connector software manually. The Connector software is published to the NetApp Support Site at undefined intervals.

User interface access

The user interface is accessible from the Connector that's deployed in your cloud region or on-premises.

API endpoint

API calls are made to the Connector virtual machine.

Authentication

Authentication is provided through local user management and access. Authentication is not provided through BlueXP's cloud service.

Supported BlueXP services in cloud deployments

BlueXP supports the following storage and data services with private mode when the Connector is installed in the cloud:

Supported services	Notes
Backup and recovery	Supported in AWS and Azure commercial regions. Not supported in Google Cloud or in AWS Secret Cloud, AWS Top Secret Cloud, or Azure IL6 In private mode, BlueXP backup and recovery supports back up and restore of ONTAP volume data only. View the list of supported backup destinations for ONTAP data Back up and restore of application data and virtual machine data is not supported.
Cloud Volumes ONTAP	Because there's no internet access, the following features aren't available: automated software upgrades and AutoSupport.
Digital wallet	You can use the digital wallet with the supported licensing options listed below for private mode.
On-premises ONTAP clusters	Requires connectivity from the cloud (where the Connector is installed) to the on-premises environment. Discovery without a Connector (direct discovery) is not supported.

Supported BlueXP services in on-premises deployments

BlueXP supports the following storage and data services with private mode when the Connector is installed on your premises:

Supported services	Notes
Backup and recovery	In private mode, BlueXP backup and recovery supports back up and restore of ONTAP volume data only. View the list of supported backup destinations for ONTAP volume data Back up and restore of application data and virtual machine data is not supported.
Classification	• The only supported data sources are the ones that you can discover locally. View the sources that you can discover locally • Features that require outbound internet access are not supported. View the feature limitations
Digital wallet	You can use the digital wallet with the supported licensing options listed below for private mode.
On-premises ONTAP clusters	Discovery without a Connector (direct discovery) is not supported.
Replication	Full support

Supported licensing options

Only BYOL is supported with private mode.

For Cloud Volumes ONTAP BYOL, only node-based licensing is supported. Capacity-based licensing is not supported. Because an outbound internet connection isn't available, you need to manually upload your Cloud Volumes ONTAP licensing file in the BlueXP digital wallet.

Learn how to add licenses to the BlueXP digital wallet

How to get started with private mode

Private mode is available by downloading the "offline" installer from the NetApp Support Site.

Learn how to get started with private mode.

> 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

Service and feature comparison

The following table can help you quickly identify which BlueXP services and features are supported with restricted mode and private mode.

Note that some services might be supported with limitations. For more details about how these services are supported with restricted mode and private mode, refer to the sections above.

Product area	BlueXP service or feature	Restricted mode	Private mode
Working environments This portion of the table lists support for working environment management from the BlueXP canvas. It does not indicate the supported backup destinations for BlueXP backup and recovery.	Amazon FSx for ONTAP	No	No
	Amazon S3	No	No
	Azure Blob	No	No
	Azure NetApp Files	Yes	No
	Cloud Volumes ONTAP	Yes	Yes
	Google Cloud NetApp Volumes	No	No
	Google Cloud Storage	No	No
	On-premisesONTAP clusters	Yes	Yes
	E-Series	No	No
	StorageGRID	No	No

Product area	BlueXP service or feature	Restricted mode	Private mode
Services	Alerts	No	No
	Backup and recovery	Yes View the list of supported backup destinations for ONTAP volume data	Yes View the list of supported backup destinations for ONTAP volume data
	Classification	Yes	Yes
	Copy and sync	No	No
	Digital advisor	No	No
	Digital wallet	Yes	Yes
	Disaster recovery	No	No
	Economic efficiency	No	No
	Ransomware protection	No	No
	Replication	Yes	Yes
	Software updates	No	No
	Sustainability	No	No
	Tiering	No	No
	Volume caching	No	No
	Workload factory	No	No
Features	Identity and access management	Yes	Yes
	Credentials	Yes	Yes
	Federation	Yes	No
	Multi-factor authentication	Yes	No
	NSS accounts	Yes	No
	Notifications	Yes	No
	Search	Yes	No
	Timeline	Yes	Yes

Get started with standard mode

Getting started workflow (standard mode)

Get started with BlueXP in standard mode by preparing networking for the BlueXP console, signing up and creating an account, optionally creating a Connector, and subscribing to NetApp Intelligent Services.

In standard mode, you access a web-based console that is hosted as a Software-as-a-service (SaaS) product from NetApp. Before you get started, you should have an understanding of deployment modes and Connectors.

1

Prepare networking for using the BlueXP console

Computers that access the BlueXP console should have connections to specific endpoints to complete a few administrative tasks. If your network restricts outbound access, you should ensure that these endpoints are allowed.

2

Sign up and create an organization

Go to the BlueXP console and sign up. You'll be given the option to create an organization, but you can skip that step if you're being invited to an existing organization.

At this point, you're logged in and can start using several BlueXP services like Digital Advisor, Amazon FSx for ONTAP, Azure NetApp Files, and more. Learn what you can do without a Connector.

3

Create a Connector

You don't need a Connector to get started with BlueXP, but you can create a Connector to unlock all BlueXP features and services. The Connector is NetApp software that enables BlueXP to manage resources and processes within your hybrid cloud environment.

You can create a Connector in your cloud or on-premises network.

- Learn more about when Connectors are required and how they work
- Learn how to create a Connector in AWS
- Learn how to create a Connector in Azure
- Learn how to create a Connector in Google Cloud
- Learn how to create a Connector on-premises

Note that if you want to use NetApp Intelligent Data Services to manage storage and data in Google Cloud, then the Connector must be running in Google Cloud.
Note that if you want to use NetApp's intelligent data services to manage storage and data in Google Cloud, then the Connector must be running in Google Cloud.

4

Subscribe to NetApp Intelligent Services (optional)

Subscribe to NetApp Intelligent Services from your cloud provider's marketplace to pay for data services at an hourly rate (PAYGO) or through an annual contract. NetApp Intelligent Services include Backup and recovery, Cloud Volumes ONTAP, Tiering, Ransomware protection, and Disaster recovery. Classification is included with your subscription at no additional cost.

Prepare networking for the BlueXP console

When you log in and use the web-based console, BlueXP contacts several endpoints to complete the actions that you initiate. Computers that access the console must have connections to these endpoints.

These endpoints are contacted in two scenarios:

- From a user's computer when completing sections from the BlueXP web-based console that's available as software as a service (SaaS).
- From a user's computer when opening a web browser, entering the IP address of the Connector host, and then logging in and setting up the Connector. These steps are required if you manually install the Connector.

Endpoints	Purpose
https://console.bluexp.netapp.com https://*.console.bluexp.netapp.com	This is the endpoint that you enter in your web browser to use the web-based console.
https://api.bluexp.netapp.com	The web-based console contacts this endpoint to interact with the API for actions related to authorization, licensing, subscriptions, credentials, notifications, and more.
https://aiq.netapp.com	Required to access digital advisor.
AWS services (amazonaws.com): • CloudFormation • Elastic Compute Cloud (EC2) • Key Management Service (KMS) • Security Token Service (STS) • Simple Storage Service (S3)	Required to deploy a Connector from BlueXP in AWS. The exact endpoint depends on the region in which you deploy the Connector. See AWS documentation for details. Suggestion: See AWS documentation for details.
https://management.azure.com https://login.microsoftonline.com	Required to deploy a Connector from BlueXP in most Azure regions.
https://management.microsoftazure.de https://login.microsoftonline.de	Required to deploy a Connector from BlueXP in Azure Germany regions.
https://management.usgovcloudapi.net https://login.microsoftonline.com	Required to deploy a Connector from BlueXP in Azure US Gov regions.
https://www.googleapis.com	Required to deploy a Connector from BlueXP in Google Cloud.
https://signin.b2c.netapp.com	Required to update NetApp Support Site (NSS) credentials or to add new NSS credentials to BlueXP.
https://netapp-cloud-account.auth0.com https://cdn.auth0.com https://services.cloud.netapp.com	Your web browser connects to these endpoints for centralized user authentication through BlueXP.
https://widget.intercom.io	For in-product chat that enables you to talk to NetApp support.

Ensure the Connector has outbound internet access to contact endpoints for daily operations. Follow the links in the next section below to find the list of these endpoints.

Related information

- Prepare networking for the Connector
  - Set up AWS networking
  - Set up Azure networking
  - Set up Google Cloud networking
  - Set up on-premisesnetworking
- Prepare networking for BlueXP services

  Refer to the documentation for each BlueXP service.

  BlueXP documentation

Sign up or log in to BlueXP

BlueXP is accessible from a web-based console. When you get started with BlueXP, your first step is to sign up or to log in using your NetApp Support Site credentials or SSO credentials from your corporate directory.

About this task

When you access BlueXP for the first time, BlueXP enables you to sign up or log in using one of the following options:

BlueXP login

You can sign up by creating a BlueXP login. This authentication method requires you to specify your email address and a password. After you verify your email address, you can log in and then create a BlueXP organization, if you don’t already belong to one.

NetApp Support Site (NSS) credentials

If you have existing NetApp Support Site credentials, you don’t need to sign up to BlueXP. You log in using your NSS credentials and then BlueXP prompts you to create a BlueXP organization, if you don’t already belong to one.

Note that the default password experience is a one-time passcode (OTP) to the registered email address. A new OTP is generated with each sign-in attempt.

Federated connection

You can use single sign-on to log in using credentials from your corporate directory (federated identity). The first user in your organization’s account must sign up to BlueXP or log in using NSS credentials, and then set up identity federation. After that, you can add members from your corporate identity to your organization. Those users can then log in using their SSO credentials.

Learn how to use identity federation with BlueXP.

Steps

1. Open a web browser and go to the BlueXP console
2. If you have a NetApp Support Site account or if you already set up identity federation, enter the email address associated with your account directly on the **Log in** page.

In both of these cases, BlueXP will sign you up as part of this initial login.

3. If you want to sign up by creating a BlueXP login, select **Sign up**.
    a. On the **Sign up** page, enter the required information and select **Next**.

       Note that only English characters are allowed in the sign up form.

    b. Check your inbox for an email from NetApp that includes instructions to verify your email address.

       This step is required before you can log in to BlueXP.

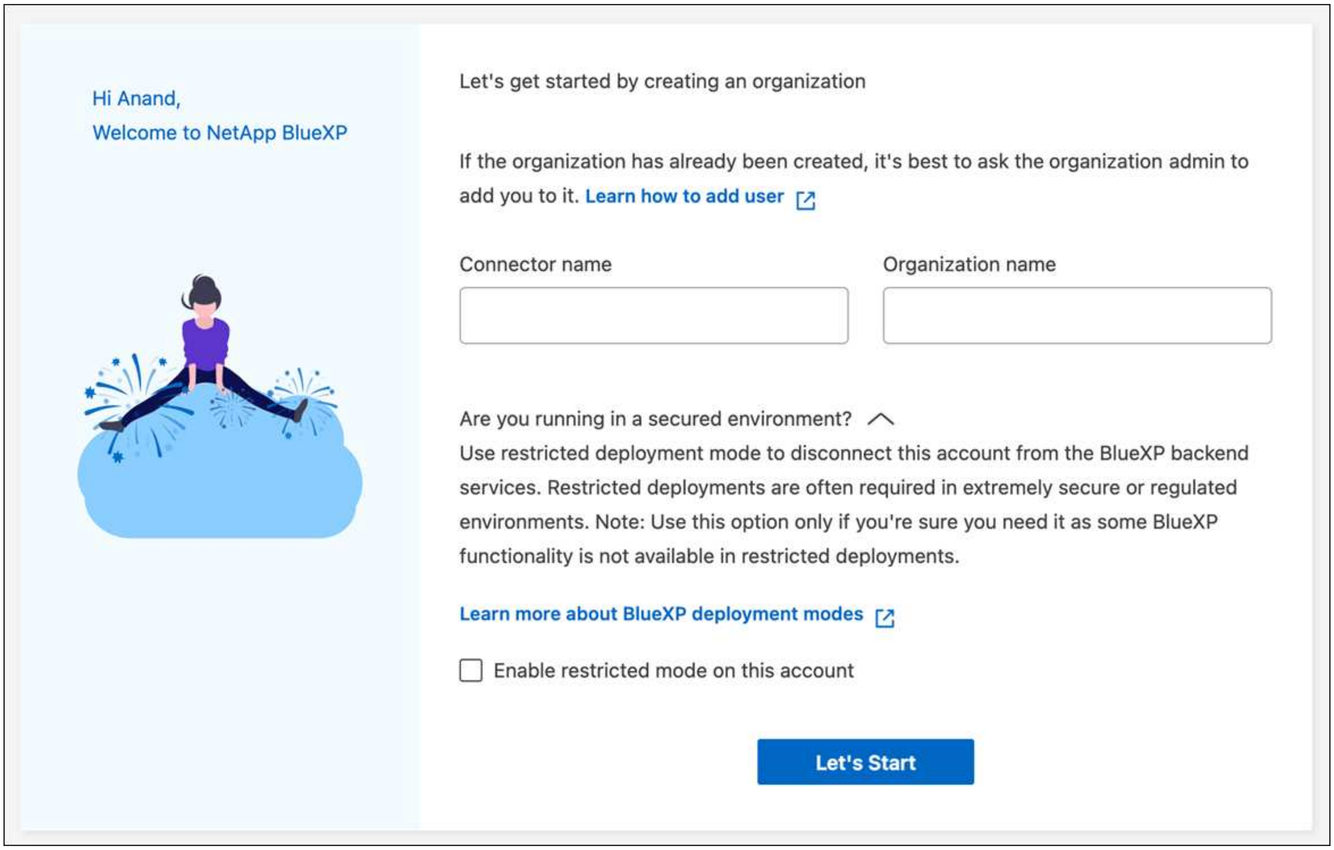
4. After you log in, review the End User License Agreement and accept the terms.

   If your user account doesn’t already belong to a BlueXP organization, you’ll be prompted to create one.

5. On the **Welcome** page, enter a name for your BlueXP organization.

   An organization is the top-level element in BlueXP identity and access management (IAM). Learn about BlueXP IAM.

   If your business already has a BlueXP organization and you want to join it, then you should close out of BlueXP and ask the owner to associate you with the organization. After the owner adds you, you can log in and you’ll have access to the account. Learn how to add members to an existing organization.



Hi Anand,
Welcome to NetApp BlueXP

Let's get started by creating an organization

If the organization has already been created, it's best to ask the organization admin to add you to it. Learn how to add user

Are you running in a secured environment?
Use restricted deployment mode to disconnect this account from the BlueXP backend services. Restricted deployments are often required in extremely secure or regulated environments. Note: Use this option only if you're sure you need it as some BlueXP functionality is not available in restricted deployments.

Learn more about BlueXP deployment modes

☐ Enable restricted mode on this account

6. Select **Let’s Start**.

Result

You now have a BlueXP login and an organization. In most cases, the next step is to create a Connector, which connects BlueXP’s services to your hybrid cloud environment.

Create a Connector

AWS

Connector installation options in AWS

There are a few different ways to create a Connector in AWS. Directly from BlueXP is the most common way.

The following installation options are available:

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

  This action launches an EC2 instance running Linux and the Connector software in a VPC of your choice.

- Create a Connector from the AWS Marketplace

  This action also launches an EC2 instance running Linux and the Connector software, but the deployment is initiated directly from the AWS Marketplace, rather than from BlueXP.

- 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 AWS.

Create a Connector in AWS from BlueXP

You can create a Connector in AWS directly from BlueXP. To create a Connector in AWS from BlueXP, you need to set up your networking, prepare AWS permissions, and then create the Connector.

Before you begin

- You should have an understanding of Connectors.
- You should review Connector limitations.

Step 1: Set up networking

Ensure that the network location where you plan to install the Connector supports the following requirements. Meeting these requirements enables the Connector to manage resources and processes within your hybrid cloud environment.

VPC and subnet

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

Connections to target networks

A Connector requires a network connection to the location where you're planning to create and manage working environments. For example, the network where you plan to create Cloud Volumes ONTAP systems or a storage system in your on-premises environment.

Outbound internet access

The network location where you deploy the Connector must have an outbound internet connection to contact specific endpoints.

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.

Note that the endpoints listed below are all CNAME entries.

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://support.netapp.com https://mysupport.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://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	To provide SaaS features and services within BlueXP.
Choose between two sets of endpoints: • Option 1 (recommended) [1] https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Option 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	To obtain images for Connector upgrades.

[1] The endpoints listed in option 1 are recommended because they are more secure. We recommend that you set up your firewall to allow the endpoints listed in option 1, while disallowing the endpoints listed in option 2. Note the following about these endpoints:

- The endpoints listed in option 1 are supported starting with the 3.9.47 release of the Connector. There is no backwards compatibility with previous releases of the Connector.
- The Connector contacts the endpoints listed in option 2 first. If those endpoints aren't accessible, the Connector automatically contacts the endpoints listed in option 1.
- The endpoints in option 1 are not supported if you use the Connector with BlueXP backup and recovery or BlueXP ransomware protection. In this case, you can disallow the endpoints listed in option 1, while

allowing the endpoints listed in option 2.

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.

Proxy server

NetApp supports both explicit and transparent proxy configurations. If you are using a transparent proxy, you only need to provide the certificate for the proxy server. If you are using an explicit proxy, you'll also need the IP address and credentials.

- 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.

Enable NTP

If you're planning to use BlueXP classification to scan your corporate data sources, you should enable a Network Time Protocol (NTP) service on both the BlueXP Connector system and the BlueXP classification system so that the time is synchronized between the systems. Learn more about BlueXP classification

You'll need to implement this networking requirement after you create the Connector.

Step 2: Set up AWS permissions

BlueXP needs to authenticate with AWS before it can deploy the Connector instance in your VPC. You can choose one of these authentication methods:

- Let BlueXP assume an IAM role that has the required permissions
- Provide an AWS access key and secret key for an IAM user who has the required permissions

With either option, the first step is to create an IAM policy. This policy contains only the permissions needed to launch the Connector instance in AWS from BlueXP.

If needed, you can restrict the IAM policy by using the IAM `Condition` element. AWS documentation: Condition element

Steps

1. Go to the AWS IAM console.
2. Select **Policies > Create policy**.
3. Select **JSON**.
4. Copy and paste the following policy:

   This policy contains only the permissions needed to launch the Connector instance in AWS from BlueXP. When BlueXP creates the Connector, it applies a new set of permissions to the Connector instance that enables the Connector to manage AWS resources. View permissions required for the Connector instance itself.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:PassRole",
        "iam:ListRoles",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DescribeInstances",
        "ec2:CreateTags",
        "ec2:DescribeImages",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeLaunchTemplates",
        "ec2:CreateLaunchTemplate",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "iam:GetRole",
        "iam:TagRole",
        "kms:ListAliases",
        "cloudformation:ListStacks"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:TerminateInstances"
      ],
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/OCCMInstance": "*"
        }
      },
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

5. Select **Next** and add tags, if needed.
6. Select **Next** and enter a name and description.
7. Select **Create policy**.
8. Either attach the policy to an IAM role that BlueXP can assume or to an IAM user so that you can provide BlueXP with access keys:
    - (Option 1) Set up an IAM role that BlueXP can assume:
        a. Go to the AWS IAM console in the target account.

b. Under Access Management, select **Roles > Create Role** and follow the steps to create the role.

c. Under **Trusted entity type**, select **AWS account**.

d. Select **Another AWS account** and enter the ID of the BlueXP SaaS account: 952013314444

e. Select the policy that you created in the previous section.

f. After you create the role, copy the Role ARN so that you can paste it in BlueXP when you create the Connector.

- (Option 2) Set up permissions for an IAM user so that you can provide BlueXP with access keys:

  a. From the AWS IAM console, select **Users** and then select the user name.

  b. Select **Add permissions > Attach existing policies directly**.

  c. Select the policy that you created.

  d. Select **Next** and then select **Add permissions**.

  e. Ensure that you have the access key and secret key for the IAM user.

Result

You should now have an IAM role that has the required permissions or an IAM user that has the required permissions. When you create the Connector from BlueXP, you can provide information about the role or access keys.

Step 3: Create the Connector

Create the Connector directly from the BlueXP web-based console.

About this task

- Creating the Connector from BlueXP deploys an EC2 instance in AWS using a default configuration. After you create the Connector, you should not change to a smaller EC2 instance type that has less CPU or RAM. Learn about the default configuration for the Connector.
- When BlueXP creates the Connector, it creates an IAM role and an instance profile for the instance. This role includes permissions that enables the Connector to manage AWS resources. You need to ensure that the role is kept up to date as new permissions are added in subsequent releases. Learn more about the IAM policy for the Connector.

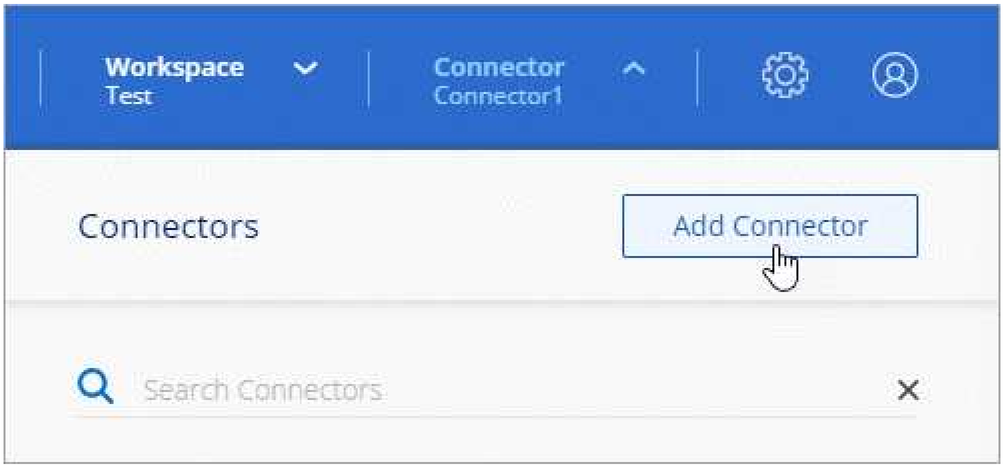
Before you begin

You should have the following:

- An AWS authentication method: either an IAM role or access keys for an IAM user with the required permissions.
- A VPC and subnet that meets networking requirements.
- A key pair for the EC2 instance.
- Details about a proxy server, if a proxy is required for internet access from the Connector.

Steps

1. Select the **Connector** drop-down and select **Add Connector**.



2. Choose **Amazon Web Services** as your cloud provider and select **Continue**.
3. On the **Deploying a Connector** page, review the details about what you'll need. You have two options:
   a. Select **Continue** to prepare for deployment by using the in-product guide. Each step in the in-product guide includes the information that's contained on this page of the documentation.
   b. Select **Skip to Deployment** if you already prepared by following the steps on this page.
4. Follow the steps in the wizard to create the Connector:
   - **Get Ready**: Review what you'll need.
   - **AWS Credentials**: Specify your AWS region and then choose an authentication method, which is either an IAM role that BlueXP can assume or an AWS access key and secret key.

     > If you choose **Assume Role**, you can create the first set of credentials from the Connector deployment wizard. Any additional set of credentials must be created from the Credentials page. They will then be available from the wizard in a drop-down list. Learn how to add additional credentials.

   - **Details**: Provide details about the Connector.
     - Enter a name for the instance.
     - Add custom tags (metadata) to the instance.
     - 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.
     - Choose whether you want to encrypt the Connector's EBS disks. You have the option to use the default encryption key or to use a custom key.
   - **Network**: Specify a VPC, subnet, and key pair for the instance, choose whether to enable a public IP address, and optionally specify a proxy configuration.

     Make sure that you have the correct key pair to use with the Connector. Without a key pair, you will not be able to access the Connector virtual machine.

   - **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 AWS.

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

5. Select **Add**.

   The instance 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.

If you have Amazon S3 buckets in the same AWS account where you created the Connector, you'll see an Amazon S3 working environment appear on the BlueXP canvas automatically. Learn how to manage S3 buckets from BlueXP

Create a Connector from the AWS Marketplace

You create a Connector in AWS directly from the AWS Marketplace. To create a Connector from the AWS Marketplace, you need to set up your networking, prepare AWS permissions, review instance requirements, and then create the Connector.

Before you begin

- You should have an understanding of Connectors.
- You should review Connector limitations.

Step 1: Set up networking

Ensure that the network location where you plan to install the Connector supports the following requirements. Meeting these requirements enables the Connector to manage resources and processes within your hybrid cloud environment.

VPC and subnet

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

Connections to target networks

A Connector requires a network connection to the location where you're planning to create and manage working environments. For example, the network where you plan to create Cloud Volumes ONTAP systems or a storage system in your on-premises environment.

Outbound internet access

The network location where you deploy the Connector must have an outbound internet connection to contact specific endpoints.

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.

Note that the endpoints listed below are all CNAME entries.

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://support.netapp.com https://mysupport.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://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	To provide SaaS features and services within BlueXP.
Choose between two sets of endpoints: • Option 1 (recommended) [1] https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Option 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	To obtain images for Connector upgrades.

[1] The endpoints listed in option 1 are recommended because they are more secure. We recommend that you set up your firewall to allow the endpoints listed in option 1, while disallowing the endpoints listed in option 2. Note the following about these endpoints:

- The endpoints listed in option 1 are supported starting with the 3.9.47 release of the Connector. There is no backwards compatibility with previous releases of the Connector.
- The Connector contacts the endpoints listed in option 2 first. If those endpoints aren't accessible, the Connector automatically contacts the endpoints listed in option 1.
- The endpoints in option 1 are not supported if you use the Connector with BlueXP backup and recovery or BlueXP ransomware protection. In this case, you can disallow the endpoints listed in option 1, while allowing the endpoints listed in option 2.

Proxy server

NetApp supports both explicit and transparent proxy configurations. If you are using a transparent proxy, you only need to provide the certificate for the proxy server. If you are using an explicit proxy, you'll also need the IP address and credentials.

- 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.

Enable NTP

If you’re planning to use BlueXP classification to scan your corporate data sources, you should enable a Network Time Protocol (NTP) service on both the BlueXP Connector system and the BlueXP classification system so that the time is synchronized between the systems. Learn more about BlueXP classification

You’ll need to implement this networking requirement after you create the Connector.

Step 2: Set up AWS permissions

To prepare for a marketplace deployment, create IAM policies in AWS and attach them to an IAM role. When you create the Connector from the AWS Marketplace, you’ll be prompted to select that IAM role.

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. 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 that you can associate with the EC2 instance during deployment from the AWS Marketplace.

Step 3: Review instance requirements

When you create the Connector, you need to choose an EC2 instance type that meets the following requirements.

CPU
8 cores or 8 vCPUs

RAM
32 GB

AWS EC2 instance type
An instance type that meets the CPU and RAM requirements above. We recommend t3.2xlarge.

Step 4: Create the Connector

Create the Connector directly from the AWS Marketplace.

About this task

Creating the Connector from the AWS Marketplace deploys an EC2 instance in AWS using a default configuration. Learn about the default configuration for the Connector.

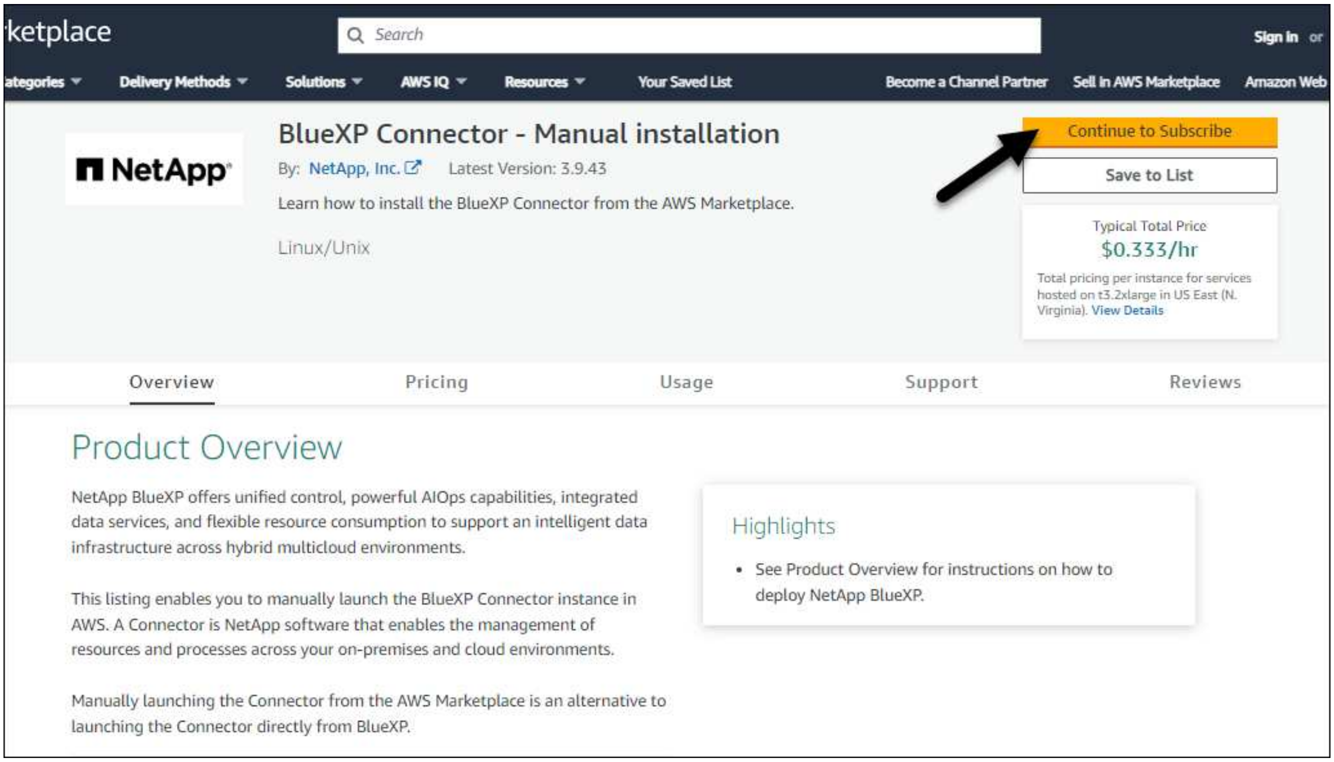
Before you begin

You should have the following:

- A VPC and subnet that meets networking requirements.
- An IAM role with an attached policy that includes the required permissions for the Connector.
- Permissions to subscribe and unsubscribe from the AWS Marketplace for your IAM user.
- An understanding of CPU and RAM requirements for the instance.
- A key pair for the EC2 instance.

Steps

1. Go to the BlueXP Connector listing on the AWS Marketplace
2. On the Marketplace page, select **Continue to Subscribe**.



BlueXP Connector - Manual installation

By: NetApp, Inc. Latest Version: 3.9.43

Learn how to install the BlueXP Connector from the AWS Marketplace.

Linux/Unix

Typical Total Price
$0.333/hr
Total pricing per instance for services hosted on t3.2xlarge in US East (N. Virginia). View Details

Product Overview

NetApp BlueXP offers unified control, powerful AIOps capabilities, integrated data services, and flexible resource consumption to support an intelligent data infrastructure across hybrid multicloud environments.

This listing enables you to manually launch the BlueXP Connector instance in AWS. A Connector is NetApp software that enables the management of resources and processes across your on-premises and cloud environments.

Manually launching the Connector from the AWS Marketplace is an alternative to launching the Connector directly from BlueXP.

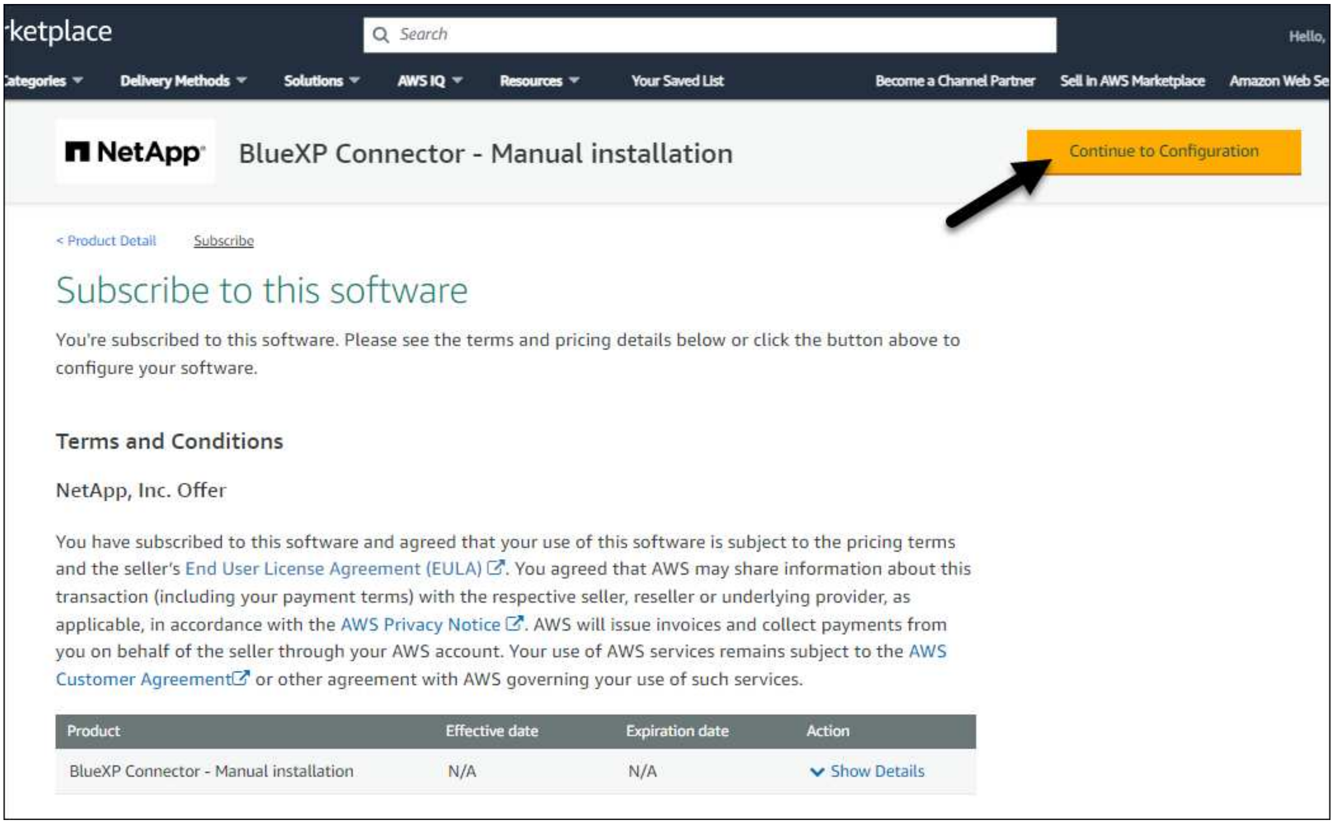
Highlights

- See Product Overview for instructions on how to deploy NetApp BlueXP.

3. To subscribe to the software, select **Accept Terms**.

   The subscription process can take a few minutes.

4. After the subscription process is complete, select **Continue to Configuration**.



BlueXP Connector - Manual installation

Subscribe to this software

You're subscribed to this software. Please see the terms and pricing details below or click the button above to configure your software.

Terms and Conditions

NetApp, Inc. Offer

You have subscribed to this software and agreed that your use of this software is subject to the pricing terms and the seller's End User License Agreement (EULA). You agreed that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the AWS Privacy Notice. AWS will issue invoices and collect payments from you on behalf of the seller through your AWS account. Your use of AWS services remains subject to the AWS Customer Agreement or other agreement with AWS governing your use of such services.

Product	Effective date	Expiration date	Action
BlueXP Connector - Manual installation	N/A	N/A	Show Details

5. On the **Configure this software** page, ensure that you've selected the correct region and then select

Continue to Launch.

6. On the **Launch this software** page, under **Choose Action**, select **Launch through EC2** and then select **Launch**.

   These steps describe how to launch the instance from the EC2 Console because the console enables you to attach an IAM role to the Connector instance. This isn't possible using the **Launch from Website** action.

7. Follow the prompts to configure and deploy the instance:

   - **Name and tags**: Enter a name and tags for the instance.
   - **Application and OS Images**: Skip this section. The Connector AMI is already selected.
   - **Instance type**: Depending on region availability, choose an instance type that meets RAM and CPU requirements (t3.2xlarge is preselected and recommended).
   - **Key pair (login)**: Select the key pair that you want to use to securely connect to the instance.
   - **Network settings**: Edit the network settings as needed:
     - Choose the desired VPC and subnet.
     - Specify whether the instance should have a public IP address.
     - Specify security group settings that enable the required connection methods for the Connector instance: SSH, HTTP, and HTTPS.

       View security group rules for AWS.
   - **Configure storage**: Keep the default size and disk type for the root volume.

     If you want to enable Amazon EBS encryption on the root volume, select **Advanced**, expand **Volume 1**, select **Encrypted**, and then choose a KMS key.
   - **Advanced details**: Under **IAM instance profile**, choose the IAM role that includes the required permissions for the Connector.
   - **Summary**: Review the summary and select **Launch instance**.

   AWS launches the software with the specified settings. The Connector instance and software should be running in approximately five minutes.

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

   https://*ipaddress*

9. After you log in, set up the Connector:

   a. Specify the BlueXP organization 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 set up with your BlueXP organization.

Open a web browser and go to the BlueXP console to start using the Connector with BlueXP.

If you have Amazon S3 buckets in the same AWS account where you created the Connector, you'll see an Amazon S3 working environment appear on the BlueXP canvas automatically. Learn how to manage S3 buckets from BlueXP

Manually install the Connector in AWS

You can manually install a Connector on a Linux host running in AWS. To manually install the Connector on your own Linux host, you need to review host requirements, set up your networking, prepare AWS permissions, install the Connector, and then provide the permissions that you prepared.

Before you begin

- You should have an understanding of Connectors.
- You should review Connector limitations.

Step 1: Review host requirements

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

> ⓘ The Connector reserves the UID and GID range of 19000 to 19200. This range is fixed and cannot be modified. If any third-party software on your host is using UIDs or GIDs within this range, the Connector installation will fail. NetApp recommends using a host that is free of third-party software to avoid conflicts.

Dedicated host

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

Host can be of any architecture that meets the following size requirements:

- CPU: 8 cores or 8 vCPUs
- RAM: 32 GB

Hypervisor

A bare metal or hosted hypervisor that is certified to run a supported operating system is required.

Operating system and container requirements

BlueXP supports the Connector with the following operating systems when using BlueXP in standard mode or restricted mode. A container orchestration tool is required before you install the Connector.

Operating system	Supported OS versions	Supported Connector versions	Required container tool	SELinux
Red Hat Enterprise Linux	9.1 to 9.4 8.6 to 8.10 7.9	3.9.40 or later with BlueXP in standard mode or restricted mode	Podman version 4.6.1 or 4.9.4 View Podman configuration requirements.	Supported in enforcing mode or permissive mode [1]
Ubuntu	24.04 LTS	3.9.45 or later with BlueXP in standard mode or restricted mode	Docker Engine 23.06 to 28.0.0.	Not supported
	22.04 LTS	3.9.29 or later	Docker Engine 23.0.6 to 28.0.0.	Not supported

Notes:

1. Management of Cloud Volumes ONTAP systems is not supported by Connectors that have SELinux enabled on the operating system.
2. The Connector is supported on English-language versions of these operating systems.
3. For RHEL, 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.

AWS EC2 instance type

An instance type that meets the CPU and RAM requirements above. We recommend t3.2xlarge.

Key pair

When you create the Connector, you'll need to select an EC2 key pair to use with the instance.

PUT response hop limit when using IMDSv2

If IMDSv2 is enabled on the EC2 instance (this is the default setting for new EC2 instances), you must change the PUT response hop limit on the instance to 3. If you don't change the limit on the EC2 instance, you'll receive a UI initialization error when you try to set up the Connector.

- Require the use of IMDSv2 on Amazon EC2 instances
- AWS documentation: Change the PUT response hop limit

Disk space in /opt

100 GiB of space must be available

BlueXP uses `/opt` to install the `/opt/application/netapp` directory and its contents.

Disk space in /var

20 GiB of space must be available

BlueXP requires this space in `/var` because Docker or Podman are architected to create the containers within this directory. Specifically, they will create containers in the `/var/lib/containers/storage` directory. External mounts or symlinks do not work for this space.

Step 2: Install Podman or Docker Engine

Depending on your operating system, either Podman or Docker Engine is required before you install the Connector.

- Podman is required for Red Hat Enterprise Linux 8 and 9.

  View the Podman versions that BlueXP supports.

- Docker Engine is required for Ubuntu.

  View the Docker Engine versions that BlueXP supports.

Example 1. Steps

Podman

Follow these steps to install Podman and configure it to meet the following requirements:

- Enable and start the podman.socket service
- Install python3
- Install the podman-compose package version 1.0.6
- Add podman-compose to the PATH environment variable

> When using Podman, adjust the aardvark-dns service port (default: 53) after installing the Connector to avoid conflicts with the DNS port on the host. Follow the instructions to configure the port.

Steps

1. Remove the podman-docker package if it’s installed on the host.

   ```
   dnf remove podman-docker
   rm /var/run/docker.sock
   ```

2. Install Podman.

   Podman is available from official Red Hat Enterprise Linux repositories.

   For Red Hat Enterprise Linux 9:

   ```
   sudo dnf install podman-2:<version>
   ```

   Where <version> is the supported version of Podman that you’re installing. View the Podman versions that BlueXP supports.

   For Red Hat Enterprise Linux 8:

   ```
   sudo dnf install podman-3:<version>
   ```

   Where <version> is the supported version of Podman that you’re installing. View the Podman versions that BlueXP supports.

3. Enable and start the podman.socket service.

   ```
   sudo systemctl enable --now podman.socket
   ```

4. Install python3.

```
sudo dnf install python3
```

5. Install the EPEL repository package if it’s not already available on your system.

   This step is required because podman-compose is available from the Extra Packages for Enterprise Linux (EPEL) repository.

   For Red Hat Enterprise Linux 9:

   ```
   sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-
   latest-9.noarch.rpm
   ```

   For Red Hat Enterprise Linux 8:

   ```
   sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-
   latest-8.noarch.rpm
   ```

6. Install podman-compose package 1.0.6.

   ```
   sudo dnf install podman-compose-1.0.6
   ```

   > ⓘ Using the `dnf install` command meets the requirement for adding podman-compose to the PATH environment variable. The installation command adds podman-compose to /usr/bin, which is already included in the `secure_path` option on the host.

Docker Engine

Follow the documentation from Docker to install Docker Engine.

Steps

1. View installation instructions from Docker

   Be sure to follow the steps to install a specific version of Docker Engine. Installing the latest version will install a version of Docker that BlueXP doesn’t support.

2. Verify that Docker is enabled and running.

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

Step 3: Set up networking

Ensure that the network location where you plan to install the Connector supports the following requirements. Meeting these requirements enables the Connector to manage resources and processes within your hybrid cloud environment.

Connections to target networks

A Connector requires a network connection to the location where you're planning to create and manage working environments. For example, the network where you plan to create Cloud Volumes ONTAP systems or a storage system in your on-premises environment.

Outbound internet access

The network location where you deploy the Connector must have an outbound internet connection to contact specific endpoints.

Endpoints contacted from computers when using the BlueXP web-based console

Computers that access the BlueXP console from a web browser must have the ability to contact several endpoints. You'll need to use the BlueXP console to set up the Connector and for day-to-day use of BlueXP.

Prepare networking for 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://mysupport.netapp.com
- https://signin.b2c.netapp.com (this endpoint is the CNAME URL for https://mysupport.netapp.com)
- https://cloudmanager.cloud.netapp.com/tenancy
- https://stream.cloudmanager.cloud.netapp.com
- https://production-artifacts.cloudmanager.cloud.netapp.com
- To obtain images, the installer needs access to one of these two sets of endpoints:
  - Option 1 (recommended):
    - https://bluexpinfraprod.eastus2.data.azurecr.io
    - https://bluexpinfraprod.azurecr.io
  - Option 2:
    - https://*.blob.core.windows.net
    - https://cloudmanagerinfraprod.azurecr.io

  The endpoints listed in option 1 are recommended because they are more secure. We recommend that you set up your firewall to allow the endpoints listed in option 1, while disallowing the endpoints listed in option 2. Note the following about these endpoints:

  - The endpoints listed in option 1 are supported starting with the 3.9.47 release of the Connector. There is no backwards compatibility with previous releases of the Connector.
  - The Connector contacts the endpoints listed in option 2 first. If those endpoints aren't accessible, the Connector automatically contacts the endpoints listed in option 1.
  - The endpoints in option 1 are not supported if you use the Connector with BlueXP backup and recovery or BlueXP ransomware protection. In this case, you can disallow the endpoints listed in option 1, while allowing the endpoints listed in option 2.

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.

Note that the endpoints listed below are all CNAME entries.

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://support.netapp.com https://mysupport.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://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	To provide SaaS features and services within BlueXP.
Choose between two sets of endpoints: • Option 1 (recommended) [1] https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Option 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	To obtain images for Connector upgrades.

[1] The endpoints listed in option 1 are recommended because they are more secure. We recommend that you set up your firewall to allow the endpoints listed in option 1, while disallowing the endpoints listed in option 2. Note the following about these endpoints:

- The endpoints listed in option 1 are supported starting with the 3.9.47 release of the Connector. There is no backwards compatibility with previous releases of the Connector.
- The Connector contacts the endpoints listed in option 2 first. If those endpoints aren't accessible, the Connector automatically contacts the endpoints listed in option 1.
- The endpoints in option 1 are not supported if you use the Connector with BlueXP backup and recovery or BlueXP ransomware protection. In this case, you can disallow the endpoints listed in option 1, while

allowing the endpoints listed in option 2.

Proxy server

NetApp supports both explicit and transparent proxy configurations. If you are using a transparent proxy, you only need to provide the certificate for the proxy server. If you are using an explicit proxy, you'll also need the IP address and credentials.

- 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.

Enable NTP

If you're planning to use BlueXP classification to scan your corporate data sources, you should enable a Network Time Protocol (NTP) service on both the BlueXP Connector system and the BlueXP classification system so that the time is synchronized between the systems. Learn more about BlueXP classification

Step 4: Set up permissions

You need to provide AWS permissions to BlueXP by using one of the following options:

- Option 1: Create IAM policies and attach the policies to an IAM role that you can associate with the EC2 instance.
- Option 2: Provide BlueXP with the AWS access key for an IAM user who has the required permissions.

Follow the steps to prepare permissions for BlueXP.

IAM role

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. 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 that you can associate with the EC2 instance after you install the Connector.

AWS access key

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

You now have an IAM user that has the required permissions and an access key that you can provide to BlueXP.

Step 5: Install the Connector

After the pre-requisites are complete, you can manually install the software on your own Linux host.

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.

> You cannot set a certificate for a transparent proxy server when manually installing the Connector. If you need to set a certificate for a transparent proxy server, you must use the Maintenance Console after installation. Learn more about the Connector Maintenance Console.

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. 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.

2. 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.

3. Assign permissions to run the script.

   ```
   chmod +x BlueXP-Connector-Cloud-<version>
   ```

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

4. Run the installation script.

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

You'll need to add proxy information if your network requires a proxy for internet access. You can add either a transparent or explicit proxy. The --proxy and --cacert parameters are optional and you won't be prompted to add them. If you have a proxy server, you will need to enter the parameters as shown.

Here is an example configuring an explicit proxy server with a CA-signed certificate:

```
 ./BlueXP-Connector-Cloud-v3.9.40--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://user-name:password@address:port
- http://domain-name%92user-name:password@address:port
- https://address:port
- https://user-name:password@address:port
- https://domain-name%92user-name:password@address:port

  Note the following:

  - The user can be a local user or domain user.
  - For a domain user, you must use the ASCII code for a \ as shown above.
  - BlueXP doesn't support user names or passwords that include the @ character.
  - If the password includes any of the following special characters, you must escape that special character by prepending it with a backslash: & or !

    For example:

    http://bxpproxyuser:netapp1\!@address:3128

    --cacert specifies a CA-signed certificate to use for HTTPS access between the Connector and the proxy server. This parameter is required for HTTPS proxy servers, intercepting proxy servers, and transparent proxy servers.

  Here is an example configuring a transparent proxy server. When you configure a transparent proxy, you don't need to define the proxy server. You only add a CA-signed certificate to your Connector host:

```
./BlueXP-Connector-Cloud-v3.9.40 --cacert /tmp/cacert/certificate.cer
```

5. If you used Podman, you'll need to adjust the aardvark-dns port.

   a. SSH to the BlueXP Connector virtual machine.

   b. Open podman */usr/share/containers/containers.conf* file and modify the chosen port for Aardvark DNS service. For example, change it to 54.

```
vi /usr/share/containers/containers.conf
...
# Port to use for dns forwarding daemon with netavark in rootful
bridge
# mode and dns enabled.
# Using an alternate port might be useful if other DNS services
should
# run on the machine.
#
dns_bind_port = 54
...
Esc:wq
```

   c. Reboot the Connector virtual machine.

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 organization 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**.

If you have Amazon S3 buckets in the same AWS account where you created the Connector, you'll see an Amazon S3 working environment appear on the BlueXP canvas automatically. Learn how to manage S3 buckets from BlueXP

Step 6: Provide permissions to BlueXP

Now that you've installed the Connector, you need to provide BlueXP with the AWS permissions that you previously set up. Providing the permissions enables BlueXP to manage your data and storage infrastructure in 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.

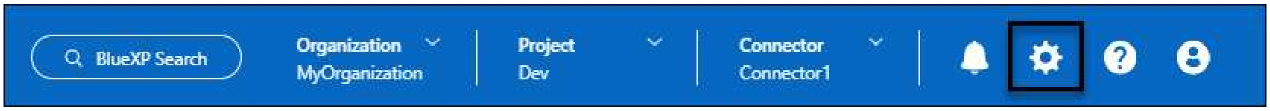
Go to the BlueXP console to start using the Connector with BlueXP.

AWS access key

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

Steps

1. Ensure that the correct Connector is currently selected in BlueXP.
2. In the upper right of the BlueXP console, select the Settings icon, and select **Credentials**.



3. 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.

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

Azure

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 following installation options are available:

- Create a 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, but the deployment is initiated directly from the Azure Marketplace, rather than from BlueXP.

- 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.

Create a Connector in Azure from BlueXP

You can install a Connector in Azure directly from BlueXP. To create a Connector in Azure from BlueXP, you need to set up your networking, prepare an Azure role to use to deploy the Connector, and then deploy the Connector.

Before you begin

- You should have an understanding of Connectors.
- You should review Connector limitations.

Step 1: Set up networking

Ensure that the network location where you plan to install the Connector supports the following requirements. Meeting these requirements enables the Connector to manage resources and processes within your hybrid cloud environment.

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

VNet and subnet

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

Connections to target networks

A Connector requires a network connection to the location where you're planning to create and manage working environments. For example, the network where you plan to create Cloud Volumes ONTAP systems or a storage system in your on-premises environment.

Outbound internet access

The network location where you deploy the Connector must have an outbound internet connection to contact specific endpoints.

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.

Note that the endpoints listed below are all CNAME entries.

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 https://mysupport.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://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	To provide SaaS features and services within BlueXP.
Choose between two sets of endpoints: • Option 1 (recommended) [1] https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Option 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	To obtain images for Connector upgrades.

[1] The endpoints listed in option 1 are recommended because they are more secure. We recommend that you set up your firewall to allow the endpoints listed in option 1, while disallowing the endpoints listed in option 2. Note the following about these endpoints:

- The endpoints listed in option 1 are supported starting with the 3.9.47 release of the Connector. There is no backwards compatibility with previous releases of the Connector.
- The Connector contacts the endpoints listed in option 2 first. If those endpoints aren’t accessible, the Connector automatically contacts the endpoints listed in option 1.
- The endpoints in option 1 are not supported if you use the Connector with BlueXP backup and recovery or BlueXP ransomware protection. In this case, you can disallow the endpoints listed in option 1, while allowing the endpoints listed in option 2.

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.

Proxy server

NetApp supports both explicit and transparent proxy configurations. If you are using a transparent proxy, you only need to provide the certificate for the proxy server. If you are using an explicit proxy, you'll also need the IP address and credentials.

- 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.

Enable NTP

If you're planning to use BlueXP classification to scan your corporate data sources, you should enable a Network Time Protocol (NTP) service on both the BlueXP Connector system and the BlueXP classification system so that the time is synchronized between the systems. Learn more about BlueXP classification

You'll need to implement this networking requirement after you create the Connector.

Step 2: Create a Connector deployment policy (custom role)

You need to create a custom role that has permissions to deploy the Connector in Azure.

Create an Azure custom role that you can assign to your Azure account or to a Microsoft Entra service principal. BlueXP authenticates with Azure and uses these permissions to create the Connector instance on your behalf.

After BlueXP deploys the Connector virtual machine in Azure, it enables a system-assigned managed identity on the virtual machine, automatically creates the role it needs, and assigns it to the virtual machine. The automatically created role provides BlueXP with the permissions required to manage resources and processes within that Azure subscription. Review how BlueXP uses the permissions.

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 custom role 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 Azure resources.

```
{
    "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

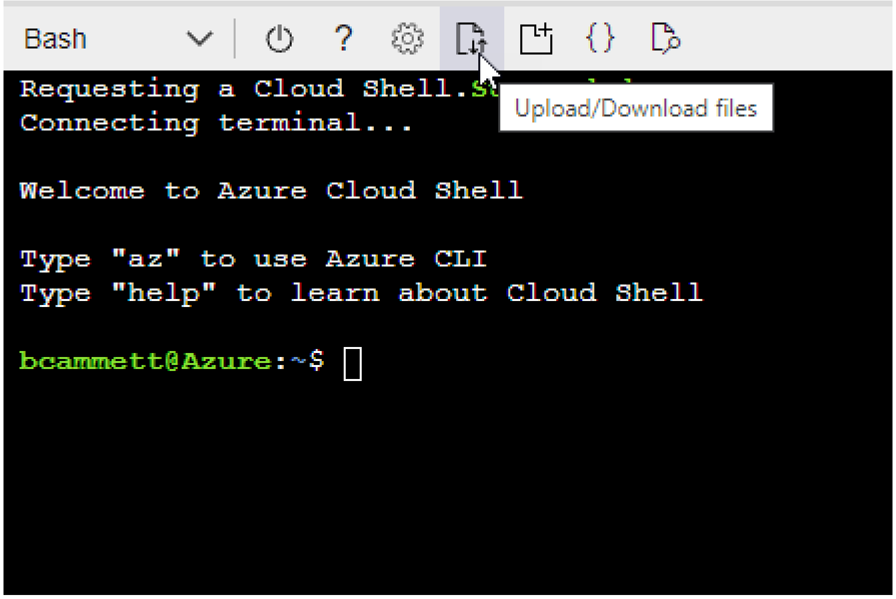
```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"
],
```

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.



```
Requesting a Cloud Shell.Su
Connecting terminal...

Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

bcammett@Azure:~$
```

   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.

Step 3: Set up authentication

When creating the Connector from BlueXP, you need to provide a login that enables BlueXP to authenticate with Azure and deploy the VM. You have two options:

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

Follow the steps to prepare one of these authentication methods for use with BlueXP.

Azure 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. Click **Access control (IAM)**.
3. Click **Add** > **Add role assignment** and then add the permissions:
   a. Select the **Azure SetupAsService** role and click **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. Click **Select members**, choose your user account, and click **Select**.
   d. Click **Next**.
   e. Click **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.

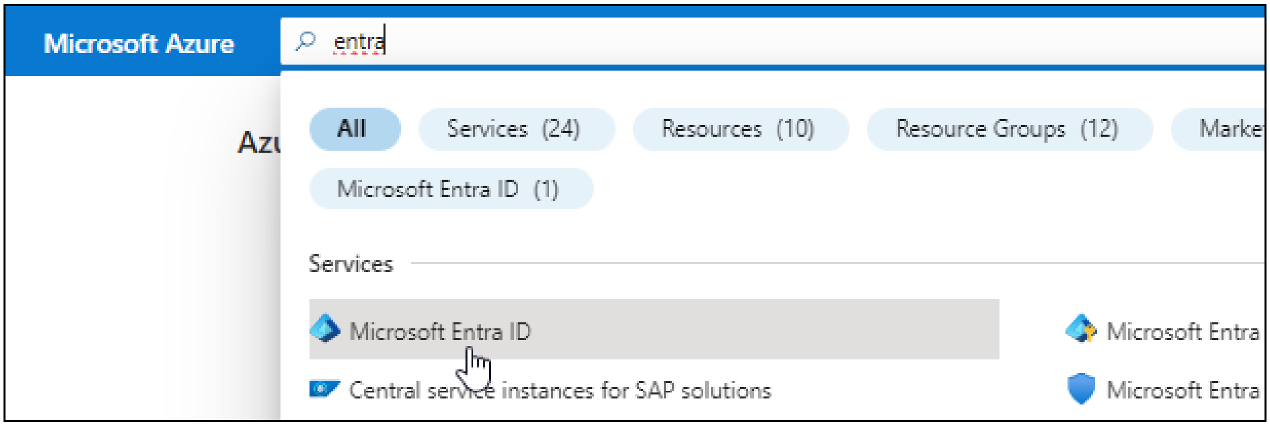
Create and set up a service principal in Microsoft Entra ID and obtain the Azure credentials that BlueXP needs.

Create a Microsoft Entra 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 **Microsoft Entra ID** service.

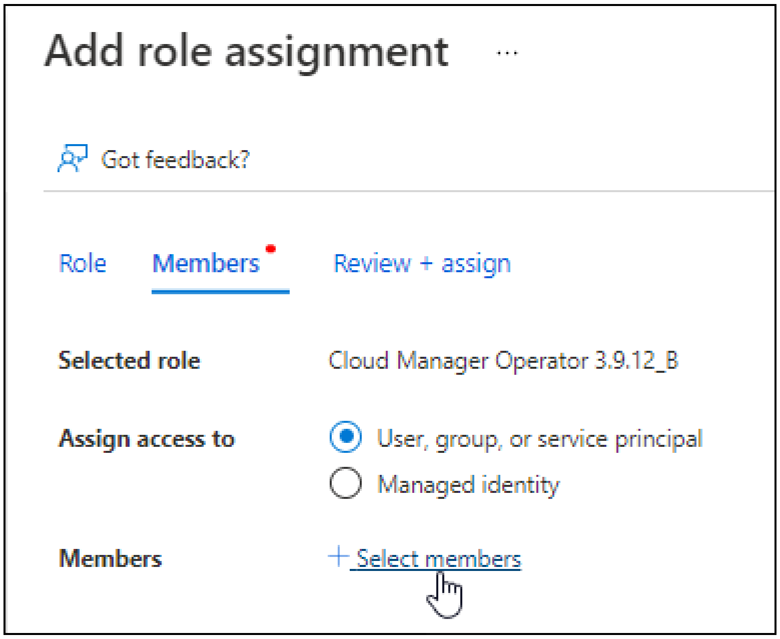


3. In the menu, select **App registrations**.
4. Select **New registration**.
5. Specify details about the application:
   - **Name**: Enter a name for the application.
   - **Account type**: Select an account type (any will work with BlueXP).
   - **Redirect URI**: You can leave this field blank.
6. 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. Click **Access control (IAM) > Add > Add role assignment**.
4. In the **Role** tab, select the **BlueXP Operator** role and click **Next**.
5. In the **Members** tab, complete the following steps:
   a. Keep **User, group, or service principal** selected.
   b. Click **Select members**.



Add role assignment

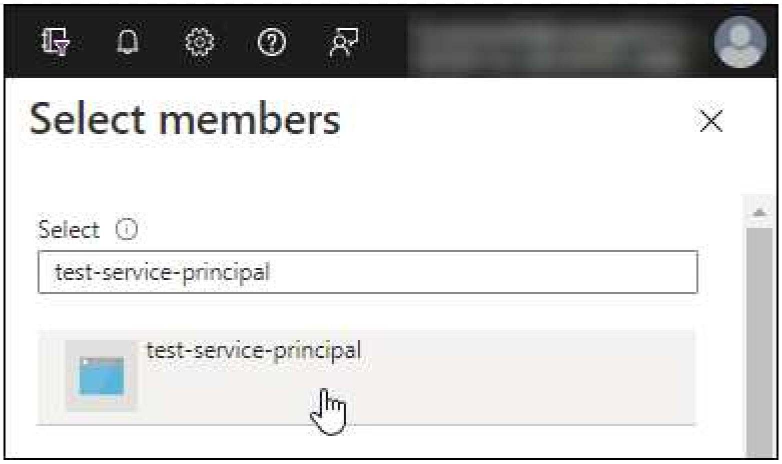
Selected role: Cloud Manager Operator 3.9.12_B

Assign access to: ● User, group, or service principal ○ Managed identity

Members: + Select members

   c. Search for the name of the application.

   Here's an example:


Select members

Select

test-service-principal

test-service-principal

d. Select the application and click **Select**.

e. Click **Next**.

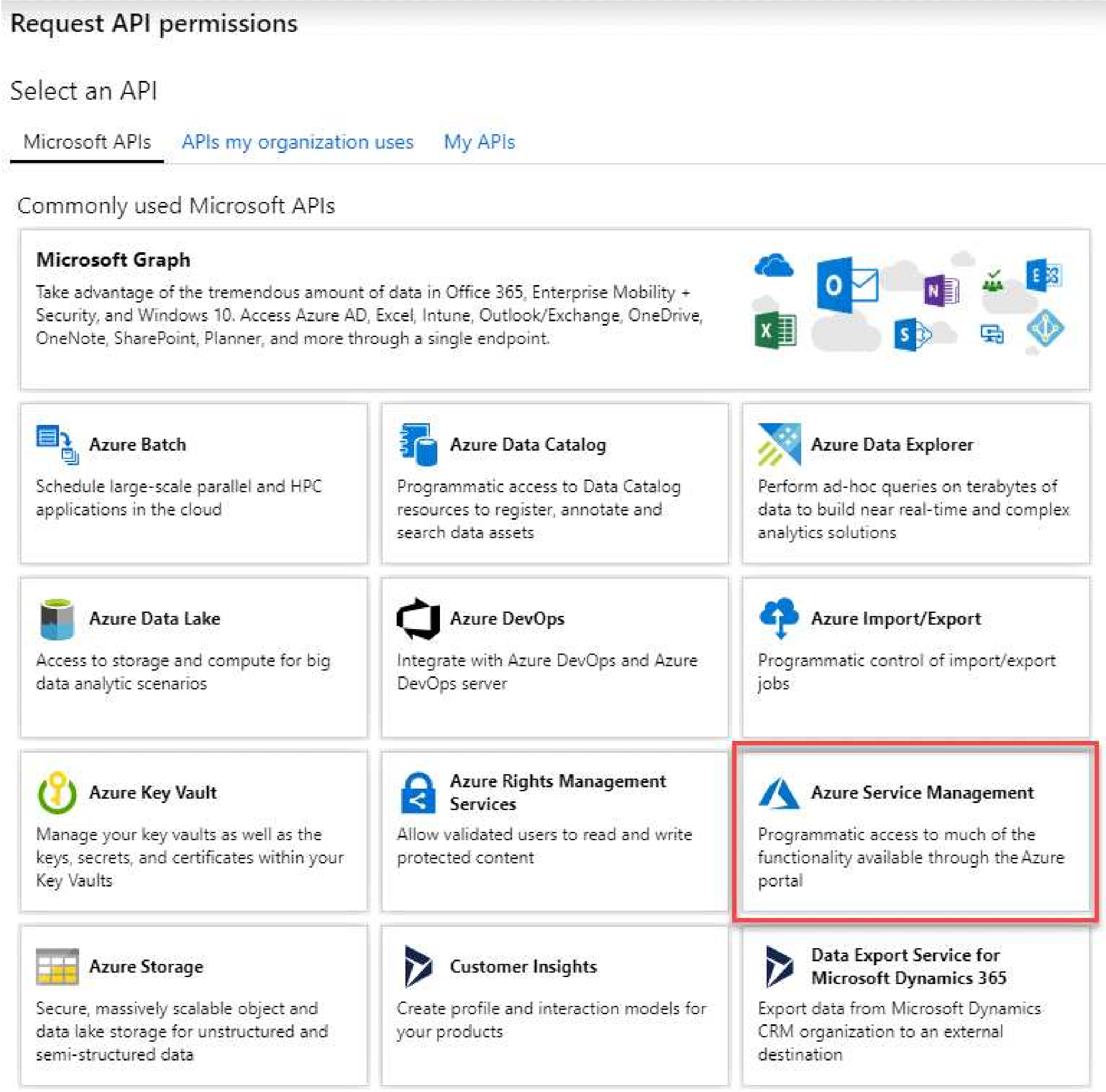
6. Click **Review + assign**.

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



Request API permissions

Select an API

Microsoft APIs | APIs my organization uses | My APIs

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Batch
Schedule large-scale parallel and HPC applications in the cloud

Azure Data Catalog
Programmatic access to Data Catalog resources to register, annotate and search data assets

Azure Data Explorer
Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

Azure Data Lake
Access to storage and compute for big data analytic scenarios

Azure DevOps
Integrate with Azure DevOps and Azure DevOps server

Azure Import/Export
Programmatic control of import/export jobs

Azure Key Vault
Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Rights Management Services
Allow validated users to read and write protected content

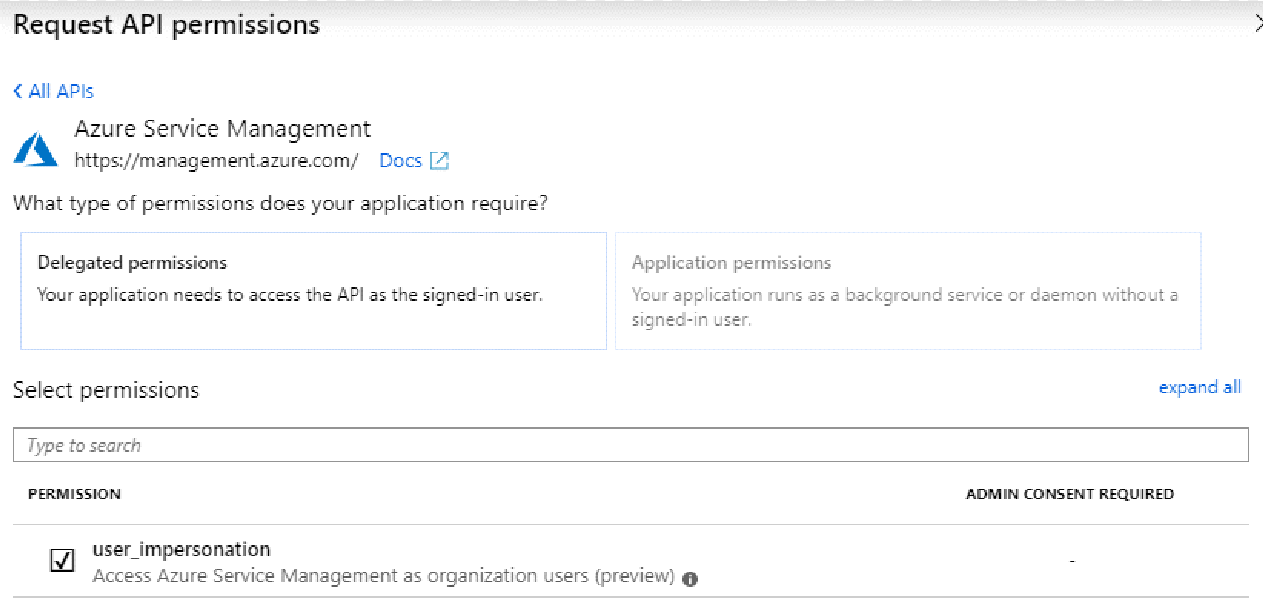
Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

Azure Storage
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Customer Insights
Create profile and interaction models for your products

Data Export Service for Microsoft Dynamics 365
Export data from Microsoft Dynamics CRM organization to an external destination

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



Request API permissions

< All APIs

Azure Service Management
https://management.azure.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions

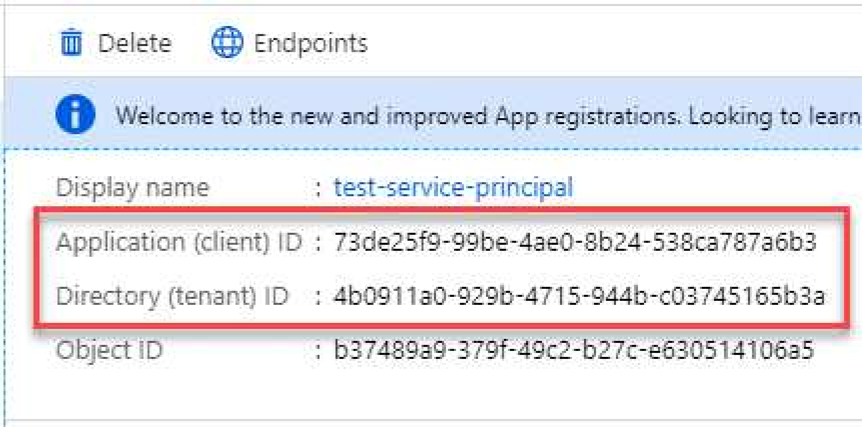
expand all

Type to search

PERMISSION	ADMIN CONSENT REQUIRED
☑ user_impersonation Access Azure Service Management as organization users (preview)	-

Get the application ID and directory ID for the application

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



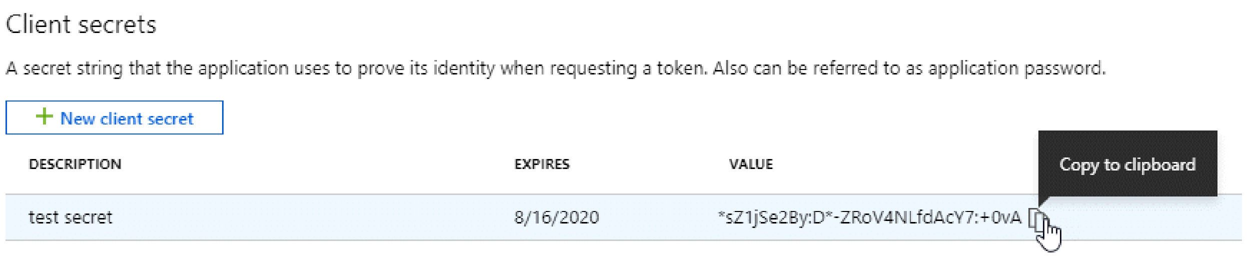
Welcome to the new and improved App registrations. Looking to learn

Display name : test-service-principal
Application (client) ID : 73de25f9-99be-4ae0-8b24-538ca787a6b3
Directory (tenant) ID : 4b0911a0-929b-4715-944b-c03745165b3a
Object ID : b37489a9-379f-49c2-b27c-e630514106a5

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 **Microsoft Entra ID** 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.

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

You now have a client secret that BlueXP can use it to authenticate with Microsoft Entra ID.

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.

Step 4: Create the Connector

Create the Connector directly from the BlueXP web-based console.

About this task

- Creating the Connector from BlueXP deploys a virtual machine in Azure using a default configuration. After you create the Connector, you should not change to a smaller VM type that has less CPU or RAM. Learn about the default configuration for the Connector.
- When BlueXP deploys the Connector, it creates a custom role and assigns it to the Connector VM. This role includes permissions that enables the Connector to manage Azure resources. You need to ensure that the role is kept up to date as new permissions are added in subsequent releases. Learn more about the custom role for the Connector.

Before you begin

You should have the following:

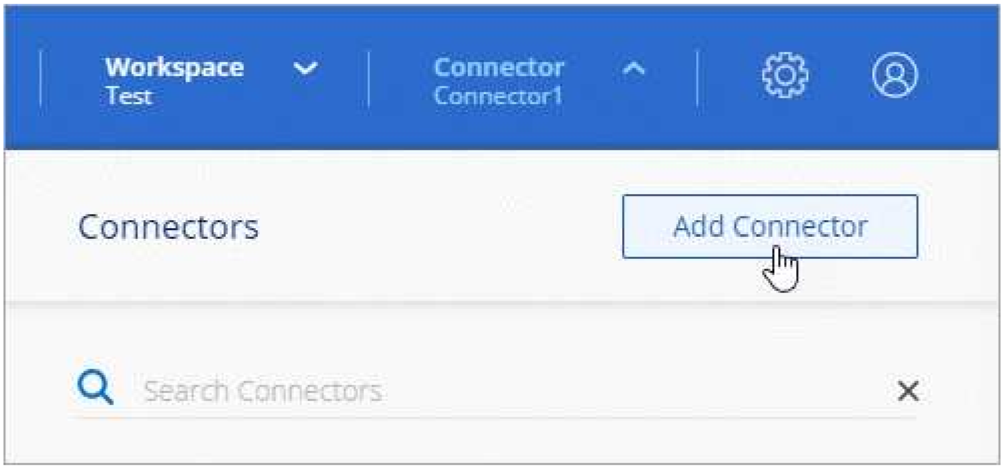
- An Azure subscription.
- A VNet and subnet in your Azure region of choice.
- Details about a proxy server, if your organization requires a proxy for all outgoing internet traffic:
  - IP address
  - Credentials
  - HTTPS certificate
- An SSH public key, if you want to use that authentication method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

Steps

1. 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 Microsoft Entra 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. Click **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.

If you have Azure Blob storage in the same Azure subscription where you created the Connector, you'll see an Azure Blob storage working environment appear on the BlueXP canvas automatically. Learn how to manage Azure Blob storage from BlueXP

Create a Connector from the Azure Marketplace

You can create a Connector in Azure directly from the Azure Marketplace. To create a Connector from the Azure Marketplace, you need to set up your networking, prepare Azure permissions, review instance requirements, and then create the Connector.

Before you begin

- You should have an understanding of Connectors.
- Review Connector limitations.

Step 1: Set up networking

Ensure that the network location where you plan to install the Connector supports the following requirements.These requirements enable the Connector to manage resources in your hybrid cloud.

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

VNet and subnet

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

Connections to target networks

A Connector requires a network connection to the location where you're planning to create and manage working environments. For example, the network where you plan to create Cloud Volumes ONTAP systems or a storage system in your on-premises environment.

Outbound internet access

The network location where you deploy the Connector must have an outbound internet connection to contact specific endpoints.

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.

Note that the endpoints listed below are all CNAME entries.

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 https://mysupport.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://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	To provide SaaS features and services within BlueXP.
Choose between two sets of endpoints: • Option 1 (recommended) [1] https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Option 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	To obtain images for Connector upgrades.

[1] The endpoints listed in option 1 are recommended because they are more secure. We recommend that you set up your firewall to allow the endpoints listed in option 1, while disallowing the endpoints listed in option 2. Note the following about these endpoints:

- The endpoints listed in option 1 are supported starting with the 3.9.47 release of the Connector. There is no backwards compatibility with previous releases of the Connector.
- The Connector contacts the endpoints listed in option 2 first. If those endpoints aren't accessible, the Connector automatically contacts the endpoints listed in option 1.
- The endpoints in option 1 are not supported if you use the Connector with BlueXP backup and recovery or BlueXP ransomware protection. In this case, you can disallow the endpoints listed in option 1, while allowing the endpoints listed in option 2.

Proxy server

NetApp supports both explicit and transparent proxy configurations. If you are using a transparent proxy, you only need to provide the certificate for the proxy server. If you are using an explicit proxy, you'll also need the IP address and credentials.

- 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.

Enable NTP

If you're planning to use BlueXP classification to scan your corporate data sources, you should enable a Network Time Protocol (NTP) service on both the BlueXP Connector system and the BlueXP classification system so that the time is synchronized between the systems. Learn more about BlueXP classification

Implement the networking requirements after creating the Connector.

Step 2: Review VM requirements

When you create the Connector, choose a virtual machine type that meets the following requirements.

CPU

8 cores or 8 vCPUs

RAM

32 GB

Azure VM size

An instance type that meets the CPU and RAM requirements above. We recommend Standard_D8s_v3.

Step 3: Set up permissions

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.

Follow these steps to set up permissions for BlueXP.

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

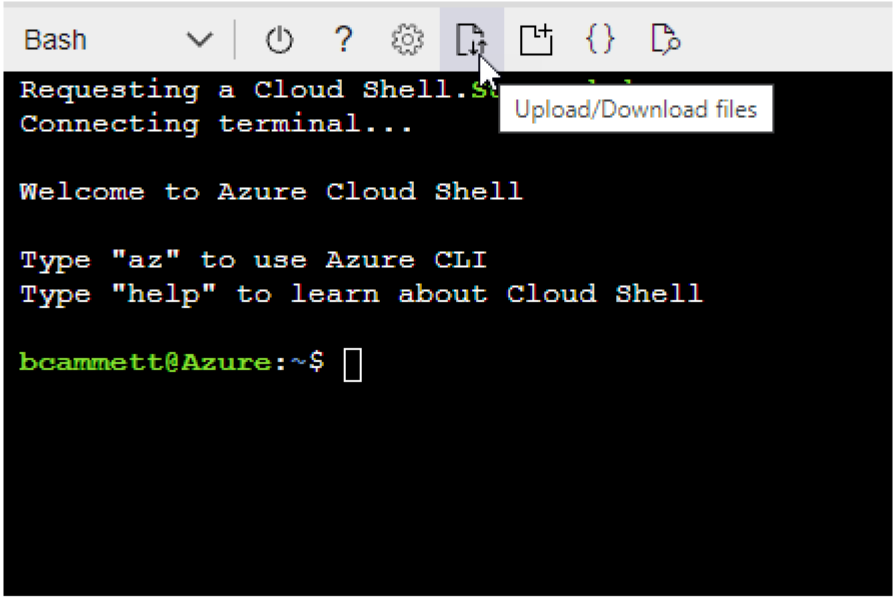
   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ```

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.



```
Requesting a Cloud Shell.S
Connecting terminal...

Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

bcammett@Azure:~$ 
```

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.

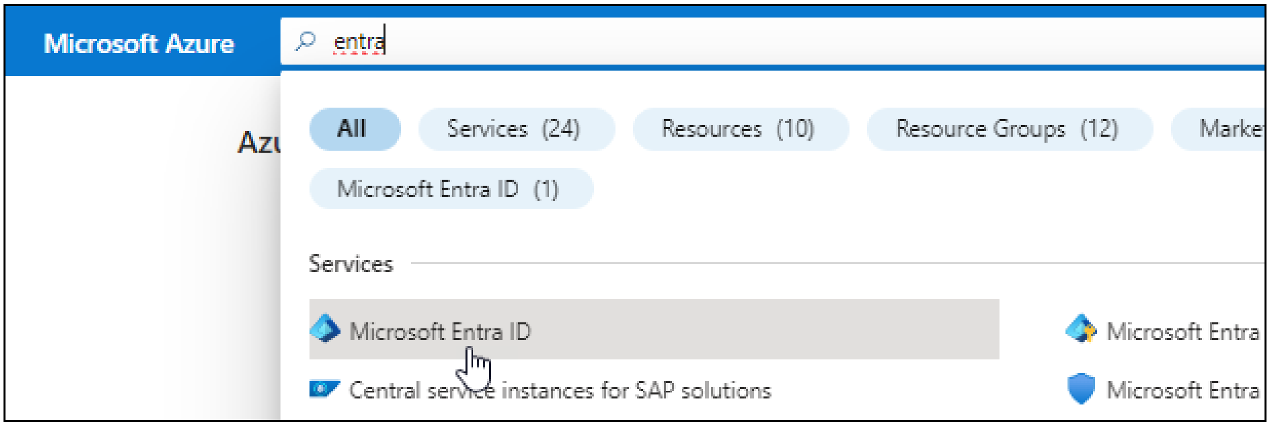
Service principal
Create and set up a service principal in Microsoft Entra ID and obtain the Azure credentials that BlueXP needs.

Create a Microsoft Entra 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 **Microsoft Entra ID** 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.

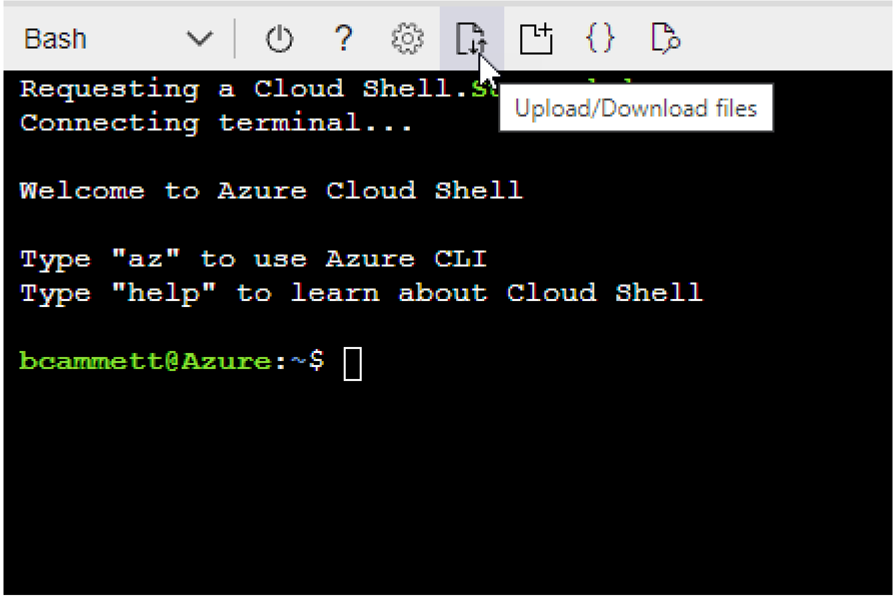
   Example

   ```
   "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.



```
Requesting a Cloud Shell.Su
Connecting terminal...

Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

bcammett@Azure:~$
```

   - 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.

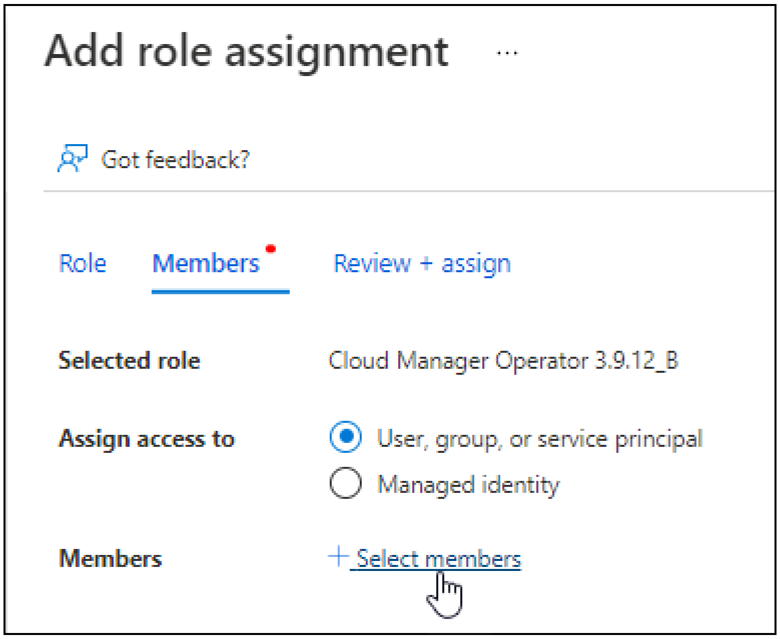
b. Select the subscription.

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**.



Add role assignment ···

Got feedback?

Role | Members | Review + assign

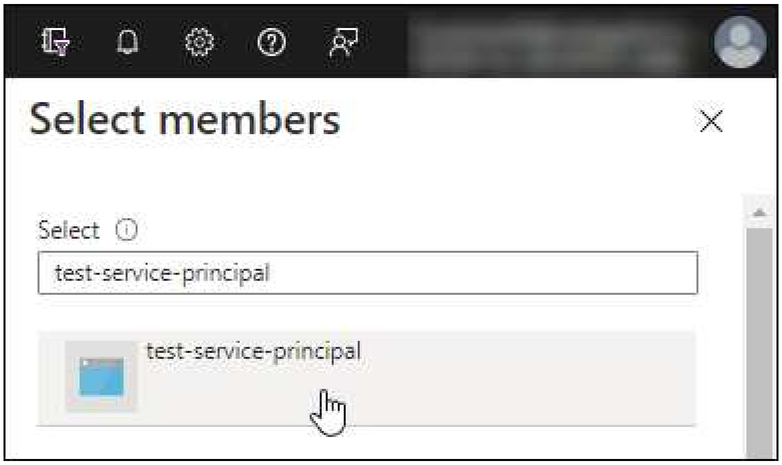
Selected role: Cloud Manager Operator 3.9.12_B

Assign access to: ● User, group, or service principal ○ Managed identity

Members: + Select members

  - Search for the name of the application.

    Here’s an example:



Select members

Select ⓘ

test-service-principal

test-service-principal

  - Select the application and select **Select**.
  - Select **Next**.

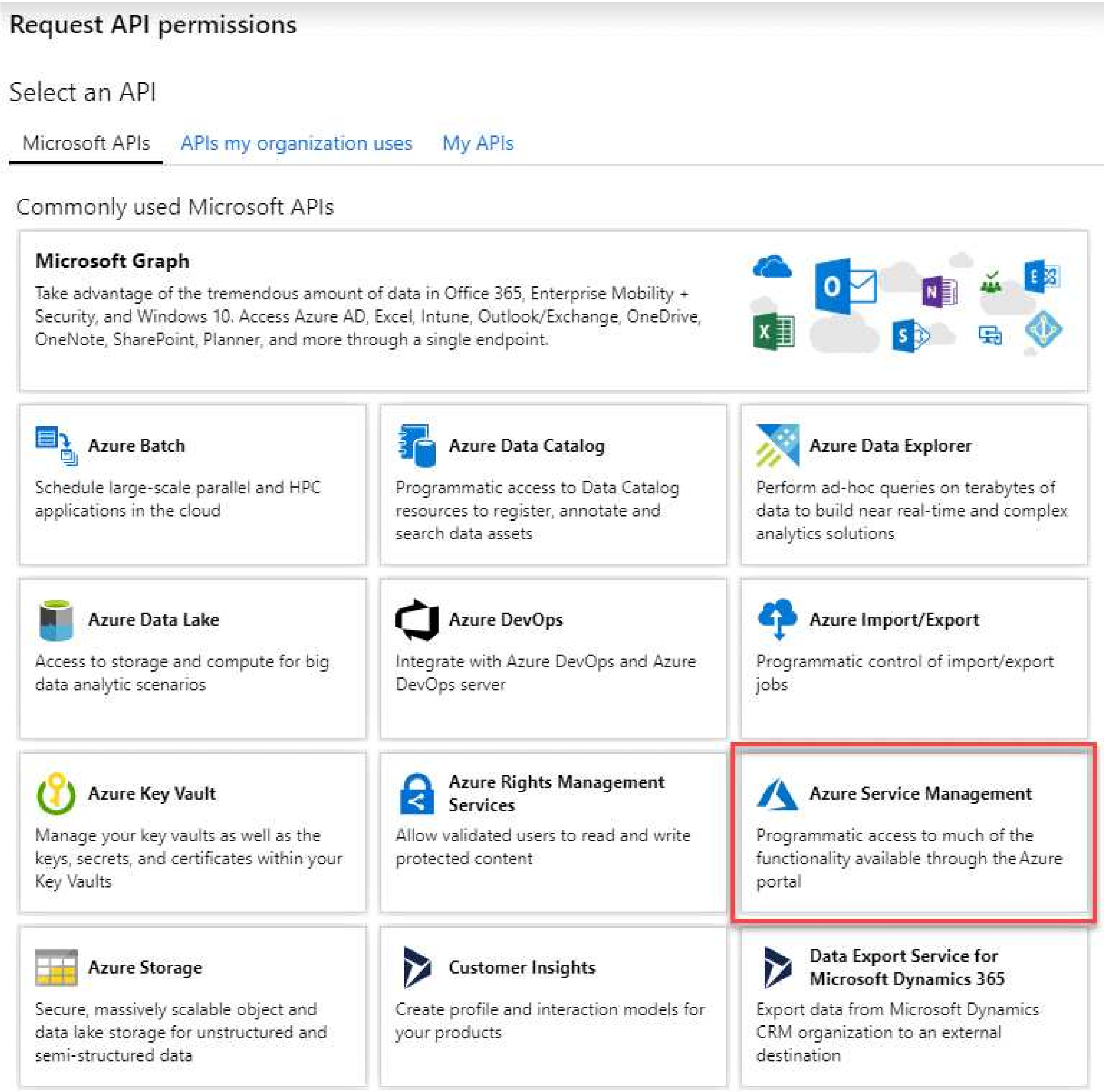
f. Select **Review + assign**.

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



Request API permissions

Select an API

Microsoft APIs | APIs my organization uses | My APIs

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Batch
Schedule large-scale parallel and HPC applications in the cloud

Azure Data Catalog
Programmatic access to Data Catalog resources to register, annotate and search data assets

Azure Data Explorer
Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

Azure Data Lake
Access to storage and compute for big data analytic scenarios

Azure DevOps
Integrate with Azure DevOps and Azure DevOps server

Azure Import/Export
Programmatic control of import/export jobs

Azure Key Vault
Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Rights Management Services
Allow validated users to read and write protected content

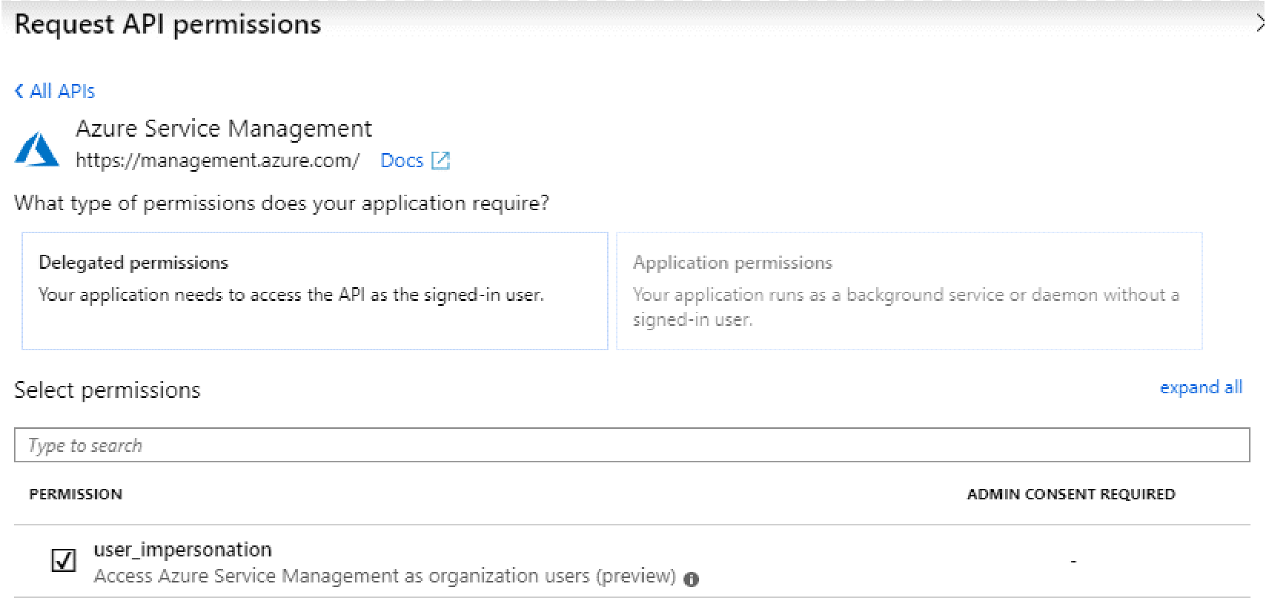
Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

Azure Storage
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Customer Insights
Create profile and interaction models for your products

Data Export Service for Microsoft Dynamics 365
Export data from Microsoft Dynamics CRM organization to an external destination

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


Request API permissions

< All APIs

Azure Service Management
https://management.azure.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions

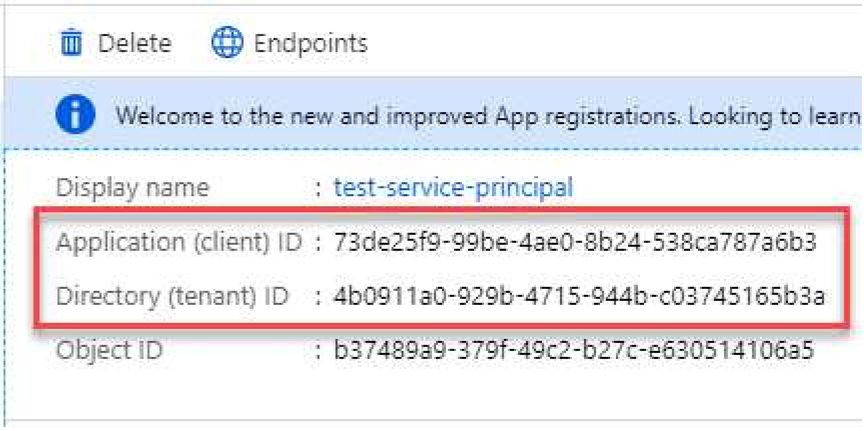
expand all

Type to search

PERMISSION	ADMIN CONSENT REQUIRED
☑ user_impersonation Access Azure Service Management as organization users (preview)	-

Get the application ID and directory ID for the application

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



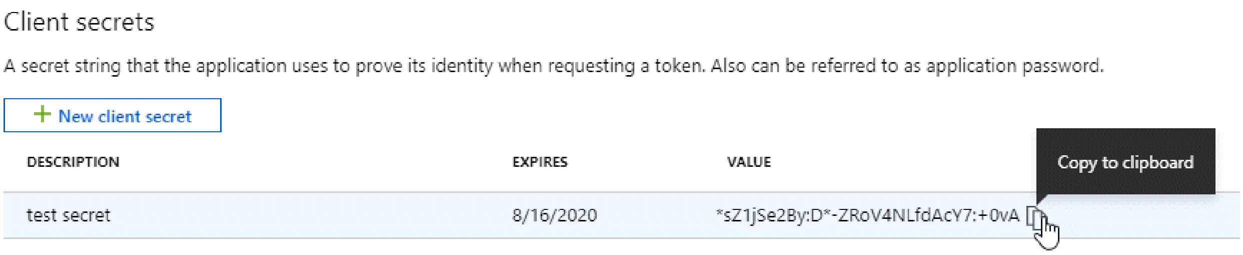
Welcome to the new and improved App registrations. Looking to learn

Display name : test-service-principal
Application (client) ID : 73de25f9-99be-4ae0-8b24-538ca787a6b3
Directory (tenant) ID : 4b0911a0-929b-4715-944b-c03745165b3a
Object ID : b37489a9-379f-49c2-b27c-e630514106a5

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 **Microsoft Entra ID** 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.

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

You now have a client secret that BlueXP can use it to authenticate with Microsoft Entra ID.

Step 4: Create the Connector

Launch the Connector directly from the Azure Marketplace.

About this task

Creating the Connector from the Azure Marketplace sets up a virtual machine with a default configuration. Learn about the default configuration for the Connector.

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 deploy the Connector VM.

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 Standard_D8s_v3.
- **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 Microsoft Entra ID 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. You should see the virtual machine and Connector software running in about 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 organization 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.

      Keep restricted mode disabled 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

You have now installed the Connector and set it up with your BlueXP organization.

If you have Azure Blob storage in the same Azure subscription where you created the Connector, you'll see an Azure Blob storage working environment appear on the BlueXP canvas automatically. Learn how to manage Azure Blob storage from BlueXP

Step 5: Provide permissions to BlueXP

Now that you've created the Connector, 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.

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.

   It’s important to assign the role from the **Subscriptions** service because this specifies the scope of the role assignment at the subscription level. The *scope* defines the set of resources that the access applies to. If you specify a scope at a different level (for example, at the virtual machine level), your ability to complete actions from within BlueXP will be affected.

   Microsoft Azure documentation: Understand scope for Azure RBAC

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, under **Managed identity**, 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.

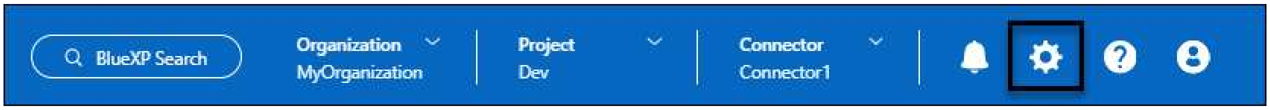
What’s next?

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 Microsoft Entra 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.

Manually install the Connector in Azure

A Connector is NetApp software running in your cloud network or on-premises network that gives you the ability to use all BlueXP features and services. One of the available installation options is to manually install the Connector software on a Linux host running in Azure. To manually install the Connector on your own Linux host, you need to review host requirements, set up your networking, prepare Azure permissions, install the Connector, and then provide the permissions that you prepared.

Before you begin

- You should have an understanding of Connectors.
- You should review Connector limitations.

Step 1: Review host requirements

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

> The Connector reserves the UID and GID range of 19000 to 19200. This range is fixed and cannot be modified. If any third-party software on your host is using UIDs or GIDs within this range, the Connector installation will fail. NetApp recommends using a host that is free of third-party software to avoid conflicts.

Dedicated host

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

Host can be of any architecture that meets the following size requirements:

- CPU: 8 cores or 8 vCPUs
- RAM: 32 GB

Hypervisor

A bare metal or hosted hypervisor that is certified to run a supported operating system is required.

Operating system and container requirements

BlueXP supports the Connector with the following operating systems when using BlueXP in standard mode or restricted mode. A container orchestration tool is required before you install the Connector.

Operating system	Supported OS versions	Supported Connector versions	Required container tool	SELinux
Red Hat Enterprise Linux	9.1 to 9.4 8.6 to 8.10 7.9	3.9.40 or later with BlueXP in standard mode or restricted mode	Podman version 4.6.1 or 4.9.4 View Podman configuration requirements.	Supported in enforcing mode or permissive mode [1]
Ubuntu	24.04 LTS	3.9.45 or later with BlueXP in standard mode or restricted mode	Docker Engine 23.06 to 28.0.0.	Not supported
	22.04 LTS	3.9.29 or later	Docker Engine 23.0.6 to 28.0.0.	Not supported

Notes:

1. Management of Cloud Volumes ONTAP systems is not supported by Connectors that have SELinux enabled on the operating system.
2. The Connector is supported on English-language versions of these operating systems.
3. For RHEL, 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.

Azure VM size

An instance type that meets the CPU and RAM requirements above. We recommend Standard_D8s_v3.

Disk space in /opt

100 GiB of space must be available

BlueXP uses `/opt` to install the `/opt/application/netapp` directory and its contents.

Disk space in /var

20 GiB of space must be available

BlueXP requires this space in `/var` because Docker or Podman are architected to create the containers within this directory. Specifically, they will create containers in the `/var/lib/containers/storage` directory. External mounts or symlinks do not work for this space.

Step 2: Install Podman or Docker Engine

Depending on your operating system, either Podman or Docker Engine is required before you install the Connector.

- Podman is required for Red Hat Enterprise Linux 8 and 9.

  View the Podman versions that BlueXP supports.

- Docker Engine is required for Ubuntu.

  View the Docker Engine versions that BlueXP supports.

Example 2. Steps

Podman

Follow these steps to install Podman and configure it to meet the following requirements:

- Enable and start the podman.socket service
- Install python3
- Install the podman-compose package version 1.0.6
- Add podman-compose to the PATH environment variable

ⓘ When using Podman, adjust the aardvark-dns service port (default: 53) after installing the Connector to avoid conflicts with the DNS port on the host. Follow the instructions to configure the port.

Steps

1. Remove the podman-docker package if it’s installed on the host.

   ```
   dnf remove podman-docker
   rm /var/run/docker.sock
   ```

2. Install Podman.

   Podman is available from official Red Hat Enterprise Linux repositories.

   For Red Hat Enterprise Linux 9:

   ```
   sudo dnf install podman-2:<version>
   ```

   Where <version> is the supported version of Podman that you’re installing. View the Podman versions that BlueXP supports.

   For Red Hat Enterprise Linux 8:

   ```
   sudo dnf install podman-3:<version>
   ```

   Where <version> is the supported version of Podman that you’re installing. View the Podman versions that BlueXP supports.

3. Enable and start the podman.socket service.

   ```
   sudo systemctl enable --now podman.socket
   ```

4. Install python3.

```
sudo dnf install python3
```

5. Install the EPEL repository package if it’s not already available on your system.

   This step is required because podman-compose is available from the Extra Packages for Enterprise Linux (EPEL) repository.

   For Red Hat Enterprise Linux 9:

   ```
   sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
   ```

   For Red Hat Enterprise Linux 8:

   ```
   sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
   ```

6. Install podman-compose package 1.0.6.

   ```
   sudo dnf install podman-compose-1.0.6
   ```

   ⓘ Using the `dnf install` command meets the requirement for adding podman-compose to the PATH environment variable. The installation command adds podman-compose to /usr/bin, which is already included in the `secure_path` option on the host.

Docker Engine

Follow the documentation from Docker to install Docker Engine.

Steps

1. View installation instructions from Docker

   Be sure to follow the steps to install a specific version of Docker Engine. Installing the latest version will install a version of Docker that BlueXP doesn’t support.

2. Verify that Docker is enabled and running.

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

Step 3: Set up networking

Ensure that the network location where you plan to install the Connector supports the following requirements. Meeting these requirements enables the Connector to manage resources and processes within your hybrid cloud environment.

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. For example, the network where you plan to create Cloud Volumes ONTAP systems or a storage system in your on-premises environment.

Outbound internet access

The network location where you deploy the Connector must have an outbound internet connection to contact specific endpoints.

Endpoints contacted from computers when using the BlueXP web-based console

Computers that access the BlueXP console from a web browser must have the ability to contact several endpoints. You’ll need to use the BlueXP console to set up the Connector and for day-to-day use of BlueXP.

Prepare networking for 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://mysupport.netapp.com
- https://signin.b2c.netapp.com (this endpoint is the CNAME URL for https://mysupport.netapp.com)
- https://cloudmanager.cloud.netapp.com/tenancy
- https://stream.cloudmanager.cloud.netapp.com
- https://production-artifacts.cloudmanager.cloud.netapp.com
- To obtain images, the installer needs access to one of these two sets of endpoints:
  - Option 1 (recommended):
    - https://bluexpinfraprod.eastus2.data.azurecr.io
    - https://bluexpinfraprod.azurecr.io
  - Option 2:
    - https://*.blob.core.windows.net
    - https://cloudmanagerinfraprod.azurecr.io

  The endpoints listed in option 1 are recommended because they are more secure. We recommend that you set up your firewall to allow the endpoints listed in option 1, while disallowing the endpoints listed in option 2. Note the following about these endpoints:

  - The endpoints listed in option 1 are supported starting with the 3.9.47 release of the Connector. There is no backwards compatibility with previous releases of the Connector.

- The Connector contacts the endpoints listed in option 2 first. If those endpoints aren't accessible, the Connector automatically contacts the endpoints listed in option 1.
- The endpoints in option 1 are not supported if you use the Connector with BlueXP backup and recovery or BlueXP ransomware protection. In this case, you can disallow the endpoints listed in option 1, while allowing the endpoints listed in option 2.

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.

Note that the endpoints listed below are all CNAME entries.

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 https://mysupport.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://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	To provide SaaS features and services within BlueXP.
Choose between two sets of endpoints: • Option 1 (recommended) [1] https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Option 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	To obtain images for Connector upgrades.

[1] The endpoints listed in option 1 are recommended because they are more secure. We recommend that you set up your firewall to allow the endpoints listed in option 1, while disallowing the endpoints listed in option 2. Note the following about these endpoints:

- The endpoints listed in option 1 are supported starting with the 3.9.47 release of the Connector. There is no backwards compatibility with previous releases of the Connector.
- The Connector contacts the endpoints listed in option 2 first. If those endpoints aren't accessible, the Connector automatically contacts the endpoints listed in option 1.
- The endpoints in option 1 are not supported if you use the Connector with BlueXP backup and recovery or BlueXP ransomware protection. In this case, you can disallow the endpoints listed in option 1, while allowing the endpoints listed in option 2.

Proxy server

NetApp supports both explicit and transparent proxy configurations. If you are using a transparent proxy, you only need to provide the certificate for the proxy server. If you are using an explicit proxy, you'll also need the IP address and credentials.

- 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.

Enable NTP

If you're planning to use BlueXP classification to scan your corporate data sources, you should enable a Network Time Protocol (NTP) service on both the BlueXP Connector system and the BlueXP classification system so that the time is synchronized between the systems. Learn more about BlueXP classification

Step 4: Set up Connector deployment permissions

You need to provide Azure permissions to BlueXP by using one of the following options:

- 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.

Follow the steps to prepare permissions for BlueXP.

Create a custom role for Connector deployment

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

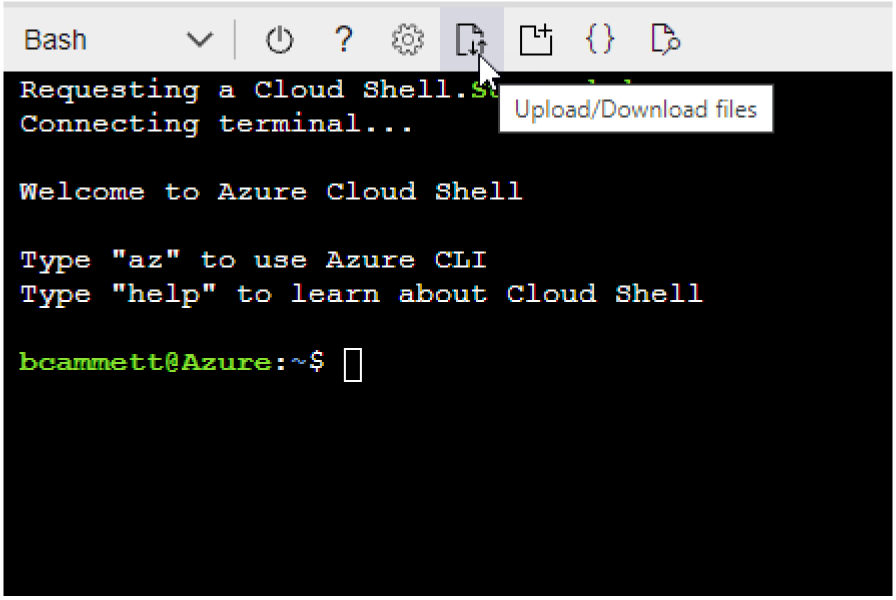
   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ```

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.



```
Requesting a Cloud Shell.Su
Connecting terminal...

Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

bcammett@Azure:~$ 
```

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.

Service principal

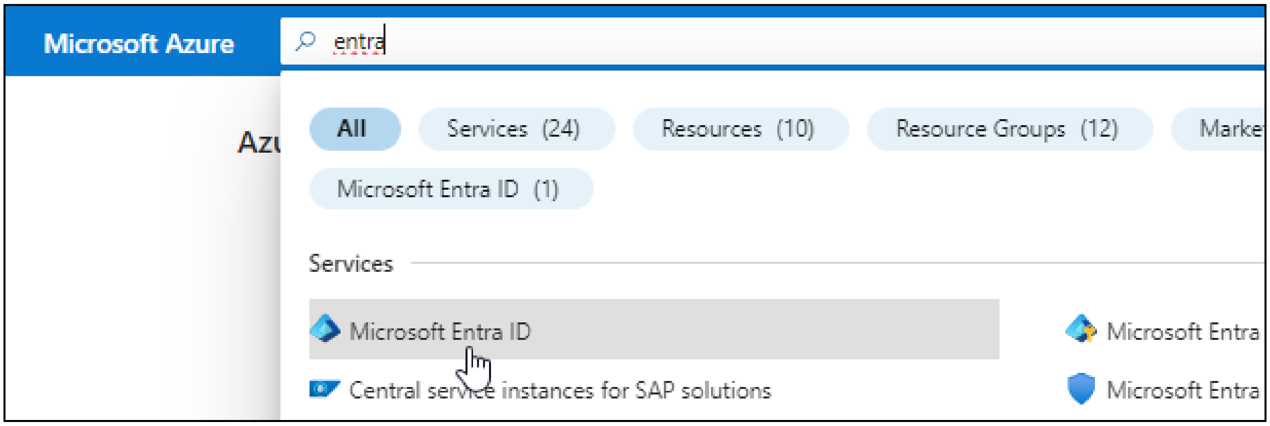
Create and set up a service principal in Microsoft Entra ID and obtain the Azure credentials that BlueXP needs.

Create a Microsoft Entra 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 **Microsoft Entra ID** 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.

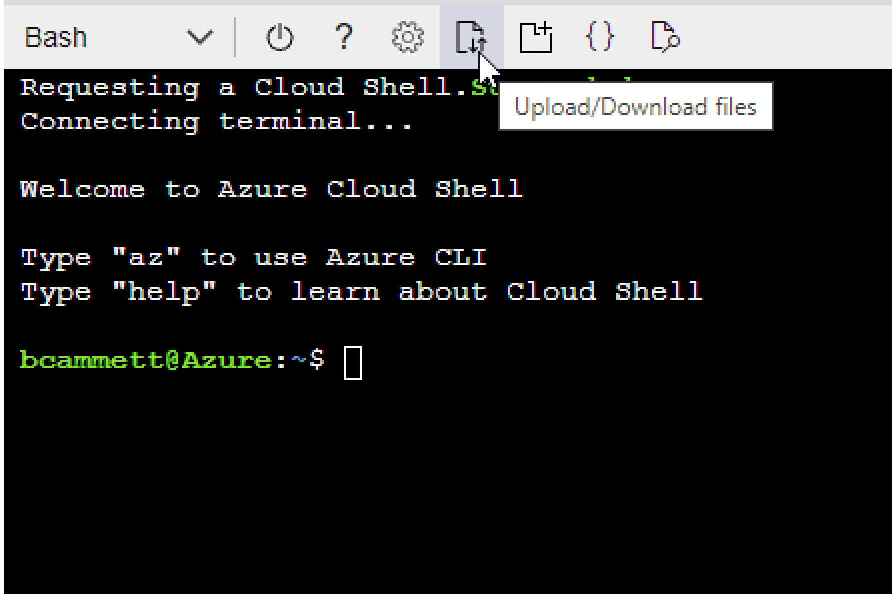
   Example

   ```
   "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.

     ```
     Requesting a Cloud Shell.Su
     Connecting terminal...

     Welcome to Azure Cloud Shell

     Type "az" to use Azure CLI
     Type "help" to learn about Cloud Shell

     bcammett@Azure:~$
     ```

   - 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.

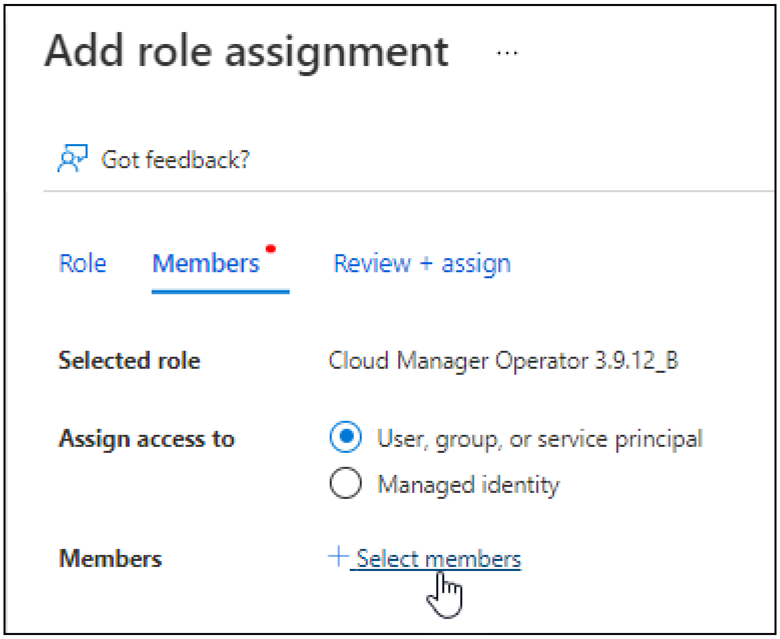
b. Select the subscription.

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**.



Add role assignment ...

Got feedback?

Role | Members | Review + assign

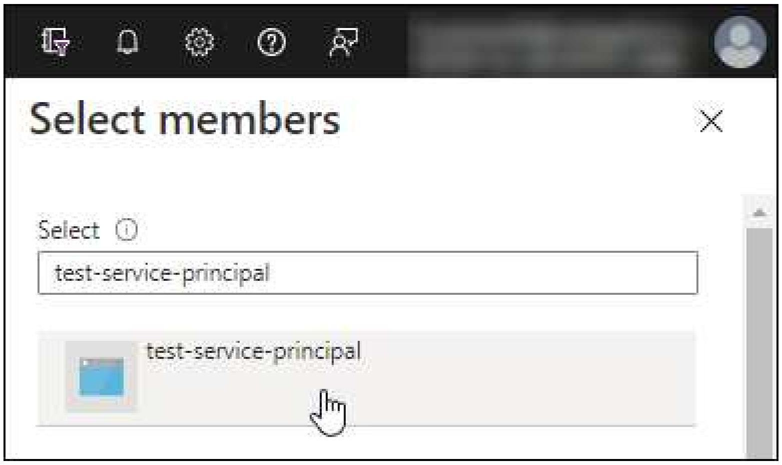
Selected role: Cloud Manager Operator 3.9.12_B

Assign access to: ● User, group, or service principal ○ Managed identity

Members: + Select members

   - Search for the name of the application.

     Here's an example:



Select members

Select: test-service-principal

test-service-principal

   - Select the application and select **Select**.
   - Select **Next**.

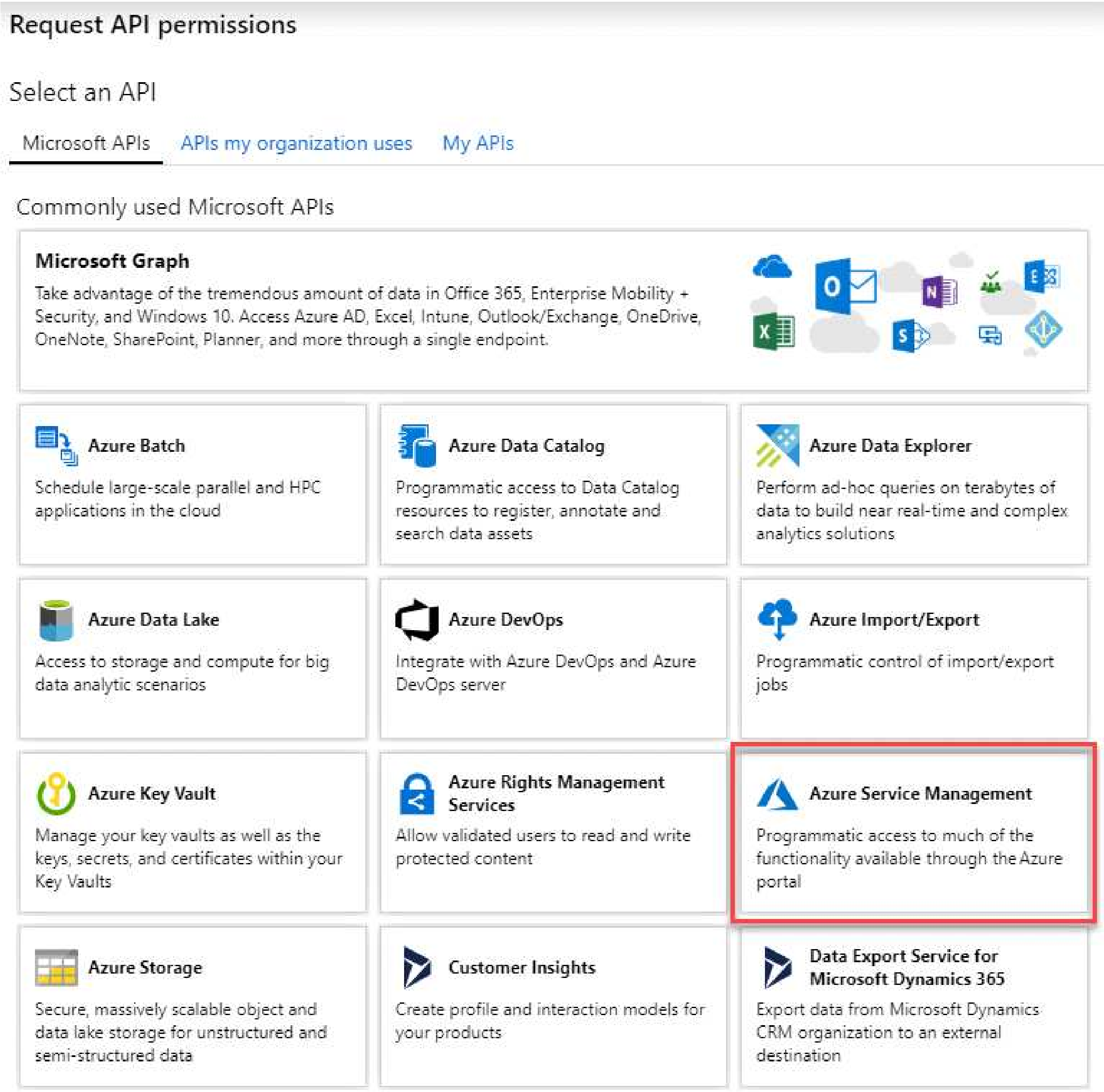
f. Select **Review + assign**.

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



Request API permissions

Select an API

Microsoft APIs | APIs my organization uses | My APIs

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Batch
Schedule large-scale parallel and HPC applications in the cloud

Azure Data Catalog
Programmatic access to Data Catalog resources to register, annotate and search data assets

Azure Data Explorer
Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

Azure Data Lake
Access to storage and compute for big data analytic scenarios

Azure DevOps
Integrate with Azure DevOps and Azure DevOps server

Azure Import/Export
Programmatic control of import/export jobs

Azure Key Vault
Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Rights Management Services
Allow validated users to read and write protected content

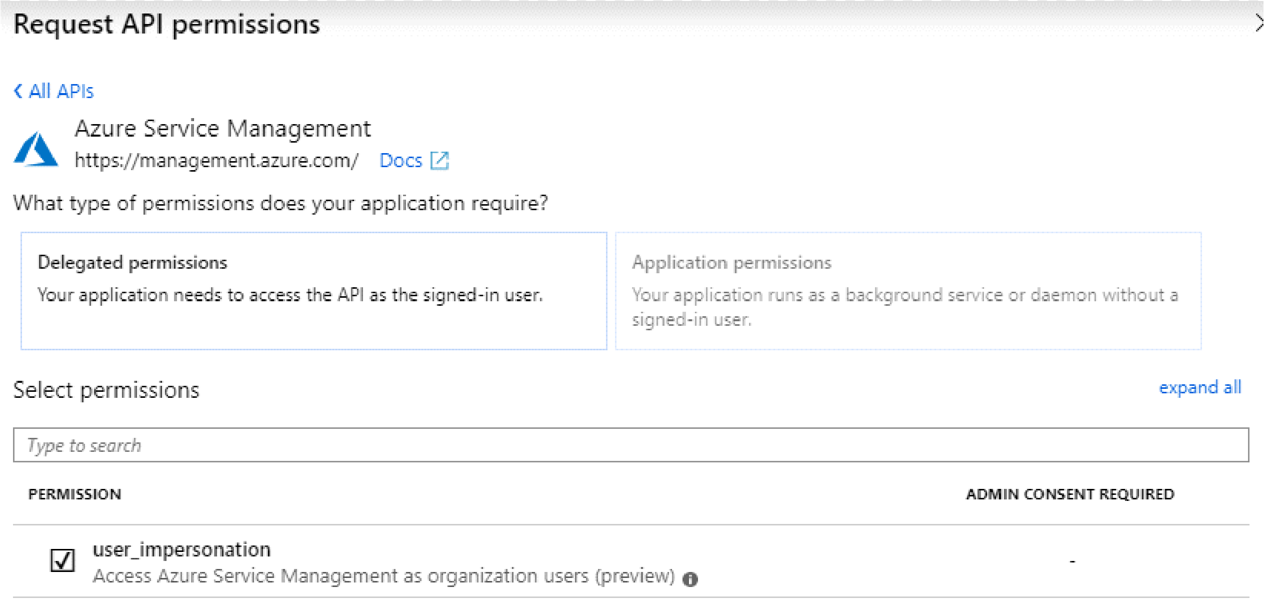
Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

Azure Storage
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Customer Insights
Create profile and interaction models for your products

Data Export Service for Microsoft Dynamics 365
Export data from Microsoft Dynamics CRM organization to an external destination

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



Request API permissions

‹ All APIs

Azure Service Management
https://management.azure.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions

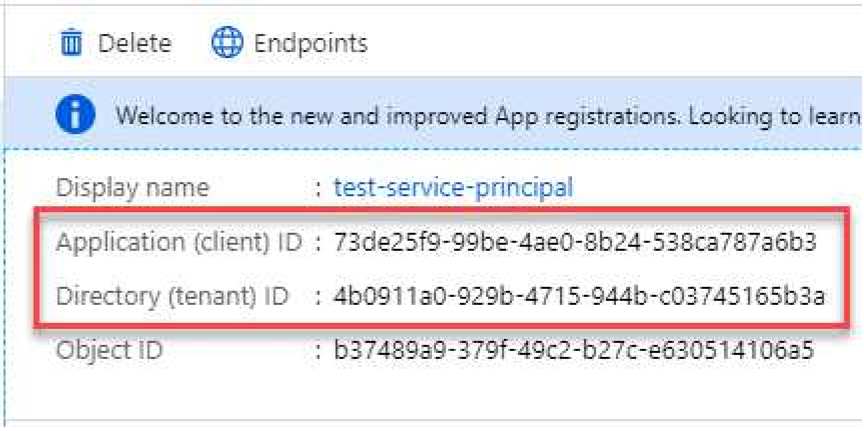
expand all

Type to search

PERMISSION	ADMIN CONSENT REQUIRED
☑ user_impersonation Access Azure Service Management as organization users (preview)	-

Get the application ID and directory ID for the application

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



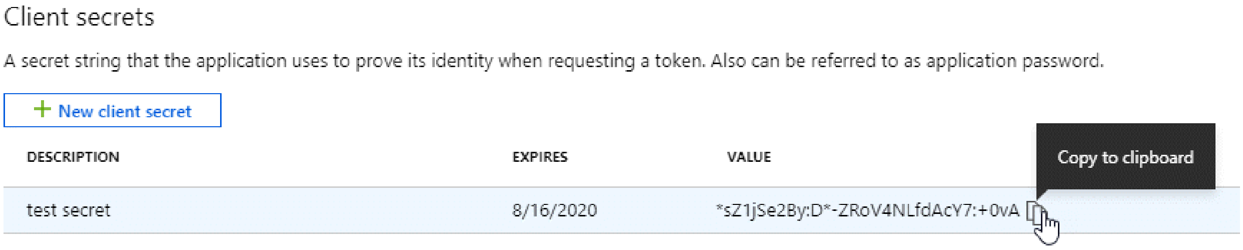
Welcome to the new and improved App registrations. Looking to learn

Display name : test-service-principal
Application (client) ID : 73de25f9-99be-4ae0-8b24-538ca787a6b3
Directory (tenant) ID : 4b0911a0-929b-4715-944b-c03745165b3a
Object ID : b37489a9-379f-49c2-b27c-e630514106a5

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 **Microsoft Entra ID** 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.

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

You now have a client secret that BlueXP can use it to authenticate with Microsoft Entra ID.

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.

Step 5: Install the Connector

After the pre-requisites are complete, you can manually install the software on your own Linux host.

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.

> ⓘ You cannot set a certificate for a transparent proxy server when manually installing the Connector. If you need to set a certificate for a transparent proxy server, you must use the Maintenance Console after installation. Learn more about the Connector Maintenance Console.

- 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. 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.

2. 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.

3. Assign permissions to run the script.

   ```
   chmod +x BlueXP-Connector-Cloud-<version>
   ```

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

4. Run the installation script.

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

   You’ll need to add proxy information if your network requires a proxy for internet access. You can add either a transparent or explicit proxy. The --proxy and --cacert parameters are optional and you won’t be prompted to add them. If you have a proxy server, you will need to enter the parameters as shown.

   Here is an example configuring an explicit proxy server with a CA-signed certificate:

   ```
    ./BlueXP-Connector-Cloud-v3.9.40--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://user-name:password@address:port
   - http://domain-name%92user-name:password@address:port
   - https://address:port
   - https://user-name:password@address:port
   - https://domain-name%92user-name:password@address:port

     Note the following:

     - The user can be a local user or domain user.

- For a domain user, you must use the ASCII code for a \ as shown above.
- BlueXP doesn’t support user names or passwords that include the @ character.
- If the password includes any of the following special characters, you must escape that special character by prepending it with a backslash: & or !

  For example:

  http://bxpproxyuser:netapp1\!@address:3128

  --cacert specifies a CA-signed certificate to use for HTTPS access between the Connector and the proxy server. This parameter is required for HTTPS proxy servers, intercepting proxy servers, and transparent proxy servers.

Here is an example configuring a transparent proxy server. When you configure a transparent proxy, you don’t need to define the proxy server. You only add a CA-signed certificate to your Connector host:

```
./BlueXP-Connector-Cloud-v3.9.40 --cacert /tmp/cacert/certificate.cer
```

5. If you used Podman, you’ll need to adjust the aardvark-dns port.

   a. SSH to the BlueXP Connector virtual machine.

   b. Open podman */usr/share/containers/containers.conf* file and modify the chosen port for Aardvark DNS service. For example, change it to 54.

   ```
   vi /usr/share/containers/containers.conf
   ...
   # Port to use for dns forwarding daemon with netavark in rootful
   bridge
   # mode and dns enabled.
   # Using an alternate port might be useful if other DNS services
   should
   # run on the machine.
   #
   dns_bind_port = 54
   ...
   Esc:wq
   ```

   c. Reboot the Connector virtual machine.

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 organization 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**.

If you have Azure Blob storage in the same Azure subscription where you created the Connector, you'll see an Azure Blob storage working environment appear on the BlueXP canvas automatically. Learn how to manage Azure Blob storage from BlueXP

Step 6: Provide permissions to BlueXP

Now that you've installed the Connector, you need to provide BlueXP with the Azure permissions that you previously set up. Providing the permissions enables BlueXP to manage your data and storage infrastructure in Azure.

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.

   It's important to assign the role from the **Subscriptions** service because this specifies the scope of the role assignment at the subscription level. The *scope* defines the set of resources that the access applies to. If you specify a scope at a different level (for example, at the virtual machine level), your ability to complete actions from within BlueXP will be affected.

   Microsoft Azure documentation: Understand scope for Azure RBAC

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, under **Managed identity**, 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.

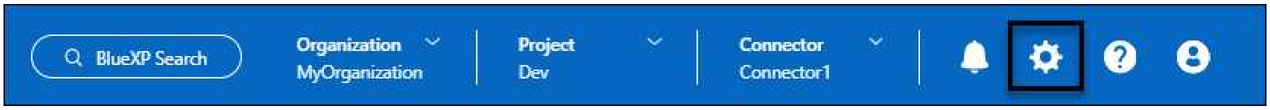
What's next?

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 Microsoft Entra 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

Connector installation options in Google Cloud

There are a few different ways to create a Connector in Google Cloud. Directly from BlueXP is the most common way.

The following installation options are available:

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

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

- Create the Connector using gcloud

  This action also launches a VM instance running Linux and the Connector software, but the deployment is initiated directly from Google Cloud, rather than from BlueXP.

- 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 Google Cloud.

Create a Connector in Google Cloud from BlueXP or gcloud

You can create a Connector in Google Cloud from BlueXP or by using Google Cloud. You need to set up your networking, prepare Google Cloud permissions, enable Google Cloud APIs, and then create the Connector.

Before you begin

- You should have an understanding of Connectors.
- You should review Connector limitations.

Step 1: Set up networking

Set up networking to ensure the Connector can manage resources, with connections to target networks and outbound internet access.

VPC and subnet

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

Connections to target networks

A Connector requires a network connection to the location where you're planning to create and manage working environments. For example, the network where you plan to create Cloud Volumes ONTAP systems or a storage system in your on-premises environment.

Outbound internet access

The network location where you deploy the Connector must have an outbound internet connection to contact specific endpoints.

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.

Note that the endpoints listed below are all CNAME entries.

Endpoints	Purpose
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.
https://support.netapp.com https://mysupport.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://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	To provide SaaS features and services within BlueXP.

Endpoints	Purpose
Choose between two sets of endpoints: • Option 1 (recommended) [1] https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Option 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	To obtain images for Connector upgrades.

[1] The endpoints listed in option 1 are recommended because they are more secure. We recommend that you set up your firewall to allow the endpoints listed in option 1, while disallowing the endpoints listed in option 2. Note the following about these endpoints:

- The endpoints listed in option 1 are supported starting with the 3.9.47 release of the Connector. There is no backwards compatibility with previous releases of the Connector.
- The Connector contacts the endpoints listed in option 2 first. If those endpoints aren't accessible, the Connector automatically contacts the endpoints listed in option 1.
- The endpoints in option 1 are not supported if you use the Connector with BlueXP backup and recovery or BlueXP ransomware protection. In this case, you can disallow the endpoints listed in option 1, while allowing the endpoints listed in option 2.

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.

Proxy server

NetApp supports both explicit and transparent proxy configurations. If you are using a transparent proxy, you only need to provide the certificate for the proxy server. If you are using an explicit proxy, you'll also need the IP address and credentials.

- 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.

Enable NTP

If you’re planning to use BlueXP classification to scan your corporate data sources, you should enable a Network Time Protocol (NTP) service on both the BlueXP Connector system and the BlueXP classification system so that the time is synchronized between the systems. Learn more about BlueXP classification

Implement this networking requirement after creating the Connector.

Step 2: Set up permissions to create the Connector

Before you can deploy a Connector from BlueXP or by using gcloud, you need to set up permissions for the Google Cloud user who will deploy the Connector VM.

Steps

1. Create a custom role in Google Cloud:

   a. Create a YAML file that includes the following permissions:

```
title: Connector deployment policy
description: Permissions for the user who deploys the Connector from BlueXP
stage: GA
includedPermissions:
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.list
```

b. From Google Cloud, activate cloud shell.

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

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

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

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

Google Cloud docs: Creating and managing custom roles

2. Assign this custom role to the user who will deploy the Connector from BlueXP or by using gcloud.

Google Cloud docs: Grant a single role

Step 3: Set up permissions for the Connector

A Google Cloud service account is required to provide the Connector with the permissions that BlueXP needs to manage resources in Google Cloud. When you create the Connector, you'll need to associate this service account with the Connector VM.

It's your responsibility to update the custom role as new permissions are added in subsequent releases. If new permissions are required, they will be listed in the release notes.

Steps

1. Create a custom role in Google Cloud:
   a. Create a YAML file that includes the contents of the service account permissions for the Connector.
   b. From Google Cloud, activate cloud shell.
   c. Upload the YAML file that includes the required permissions.
   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 and assign the role to the service account:
   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

3. If you plan to deploy Cloud Volumes ONTAP systems in different projects than the project where the Connector resides, then you'll need to provide the Connector's service account with access to those projects.

   For example, let's say the Connector is in project 1 and you want to create Cloud Volumes ONTAP systems in project 2. You'll need to grant access to the service account in project 2.

   a. From the IAM & Admin service, select the Google Cloud project where you want to create Cloud Volumes ONTAP systems.
   b. On the **IAM** page, select **Grant Access** and provide the required details.
      - Enter the email of the Connector's service account.
      - Select the Connector's custom role.
      - Select **Save**.

   For more details, refer to Google Cloud documentation

Result

The service account for the Connector VM is set up.

Step 4: Set up shared VPC permissions

If you are using a shared VPC to deploy resources into a service project, then you’ll need to prepare your permissions.

This table is for reference and your environment should reflect the permissions table when IAM configuration is complete.

View shared VPC permissions

Identity	Creator	Hosted in	Service project permissions	Host project permissions	Purpose
Google account to deploy the Connector	Custom	Service Project	Connector deployment policy	compute.network User	Deploying the Connector in the service project
Connector service account	Custom	Service project	Connector service account policy	compute.network User deploymentmanager.editor	Deploying and maintaining Cloud Volumes ONTAP and services in the service project
Cloud Volumes ONTAP service account	Custom	Service project	storage.admin member: BlueXP service account as serviceAccount.user	N/A	(Optional) For data tiering and BlueXP backup and recovery
Google APIs service agent	Google Cloud	Service project	(Default) Editor	compute.network User	Interacts with Google Cloud APIs on behalf of deployment. Allows BlueXP to use the shared network.
Google Compute Engine default service account	Google Cloud	Service project	(Default) Editor	compute.network User	Deploys Google Cloud instances and compute infrastructure on behalf of deployment. Allows BlueXP to use the shared network.

Notes:

1. deploymentmanager.editor is only required at the host project if you are not passing firewall rules to the deployment and are choosing to let BlueXP create them for you. BlueXP will create a deployment in the host project which contains the VPC0 firewall rule if no rule is specified.
2. firewall.create and firewall.delete are only required if you are not passing firewall rules to the deployment and are choosing to let BlueXP create them for you. These permissions reside in the BlueXP account .yaml file. If you are deploying an HA pair using a shared VPC, these permissions will be used to create the firewall rules for VPC1, 2 and 3. For all other deployments, these permissions will also be used to create rules for VPC0.
3. For data tiering, the tiering service account must have the serviceAccount.user role on the service account, not just at the project level. Currently if you assign serviceAccount.user at the project level, the permissions don’t show when you query the service account with getIAMPolicy.

Step 5: Enable Google Cloud APIs

You must enable several Google Cloud APIs before deploying the Connector and Cloud Volumes ONTAP.

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))

Google Cloud documentation: Enabling APIs

Step 6: Create the Connector

Create a Connector directly from the BlueXP web-based console or by using gcloud.

About this task

Creating the Connector deploys a virtual machine instance in Google Cloud using a default configuration. Do not change the Connector to a smaller VM instance with less CPU or RAM after creation. Learn about the default configuration for the Connector.

BlueXP

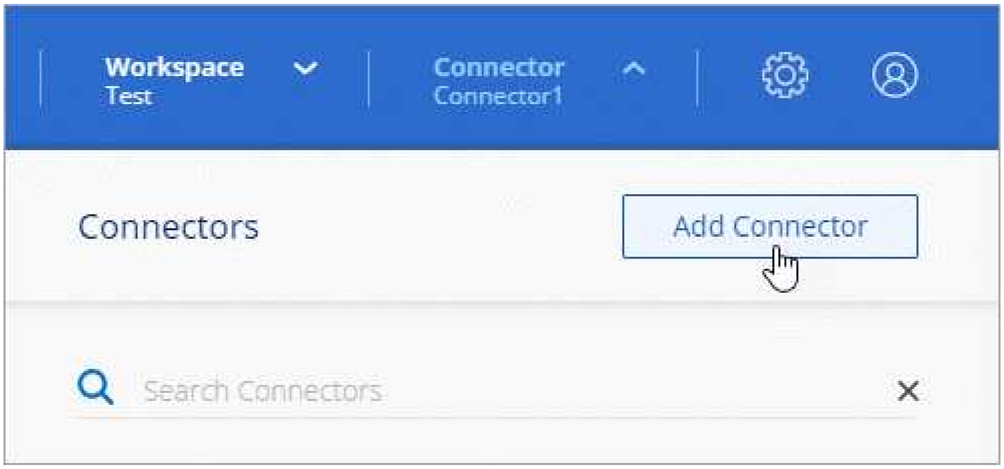
Before you begin

You should have the following:

- The required Google Cloud permissions to create the Connector and a service account for the Connector VM.
- A VPC and subnet that meets networking requirements.
- Details about a proxy server, if a proxy is required for internet access from the Connector.

Steps

1. Select the **Connector** drop-down and select **Add Connector**.



2. Choose **Google Cloud Platform** as your cloud provider.
3. On the **Deploying a Connector** page, review the details about what you'll need. You have two options:
   a. Select **Continue** to prepare for deployment by using the in-product guide. Each step in the in-product guide includes the information that's contained on this page of the documentation.
   b. Select **Skip to Deployment** if you already prepared by following the steps on this page.
4. Follow the steps in the wizard to create the Connector:
   - If you're prompted, log in to your Google account, which should have the required permissions to create the virtual machine instance.

     The form is owned and hosted by Google. Your credentials are not provided to NetApp.
   - **Details**: Enter a name for the virtual machine instance, specify tags, select a project, and then select the service account that has the required permissions (refer to the section above for details).
   - **Location**: Specify a region, zone, VPC, and subnet for the instance.
   - **Network**: Choose whether to enable a public IP address and optionally specify a proxy configuration.
   - **Network tags**: Add a network tag to the Connector instance if using a transparent proxy. Network tags must start with a lowercase letter and can contain lowercase letters, numbers, and hyphens. Tags must end with a lowercase letter or number. For example, you might use the tag "connector-proxy".

   - **Firewall Policy**: Choose whether to create a new firewall policy or whether to select an existing firewall policy that allows the required inbound and outbound rules.

     Firewall rules in Google Cloud

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

5. Select **Add**.

   The instance is ready in approximately 7 minutes; stay on the page until the process completes.

Result

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

If you have Google Cloud Storage buckets in the same Google Cloud account where you created the Connector, you'll see a Google Cloud Storage working environment appear on the BlueXP canvas automatically. Learn how to manage Google Cloud Storage from BlueXP

gcloud

Before you begin

You should have the following:

- The required Google Cloud permissions to create the Connector and a service account for the Connector VM.
- A VPC and subnet that meets networking requirements.
- An understanding of VM instance requirements.
   - **CPU**: 8 cores or 8 vCPUs
   - **RAM**: 32 GB
   - **Machine type**: We recommend n2-standard-8.

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

Steps

1. Log in to the gcloud SDK using your preferred method.

   In our examples, we'll use a local shell with the gcloud SDK installed, but you could use the native Google Cloud Shell in the Google Cloud console.

   For more information about the Google Cloud SDK, visit the Google Cloud SDK documentation page.

2. Verify that you are logged in as a user who has the required permissions that are defined in the section above:

   ```
   gcloud auth list
   ```

   The output should show the following where the * user account is the desired user account to be logged in as:

```
Credentialed Accounts
ACTIVE  ACCOUNT
     some_user_account@domain.com
*    desired_user_account@domain.com
To set the active account, run:
 $ gcloud config set account `ACCOUNT`
Updates are available for some Cloud SDK components. To install
them,
please run:
$ gcloud components update
```

3. Run the `gcloud compute instances create` command:

```
gcloud compute instances create <instance-name>
  --machine-type=n2-standard-8
  --image-project=netapp-cloudmanager
  --image-family=cloudmanager
  --scopes=cloud-platform
  --project=<project>
  --service-account=<service-account>
  --zone=<zone>
  --no-address
  --tags <network-tag>
  --network <network-path>
  --subnet <subnet-path>
  --boot-disk-kms-key <kms-key-path>
```

instance-name

The desired instance name for the VM instance.

project

(Optional) The project where you want to deploy the VM.

service-account

The service account specified in the output from step 2.

zone

The zone where you want to deploy the VM

no-address

(Optional) No external IP address is used (you need a cloud NAT or proxy to route traffic to the public internet)

network-tag

(Optional) Add network tagging to link a firewall rule using tags to the Connector instance

network-path

(Optional) Add the name of the network to deploy the Connector into (for a Shared VPC, you need the full path)

subnet-path

(Optional) Add the name of the subnet to deploy the Connector into (for a Shared VPC, you need the full path)

kms-key-path

(Optional) Add a KMS key to encrypt the Connector's disks (IAM permissions also need to be applied)

For more information about these flags, visit the Google Cloud compute SDK documentation.

Running the command deploys the Connector using the NetApp golden image. The Connector instance and software should be running in approximately five minutes.

4. Open a web browser from a host that has a connection to the Connector instance and enter the following URL:

   https://*ipaddress*

5. After you log in, set up the Connector:
   a. Specify the BlueXP organization to associate with the Connector.

      Learn about BlueXP identity and access management.

   b. Enter a name for the system.

Result

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

Open a web browser and go to the BlueXP console to start using the Connector with BlueXP.

Manually install the Connector in Google Cloud

You can manually install q Connector on a Linux host running in Google Cloud. To manually install the Connector on your own Linux host, you need to review host requirements, set up your networking, prepare Google Cloud permissions, enable APIs, install the Connector, and then provide the permissions that you prepared.

Before you begin

- You should have an understanding of Connectors.
- You should review Connector limitations.

Step 1: Review host requirements

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

ⓘ The Connector reserves the UID and GID range of 19000 to 19200. This range is fixed and cannot be modified. If any third-party software on your host is using UIDs or GIDs within this range, the Connector installation will fail. NetApp recommends using a host that is free of third-party software to avoid conflicts.

Dedicated host

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

Host can be of any architecture that meets the following size requirements:

- CPU: 8 cores or 8 vCPUs
- RAM: 32 GB

Hypervisor

A bare metal or hosted hypervisor that is certified to run a supported operating system is required.

Operating system and container requirements

BlueXP supports the Connector with the following operating systems when using BlueXP in standard mode or restricted mode. A container orchestration tool is required before you install the Connector.

Operating system	Supported OS versions	Supported Connector versions	Required container tool	SELinux
Red Hat Enterprise Linux	9.1 to 9.4 8.6 to 8.10 7.9	3.9.40 or later with BlueXP in standard mode or restricted mode	Podman version 4.6.1 or 4.9.4 View Podman configuration requirements.	Supported in enforcing mode or permissive mode [1]
Ubuntu	24.04 LTS	3.9.45 or later with BlueXP in standard mode or restricted mode	Docker Engine 23.06 to 28.0.0.	Not supported
	22.04 LTS	3.9.29 or later	Docker Engine 23.0.6 to 28.0.0.	Not supported

Notes:

1. Management of Cloud Volumes ONTAP systems is not supported by Connectors that have SELinux enabled on the operating system.
2. The Connector is supported on English-language versions of these operating systems.
3. For RHEL, 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.

Google Cloud machine type

An instance type that meets the CPU and RAM requirements above. We recommend n2-standard-8.

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

BlueXP uses `/opt` to install the `/opt/application/netapp` directory and its contents.

Disk space in /var

20 GiB of space must be available

BlueXP requires this space in `/var` because Docker or Podman are architected to create the containers within this directory. Specifically, they will create containers in the `/var/lib/containers/storage` directory. External mounts or symlinks do not work for this space.

Step 2: Install Podman or Docker Engine

Depending on your operating system, either Podman or Docker Engine is required before you install the Connector.

- Podman is required for Red Hat Enterprise Linux 8 and 9.

  View the Podman versions that BlueXP supports.

- Docker Engine is required for Ubuntu.

  View the Docker Engine versions that BlueXP supports.

Example 3. Steps

Podman

Follow these steps to install Podman and configure it to meet the following requirements:

- Enable and start the podman.socket service
- Install python3
- Install the podman-compose package version 1.0.6
- Add podman-compose to the PATH environment variable

When using Podman, adjust the aardvark-dns service port (default: 53) after installing the Connector to avoid conflicts with the DNS port on the host. Follow the instructions to configure the port.

Steps

1. Remove the podman-docker package if it’s installed on the host.

   ```
   dnf remove podman-docker
   rm /var/run/docker.sock
   ```

2. Install Podman.

   Podman is available from official Red Hat Enterprise Linux repositories.

   For Red Hat Enterprise Linux 9:

   ```
   sudo dnf install podman-2:<version>
   ```

   Where <version> is the supported version of Podman that you’re installing. View the Podman versions that BlueXP supports.

   For Red Hat Enterprise Linux 8:

   ```
   sudo dnf install podman-3:<version>
   ```

   Where <version> is the supported version of Podman that you’re installing. View the Podman versions that BlueXP supports.

3. Enable and start the podman.socket service.

   ```
   sudo systemctl enable --now podman.socket
   ```

4. Install python3.

```
sudo dnf install python3
```

5. Install the EPEL repository package if it’s not already available on your system.

   This step is required because podman-compose is available from the Extra Packages for Enterprise Linux (EPEL) repository.

   For Red Hat Enterprise Linux 9:

   ```
   sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
   ```

   For Red Hat Enterprise Linux 8:

   ```
   sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
   ```

6. Install podman-compose package 1.0.6.

   ```
   sudo dnf install podman-compose-1.0.6
   ```

   ⓘ Using the `dnf install` command meets the requirement for adding podman-compose to the PATH environment variable. The installation command adds podman-compose to /usr/bin, which is already included in the `secure_path` option on the host.

Docker Engine

Follow the documentation from Docker to install Docker Engine.

Steps

1. View installation instructions from Docker

   Be sure to follow the steps to install a specific version of Docker Engine. Installing the latest version will install a version of Docker that BlueXP doesn’t support.

2. Verify that Docker is enabled and running.

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

Step 3: Set up 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.

Connections to target networks

A Connector requires a network connection to the location where you're planning to create and manage working environments. For example, the network where you plan to create Cloud Volumes ONTAP systems or a storage system in your on-premises environment.

Outbound internet access

The network location where you deploy the Connector must have an outbound internet connection to contact specific endpoints.

Endpoints contacted from computers when using the BlueXP web-based console

Computers that access the BlueXP console from a web browser must have the ability to contact several endpoints. You'll need to use the BlueXP console to set up the Connector and for day-to-day use of BlueXP.

Prepare networking for 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://mysupport.netapp.com
- https://signin.b2c.netapp.com (this endpoint is the CNAME URL for https://mysupport.netapp.com)
- https://cloudmanager.cloud.netapp.com/tenancy
- https://stream.cloudmanager.cloud.netapp.com
- https://production-artifacts.cloudmanager.cloud.netapp.com
- To obtain images, the installer needs access to one of these two sets of endpoints:
  - Option 1 (recommended):
    - https://bluexpinfraprod.eastus2.data.azurecr.io
    - https://bluexpinfraprod.azurecr.io
  - Option 2:
    - https://*.blob.core.windows.net
    - https://cloudmanagerinfraprod.azurecr.io

  The endpoints listed in option 1 are recommended because they are more secure. We recommend that you set up your firewall to allow the endpoints listed in option 1, while disallowing the endpoints listed in option 2. Note the following about these endpoints:

  - The endpoints listed in option 1 are supported starting with the 3.9.47 release of the Connector. There is no backwards compatibility with previous releases of the Connector.
  - The Connector contacts the endpoints listed in option 2 first. If those endpoints aren't accessible, the Connector automatically contacts the endpoints listed in option 1.
  - The endpoints in option 1 are not supported if you use the Connector with BlueXP backup and recovery or BlueXP ransomware protection. In this case, you can disallow the endpoints listed in option 1, while allowing the endpoints listed in option 2.

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.

Note that the endpoints listed below are all CNAME entries.

Endpoints	Purpose
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.
https://support.netapp.com https://mysupport.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://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	To provide SaaS features and services within BlueXP.
Choose between two sets of endpoints: • Option 1 (recommended) [1] https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Option 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	To obtain images for Connector upgrades.

[1] The endpoints listed in option 1 are recommended because they are more secure. We recommend that you set up your firewall to allow the endpoints listed in option 1, while disallowing the endpoints listed in option 2. Note the following about these endpoints:

- The endpoints listed in option 1 are supported starting with the 3.9.47 release of the Connector. There is no backwards compatibility with previous releases of the Connector.
- The Connector contacts the endpoints listed in option 2 first. If those endpoints aren’t accessible, the Connector automatically contacts the endpoints listed in option 1.
- The endpoints in option 1 are not supported if you use the Connector with BlueXP backup and recovery or BlueXP ransomware protection. In this case, you can disallow the endpoints listed in option 1, while

allowing the endpoints listed in option 2.

Proxy server

NetApp supports both explicit and transparent proxy configurations. If you are using a transparent proxy, you only need to provide the certificate for the proxy server. If you are using an explicit proxy, you'll also need the IP address and credentials.

- 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.

Enable NTP

If you're planning to use BlueXP classification to scan your corporate data sources, you should enable a Network Time Protocol (NTP) service on both the BlueXP Connector system and the BlueXP classification system so that the time is synchronized between the systems. Learn more about BlueXP classification

Step 4: Set up permissions for the Connector

A Google Cloud service account is required to provide the Connector with the permissions that BlueXP needs to manage resources in Google Cloud. When you create the Connector, you'll need to associate this service account with the Connector VM.

It's your responsibility to update the custom role as new permissions are added in subsequent releases. If new permissions are required, they will be listed in the release notes.

Steps

1. Create a custom role in Google Cloud:
   a. Create a YAML file that includes the contents of the service account permissions for the Connector.
   b. From Google Cloud, activate cloud shell.
   c. Upload the YAML file that includes the required permissions.
   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 and assign the role to the service account:
   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

3. If you plan to deploy Cloud Volumes ONTAP systems in different projects than the project where the Connector resides, then you'll need to provide the Connector's service account with access to those projects.

   For example, let's say the Connector is in project 1 and you want to create Cloud Volumes ONTAP systems in project 2. You'll need to grant access to the service account in project 2.

   a. From the IAM & Admin service, select the Google Cloud project where you want to create Cloud Volumes ONTAP systems.
   b. On the **IAM** page, select **Grant Access** and provide the required details.
      - Enter the email of the Connector's service account.
      - Select the Connector's custom role.
      - Select **Save**.

   For more details, refer to Google Cloud documentation

Result

The service account for the Connector VM is set up.

Step 5: Set up shared VPC permissions

If you are using a shared VPC to deploy resources into a service project, then you'll need to prepare your permissions.

This table is for reference and your environment should reflect the permissions table when IAM configuration is complete.

View shared VPC permissions

Identity	Creator	Hosted in	Service project permissions	Host project permissions	Purpose
Google account to deploy the Connector	Custom	Service Project	Connector deployment policy	compute.network User	Deploying the Connector in the service project
Connector service account	Custom	Service project	Connector service account policy	compute.network User deploymentmanager.editor	Deploying and maintaining Cloud Volumes ONTAP and services in the service project
Cloud Volumes ONTAP service account	Custom	Service project	storage.admin member: BlueXP service account as serviceAccount.user	N/A	(Optional) For data tiering and BlueXP backup and recovery
Google APIs service agent	Google Cloud	Service project	(Default) Editor	compute.network User	Interacts with Google Cloud APIs on behalf of deployment. Allows BlueXP to use the shared network.
Google Compute Engine default service account	Google Cloud	Service project	(Default) Editor	compute.network User	Deploys Google Cloud instances and compute infrastructure on behalf of deployment. Allows BlueXP to use the shared network.

Notes:

1. deploymentmanager.editor is only required at the host project if you are not passing firewall rules to the deployment and are choosing to let BlueXP create them for you. BlueXP will create a deployment in the host project which contains the VPC0 firewall rule if no rule is specified.
2. firewall.create and firewall.delete are only required if you are not passing firewall rules to the deployment and are choosing to let BlueXP create them for you. These permissions reside in the BlueXP account .yaml file. If you are deploying an HA pair using a shared VPC, these permissions will be used to create the firewall rules for VPC1, 2 and 3. For all other deployments, these permissions will also be used to create rules for VPC0.
3. For data tiering, the tiering service account must have the serviceAccount.user role on the service account, not just at the project level. Currently if you assign serviceAccount.user at the project level, the permissions don't show when you query the service account with getIAMPolicy.

Step 6: Enable Google Cloud APIs

Several Google Cloud APIs must be enabled before you can deploy Cloud Volumes ONTAP systems 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))

Google Cloud documentation: Enabling APIs

Step 7: Install the Connector

After the pre-requisites are complete, you can manually install the software on your own Linux host.

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.

> ⓘ You cannot set a certificate for a transparent proxy server when manually installing the Connector. If you need to set a certificate for a transparent proxy server, you must use the Maintenance Console after installation. Learn more about the Connector Maintenance Console.

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. 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.

2. 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.

3. Assign permissions to run the script.

   ```
   chmod +x BlueXP-Connector-Cloud-<version>
   ```

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

4. Run the installation script.

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

   You’ll need to add proxy information if your network requires a proxy for internet access. You can add either a transparent or explicit proxy. The --proxy and --cacert parameters are optional and you won’t be prompted to add them. If you have a proxy server, you will need to enter the parameters as shown.

   Here is an example configuring an explicit proxy server with a CA-signed certificate:

   ```
    ./BlueXP-Connector-Cloud-v3.9.40--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://user-name:password@address:port
   - http://domain-name%92user-name:password@address:port
   - https://address:port
   - https://user-name:password@address:port
   - https://domain-name%92user-name:password@address:port

     Note the following:

     - The user can be a local user or domain user.
     - For a domain user, you must use the ASCII code for a \ as shown above.
     - BlueXP doesn’t support user names or passwords that include the @ character.
     - If the password includes any of the following special characters, you must escape that special character by prepending it with a backslash: & or !

    For example:

    http://bxpproxyuser:netapp1\!@address:3128

    --cacert specifies a CA-signed certificate to use for HTTPS access between the Connector and the proxy server. This parameter is required for HTTPS proxy servers, intercepting proxy servers, and transparent proxy servers.

  Here is an example configuring a transparent proxy server. When you configure a transparent proxy, you don’t need to define the proxy server. You only add a CA-signed certificate to your Connector host:

```
./BlueXP-Connector-Cloud-v3.9.40 --cacert /tmp/cacert/certificate.cer
```

5. If you used Podman, you’ll need to adjust the aardvark-dns port.
   a. SSH to the BlueXP Connector virtual machine.
   b. Open podman */usr/share/containers/containers.conf* file and modify the chosen port for Aardvark DNS service. For example, change it to 54.

```
vi /usr/share/containers/containers.conf
...
# Port to use for dns forwarding daemon with netavark in rootful
bridge
# mode and dns enabled.
# Using an alternate port might be useful if other DNS services
should
# run on the machine.
#
dns_bind_port = 54
...
Esc:wq
```

   c. Reboot the Connector virtual machine.
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 organization 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**.

If you have Google Cloud Storage buckets in the same Google Cloud account where you created the Connector, you’ll see a Google Cloud Storage working environment appear on the BlueXP canvas automatically. Learn how to manage Google Cloud Storage from BlueXP

Step 8: Provide permissions to BlueXP

You need to provide BlueXP with the Google Cloud permissions that you previously set up. Providing the permissions enables BlueXP to manage your data and storage infrastructure in Google Cloud.

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 Google Cloud 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.

Install and set up a Connector on-premises

You can install a Connector on one of your on-premises machines. To run the Connector on-premises, you need to review host requirements, set up your networking, prepare cloud permissions, install the Connector, set up the Connector, and then provide the permissions that you prepared.

Before you begin

- Review information about Connectors.
- You should review Connector limitations.

Step 1: Review host requirements

Run the Connector software on a host that meets operating system, RAM, and port requirements. Ensure that your host meets these requirements before you install the Connector.

> ⓘ The Connector reserves the UID and GID range of 19000 to 19200. This range is fixed and cannot be modified. If any third-party software on your host is using UIDs or GIDs within this range, the Connector installation will fail. NetApp recommends using a host that is free of third-party software to avoid conflicts.

Dedicated host

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

Host can be of any architecture that meets the following size requirements:

- CPU: 8 cores or 8 vCPUs
- RAM: 32 GB

Hypervisor

A bare metal or hosted hypervisor that is certified to run a supported operating system is required.

Operating system and container requirements

BlueXP supports the Connector with the following operating systems when using BlueXP in standard mode or restricted mode. A container orchestration tool is required before you install the Connector.

Operating system	Supported OS versions	Supported Connector versions	Required container tool	SELinux
Red Hat Enterprise Linux	9.1 to 9.4 8.6 to 8.10 7.9	3.9.40 or later with BlueXP in standard mode or restricted mode	Podman version 4.6.1 or 4.9.4 View Podman configuration requirements.	Supported in enforcing mode or permissive mode [1]
Ubuntu	24.04 LTS	3.9.45 or later with BlueXP in standard mode or restricted mode	Docker Engine 23.06 to 28.0.0.	Not supported
	22.04 LTS	3.9.29 or later	Docker Engine 23.0.6 to 28.0.0.	Not supported

Notes:

1. Management of Cloud Volumes ONTAP systems is not supported by Connectors that have SELinux enabled on the operating system.
2. The Connector is supported on English-language versions of these operating systems.
3. For RHEL, 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.

Disk space in /opt

100 GiB of space must be available

BlueXP uses `/opt` to install the `/opt/application/netapp` directory and its contents.

Disk space in /var

20 GiB of space must be available

BlueXP requires this space in `/var` because Docker or Podman are architected to create the containers within this directory. Specifically, they will create containers in the `/var/lib/containers/storage` directory. External mounts or symlinks do not work for this space.

Step 2: Install Podman or Docker Engine

Depending on your operating system, either Podman or Docker Engine is required before you install the Connector.

- Podman is required for Red Hat Enterprise Linux 8 and 9.

  View the Podman versions that BlueXP supports.

- Docker Engine is required for Ubuntu.

  View the Docker Engine versions that BlueXP supports.

Example 4. Steps

Podman

Follow these steps to install Podman and configure it to meet the following requirements:

- Enable and start the podman.socket service
- Install python3
- Install the podman-compose package version 1.0.6
- Add podman-compose to the PATH environment variable

ⓘ When using Podman, adjust the aardvark-dns service port (default: 53) after installing the Connector to avoid conflicts with the DNS port on the host. Follow the instructions to configure the port.

Steps

1. Remove the podman-docker package if it's installed on the host.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Install Podman.

   Podman is available from official Red Hat Enterprise Linux repositories.

   For Red Hat Enterprise Linux 9:

```
sudo dnf install podman-2:<version>
```

   Where <version> is the supported version of Podman that you're installing. View the Podman versions that BlueXP supports.

   For Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<version>
```

   Where <version> is the supported version of Podman that you're installing. View the Podman versions that BlueXP supports.

3. Enable and start the podman.socket service.

```
sudo systemctl enable --now podman.socket
```

4. Install python3.

```
sudo dnf install python3
```

5. Install the EPEL repository package if it’s not already available on your system.

   This step is required because podman-compose is available from the Extra Packages for Enterprise Linux (EPEL) repository.

   For Red Hat Enterprise Linux 9:

   ```
   sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
   ```

   For Red Hat Enterprise Linux 8:

   ```
   sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
   ```

6. Install podman-compose package 1.0.6.

   ```
   sudo dnf install podman-compose-1.0.6
   ```

   ⓘ Using the `dnf install` command meets the requirement for adding podman-compose to the PATH environment variable. The installation command adds podman-compose to /usr/bin, which is already included in the `secure_path` option on the host.

Docker Engine

Follow the documentation from Docker to install Docker Engine.

Steps

1. View installation instructions from Docker

   Be sure to follow the steps to install a specific version of Docker Engine. Installing the latest version will install a version of Docker that BlueXP doesn’t support.

2. Verify that Docker is enabled and running.

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

Step 3: Set up networking

Set up networking to ensure the Connector can manage resources, with connections to target networks and outbound internet access.

Connections to target networks

A Connector requires a network connection to the location where you're planning to create and manage working environments. For example, the network where you plan to create Cloud Volumes ONTAP systems or a storage system in your on-premises environment.

Outbound internet access

The network location where you deploy the Connector must have an outbound internet connection to contact specific endpoints.

Endpoints contacted from computers when using the BlueXP web-based console

Computers that access the BlueXP console from a web browser must have the ability to contact several endpoints. You'll need to use the BlueXP console to set up the Connector and for day-to-day use of BlueXP.

Prepare networking for 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://mysupport.netapp.com
- https://signin.b2c.netapp.com (this endpoint is the CNAME URL for https://mysupport.netapp.com)
- https://cloudmanager.cloud.netapp.com/tenancy
- https://stream.cloudmanager.cloud.netapp.com
- https://production-artifacts.cloudmanager.cloud.netapp.com
- To obtain images, the installer needs access to one of these two sets of endpoints:
  - Option 1 (recommended):
    - https://bluexpinfraprod.eastus2.data.azurecr.io
    - https://bluexpinfraprod.azurecr.io
  - Option 2:
    - https://*.blob.core.windows.net
    - https://cloudmanagerinfraprod.azurecr.io

  The endpoints listed in option 1 are recommended because they are more secure. We recommend that you set up your firewall to allow the endpoints listed in option 1, while disallowing the endpoints listed in option 2. Note the following about these endpoints:

  - The endpoints listed in option 1 are supported starting with the 3.9.47 release of the Connector. There is no backwards compatibility with previous releases of the Connector.
  - The Connector contacts the endpoints listed in option 2 first. If those endpoints aren't accessible, the Connector automatically contacts the endpoints listed in option 1.
  - The endpoints in option 1 are not supported if you use the Connector with BlueXP backup and recovery or BlueXP ransomware protection. In this case, you can disallow the endpoints listed in option 1, while allowing the endpoints listed in option 2.

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.

Note that the endpoints listed below are all CNAME entries.

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.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.
https://support.netapp.com https://mysupport.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://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	To provide SaaS features and services within BlueXP.

Endpoints	Purpose
Choose between two sets of endpoints: • Option 1 (recommended) [1] https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Option 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	To obtain images for Connector upgrades.

[1] The endpoints listed in option 1 are recommended because they are more secure. We recommend that you set up your firewall to allow the endpoints listed in option 1, while disallowing the endpoints listed in option 2. Note the following about these endpoints:

- The endpoints listed in option 1 are supported starting with the 3.9.47 release of the Connector. There is no backwards compatibility with previous releases of the Connector.
- The Connector contacts the endpoints listed in option 2 first. If those endpoints aren't accessible, the Connector automatically contacts the endpoints listed in option 1.
- The endpoints in option 1 are not supported if you use the Connector with BlueXP backup and recovery or BlueXP ransomware protection. In this case, you can disallow the endpoints listed in option 1, while allowing the endpoints listed in option 2.

Proxy server

NetApp supports both explicit and transparent proxy configurations. If you are using a transparent proxy, you only need to provide the certificate for the proxy server. If you are using an explicit proxy, you'll also need the IP address and credentials.

- 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.

Enable NTP

If you're planning to use BlueXP classification to scan your corporate data sources, you should enable a Network Time Protocol (NTP) service on both the BlueXP Connector system and the BlueXP classification system so that the time is synchronized between the systems. Learn more about BlueXP classification

Step 4: Set up cloud permissions

If you want to use BlueXP services in AWS or Azure with an on-premises Connector, then you need to set up permissions in your cloud provider so that you can add the credentials to the Connector after you install it.

> Why not Google Cloud? When the Connector is installed on your premises, it can't manage your resources in Google Cloud. You must install the Connector in Google Cloud to manage any resources that reside there.

AWS

When the Connector is installed on-premises, you need to provide BlueXP with AWS permissions by adding access keys for an IAM user who has the required permissions.

You must use this authentication method if the Connector is installed on-premises. You can't use an IAM role.

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

You should now have access keys for an IAM user who has the required permissions. After you install the Connector, associate these credentials with the Connector from BlueXP.

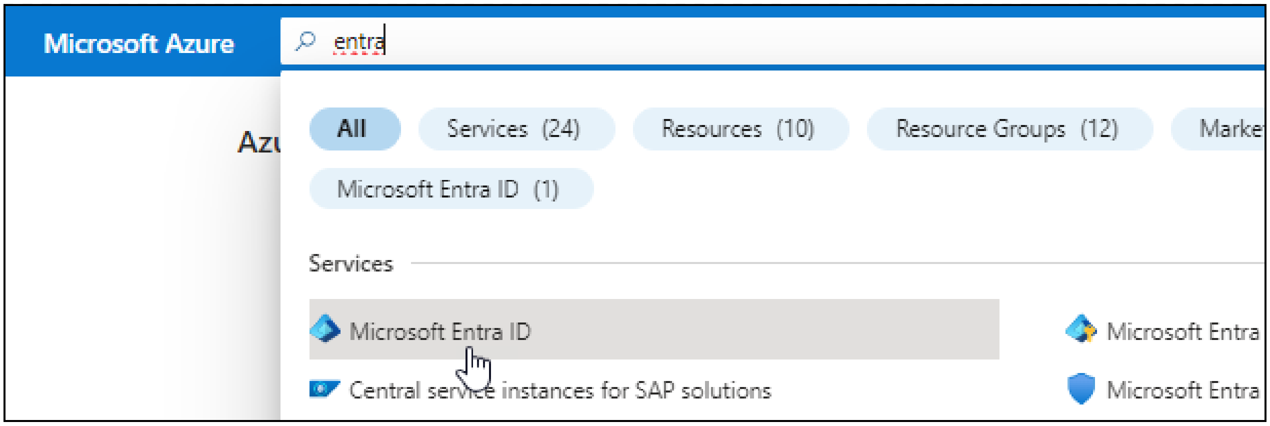
Azure

When the Connector is installed on-premises, you need to provide BlueXP with Azure permissions by setting up a service principal in Microsoft Entra ID and obtaining the Azure credentials that BlueXP needs.

Create a Microsoft Entra 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 **Microsoft Entra ID** 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

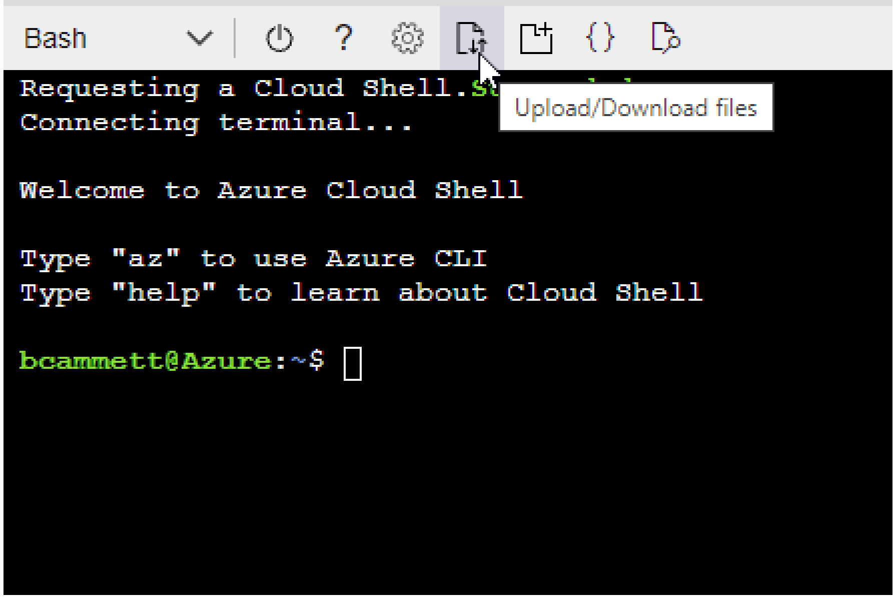
```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
"/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
"/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

   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.



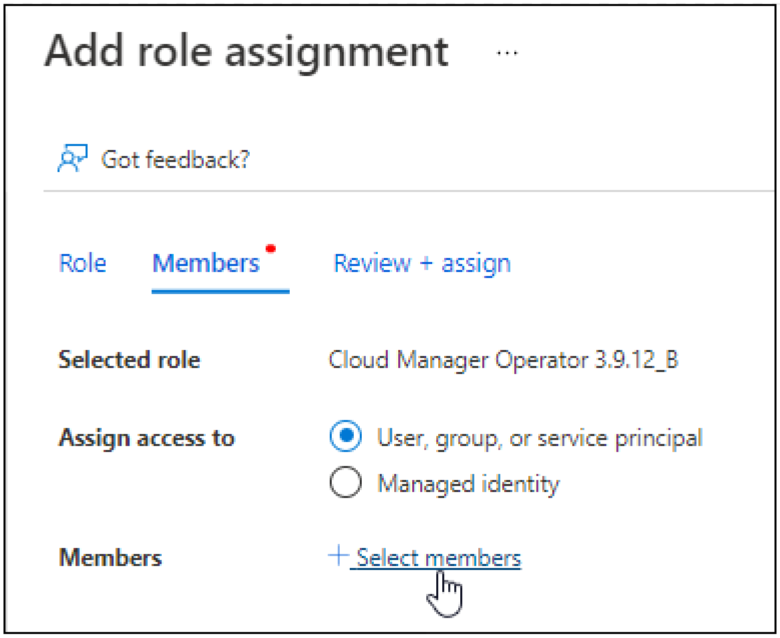
```
Requesting a Cloud Shell.Su
Connecting terminal...

Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

bcammett@Azure:~$
```

- 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**.



Add role assignment ...

Got feedback?

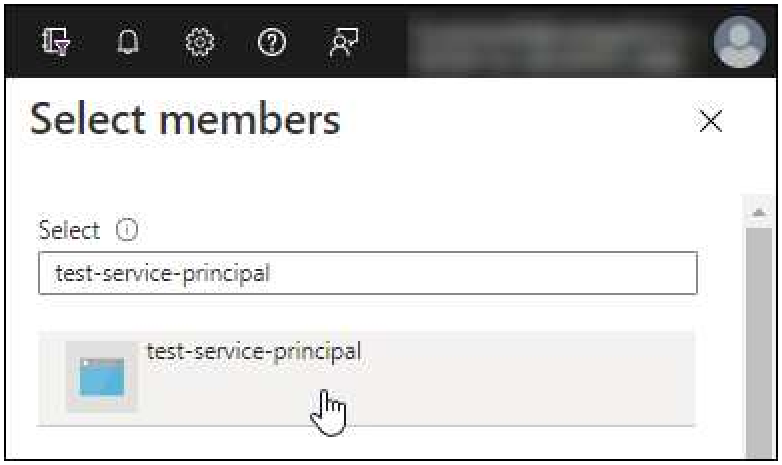
Selected role Cloud Manager Operator 3.9.12_B

Assign access to ● User, group, or service principal ○ Managed identity

Members + Select members

- Search for the name of the application.

  Here's an example:

  Select members

  Select: test-service-principal

  test-service-principal

- Select the application and select **Select**.
- Select **Next**.

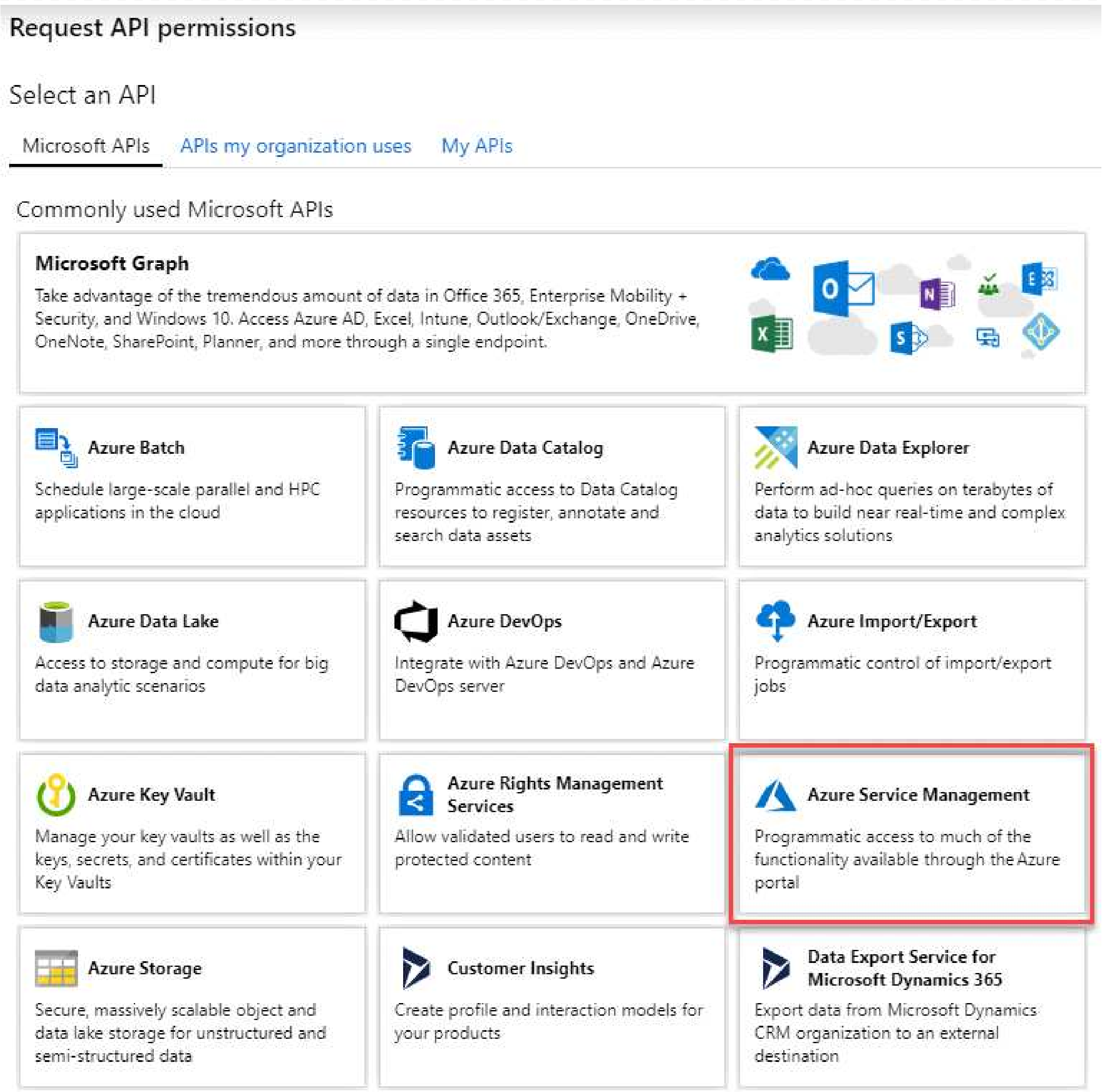
f. Select **Review + assign**.

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



Request API permissions

Select an API

Microsoft APIs | APIs my organization uses | My APIs

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Batch
Schedule large-scale parallel and HPC applications in the cloud

Azure Data Catalog
Programmatic access to Data Catalog resources to register, annotate and search data assets

Azure Data Explorer
Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

Azure Data Lake
Access to storage and compute for big data analytic scenarios

Azure DevOps
Integrate with Azure DevOps and Azure DevOps server

Azure Import/Export
Programmatic control of import/export jobs

Azure Key Vault
Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Rights Management Services
Allow validated users to read and write protected content

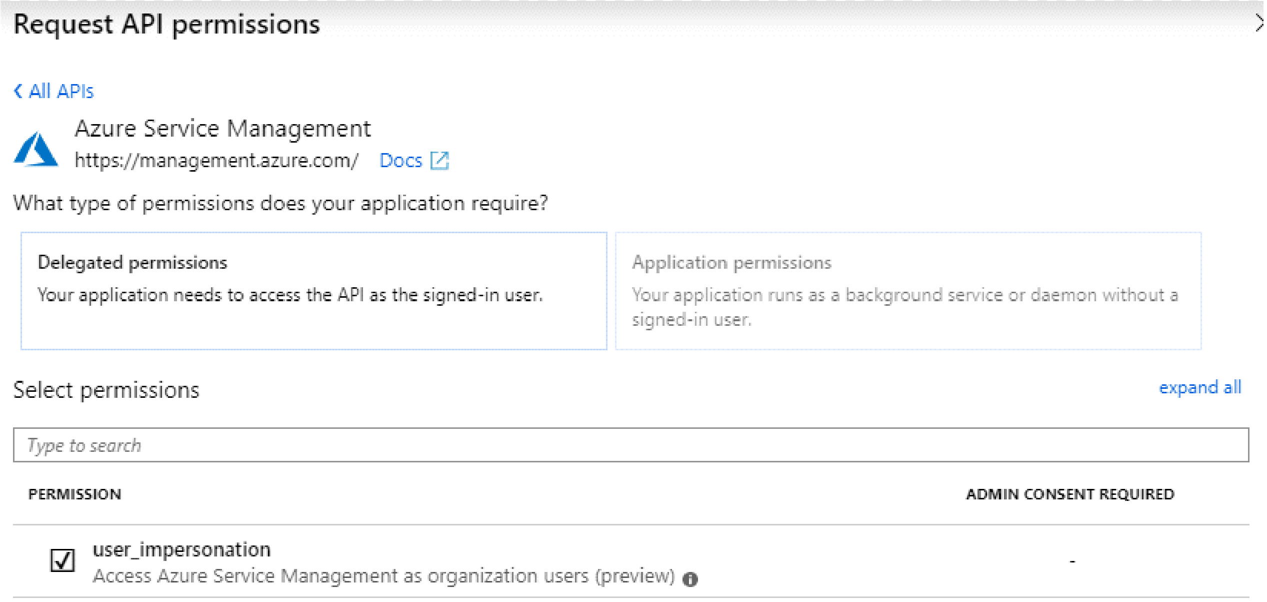
Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

Azure Storage
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Customer Insights
Create profile and interaction models for your products

Data Export Service for Microsoft Dynamics 365
Export data from Microsoft Dynamics CRM organization to an external destination

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



Request API permissions

‹ All APIs

Azure Service Management

https://management.azure.com/ Docs

What type of permissions does your application require?

Delegated permissions
Your application needs to access the API as the signed-in user.

Application permissions
Your application runs as a background service or daemon without a signed-in user.

Select permissions

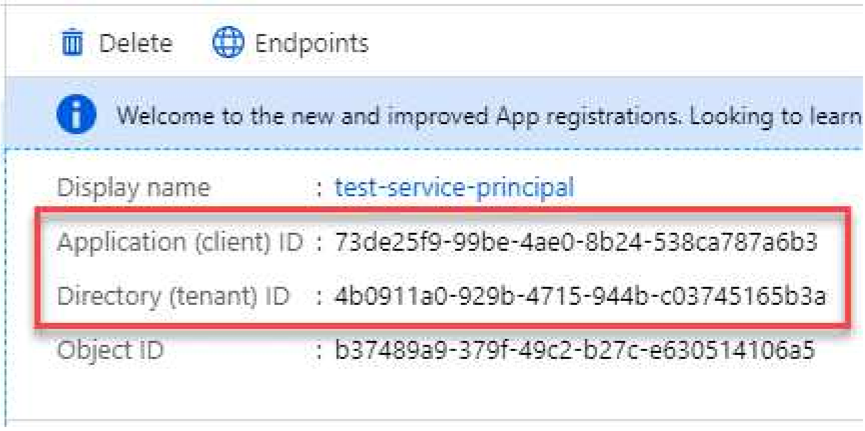
expand all

Type to search

PERMISSION	ADMIN CONSENT REQUIRED
☑ user_impersonation Access Azure Service Management as organization users (preview)	-

Get the application ID and directory ID for the application

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



Welcome to the new and improved App registrations. Looking to learn

Display name : test-service-principal

Application (client) ID : 73de25f9-99be-4ae0-8b24-538ca787a6b3

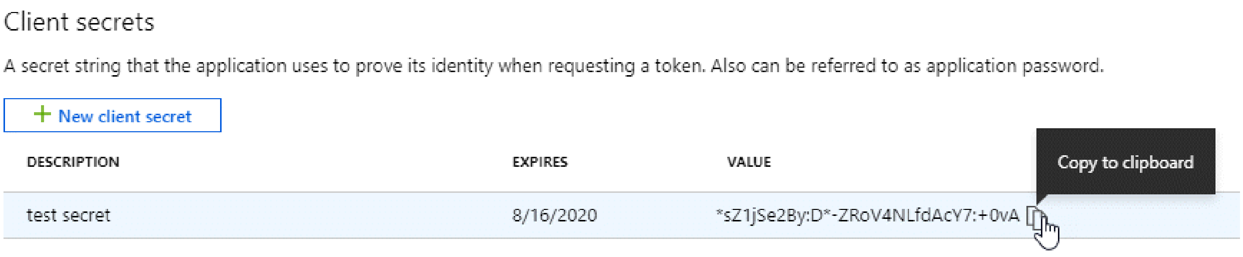
Directory (tenant) ID : 4b0911a0-929b-4715-944b-c03745165b3a

Object ID : b37489a9-379f-49c2-b27c-e630514106a5

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 **Microsoft Entra ID** 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.

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

You now have a client secret that BlueXP can use it to authenticate with Microsoft Entra ID.

Step 5: Install the Connector

Download and install the Connector software on an existing Linux host on-premises.

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.

> ⓘ You cannot set a certificate for a transparent proxy server when manually installing the Connector. If you need to set a certificate for a transparent proxy server, you must use the Maintenance Console after installation. Learn more about the Connector Maintenance Console.

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. 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.

2. 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.

3. Assign permissions to run the script.

```
chmod +x BlueXP-Connector-Cloud-<version>
```

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

4. Run the installation script.

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

   You’ll need to add proxy information if your network requires a proxy for internet access. You can add either a transparent or explicit proxy. The --proxy and --cacert parameters are optional and you won’t be prompted to add them. If you have a proxy server, you will need to enter the parameters as shown.

   Here is an example configuring an explicit proxy server with a CA-signed certificate:

   ```
    ./BlueXP-Connector-Cloud-v3.9.40--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://user-name:password@address:port
   - http://domain-name%92user-name:password@address:port
   - https://address:port
   - https://user-name:password@address:port
   - https://domain-name%92user-name:password@address:port

     Note the following:

     - The user can be a local user or domain user.
     - For a domain user, you must use the ASCII code for a \ as shown above.
     - BlueXP doesn’t support user names or passwords that include the @ character.
     - If the password includes any of the following special characters, you must escape that special character by prepending it with a backslash: & or !

       For example:

       http://bxpproxyuser:netapp1\!@address:3128

       --cacert specifies a CA-signed certificate to use for HTTPS access between the Connector and the proxy server. This parameter is required for HTTPS proxy servers, intercepting proxy servers, and transparent proxy servers.

Here is an example configuring a transparent proxy server. When you configure a transparent proxy, you don’t need to define the proxy server. You only add a CA-signed certificate to your Connector host:

```
./BlueXP-Connector-Cloud-v3.9.40 --cacert /tmp/cacert/certificate.cer
```

5. If you used Podman, you’ll need to adjust the aardvark-dns port.
   a. SSH to the BlueXP Connector virtual machine.
   b. Open podman */usr/share/containers/containers.conf* file and modify the chosen port for Aardvark DNS service. For example, change it to 54.

   ```
   vi /usr/share/containers/containers.conf
   ...
   # Port to use for dns forwarding daemon with netavark in rootful
   bridge
   # mode and dns enabled.
   # Using an alternate port might be useful if other DNS services
   should
   # run on the machine.
   #
   dns_bind_port = 54
   ...
   Esc:wq
   ```

   c. Reboot the Connector virtual machine.

Result

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

Step 6: Register the Connector with BlueXP

Log into BlueXP and associate the Connector with your organization. How you log in depends on the mode in which you are using BlueXP. If you are using BlueXP in standard mode, you log in through the SaaS website. If you are using BlueXP in restricted or private mode, you log in locally from the Connector host.

Steps

1. Open a web browser and enter the following URL:

   https://*ipaddress*

   ipaddress can be localhost, a private IP address, or a public IP address, depending on the configuration of the host. For example, if the Connector is in the public cloud without a public IP address, you must enter a private IP address from a host that has a connection to the Connector host.

2. Sign up or log in.
3. After you log in, set up BlueXP:
   a. Specify the BlueXP organization 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.

   Keep restricted mode disabled because these steps use BlueXP in standard mode. (In addition, restricted mode isn’t supported when the Connector is installed on-premises.)

d. Select **Let’s start**.

Step 7: Provide permissions to BlueXP

After you install and set up the Connector, add your cloud credentials so that BlueXP has the required permissions to perform actions in AWS or Azure.

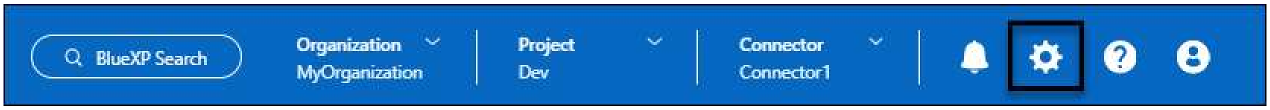
AWS

Before you begin

If you just created these AWS credentials, they may take a few minutes to become available. Wait a few minutes before you add the credentials to BlueXP.

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.

You can now go to the BlueXP console to start using the Connector with BlueXP.

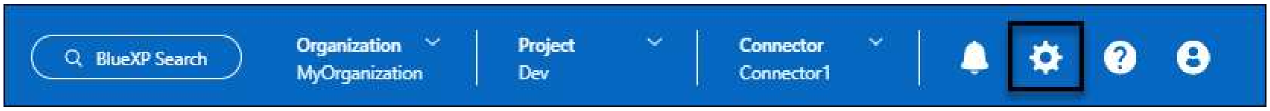
Azure

Before you begin

If you just created these Azure credentials, they may take a few minutes to become available. Wait a few minutes before you add the credentials to BlueXP.

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 Microsoft Entra 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. You can now go to the BlueXP console to start using the Connector with BlueXP.

Subscribe to NetApp Intelligent Services (standard mode)

Subscribe to NetApp Intelligent Services from your cloud provider’s marketplace to pay for data services at an hourly rate (PAYGO) or through an annual contract. If you purchased a license from NetApp (BYOL), you also need to subscribe to the marketplace offering. Your license is always charged first, but you’ll be charged at the hourly rate if you exceed your licensed capacity or if the license’s term expires.

A marketplace subscription enables charging for the following NetApp data services:

- Backup and recovery
- Cloud Volumes ONTAP
- Tiering
- Ransomware protection
- Disaster recovery

Classification is enabled through your subscription, but there is no charge for using classification.

Before you begin

Subscribing to data services involves associating a marketplace subscription with the cloud credentials that are associated with a Connector. If you followed the "Get started with standard mode" workflow, then you should already have a Connector. To learn more, view the Quick start for BlueXP in standard mode.

AWS

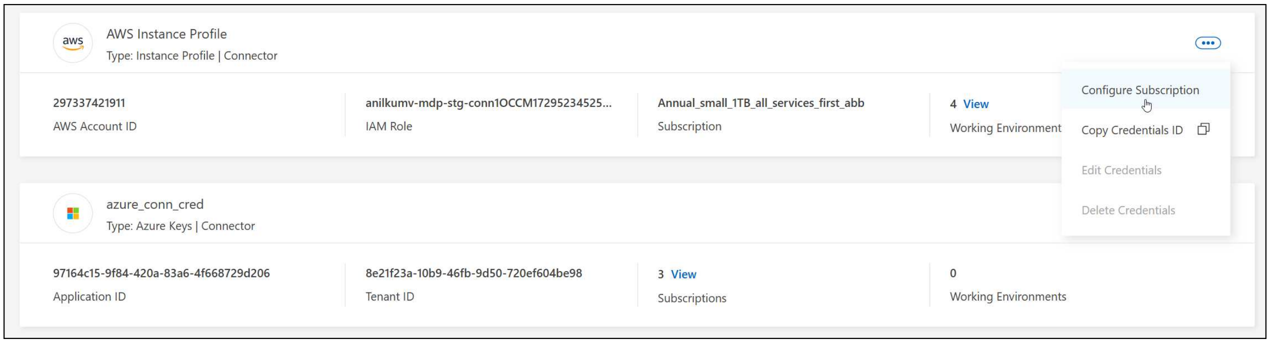
The following video shows the steps to subscribe to NetApp Intelligent Services from the AWS Marketplace:

Subscribe to NetApp Intelligent Services from the AWS Marketplace

Steps

1. In the upper right of the BlueXP console, select the Settings icon, and select **Credentials**.
2. Select the action menu for a set of credentials and then select **Configure Subscription**.

   You must select credentials that are associated with a Connector. You can't associate a marketplace subscription with credentials that are associated with BlueXP.

   AWS Instance Profile
   Type: Instance Profile | Connector

   297337421911 AWS Account ID | anilkumv-mdp-stg-conn1OCCM17295234525... IAM Role | Annual_small_1TB_all_services_first_abb Subscription | 4 View Working Environment

   azure_conn_cred
   Type: Azure Keys | Connector

   97164c15-9f84-420a-83a6-4f668729d206 Application ID | 8e21f23a-10b9-46fb-9d50-720ef604be98 Tenant ID | 3 View Subscriptions | 0 Working Environments

3. To associate the credentials with an existing subscription, select the subscription from the down-down list and select **Configure**.
4. To associate the credentials with a new subscription, select **Add Subscription > Continue** and follow the steps in the AWS Marketplace:

   a. Select **View purchase options**.

   b. Select **Subscribe**.

   c. Select **Set up your account**.

      You'll be redirected to the BlueXP website.

   d. From the **Subscription Assignment** page:

      - Select the BlueXP organizations or accounts that you'd like to associate this subscription with.
      - In the **Replace existing subscription** field, choose whether you'd like to automatically replace the existing subscription for one organization or account with this new subscription.

        BlueXP replaces the existing subscription for all credentials in the organization or account with this new subscription. If a set of credentials wasn't ever associated with a subscription, then this new subscription won't be associated with those credentials.

        For all other organizations or accounts, you'll need to manually associate the subscription by repeating these steps.

      - Select **Save**.

Azure

Steps

1. In the upper right of the console, select the Settings icon, and select **Credentials**.
2. Select the action menu for a set of credentials and then select **Configure Subscription**.

   You must select credentials that are associated with a Connector. You can't associate a marketplace subscription with credentials that are associated with BlueXP.

3. To associate the credentials with an existing subscription, select the subscription from the down-down list and select **Configure**.
4. To associate the credentials with a new subscription, select **Add Subscription > Continue** and follow the steps in the Azure Marketplace:
   a. If prompted, log in to your Azure account.
   b. Select **Subscribe**.
   c. Fill out the form and select **Subscribe**.
   d. After the subscription process is complete, select **Configure account now**.

      You'll be redirected to BlueXP.

   e. From the **Subscription Assignment** page:
      - Select the BlueXP organizations or accounts that you'd like to associate this subscription with.
      - In the **Replace existing subscription** field, choose whether you'd like to automatically replace the existing subscription for one organization or account with this new subscription.

        BlueXP replaces the existing subscription for all credentials in the organization or account with this new subscription. If a set of credentials wasn't ever associated with a subscription, then this new subscription won't be associated with those credentials.

        For all other organizations or accounts, you'll need to manually associate the subscription by repeating these steps.

      - Select **Save**.

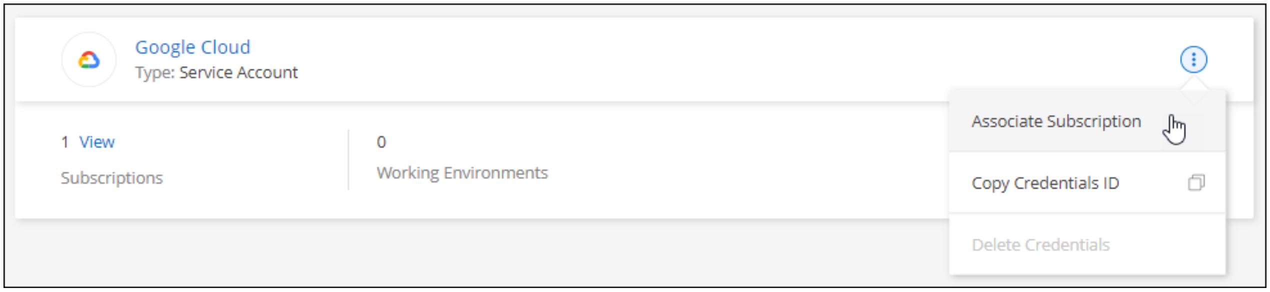
        The following video shows the steps to subscribe from the Azure Marketplace:

        Subscribe to NetApp Intelligent Services from the Azure Marketplace

Google Cloud

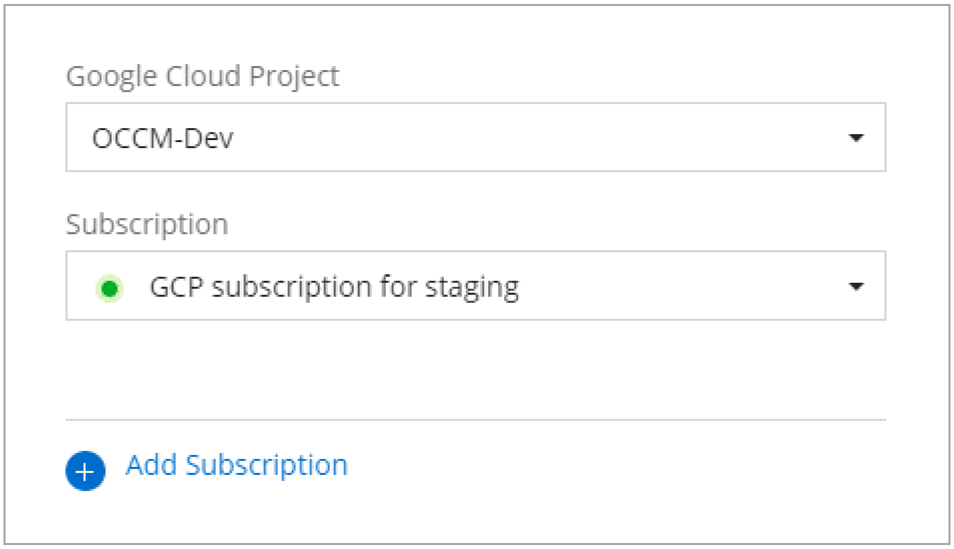
Steps

1. In the upper right of the console, select the Settings icon, and select **Credentials**.
2. Select the action menu for a set of credentials and then select **Configure Subscription**.
   +new screenshot needed (TS)



3. To configure an existing subscription with the selected credentials, select a Google Cloud project and

subscription from the drop-down list, and then select **Configure**.



Google Cloud Project

OCCM-Dev

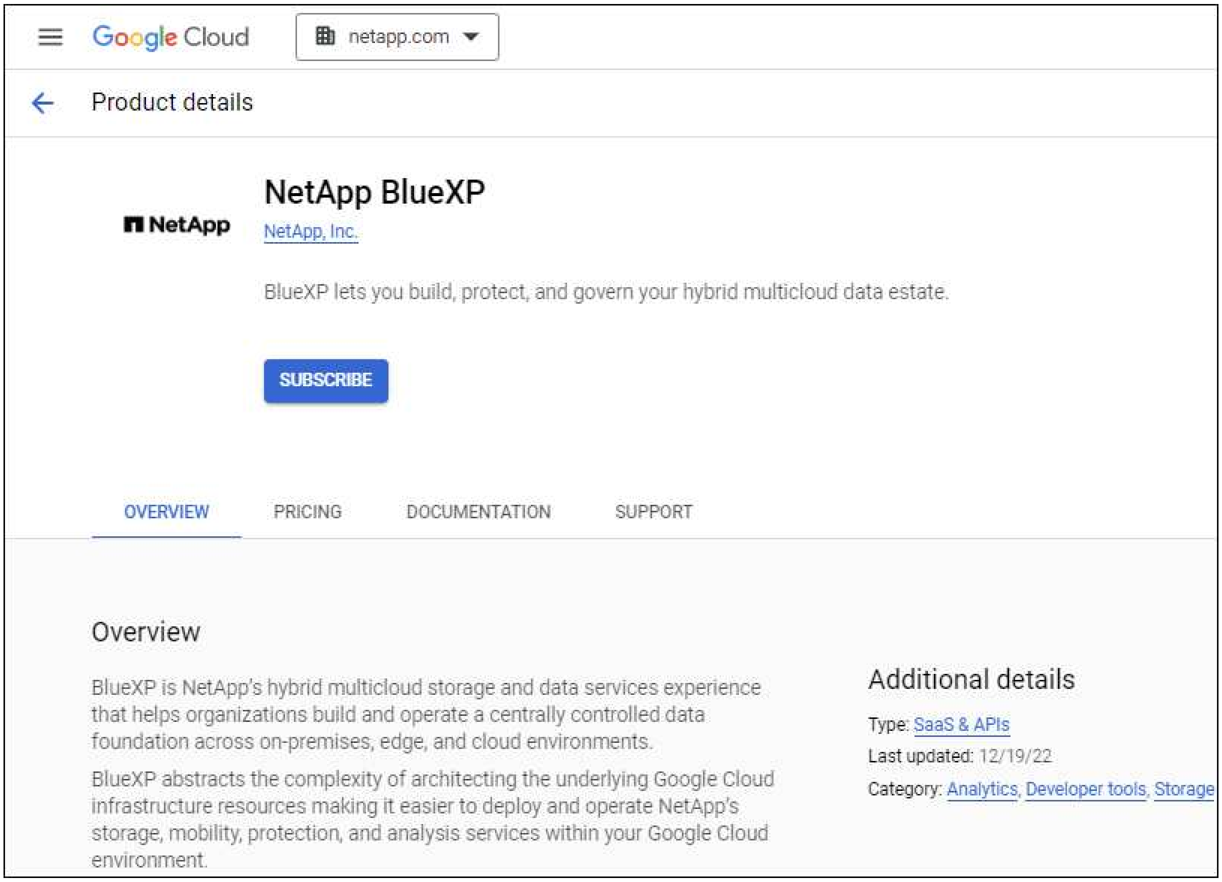
Subscription

● GCP subscription for staging

4. If you don’t already have a subscription, select **Add Subscription > Continue** and follow the steps in the Google Cloud Marketplace.

   > ⓘ Before you complete the following steps, ensure that you have both Billing Admin privileges in your Google Cloud account as well as a BlueXP login.

   a. After you’re redirected to the NetApp Intelligent Services page on the Google Cloud Marketplace, ensure that the correct project is selected at the top navigation menu.



NetApp BlueXP

NetApp, Inc.

BlueXP lets you build, protect, and govern your hybrid multicloud data estate.

Overview

BlueXP is NetApp’s hybrid multicloud storage and data services experience that helps organizations build and operate a centrally controlled data foundation across on-premises, edge, and cloud environments.

BlueXP abstracts the complexity of architecting the underlying Google Cloud infrastructure resources making it easier to deploy and operate NetApp’s storage, mobility, protection, and analysis services within your Google Cloud environment.

Additional details

Type: SaaS & APIs

Last updated: 12/19/22

Category: Analytics, Developer tools, Storage

b. Select **Subscribe**.

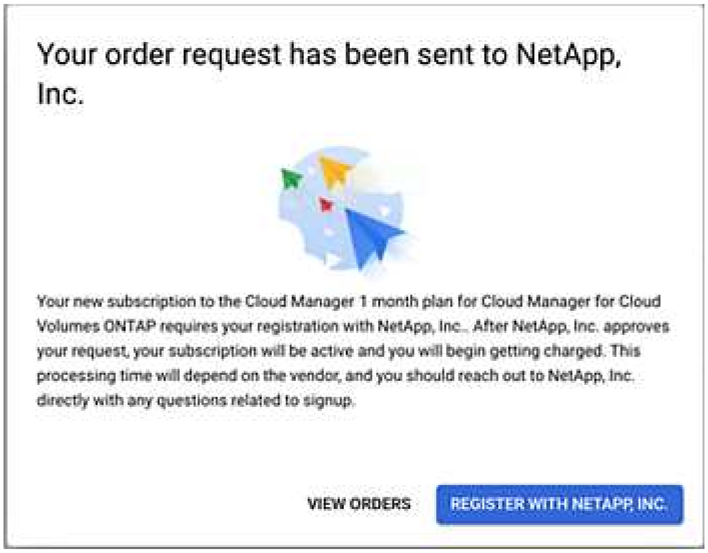
c. Select the appropriate billing account and agree to the terms and conditions.

d. Select **Subscribe**.

This step sends your transfer request to NetApp.

e. On the pop-up dialog box, select **Register with NetApp, Inc.**

This step must be completed to link the Google Cloud subscription with your BlueXP organization or account. The process of linking a subscription isn't complete until you are redirected from this page and then sign in to BlueXP.



Your order request has been sent to NetApp, Inc.

Your new subscription to the Cloud Manager 1 month plan for Cloud Manager for Cloud Volumes ONTAP requires your registration with NetApp, Inc.. After NetApp, Inc. approves your request, your subscription will be active and you will begin getting charged. This processing time will depend on the vendor, and you should reach out to NetApp, Inc. directly with any questions related to signup.

f. Complete the steps on the **Subscription Assignment** page:

> ⓘ If someone from your organization has already subscribed to the NetApp BlueXP subscription from your billing account, then you will be redirected to the Cloud Volumes ONTAP page on the BlueXP website instead. If this is unexpected, contact your NetApp sales team. Google enables only one subscription per Google billing account.

- Select the BlueXP organizations or accounts that you'd like to associate this subscription with.
- In the **Replace existing subscription** field, choose whether you'd like to automatically replace the existing subscription for one organization or account with this new subscription.

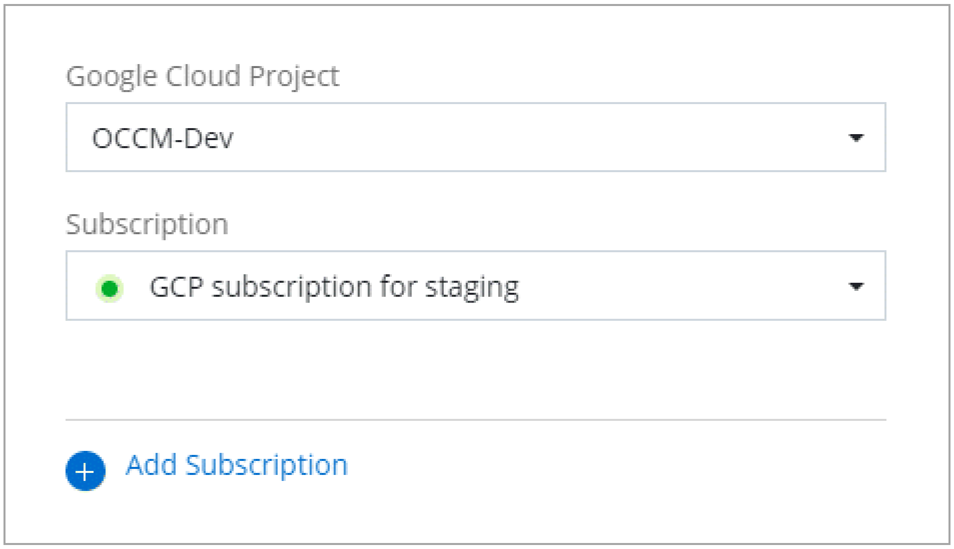
  BlueXP replaces the existing subscription for all credentials in the organization or account with this new subscription. If a set of credentials wasn't ever associated with a subscription, then this new subscription won't be associated with those credentials.

  For all other organizations or accounts, you'll need to manually associate the subscription by repeating these steps.
- Select **Save**.

  The following video shows the steps to subscribe from the Google Cloud Marketplace:

  Subscribe to BlueXP from the Google Cloud Marketplace

g. Once this process is complete, navigate back to the Credentials page in BlueXP and select this new subscription.



Google Cloud Project

OCCM-Dev

Subscription

● GCP subscription for staging

Related information

- Manage BYOL capacity-based licenses for Cloud Volumes ONTAP
- Manage BYOL licenses for data services
- Manage AWS credentials and subscriptions
- Manage Azure credentials and subscriptions
- Manage Google Cloud credentials and subscriptions

What you can do next (standard mode)

Now that you've logged in and set up BlueXP in standard mode, users can create and discover working environments and use BlueXP data services.

> If you installed a Connector in AWS, Microsoft Azure, or Google Cloud, then BlueXP automatically discovers information about the Amazon S3 buckets, Azure Blob storage, or Google Cloud Storage buckets in the location where the Connector is installed. A working environment is automatically added to the BlueXP canvas.

For help, go to the home page for the BlueXP documentation to view the docs for all BlueXP services.

Related information

BlueXP deployment modes

Get started with restricted mode

Getting started workflow (restricted mode)

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

Restricted mode is typically used by state and local governments and regulated companies, including deployments in AWS GovCloud and Azure Government regions. Before getting started, ensure you have an understanding of Connectors and deployment modes.

1

Prepare for deployment

a. Prepare a dedicated Linux host that meets requirements for CPU, RAM, disk space, container orchestration tool, and more.

b. Set up networking that provides access to the target networks, outbound internet access for manual installations, and outbound internet for day-to-day access.

c. Set up permissions in your cloud provider so that you can associate those permissions with the Connector instance after you deploy it.

2

Deploy the Connector

a. Install the Connector from your cloud provider's marketplace or by manually installing the software on your own Linux host.

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

c. Provide BlueXP with the permissions that you previously set up.

3

Subscribe to NetApp Intelligent Services (optional)

Optional: Subscribe to NetApp Intelligent Services from your cloud provider's marketplace to pay for data services at an hourly rate (PAYGO) or through an annual contract. NetApp Intelligent Services include Backup and recovery, Cloud Volumes ONTAP, Tiering, Ransomware protection, and Disaster recovery. Classification is included with your subscription at no additional cost.

Prepare for deployment in restricted mode

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

Step 1: Understand how restricted mode works

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

Step 2: Review installation options

In restricted mode, you can only install the Connector in the cloud. The following installation options are available:

- From the AWS Marketplace
- From the Azure Marketplace
- Manually installing the Connector on your own Linux host that’s running in AWS, Azure, or Google Cloud

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.

When you deploy the Connector from the AWS or Azure Marketplace, the image includes the required OS and software components. You simply need to choose an instance type that meets CPU and RAM requirements.

Dedicated host

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

Host can be of any architecture that meets the following size requirements:

- CPU: 8 cores or 8 vCPUs
- RAM: 32 GB

Hypervisor

A bare metal or hosted hypervisor that is certified to run a supported operating system is required.

Operating system and container requirements

BlueXP supports the Connector with the following operating systems when using BlueXP in standard mode or restricted mode. A container orchestration tool is required before you install the Connector.

Operating system	Supported OS versions	Supported Connector versions	Required container tool	SELinux
Red Hat Enterprise Linux	9.1 to 9.4 8.6 to 8.10 7.9	3.9.40 or later with BlueXP in standard mode or restricted mode	Podman version 4.6.1 or 4.9.4 View Podman configuration requirements.	Supported in enforcing mode or permissive mode [1]
Ubuntu	24.04 LTS	3.9.45 or later with BlueXP in standard mode or restricted mode	Docker Engine 23.06 to 28.0.0.	Not supported
	22.04 LTS	3.9.29 or later	Docker Engine 23.0.6 to 28.0.0.	Not supported

Notes:

1. Management of Cloud Volumes ONTAP systems is not supported by Connectors that have SELinux enabled on the operating system.

2. The Connector is supported on English-language versions of these operating systems.
3. For RHEL, 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.

AWS EC2 instance type

An instance type that meets the CPU and RAM requirements above. We recommend t3.2xlarge.

Azure VM size

An instance type that meets the CPU and RAM requirements above. We recommend Standard_D8s_v3.

Google Cloud machine type

An instance type that meets the CPU and RAM requirements above. We recommend n2-standard-8.

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

BlueXP uses `/opt` to install the `/opt/application/netapp` directory and its contents.

Disk space in /var

20 GiB of space must be available

BlueXP requires this space in `/var` because Docker or Podman are architected to create the containers within this directory. Specifically, they will create containers in the `/var/lib/containers/storage` directory. External mounts or symlinks do not work for this space.

Step 4: Install Podman or Docker Engine

If you're planning to manually install the Connector software, you need to prepare the host by installing Podman or Docker Engine.

Depending on your operating system, either Podman or Docker Engine is required before you install the Connector.

- Podman is required for Red Hat Enterprise Linux 8 and 9.

  View the Podman versions that BlueXP supports.

- Docker Engine is required for Ubuntu.

  View the Docker Engine versions that BlueXP supports.

Example 5. Steps

Podman

Follow these steps to install Podman and configure it to meet the following requirements:

- Enable and start the podman.socket service
- Install python3
- Install the podman-compose package version 1.0.6
- Add podman-compose to the PATH environment variable

> When using Podman, adjust the aardvark-dns service port (default: 53) after installing the Connector to avoid conflicts with the DNS port on the host. Follow the instructions to configure the port.

Steps

1. Remove the podman-docker package if it's installed on the host.

   ```
   dnf remove podman-docker
   rm /var/run/docker.sock
   ```

2. Install Podman.

   Podman is available from official Red Hat Enterprise Linux repositories.

   For Red Hat Enterprise Linux 9:

   ```
   sudo dnf install podman-2:<version>
   ```

   Where <version> is the supported version of Podman that you're installing. View the Podman versions that BlueXP supports.

   For Red Hat Enterprise Linux 8:

   ```
   sudo dnf install podman-3:<version>
   ```

   Where <version> is the supported version of Podman that you're installing. View the Podman versions that BlueXP supports.

3. Enable and start the podman.socket service.

   ```
   sudo systemctl enable --now podman.socket
   ```

4. Install python3.

```
sudo dnf install python3
```

5. Install the EPEL repository package if it’s not already available on your system.

   This step is required because podman-compose is available from the Extra Packages for Enterprise Linux (EPEL) repository.

   For Red Hat Enterprise Linux 9:

   ```
   sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
   ```

   For Red Hat Enterprise Linux 8:

   ```
   sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
   ```

6. Install podman-compose package 1.0.6.

   ```
   sudo dnf install podman-compose-1.0.6
   ```

   > ⓘ Using the `dnf install` command meets the requirement for adding podman-compose to the PATH environment variable. The installation command adds podman-compose to /usr/bin, which is already included in the `secure_path` option on the host.

Docker Engine

Follow the documentation from Docker to install Docker Engine.

Steps

1. View installation instructions from Docker

   Be sure to follow the steps to install a specific version of Docker Engine. Installing the latest version will install a version of Docker that BlueXP doesn’t support.

2. Verify that Docker is enabled and running.

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

Step 5: Prepare networking

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.

Prepare networking for user access to BlueXP console

In restricted mode, the BlueXP user interface is accessible from the Connector. As you use the BlueXP user interface, it contacts a few endpoints to complete data management tasks. These endpoints are contacted from a user's computer when completing specific actions from the BlueXP console.

Endpoints	Purpose
https://api.bluexp.netapp.com	The BlueXP web-based console contacts this endpoint to interact with the BlueXP API for actions related to authorization, licensing, subscriptions, credentials, notifications, and more.
https://signin.b2c.netapp.com	Required to update NetApp Support Site (NSS) credentials or to add new NSS credentials to BlueXP.
https://netapp-cloud-account.auth0.com https://cdn.auth0.com https://services.cloud.netapp.com	Your web browser connects to these endpoints for centralized user authentication through BlueXP.
https://widget.intercom.io	For in-product chat that enables you to talk to NetApp cloud experts.

Endpoints contacted during manual installation

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

- The following endpoints are always contacted no matter where you install the Connector:
  - https://mysupport.netapp.com
  - https://signin.b2c.netapp.com (this endpoint is the CNAME URL for https://mysupport.netapp.com)
  - https://cloudmanager.cloud.netapp.com/tenancy
  - https://stream.cloudmanager.cloud.netapp.com
  - https://production-artifacts.cloudmanager.cloud.netapp.com
- If you install the Connector in an AWS Government region, the installer also needs access to these endpoints:
  - https://*.blob.core.windows.net
  - https://cloudmanagerinfraprod.azurecr.io
- If you install the Connector in an Azure Government region, the installer also needs access to these endpoints:
  - https://*.blob.core.windows.net
  - https://occmclientinfragov.azurecr.us

- If you install the Connector in a commercial region or sovereign region, you can choose between two sets of endpoints:
  - Option 1 (recommended):
    - https://bluexpinfraprod.eastus2.data.azurecr.io
    - https://bluexpinfraprod.azurecr.io
  - Option 2:
    - https://*.blob.core.windows.net
    - https://cloudmanagerinfraprod.azurecr.io

  The endpoints listed in option 1 are recommended because they are more secure. We recommend that you set up your firewall to allow the endpoints listed in option 1, while disallowing the endpoints listed in option 2. Note the following about these endpoints:

  - The endpoints listed in option 1 are supported starting with the 3.9.47 release of the Connector. There is no backwards compatibility with previous releases of the Connector.
  - The Connector contacts the endpoints listed in option 2 first. If those endpoints aren't accessible, the Connector automatically contacts the endpoints listed in option 1.
  - The endpoints in option 1 are not supported if you use the Connector with BlueXP backup and recovery or BlueXP ransomware protection. In this case, you can disallow the endpoints listed in option 1, while allowing the endpoints listed in option 2.

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

Outbound internet access for day-to-day operations

The network location where you deploy the Connector must have an outbound internet connection. The Connector requires outbound internet access to contact the following endpoints in order 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.

Endpoints	Purpose
https://management.usgovcloudapi.net https://login.microsoftonline.us https://blob.core.usgovcloudapi.net https://core.usgovcloudapi.net	To manage resources in Azure Government 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://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.
https://support.netapp.com https://mysupport.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://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	To provide SaaS features and services within BlueXP.
If the Connector is in an AWS Government region: https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	To obtain images for Connector upgrades when the Connector is installed in an AWS Government region.
If the Connector is in an Azure Government region: https://*.blob.core.windows.net https://occmclientinfragov.azurecr.us	To obtain images for Connector upgrades when the Connector is installed in an Azure Government region.

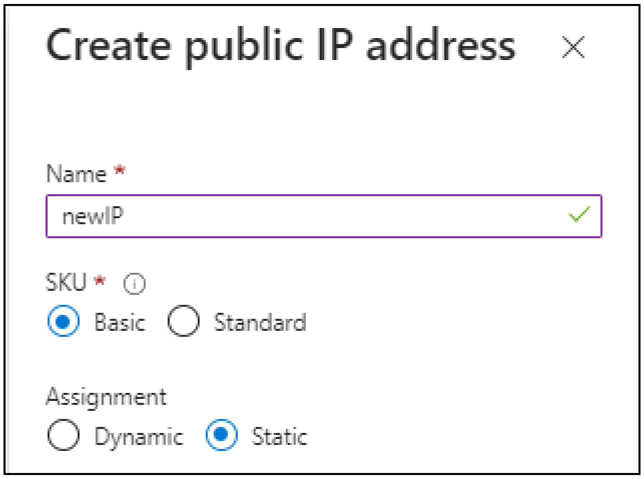
Endpoints	Purpose
If the Connector is in a commercial region or sovereign region, you can choose between two sets of endpoints: • Option 1 (recommended) [1] https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Option 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	To obtain images for Connector upgrades when the Connector is installed in a commercial region or sovereign region.

[1] The endpoints listed in option 1 are recommended because they are more secure. We recommend that you set up your firewall to allow the endpoints listed in option 1, while disallowing the endpoints listed in option 2. Note the following about these endpoints:

- The endpoints listed in option 1 are supported starting with the 3.9.47 release of the Connector. There is no backwards compatibility with previous releases of the Connector.
- The Connector contacts the endpoints listed in option 2 first. If those endpoints aren't accessible, the Connector automatically contacts the endpoints listed in option 1.
- The endpoints in option 1 are not supported if you use the Connector with BlueXP backup and recovery or BlueXP ransomware protection. In this case, you can disallow the endpoints listed in option 1, while allowing the endpoints listed in option 2.

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.



Create public IP address

Name *

newIP

SKU *

● Basic ○ Standard

Assignment

○ Dynamic ● Static

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

NetApp supports both explicit and transparent proxy configurations. If you are using a transparent proxy, you only need to provide the certificate for the proxy server. If you are using an explicit proxy, you'll also need the IP address and credentials.

- 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.

Enable NTP

If you're planning to use BlueXP classification to scan your corporate data sources, you should enable a Network Time Protocol (NTP) service on both the BlueXP Connector system and the BlueXP classification system so that the time is synchronized between the systems. Learn more about BlueXP classification

If you're planning to create the Connector from your cloud provider's marketplace, then you'll need to implement this networking requirement after you create the Connector.

Step 6: Prepare cloud permissions

BlueXP requires permissions from your cloud provider to deploy Cloud Volumes ONTAP in a virtual network and to use BlueXP data services. You need to set up permissions in your cloud provider and then associate those permissions with the Connector.

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

AWS IAM role

Use an IAM role to provide the Connector with permissions.

If you're creating the Connector from the AWS Marketplace, you'll be prompted to select that IAM role when you launch the EC2 instance.

If you're manually installing the Connector on your own Linux host, you'll need to attach the role to the EC2 instance.

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. 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

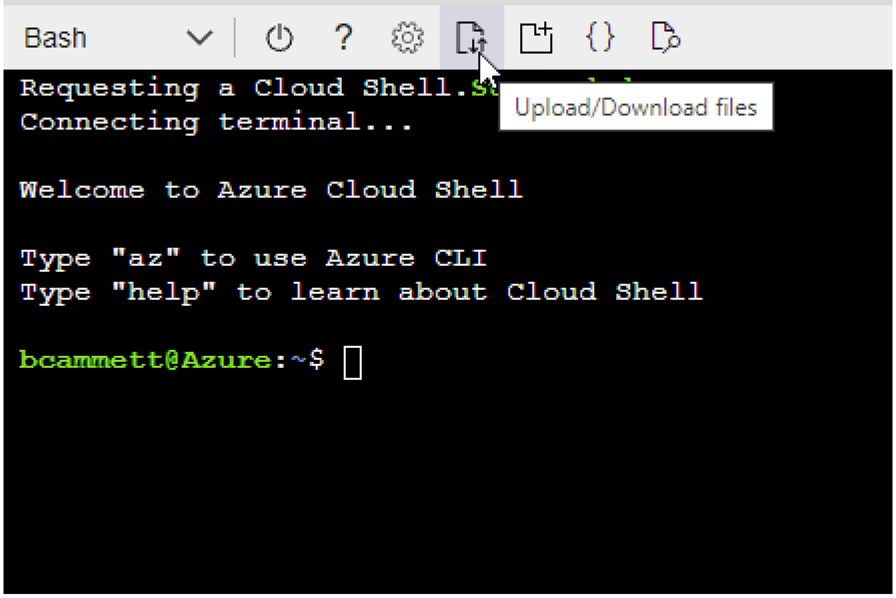
   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ```

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.



```
Requesting a Cloud Shell.Su
Connecting terminal...

Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

bcammett@Azure:~$
```

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

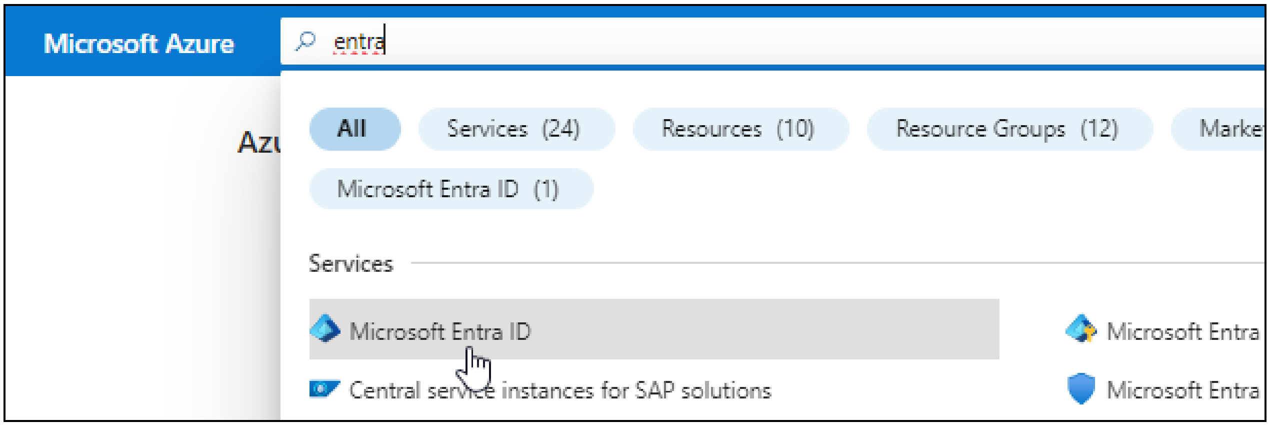
Create and set up a service principal in Microsoft Entra ID and obtain the Azure credentials that BlueXP needs. You'll need to provide BlueXP with these credentials after you install the Connector and set up BlueXP.

Create a Microsoft Entra 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 **Microsoft Entra ID** 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.

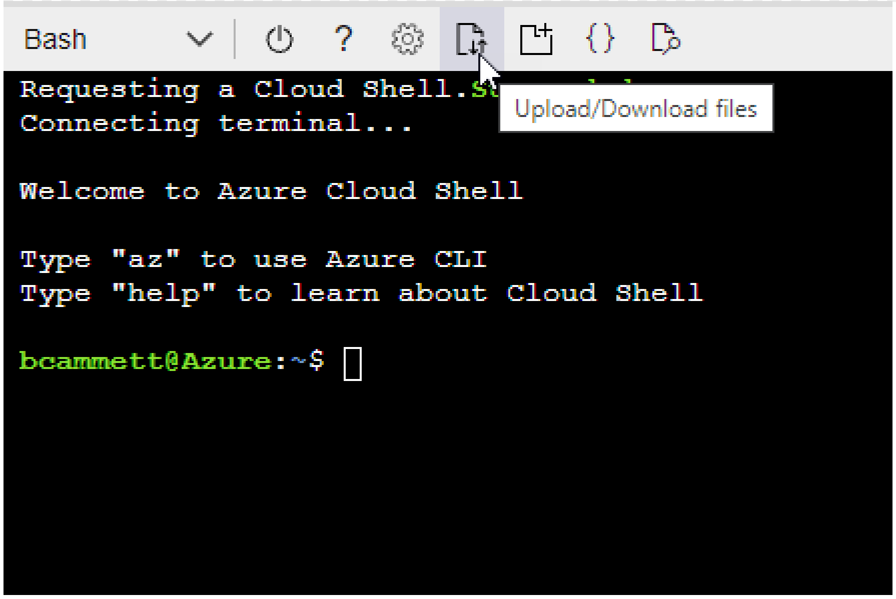
    Example

    ```
    "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.



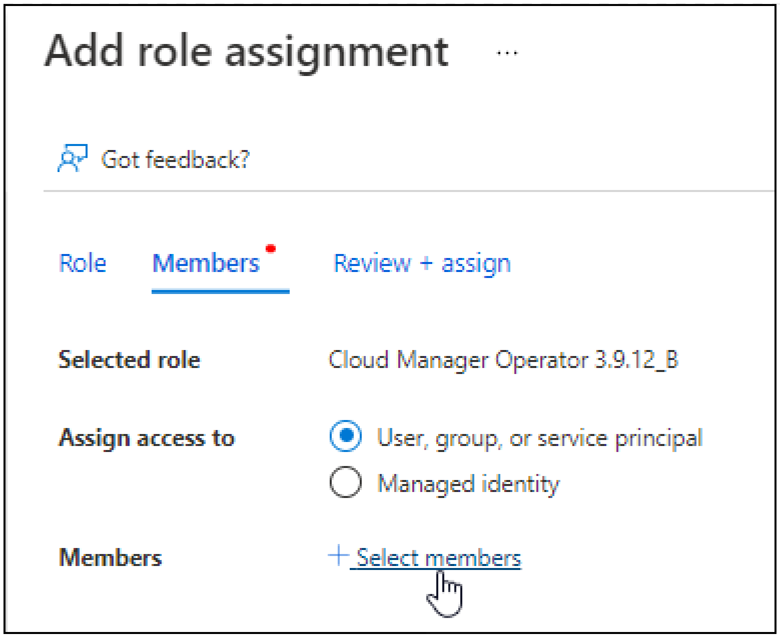
```
Requesting a Cloud Shell.Su
Connecting terminal...

Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

bcammett@Azure:~$
```

- 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**.


Add role assignment

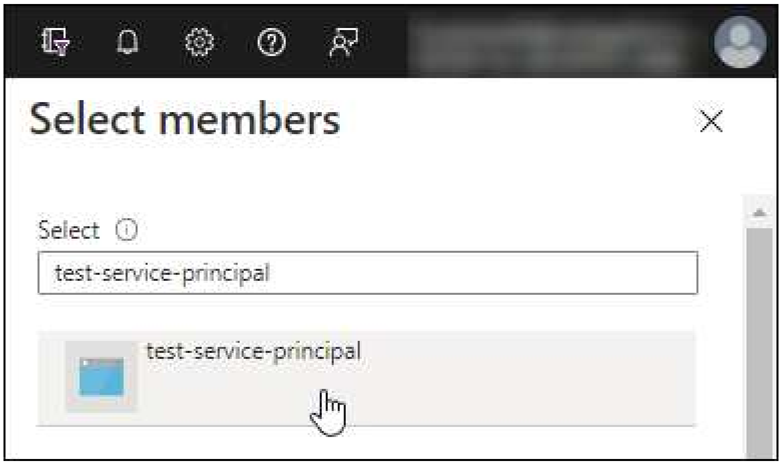
Selected role: Cloud Manager Operator 3.9.12_B

Assign access to: ● User, group, or service principal ○ Managed identity

Members: + Select members

- Search for the name of the application.

  Here’s an example:


Select members

Select: test-service-principal

test-service-principal

- Select the application and select **Select**.
- Select **Next**.

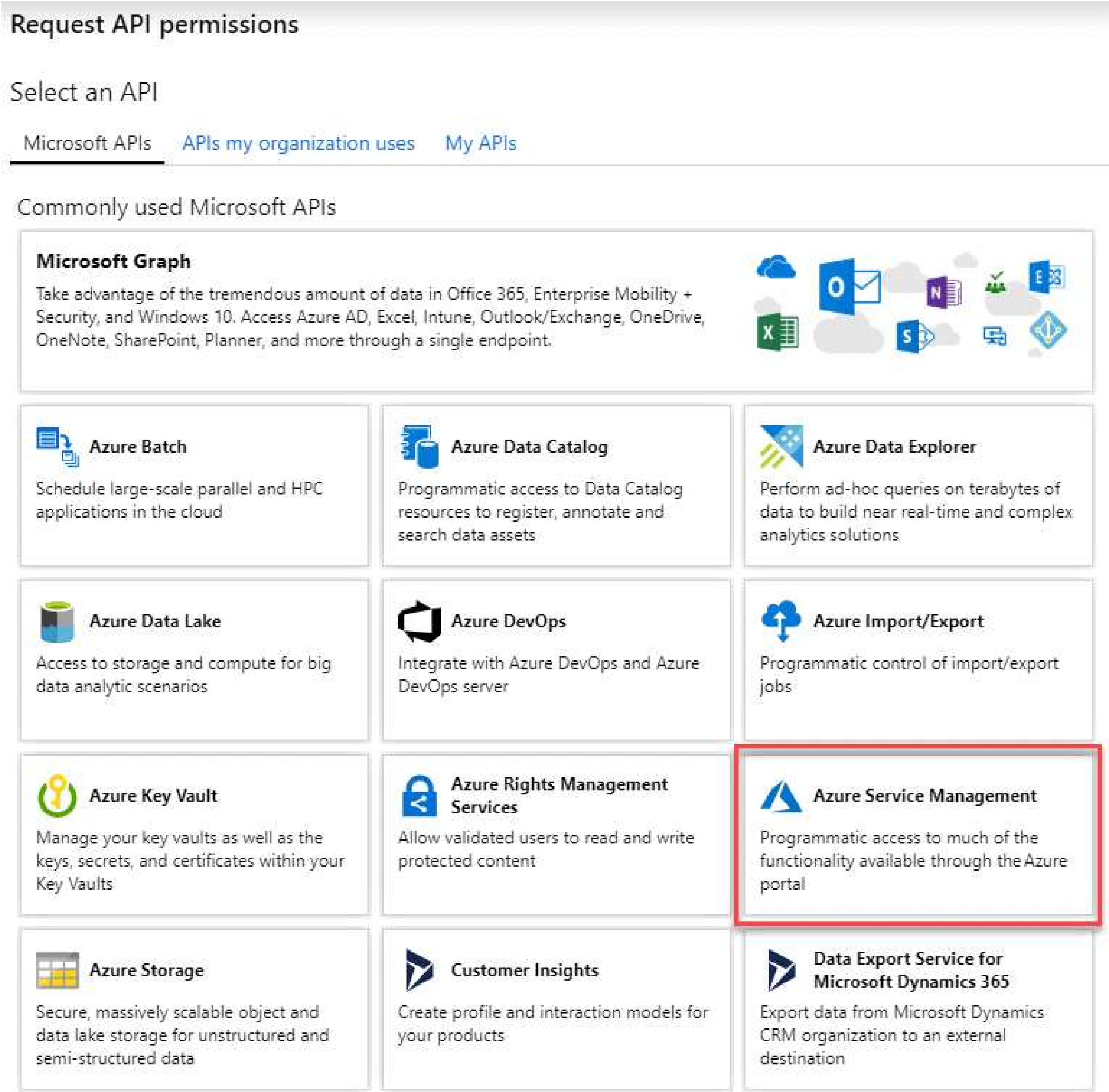
f. Select **Review + assign**.

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



Request API permissions

Select an API

Microsoft APIs | APIs my organization uses | My APIs

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Batch
Schedule large-scale parallel and HPC applications in the cloud

Azure Data Catalog
Programmatic access to Data Catalog resources to register, annotate and search data assets

Azure Data Explorer
Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

Azure Data Lake
Access to storage and compute for big data analytic scenarios

Azure DevOps
Integrate with Azure DevOps and Azure DevOps server

Azure Import/Export
Programmatic control of import/export jobs

Azure Key Vault
Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Rights Management Services
Allow validated users to read and write protected content

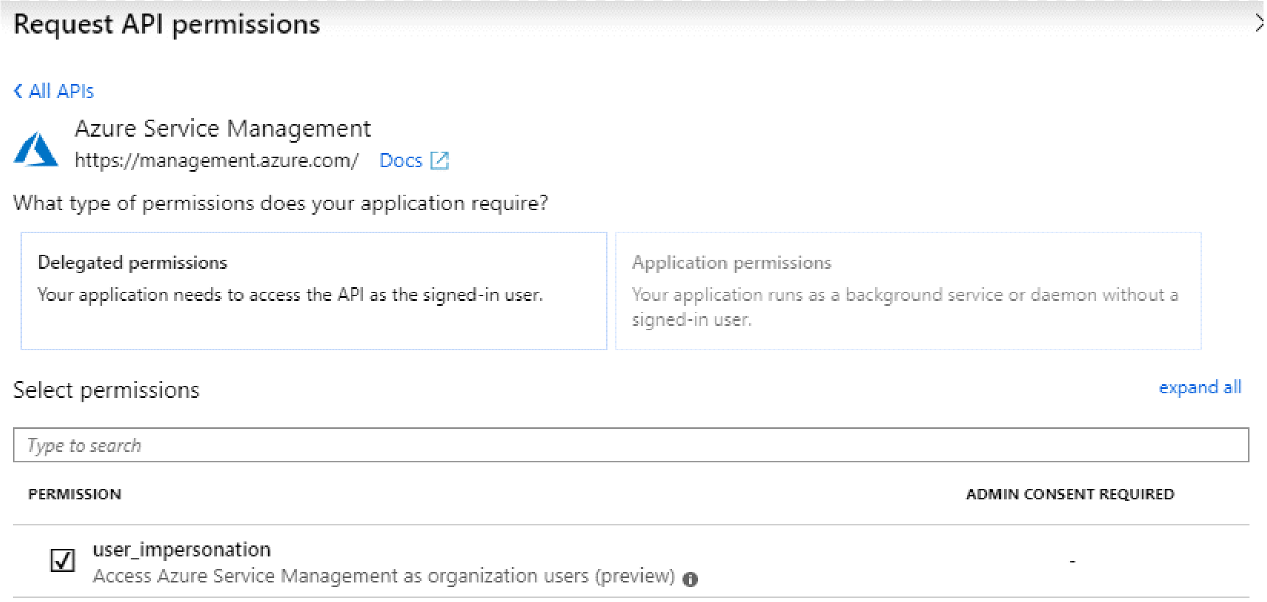
Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

Azure Storage
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Customer Insights
Create profile and interaction models for your products

Data Export Service for Microsoft Dynamics 365
Export data from Microsoft Dynamics CRM organization to an external destination

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



Request API permissions

< All APIs

Azure Service Management

https://management.azure.com/ Docs

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

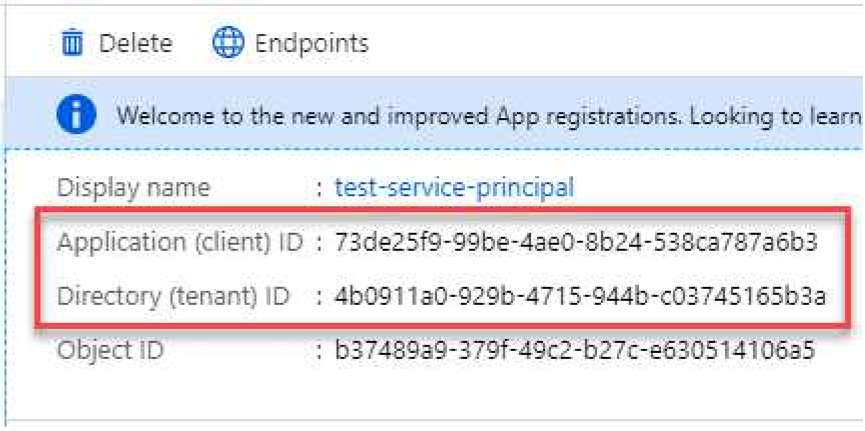
expand all

Type to search

PERMISSION	ADMIN CONSENT REQUIRED
☑ user_impersonation Access Azure Service Management as organization users (preview)	-

Get the application ID and directory ID for the application

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



Welcome to the new and improved App registrations. Looking to learn

Display name : test-service-principal

Application (client) ID : 73de25f9-99be-4ae0-8b24-538ca787a6b3

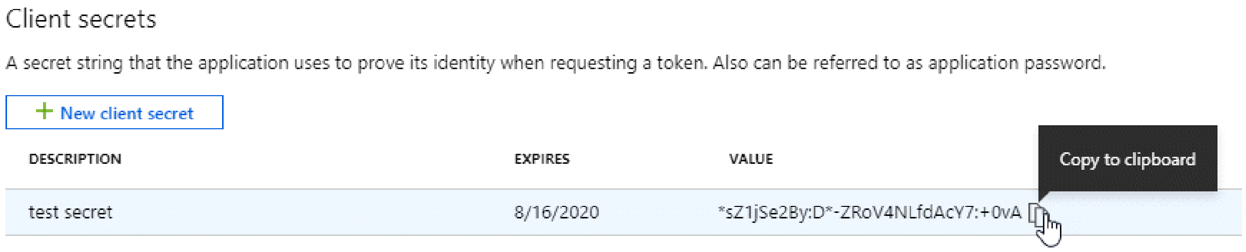
Directory (tenant) ID : 4b0911a0-929b-4715-944b-c03745165b3a

Object ID : b37489a9-379f-49c2-b27c-e630514106a5

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 **Microsoft Entra ID** 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.

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

You now have a client secret that BlueXP can use it to authenticate with Microsoft Entra ID.

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 7: 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 restricted mode

Deploy the Connector in restricted mode so that you can use BlueXP with limited outbound connectivity. 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

Install the Connector from your cloud provider's marketplace or by manually installing the software on your own Linux host.

AWS Commercial Marketplace

Before you begin

You should have the following:

- A VPC and subnet that meets networking requirements.

  Learn about networking requirements

- An IAM role with an attached policy that includes the required permissions for the Connector.

  Learn how to set up AWS permissions

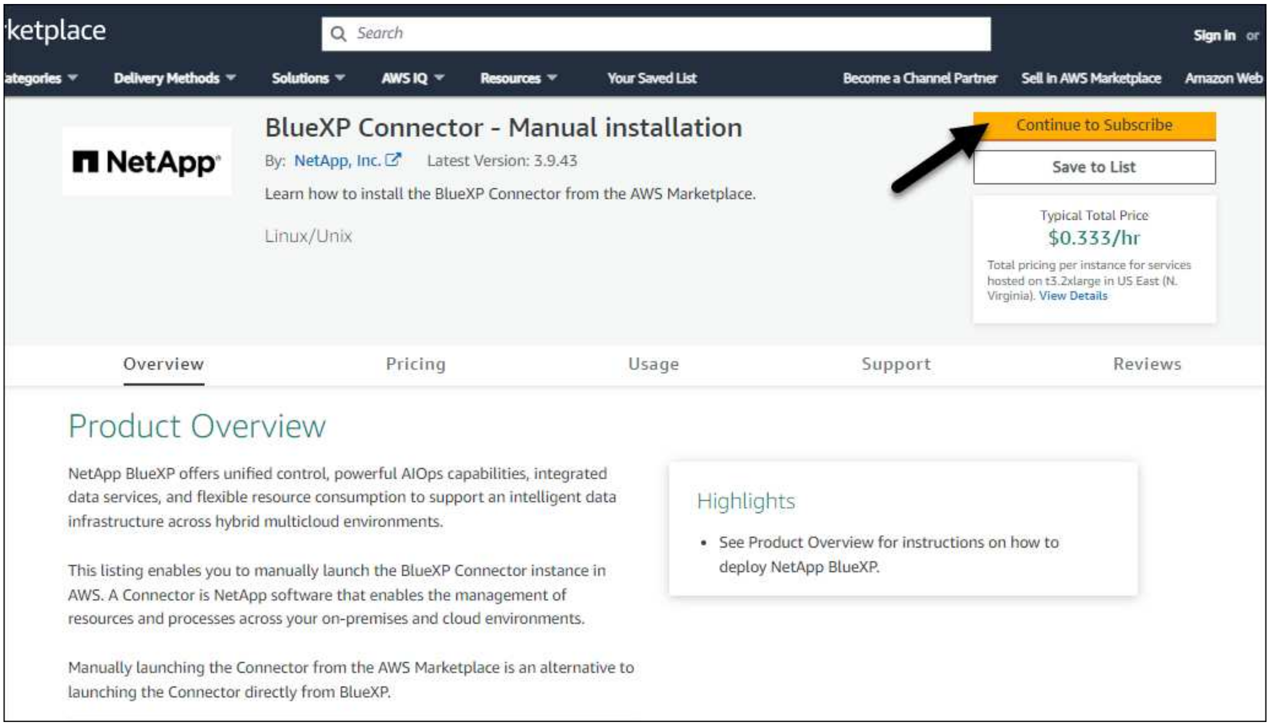
- Permissions to subscribe and unsubscribe from the AWS Marketplace for your IAM user.
- An understanding of CPU and RAM requirements for the instance.

  Review instance requirements.

- A key pair for the EC2 instance.

Steps

1. Go to the BlueXP Connector listing on the AWS Marketplace
2. On the Marketplace page, select **Continue to Subscribe**.



BlueXP Connector - Manual installation

By: NetApp, Inc. Latest Version: 3.9.43

Learn how to install the BlueXP Connector from the AWS Marketplace.

Linux/Unix

Typical Total Price
$0.333/hr
Total pricing per instance for services hosted on t3.2xlarge in US East (N. Virginia). View Details

Product Overview

NetApp BlueXP offers unified control, powerful AIOps capabilities, integrated data services, and flexible resource consumption to support an intelligent data infrastructure across hybrid multicloud environments.

This listing enables you to manually launch the BlueXP Connector instance in AWS. A Connector is NetApp software that enables the management of resources and processes across your on-premises and cloud environments.

Manually launching the Connector from the AWS Marketplace is an alternative to launching the Connector directly from BlueXP.

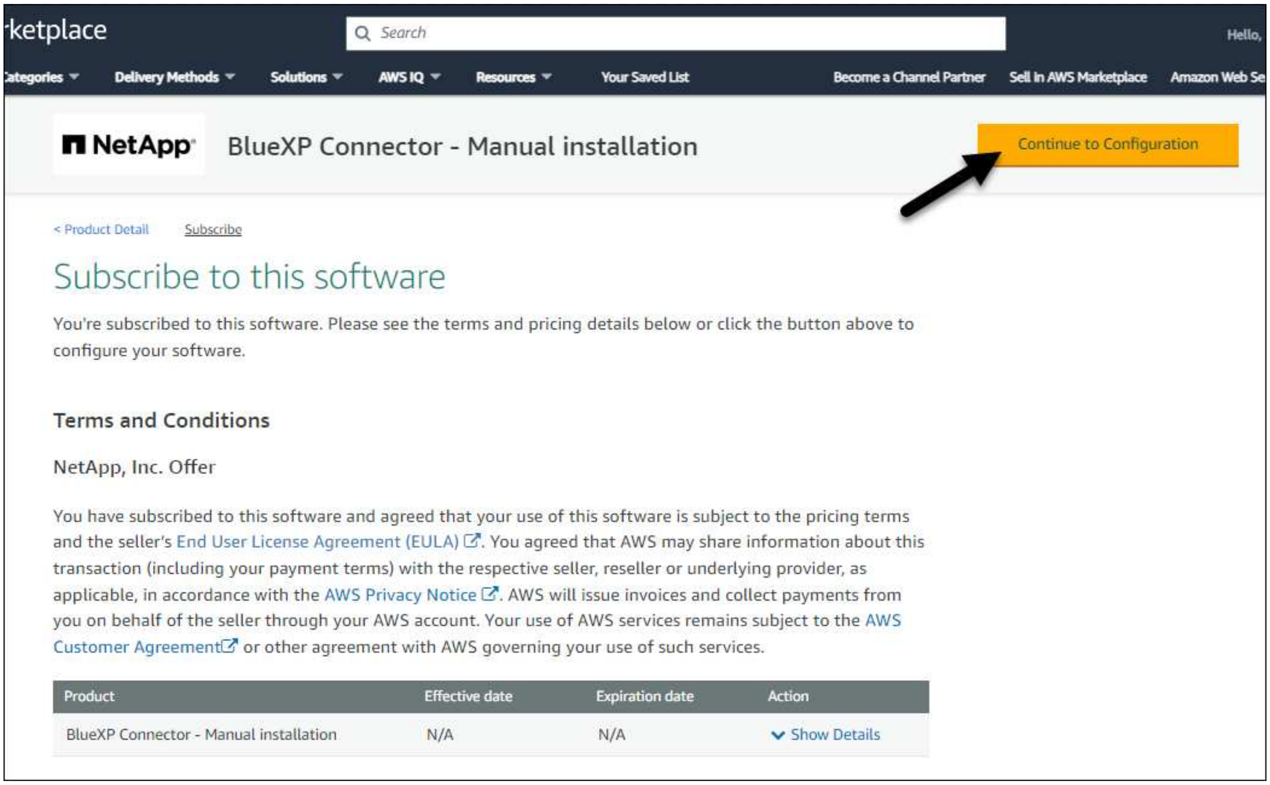
Highlights

- See Product Overview for instructions on how to deploy NetApp BlueXP.

3. To subscribe to the software, select **Accept Terms**.

   The subscription process can take a few minutes.

4. After the subscription process is complete, select **Continue to Configuration**.



Subscribe to this software

You're subscribed to this software. Please see the terms and pricing details below or click the button above to configure your software.

Terms and Conditions

NetApp, Inc. Offer

You have subscribed to this software and agreed that your use of this software is subject to the pricing terms and the seller's End User License Agreement (EULA). You agreed that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the AWS Privacy Notice. AWS will issue invoices and collect payments from you on behalf of the seller through your AWS account. Your use of AWS services remains subject to the AWS Customer Agreement or other agreement with AWS governing your use of such services.

Product	Effective date	Expiration date	Action
BlueXP Connector - Manual installation	N/A	N/A	Show Details

5. On the **Configure this software** page, ensure that you've selected the correct region and then select **Continue to Launch**.
6. On the **Launch this software** page, under **Choose Action**, select **Launch through EC2** and then select **Launch**.

   These steps describe how to launch the instance from the EC2 Console because the console enables you to attach an IAM role to the Connector instance. This isn't possible using the **Launch from Website** action.

7. Follow the prompts to configure and deploy the instance:
   - **Name and tags**: Enter a name and tags for the instance.
   - **Application and OS Images**: Skip this section. The Connector AMI is already selected.
   - **Instance type**: Depending on region availability, choose an instance type that meets RAM and CPU requirements (t3.2xlarge is preselected and recommended).
   - **Key pair (login)**: Select the key pair that you want to use to securely connect to the instance.
   - **Network settings**: Edit the network settings as needed:
     - Choose the desired VPC and subnet.
     - Specify whether the instance should have a public IP address.
     - Specify security group settings that enable the required connection methods for the Connector instance: SSH, HTTP, and HTTPS.

       View security group rules for AWS.
   - **Configure storage**: Keep the default size and disk type for the root volume.

     If you want to enable Amazon EBS encryption on the root volume, select **Advanced**, expand **Volume 1**, select **Encrypted**, and then choose a KMS key.

- **Advanced details**: Under **IAM instance profile**, choose the IAM role that includes the required permissions for the Connector.
- **Summary**: Review the summary and select **Launch instance**.

Result

AWS launches the software with the specified settings. The Connector instance and software should be running in approximately five minutes.

What's next?

Set up BlueXP.

AWS Gov Marketplace

Before you begin

You should have the following:

- A VPC and subnet that meets networking requirements.

  Learn about networking requirements

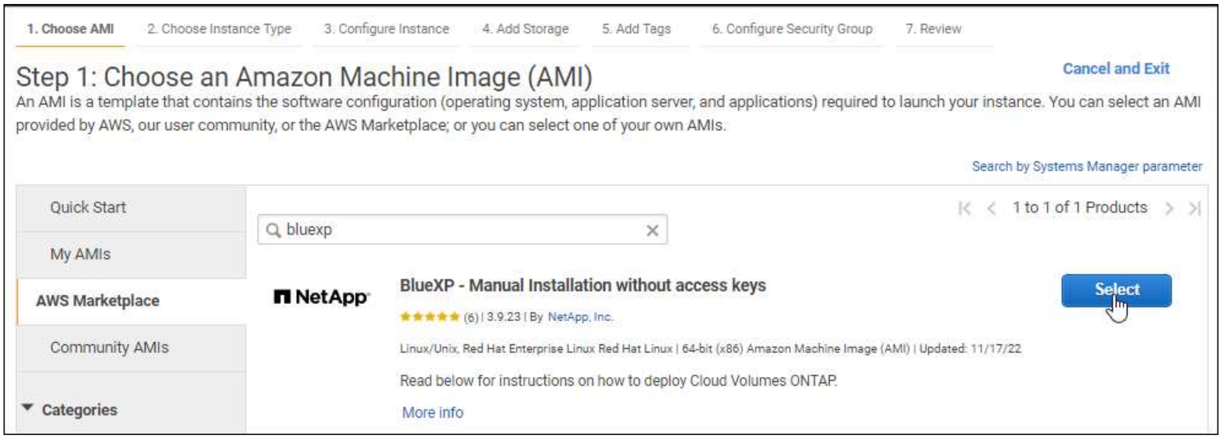
- An IAM role with an attached policy that includes the required permissions for the Connector.

  Learn how to set up AWS permissions

- Permissions to subscribe and unsubscribe from the AWS Marketplace for your IAM user.
- A key pair for the EC2 instance.

Steps

1. Go to the BlueXP offering in the AWS Marketplace.
   a. Open the EC2 service and select **Launch instance**.
   b. Select **AWS Marketplace**.
   c. Search for BlueXP and select the offering.



Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

bluexp

BlueXP - Manual Installation without access keys

★★★★★ (6) | 3.9.23 | By NetApp, Inc.

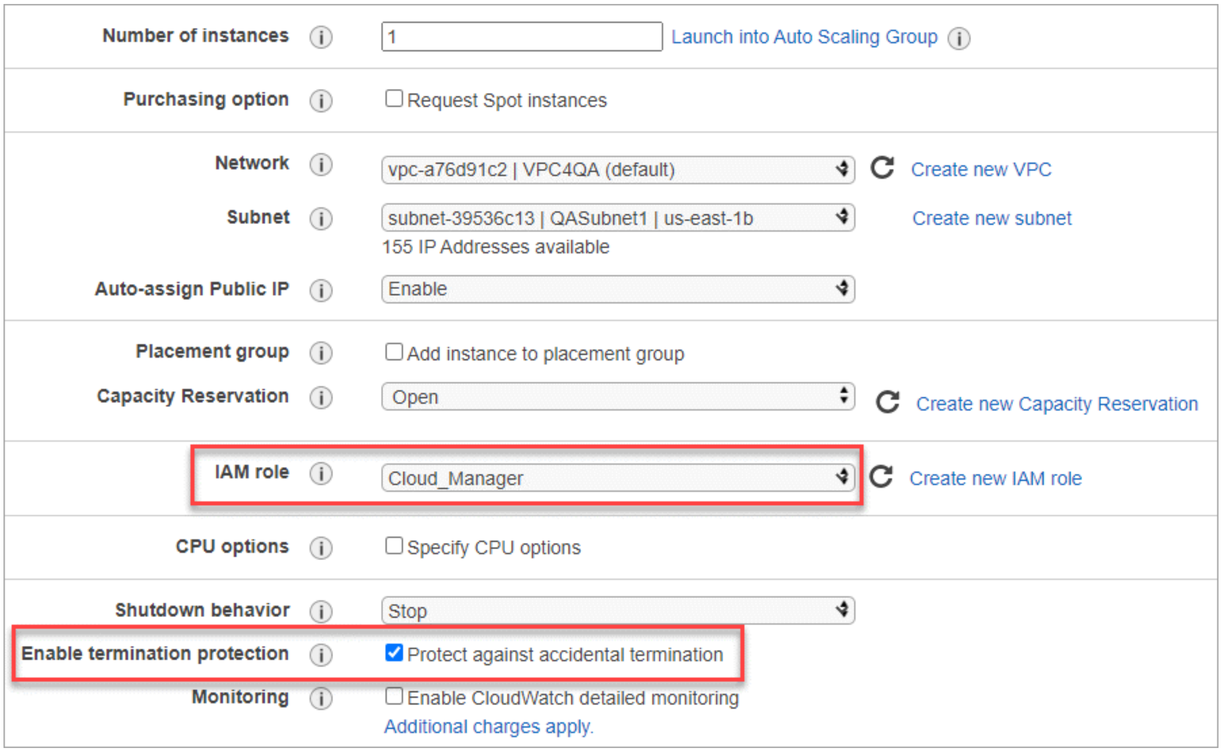
Linux/Unix, Red Hat Enterprise Linux Red Hat Linux | 64-bit (x86) Amazon Machine Image (AMI) | Updated: 11/17/22

Read below for instructions on how to deploy Cloud Volumes ONTAP.

   d. Select **Continue**.
2. Follow the prompts to configure and deploy the instance:
   - **Choose an Instance Type**: Depending on region availability, choose one of the supported instance types (t3.2xlarge is recommended).

Review the instance requirements.

- **Configure Instance Details**: Select a VPC and subnet, choose the IAM role that you created in step 1, enable termination protection (recommended), and choose any other configuration options that meet your requirements.



Number of instances	1 Launch into Auto Scaling Group
Purchasing option	□ Request Spot instances
Network	vpc-a76d91c2 | VPC4QA (default) Create new VPC
Subnet	subnet-39536c13 | QASubnet1 | us-east-1b 155 IP Addresses available Create new subnet
Auto-assign Public IP	Enable
Placement group	□ Add instance to placement group
Capacity Reservation	Open Create new Capacity Reservation
IAM role	Cloud_Manager Create new IAM role
CPU options	□ Specify CPU options
Shutdown behavior	Stop
Enable termination protection	☑ Protect against accidental termination
Monitoring	□ Enable CloudWatch detailed monitoring Additional charges apply.

- **Add Storage**: Keep the default storage options.
- **Add Tags**: Enter tags for the instance, if desired.
- **Configure Security Group**: Specify the required connection methods for the Connector instance: SSH, HTTP, and HTTPS.
- **Review**: Review your selections and select **Launch**.

Result

AWS launches the software with the specified settings. The Connector instance and software should be running in approximately five minutes.

What's next?

Set up BlueXP.

Azure Marketplace

Before you begin

You should have the following:

- A VNet and subnet that meets networking requirements.

  Learn about networking requirements

- An Azure custom role that includes the required permissions for the Connector.

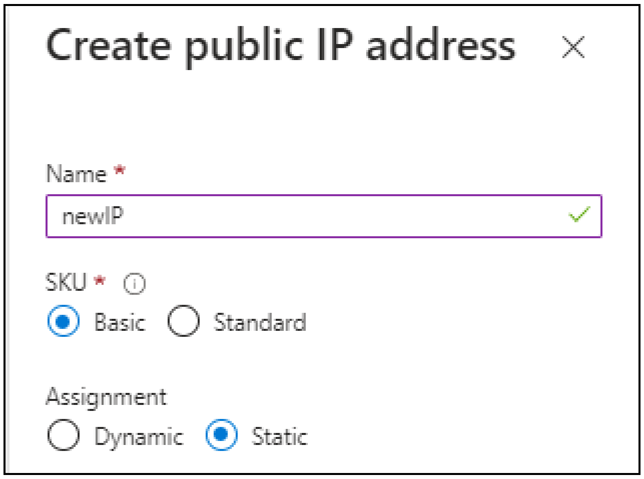
  Learn how to set up Azure permissions

Steps

1. Go to the NetApp Connector VM page in the Azure Marketplace.
    - Azure Marketplace page for commercial regions
    - Azure Marketplace page for Azure Government 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 Standard_D8s_v3.
    - **Disks**: The Connector can perform optimally with either HDD or SSD disks.
    - **Public IP**: If you want to use a public IP address with the Connector VM, the IP address must use a Basic SKU to ensure that BlueXP uses this public IP address.

        Create public IP address ×

        Name *

        newIP ✓

        SKU * ⓘ

        ● Basic ○ Standard

        Assignment

        ○ Dynamic ● Static

        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

    - **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 Microsoft Entra ID 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.

Result

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

What’s next?

Set up BlueXP.

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.

  ⓘ You cannot set a certificate for a transparent proxy server when manually installing the Connector. If you need to set a certificate for a transparent proxy server, you must use the Maintenance Console after installation. Learn more about the Connector Maintenance Console.
- Depending on your operating system, either Podman or Docker Engine is required before you install the Connector.

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. 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.

2. 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.

3. Assign permissions to run the script.

   ```
   chmod +x BlueXP-Connector-Cloud-<version>
   ```

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

4. Run the installation script.

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

You’ll need to add proxy information if your network requires a proxy for internet access. You can add either a transparent or explicit proxy. The --proxy and --cacert parameters are optional and you won’t be prompted to add them. If you have a proxy server, you will need to enter the parameters as shown.

Here is an example configuring an explicit proxy server with a CA-signed certificate:

```
 ./BlueXP-Connector-Cloud-v3.9.40--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://user-name:password@address:port
- http://domain-name%92user-name:password@address:port
- https://address:port
- https://user-name:password@address:port
- https://domain-name%92user-name:password@address:port

  Note the following:

  - The user can be a local user or domain user.
  - For a domain user, you must use the ASCII code for a \ as shown above.
  - BlueXP doesn’t support user names or passwords that include the @ character.
  - If the password includes any of the following special characters, you must escape that special character by prepending it with a backslash: & or !

    For example:

    http://bxpproxyuser:netapp1\!@address:3128

    --cacert specifies a CA-signed certificate to use for HTTPS access between the Connector and the proxy server. This parameter is required for HTTPS proxy servers, intercepting proxy servers, and transparent proxy servers.

  Here is an example configuring a transparent proxy server. When you configure a transparent proxy, you don’t need to define the proxy server. You only add a CA-signed certificate to your Connector host:

```
 ./BlueXP-Connector-Cloud-v3.9.40 --cacert
/tmp/cacert/certificate.cer
```

5. If you used Podman, you'll need to adjust the aardvark-dns port.

   a. SSH to the BlueXP Connector virtual machine.

   b. Open podman */usr/share/containers/containers.conf* file and modify the chosen port for Aardvark DNS service. For example, change it to 54.

   ```
   vi /usr/share/containers/containers.conf
   ...
   # Port to use for dns forwarding daemon with netavark in rootful
   bridge
   # mode and dns enabled.
   # Using an alternate port might be useful if other DNS services
   should
   # run on the machine.
   #
   dns_bind_port = 54
   ...
   Esc:wq
   ```

   c. Reboot the Connector virtual machine.

Result

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

What's next?

Set up BlueXP.

Step 2: Set up BlueXP

When you access the BlueXP console for the first time, you'll be prompted to choose an account to associate the Connector with and you'll need to enable restricted mode.

Before you begin

The person who sets up the BlueXP Connector must log in to BlueXP using a login that doesn't belong to a BlueXP account or organization.

If your BlueXP login is associated with another account or organization, you'll need to sign up with a new BlueXP login. Otherwise, you won't see the option to enable restricted mode on the setup screen.

Steps

1. Open a web browser from a host that has a connection to the Connector instance and enter the following URL:

   https://*ipaddress*

2. Sign up or log in to BlueXP.
3. After you're logged in, set up BlueXP:

a. Enter a name for the Connector.

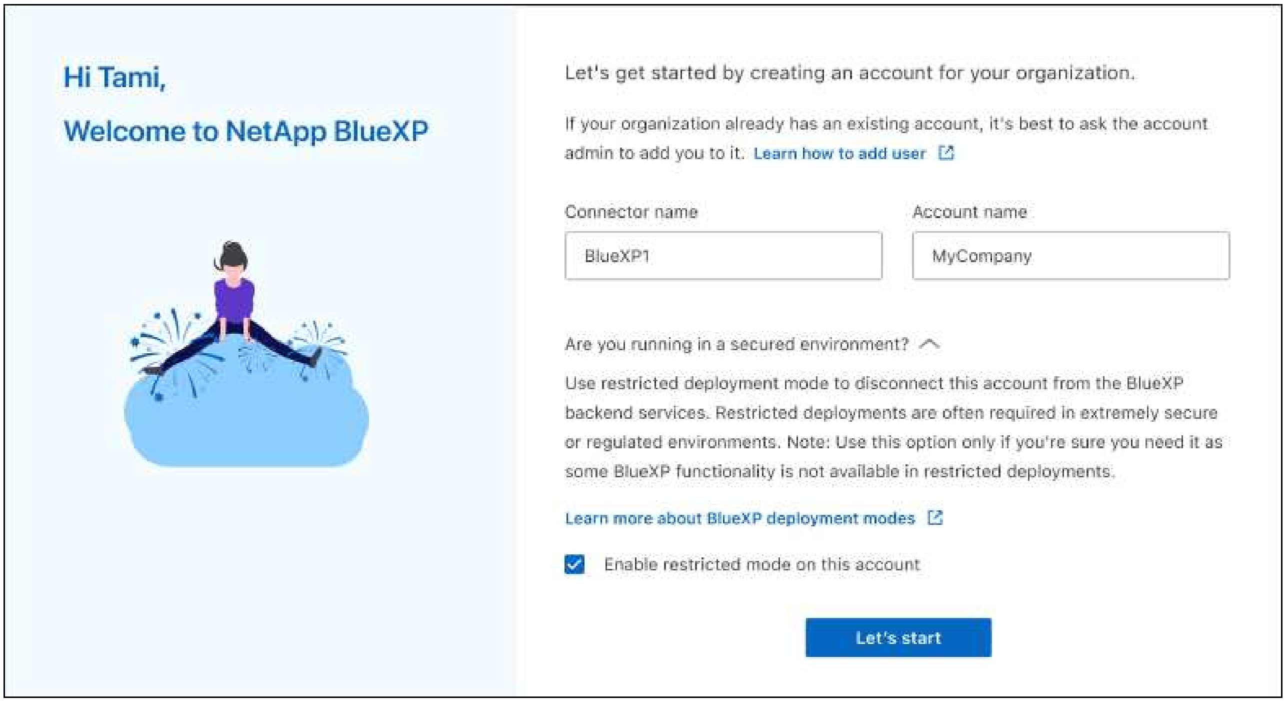
b. Enter a name for a new BlueXP account.

c. Select **Are you running in a secured environment?**

d. Select **Enable restricted mode on this account**.

Note that you can’t change this setting after BlueXP creates the account. You can’t enable restricted mode later and you can’t disable it later.

If you deployed the Connector in a Government region, the checkbox is already enabled and can’t be changed. This is because restricted mode is the only mode supported in Government regions.



Hi Tami,

Welcome to NetApp BlueXP

Let's get started by creating an account for your organization.

If your organization already has an existing account, it's best to ask the account admin to add you to it. Learn how to add user

Connector name: BlueXP1

Account name: MyCompany

Are you running in a secured environment?

Use restricted deployment mode to disconnect this account from the BlueXP backend services. Restricted deployments are often required in extremely secure or regulated environments. Note: Use this option only if you're sure you need it as some BlueXP functionality is not available in restricted deployments.

Learn more about BlueXP deployment modes

☑ Enable restricted mode on this account

e. Select **Let’s start**.

Result

The Connector is now installed and set up with your BlueXP account. All users need to access BlueXP using the IP address of the Connector instance.

What’s next?

Provide BlueXP with the permissions that you previously set up.

Step 3: Provide permissions to BlueXP

If you deployed the Connector from the Azure Marketplace or if you manually installed the Connector software, you need to provide the permissions that you previously set up so that you can use BlueXP services.

These steps don’t apply if you deployed the Connector from the AWS Marketplace because you chose the required IAM role during deployment.

Learn how to prepare cloud permissions.

AWS IAM role

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

These steps apply only if you manually installed the Connector in AWS. For AWS Marketplace deployments, you already associated the Connector instance with an IAM role that includes the required permissions.

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

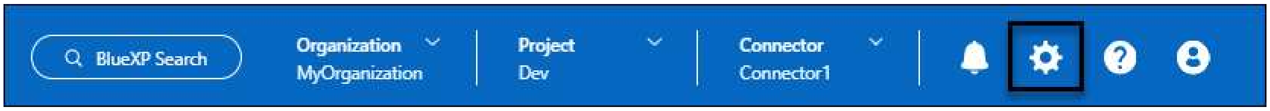
BlueXP now has the permissions that it needs to perform actions in AWS on your behalf.

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.

   It's important to assign the role from the **Subscriptions** service because this specifies the scope of the role assignment at the subscription level. The *scope* defines the set of resources that the access applies to. If you specify a scope at a different level (for example, at the virtual machine level), your ability to complete actions from within BlueXP will be affected.

Microsoft Azure documentation: Understand scope for Azure RBAC

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, under **Managed identity**, 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

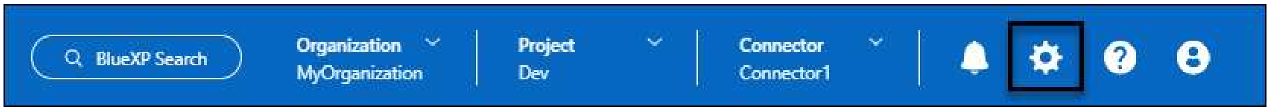
BlueXP now has the permissions that it needs to perform actions in Azure on your behalf.

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 Microsoft Entra 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.

Subscribe to NetApp Intelligent Services (restricted mode)

Subscribe to NetApp Intelligent Services from your cloud provider's marketplace to pay for data services at an hourly rate (PAYGO) or through an annual contract. If you purchased a license from NetApp (BYOL), you also need to subscribe to the marketplace offering. Your license is always charged first, but you'll be charged at the hourly rate if you exceed your licensed capacity or if the license's term expires.

A marketplace subscription enables charging for the following data services with restricted mode:

- Backup and recovery
- Cloud Volumes ONTAP
- Tiering
- Ransomware protection
- Disaster recovery

Classification is enabled through your subscription, but there is no charge for using classification.

Before you begin

Subscribing to data services involves associating a marketplace subscription with the cloud credentials that are associated with a Connector. If you followed the "Get started with restricted mode" workflow, then you should already have a Connector. To learn more, view the Quick start for BlueXP in restricted mode.

AWS

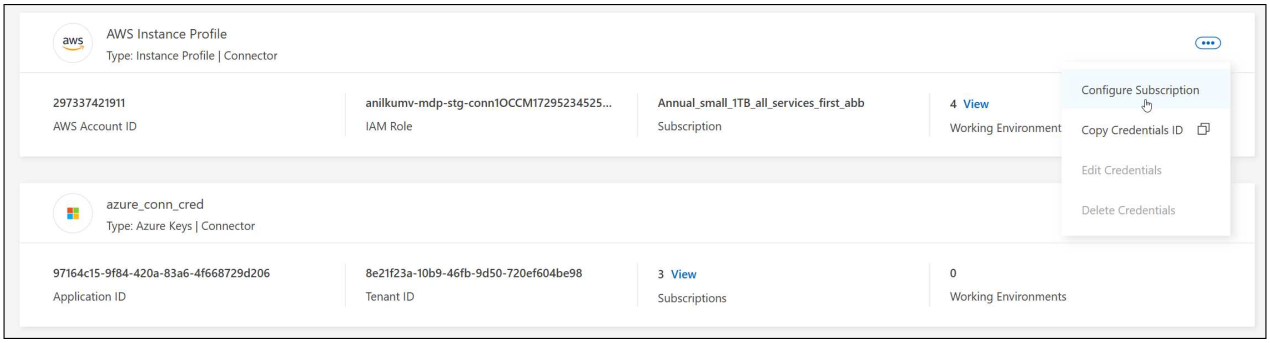
The following video shows the steps to subscribe to NetApp Intelligent Services from the AWS Marketplace:

Subscribe to NetApp Intelligent Services from the AWS Marketplace

Steps

1. In the upper right of the BlueXP console, select the Settings icon, and select **Credentials**.
2. Select the action menu for a set of credentials and then select **Configure Subscription**.

   You must select credentials that are associated with a Connector. You can’t associate a marketplace subscription with credentials that are associated with BlueXP.

   AWS Instance Profile
   Type: Instance Profile | Connector

   297337421911
   AWS Account ID

   anilkumv-mdp-stg-conn1OCCM17295234525...
   IAM Role

   Annual_small_1TB_all_services_first_abb
   Subscription

   4 View
   Working Environment

   azure_conn_cred
   Type: Azure Keys | Connector

   97164c15-9f84-420a-83a6-4f668729d206
   Application ID

   8e21f23a-10b9-46fb-9d50-720ef604be98
   Tenant ID

   3 View
   Subscriptions

   0
   Working Environments

3. To associate the credentials with an existing subscription, select the subscription from the down-down list and select **Configure**.
4. To associate the credentials with a new subscription, select **Add Subscription > Continue** and follow the steps in the AWS Marketplace:
   a. Select **View purchase options**.
   b. Select **Subscribe**.
   c. Select **Set up your account**.

      You’ll be redirected to the BlueXP website.

   d. From the **Subscription Assignment** page:
      - Select the BlueXP organizations or accounts that you’d like to associate this subscription with.
      - In the **Replace existing subscription** field, choose whether you’d like to automatically replace the existing subscription for one organization or account with this new subscription.

        BlueXP replaces the existing subscription for all credentials in the organization or account with this new subscription. If a set of credentials wasn’t ever associated with a subscription, then this new subscription won’t be associated with those credentials.

        For all other organizations or accounts, you’ll need to manually associate the subscription by repeating these steps.
      - Select **Save**.

Azure

Steps

1. In the upper right of the console, select the Settings icon, and select **Credentials**.
2. Select the action menu for a set of credentials and then select **Configure Subscription**.

   You must select credentials that are associated with a Connector. You can't associate a marketplace subscription with credentials that are associated with BlueXP.

3. To associate the credentials with an existing subscription, select the subscription from the down-down list and select **Configure**.
4. To associate the credentials with a new subscription, select **Add Subscription > Continue** and follow the steps in the Azure Marketplace:
   a. If prompted, log in to your Azure account.
   b. Select **Subscribe**.
   c. Fill out the form and select **Subscribe**.
   d. After the subscription process is complete, select **Configure account now**.

      You'll be redirected to BlueXP.

   e. From the **Subscription Assignment** page:
      - Select the BlueXP organizations or accounts that you'd like to associate this subscription with.
      - In the **Replace existing subscription** field, choose whether you'd like to automatically replace the existing subscription for one organization or account with this new subscription.

        BlueXP replaces the existing subscription for all credentials in the organization or account with this new subscription. If a set of credentials wasn't ever associated with a subscription, then this new subscription won't be associated with those credentials.

        For all other organizations or accounts, you'll need to manually associate the subscription by repeating these steps.

      - Select **Save**.

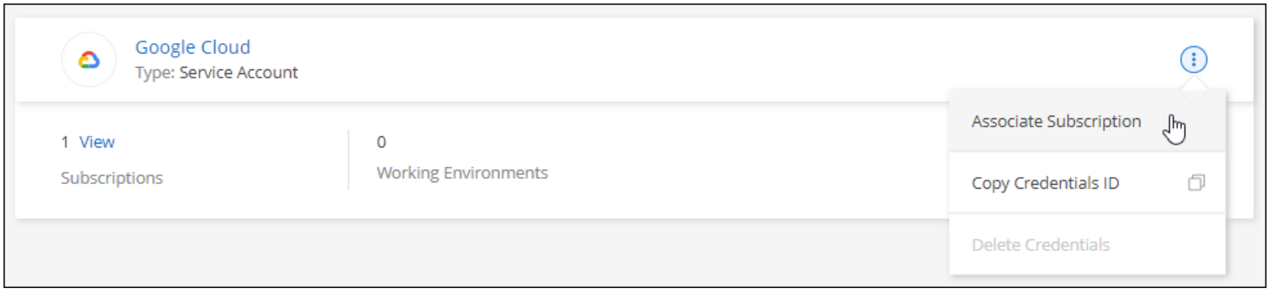
        The following video shows the steps to subscribe from the Azure Marketplace:

        Subscribe to NetApp Intelligent Services from the Azure Marketplace

Google Cloud

Steps

1. In the upper right of the console, select the Settings icon, and select **Credentials**.
2. Select the action menu for a set of credentials and then select **Configure Subscription**.
   +new screenshot needed (TS)



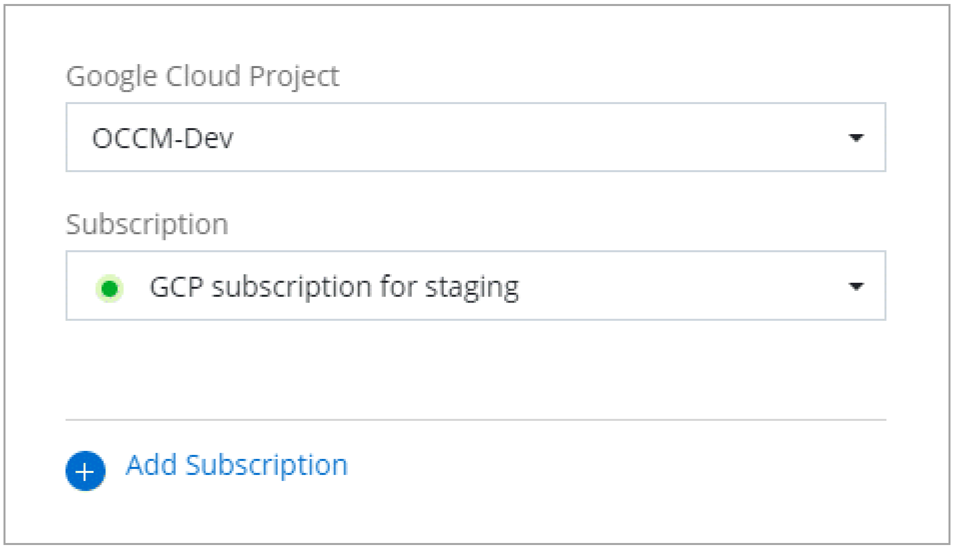
Google Cloud
Type: Service Account

1 View
Subscriptions

0
Working Environments

3. To configure an existing subscription with the selected credentials, select a Google Cloud project and

subscription from the drop-down list, and then select **Configure**.



Google Cloud Project

OCCM-Dev

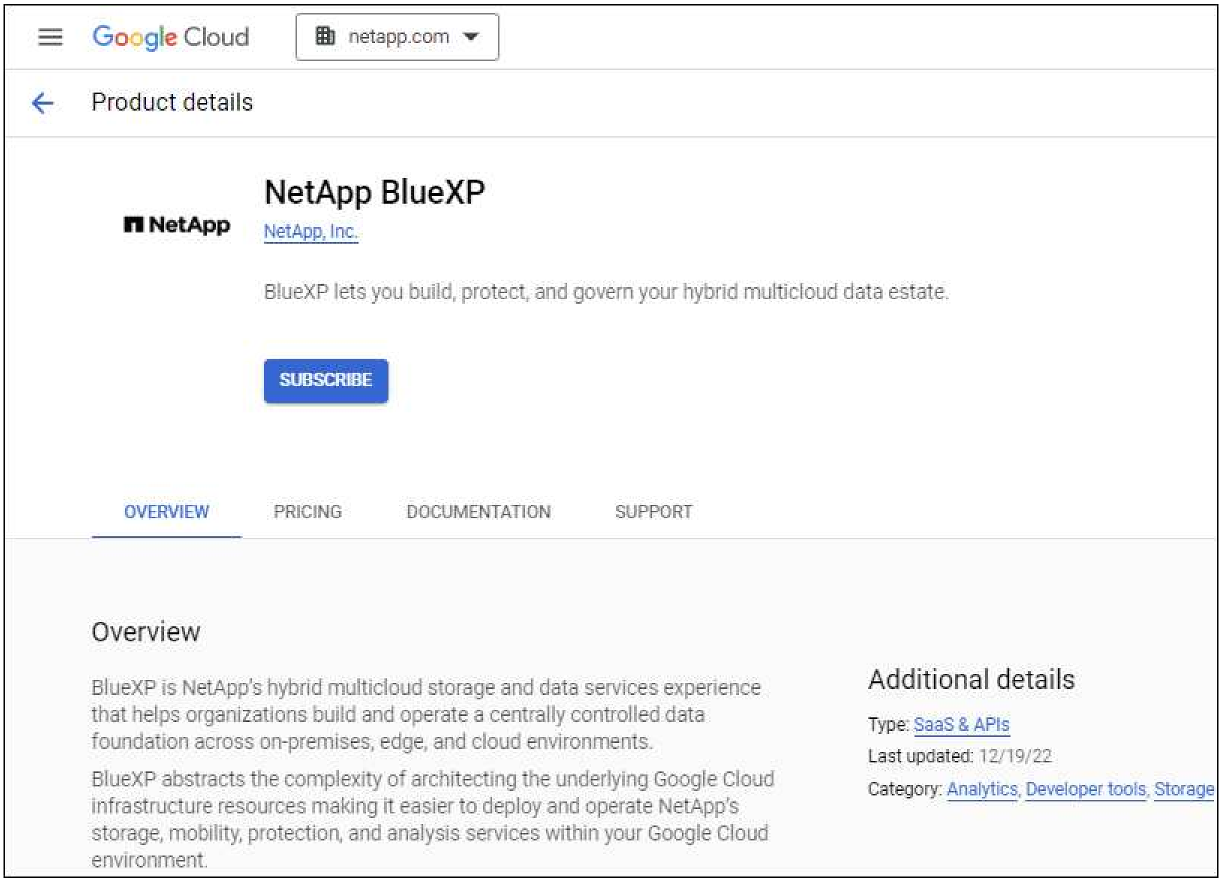
Subscription

● GCP subscription for staging

4. If you don’t already have a subscription, select **Add Subscription > Continue** and follow the steps in the Google Cloud Marketplace.

> ⓘ Before you complete the following steps, ensure that you have both Billing Admin privileges in your Google Cloud account as well as a BlueXP login.

a. After you’re redirected to the NetApp Intelligent Services page on the Google Cloud Marketplace, ensure that the correct project is selected at the top navigation menu.



NetApp BlueXP

NetApp, Inc.

BlueXP lets you build, protect, and govern your hybrid multicloud data estate.

Overview

BlueXP is NetApp’s hybrid multicloud storage and data services experience that helps organizations build and operate a centrally controlled data foundation across on-premises, edge, and cloud environments.

BlueXP abstracts the complexity of architecting the underlying Google Cloud infrastructure resources making it easier to deploy and operate NetApp’s storage, mobility, protection, and analysis services within your Google Cloud environment.

Additional details

Type: SaaS & APIs

Last updated: 12/19/22

Category: Analytics, Developer tools, Storage

b. Select **Subscribe**.

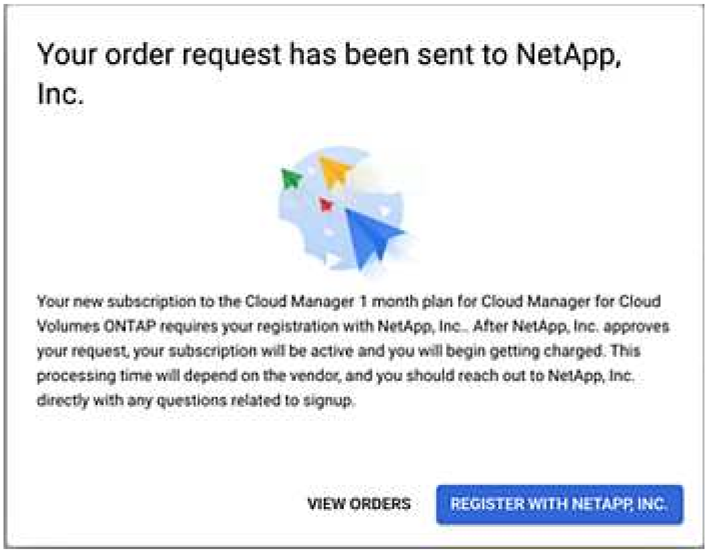
c. Select the appropriate billing account and agree to the terms and conditions.

d. Select **Subscribe**.

   This step sends your transfer request to NetApp.

e. On the pop-up dialog box, select **Register with NetApp, Inc.**

   This step must be completed to link the Google Cloud subscription with your BlueXP organization or account. The process of linking a subscription isn't complete until you are redirected from this page and then sign in to BlueXP.



Your order request has been sent to NetApp, Inc.

Your new subscription to the Cloud Manager 1 month plan for Cloud Manager for Cloud Volumes ONTAP requires your registration with NetApp, Inc.. After NetApp, Inc. approves your request, your subscription will be active and you will begin getting charged. This processing time will depend on the vendor, and you should reach out to NetApp, Inc. directly with any questions related to signup.

f. Complete the steps on the **Subscription Assignment** page:

   If someone from your organization has already subscribed to the NetApp BlueXP subscription from your billing account, then you will be redirected to the Cloud Volumes ONTAP page on the BlueXP website instead. If this is unexpected, contact your NetApp sales team. Google enables only one subscription per Google billing account.

   - Select the BlueXP organizations or accounts that you'd like to associate this subscription with.
   - In the **Replace existing subscription** field, choose whether you'd like to automatically replace the existing subscription for one organization or account with this new subscription.

     BlueXP replaces the existing subscription for all credentials in the organization or account with this new subscription. If a set of credentials wasn't ever associated with a subscription, then this new subscription won't be associated with those credentials.

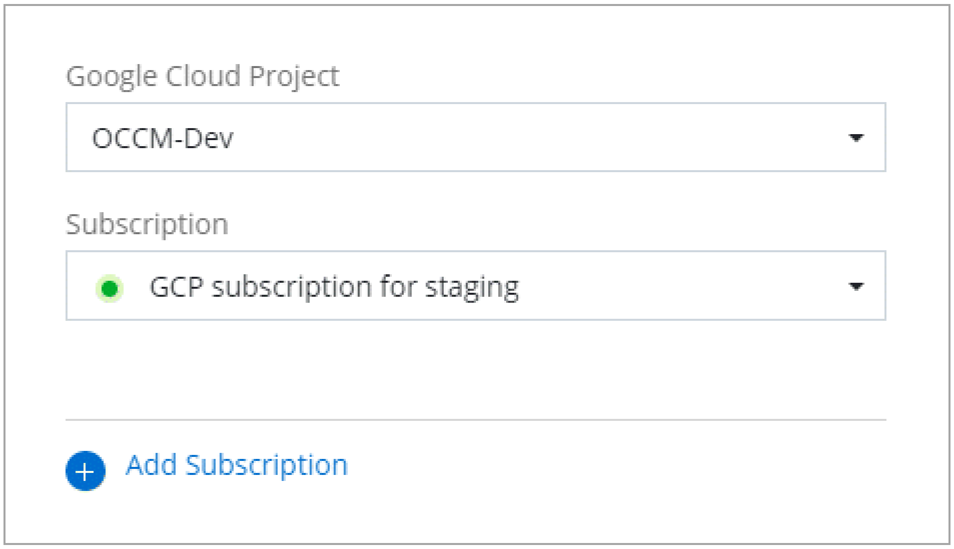
     For all other organizations or accounts, you'll need to manually associate the subscription by repeating these steps.

   - Select **Save**.

     The following video shows the steps to subscribe from the Google Cloud Marketplace:

     Subscribe to BlueXP from the Google Cloud Marketplace

g. Once this process is complete, navigate back to the Credentials page in BlueXP and select this new subscription.



Google Cloud Project

OCCM-Dev

Subscription

● GCP subscription for staging

Related information

- Manage BYOL capacity-based licenses for Cloud Volumes ONTAP
- Manage BYOL licenses for data services
- Manage AWS credentials and subscriptions
- Manage Azure credentials and subscriptions
- Manage Google Cloud credentials and subscriptions

What you can do next (restricted mode)

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

For help, refer to the documentation for these services:

- Azure NetApp Files docs
- Backup and recovery docs
- Classification docs
- Cloud Volumes ONTAP docs
- Digital wallet docs
- On-premises ONTAP cluster docs
- Replication docs

Related information

BlueXP deployment modes

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.

Private mode is typically used with on-premises environments that have no internet connection and with secure cloud regions, which includes AWS Secret Cloud, AWS Top Secret Cloud, and Azure IL6

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

1 **Prepare for deployment**

a. Prepare a dedicated Linux host that meets requirements for CPU, RAM, disk space, container orchestration tool, 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.

> ⓘ To use BlueXP in the AWS Secret Cloud or the AWS Top Secret Cloud, follow the specific instructions for 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 understand private mode.

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

In addition, not all features and 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.

Where you install the Connector determines which BlueXP services and features are available when using private mode. For example, the Connector must be installed in the cloud if you want to deploy and manage Cloud Volumes ONTAP. Learn more about private mode.

Step 3: Review host requirements

The host must meet specific operating system requirements, RAM requirements, port requirements, and so on to run the Connector software.

Dedicated host

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

Host can be of any architecture that meets the following size requirements:

- CPU: 8 cores or 8 vCPUs
- RAM: 32 GB

Operating system and container requirements

BlueXP supports the Connector with the following operating systems when using BlueXP in private mode. A container orchestration tool is required before you install the Connector.

Operating system	Supported OS versions	Supported Connector versions	Required container tool	SELinux
Red Hat Enterprise Linux	9.1 to 9.4 8.6 to 8.10	3.9.42 or later with BlueXP in private mode	Podman version 4.6.1 or 4.9.4 View Podman configuration requirements.	Supported in enforcing mode or permissive mode [1]
Ubuntu	22.04 LTS	3.9.29 or later	Docker Engine 23.0.6 to 26.0.0 26.0.0 is supported with *new* Connector 3.9.44 or later installations	Not supported

Notes:

1. Management of Cloud Volumes ONTAP systems is not supported by Connectors that have SELinux enabled on the operating system.
2. The Connector is supported on English-language versions of these operating systems.
3. For RHEL, 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.

Hypervisor
A bare metal or hosted hypervisor that is certified to run a supported operating system is required.

CPU
8 cores or 8 vCPUs

RAM
32 GB

AWS EC2 instance type
An instance type that meets the CPU and RAM requirements above. We recommend t3.2xlarge.

Azure VM size
An instance type that meets the CPU and RAM requirements above. We recommend Standard_D8s_v3.

Google Cloud machine type
An instance type that meets the CPU and RAM requirements above. We recommend n2-standard-8.

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

BlueXP uses `/opt` to install the `/opt/application/netapp` directory and its contents.

Disk space in /var
20 GiB of space must be available

BlueXP requires this space in `/var` because Docker or Podman are architected to create the containers within this directory. Specifically, they will create containers in the `/var/lib/containers/storage` directory. External mounts or symlinks do not work for this space.

Step 4: Install Podman or Docker Engine

You need to prepare the host for the Connector by installing Podman or Docker Engine.

Depending on your operating system, either Podman or Docker Engine is required before you install the Connector.

- Podman is required for Red Hat Enterprise Linux 8 and 9.

  View the Podman versions that BlueXP supports.

- Docker Engine is required for Ubuntu.

  View the Docker Engine versions that BlueXP supports.

Example 6. Steps

Podman

Follow these steps to install Podman and configure it to meet the following requirements:

- Enable and start the podman.socket service
- Install python3
- Install the podman-compose package version 1.0.6
- Add podman-compose to the PATH environment variable

> ⓘ When using Podman, adjust the aardvark-dns service port (default: 53) after installing the Connector to avoid conflicts with the DNS port on the host. Follow the instructions to configure the port.

Steps

1. Remove the podman-docker package if it's installed on the host.

   ```
   dnf remove podman-docker
   rm /var/run/docker.sock
   ```

2. Install Podman.

   Podman is available from official Red Hat Enterprise Linux repositories.

   For Red Hat Enterprise Linux 9:

   ```
   sudo dnf install podman-2:<version>
   ```

   Where <version> is the supported version of Podman that you're installing. View the Podman versions that BlueXP supports.

   For Red Hat Enterprise Linux 8:

   ```
   sudo dnf install podman-3:<version>
   ```

   Where <version> is the supported version of Podman that you're installing. View the Podman versions that BlueXP supports.

3. Enable and start the podman.socket service.

   ```
   sudo systemctl enable --now podman.socket
   ```

4. Install python3.

```
sudo dnf install python3
```

5. Install the EPEL repository package if it’s not already available on your system.

   This step is required because podman-compose is available from the Extra Packages for Enterprise Linux (EPEL) repository.

   For Red Hat Enterprise Linux 9:

   ```
   sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
   ```

   For Red Hat Enterprise Linux 8:

   ```
   sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
   ```

6. Install podman-compose package 1.0.6.

   ```
   sudo dnf install podman-compose-1.0.6
   ```

   > ⓘ Using the `dnf install` command meets the requirement for adding podman-compose to the PATH environment variable. The installation command adds podman-compose to /usr/bin, which is already included in the `secure_path` option on the host.

Docker Engine

Follow the documentation from Docker to install Docker Engine.

Steps

1. View installation instructions from Docker

   Be sure to follow the steps to install a specific version of Docker Engine. Installing the latest version will install a version of Docker that BlueXP doesn’t support.

2. Verify that Docker is enabled and running.

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

Step 5: Prepare networking

Set up networking for the Connector to manage resources in your public cloud. Other than having a virtual network and subnet for the Connector, 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.

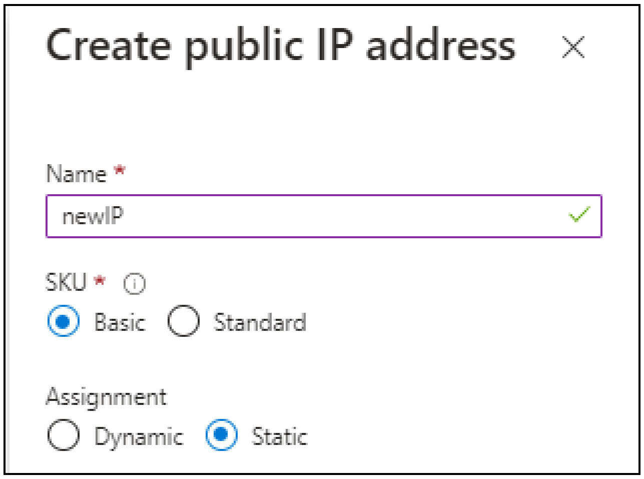
Endpoints for day-to-day operations

If you are planning to create Cloud Volumes ONTAP systems, the Connector needs connectivity to endpoints in your cloud provider's publicly available resources.

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.
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.



Create public IP address ×

Name *

newIP

SKU *

● Basic ○ Standard

Assignment

○ Dynamic ● Static

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

NetApp supports both explicit and transparent proxy configurations. If you are using a transparent proxy, you only need to provide the certificate for the proxy server. If you are using an explicit proxy, you'll also need the IP address and credentials.

- 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.

Enable NTP

If you're planning to use BlueXP classification to scan your corporate data sources, you should enable a Network Time Protocol (NTP) service on both the BlueXP Connector system and the BlueXP classification system so that the time is synchronized between the systems. Learn more about BlueXP classification

Step 6: Prepare cloud permissions

If the Connector is installed in the cloud and you plan to create Cloud Volumes ONTAP systems, BlueXP requires cloud provider permissions. 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.

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. 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. 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

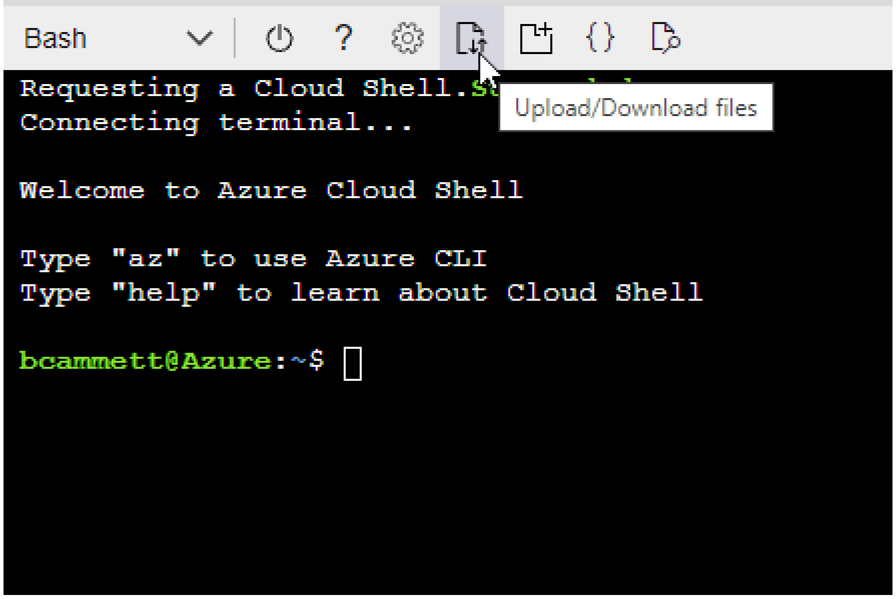
   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ```

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.



```
Requesting a Cloud Shell.Su
Connecting terminal...

Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

bcammett@Azure:~$ 
```

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

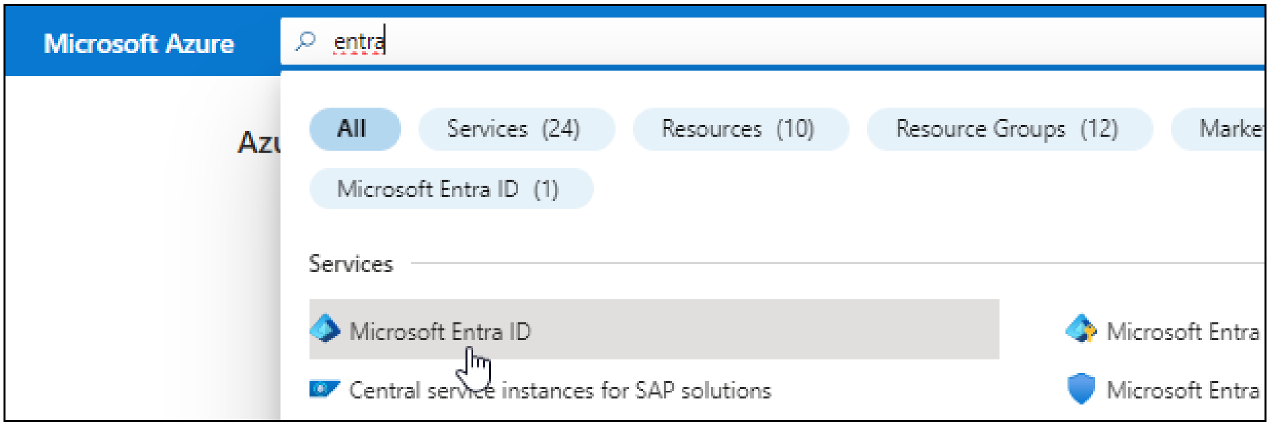
Create and set up a service principal in Microsoft Entra ID and obtain the Azure credentials that BlueXP needs. You'll need to provide BlueXP with these credentials after you install the Connector and set up BlueXP.

Create a Microsoft Entra 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 **Microsoft Entra ID** 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.

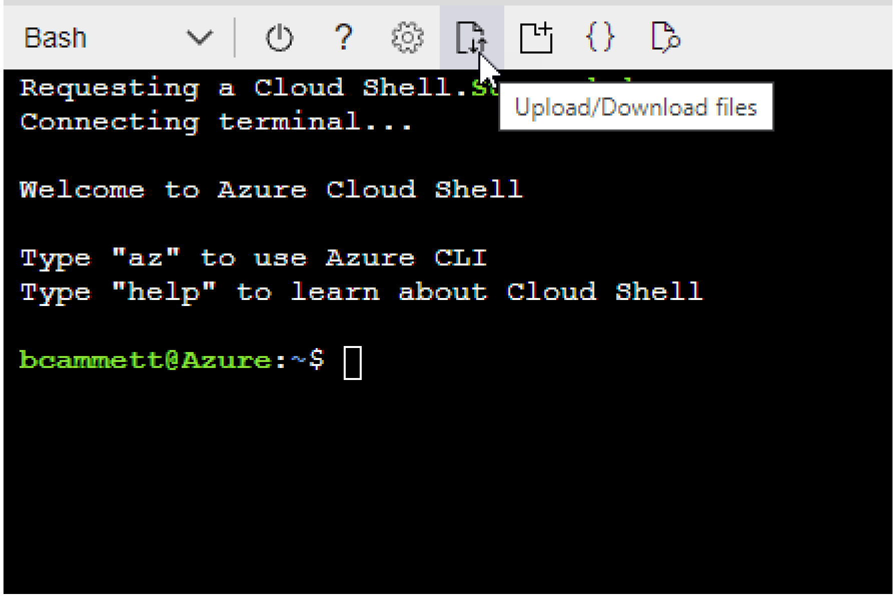
   Example

```
"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.



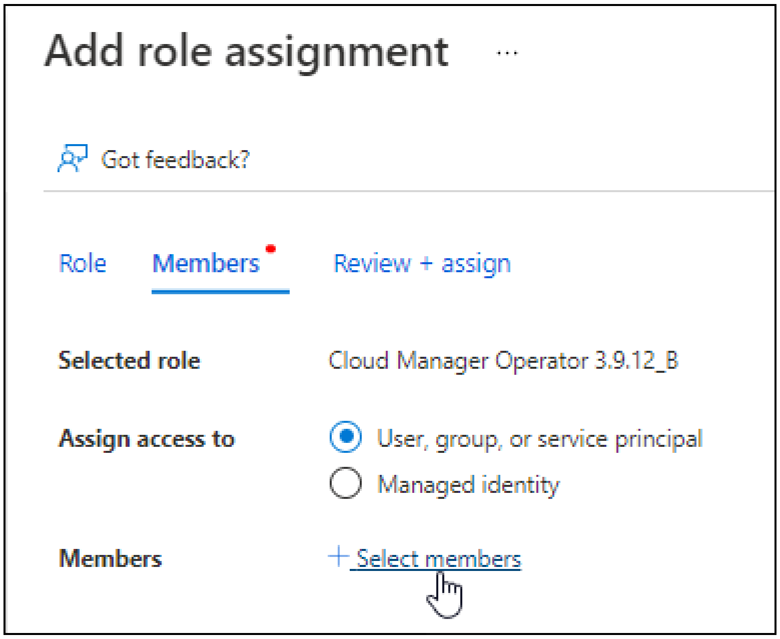
```
Requesting a Cloud Shell.Su
Connecting terminal...

Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

bcammett@Azure:~$
```

   - 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**.



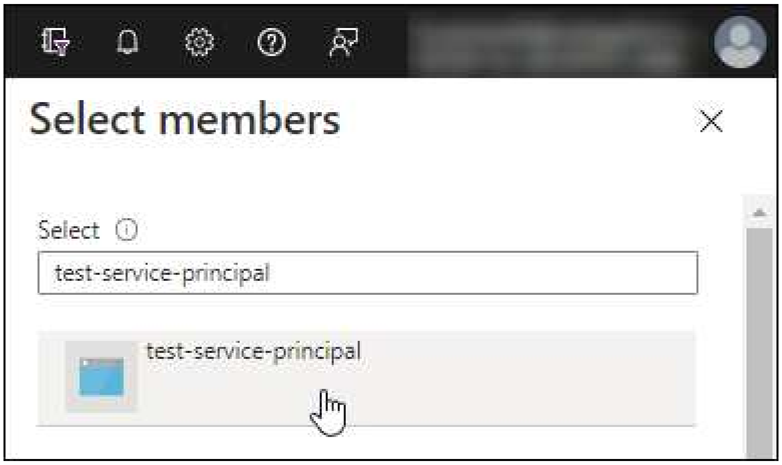
Selected role: Cloud Manager Operator 3.9.12_B

Assign access to: ● User, group, or service principal ○ Managed identity

Members

      - Search for the name of the application.

      Here’s an example:



Select ⓘ

test-service-principal

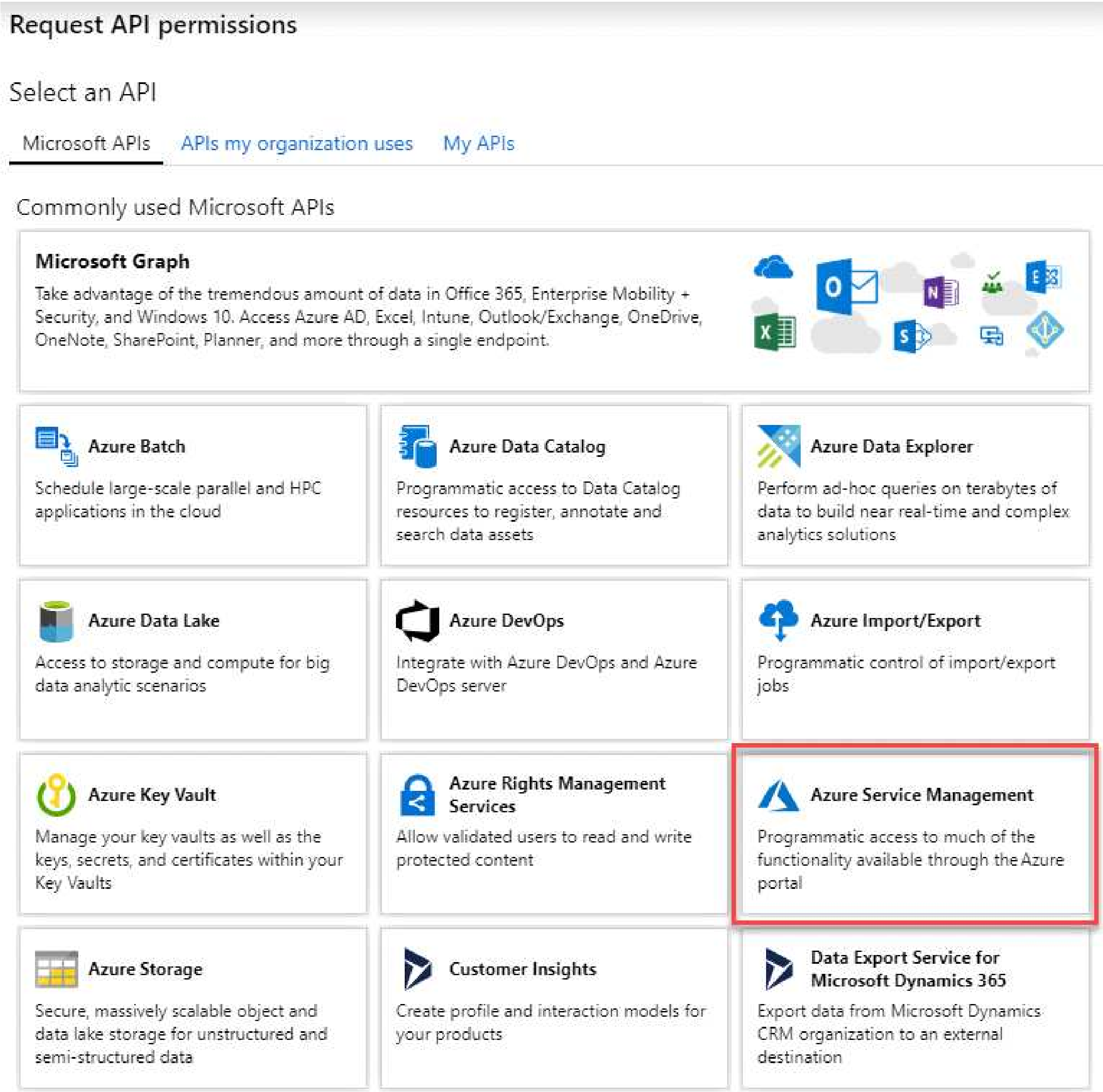
      - Select the application and select **Select**.
      - Select **Next**.
   f. Select **Review + assign**.

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



Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Batch
Schedule large-scale parallel and HPC applications in the cloud

Azure Data Catalog
Programmatic access to Data Catalog resources to register, annotate and search data assets

Azure Data Explorer
Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

Azure Data Lake
Access to storage and compute for big data analytic scenarios

Azure DevOps
Integrate with Azure DevOps and Azure DevOps server

Azure Import/Export
Programmatic control of import/export jobs

Azure Key Vault
Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Rights Management Services
Allow validated users to read and write protected content

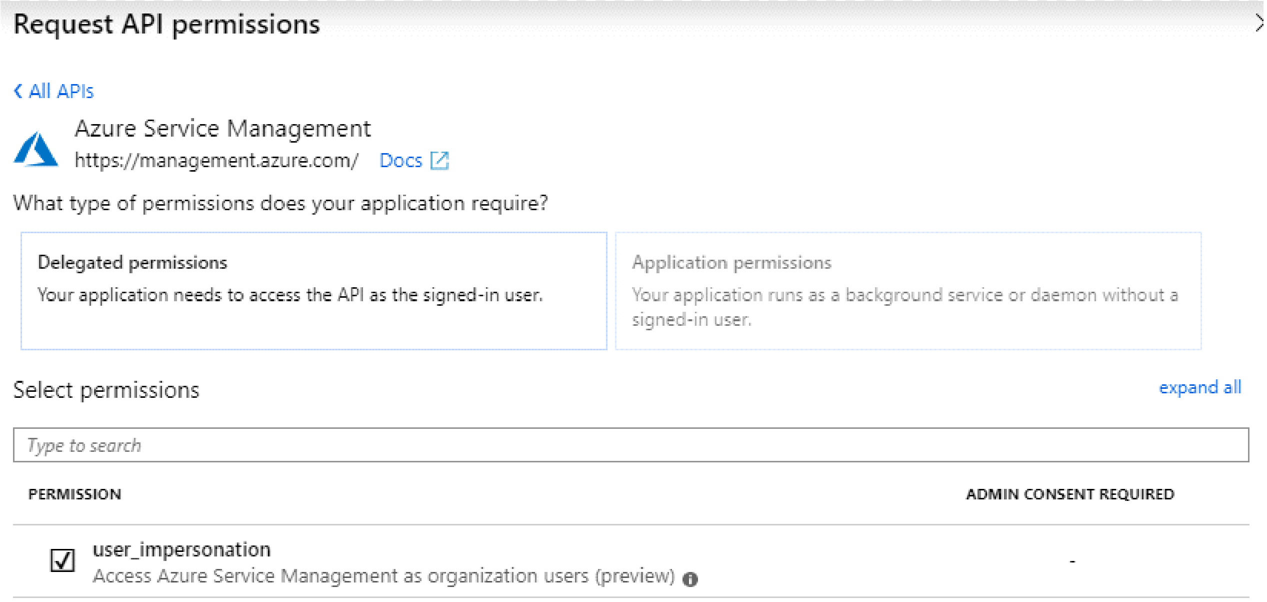
Azure Service Management
Programmatic access to much of the functionality available through the Azure portal

Azure Storage
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Customer Insights
Create profile and interaction models for your products

Data Export Service for Microsoft Dynamics 365
Export data from Microsoft Dynamics CRM organization to an external destination

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



Azure Service Management

https://management.azure.com/

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

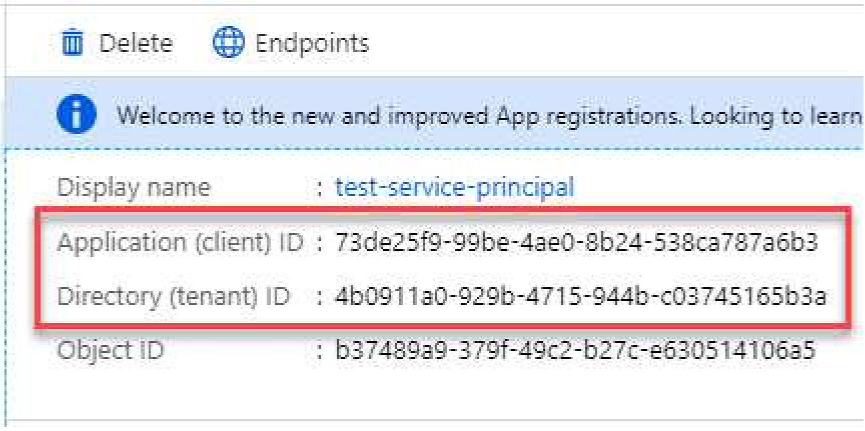
Select permissions

Type to search

PERMISSION	ADMIN CONSENT REQUIRED
☑ user_impersonation Access Azure Service Management as organization users (preview)	-

Get the application ID and directory ID for the application

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



Welcome to the new and improved App registrations. Looking to learn

Display name : test-service-principal

Application (client) ID : 73de25f9-99be-4ae0-8b24-538ca787a6b3

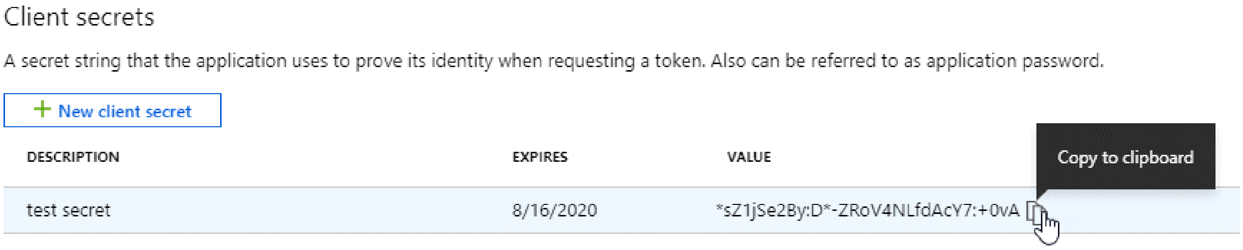
Directory (tenant) ID : 4b0911a0-929b-4715-944b-c03745165b3a

Object ID : b37489a9-379f-49c2-b27c-e630514106a5

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 **Microsoft Entra ID** 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.

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

You now have a client secret that BlueXP can use it to authenticate with Microsoft Entra ID.

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. 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 7: Enable Google Cloud APIs

You need to enable several APIs 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 software as a service (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

Before you begin

- Root privileges are required to install the Connector.
- Depending on your operating system, either Podman or Docker Engine is required before you install the Connector.

Steps

1. Download the Connector software from the NetApp Support Site

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

2. Copy the installer to the Linux host.
3. Assign permissions to run the script.

   ```
   chmod +x /path/BlueXP-Connector-offline-<version>
   ```

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

4. Run the installation script:

```
sudo /path/BlueXP-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.

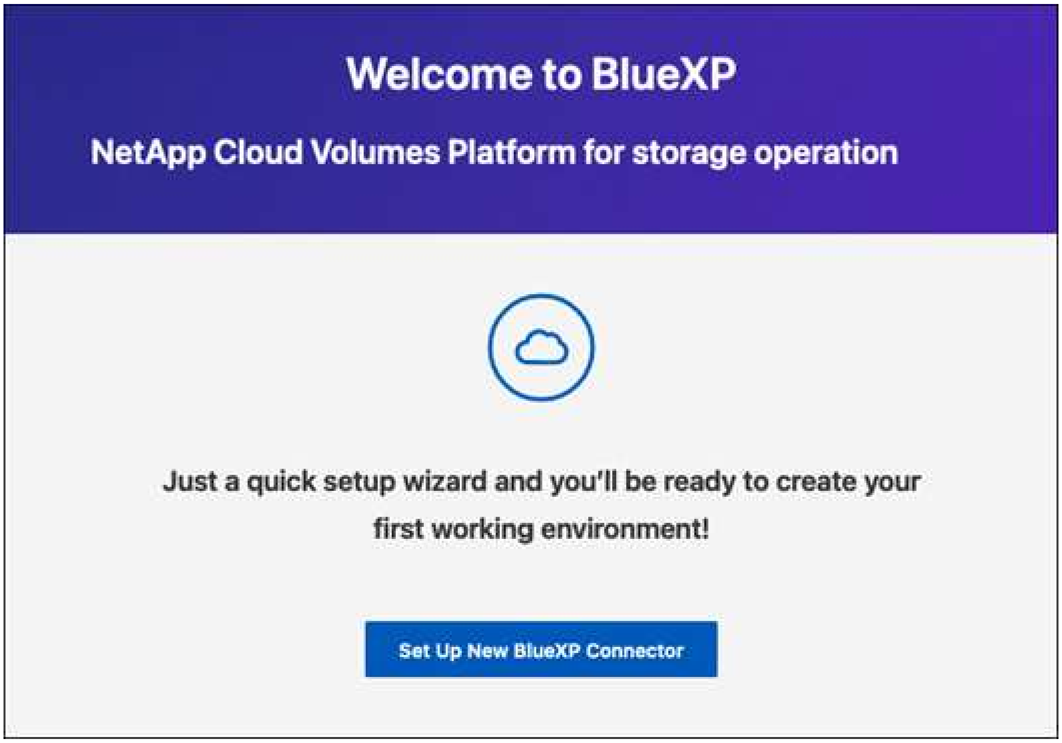
Step 2: Set up BlueXP

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.

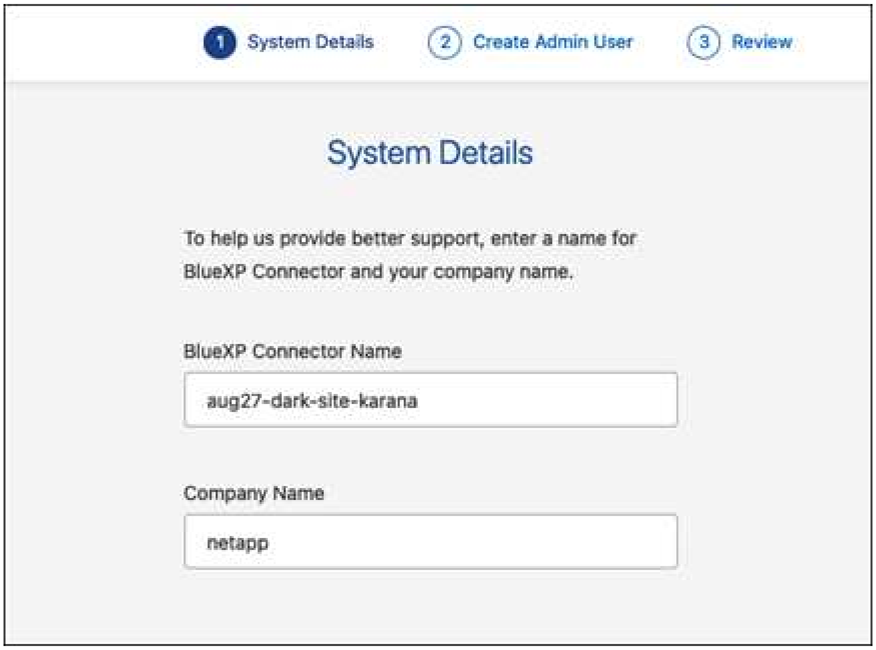


Welcome to BlueXP

NetApp Cloud Volumes Platform for storage operation

Just a quick setup wizard and you'll be ready to create your first working environment!

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.



System Details

To help us provide better support, enter a name for BlueXP Connector and your company name.

BlueXP Connector Name: aug27-dark-site-karana

Company Name: netapp

- **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

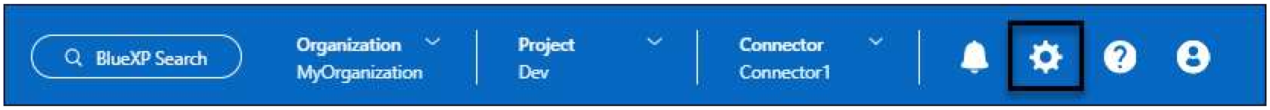
BlueXP now has the permissions that it needs to perform actions in AWS on your behalf.

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.

   It's important to assign the role from the **Subscriptions** service because this specifies the scope of the role assignment at the subscription level. The *scope* defines the set of resources that the access applies to. If you specify a scope at a different level (for example, at the virtual machine level), your ability to complete actions from within BlueXP will be affected.

   Microsoft Azure documentation: Understand scope for Azure RBAC

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, under **Managed identity**, 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

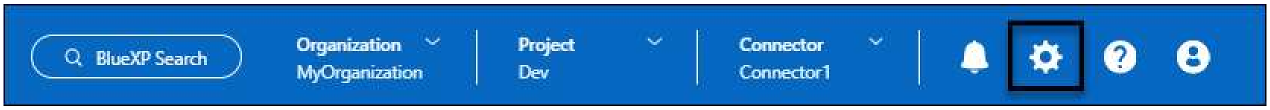
BlueXP now has the permissions that it needs to perform actions in Azure on your behalf.

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 Microsoft Entra 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:

- Discover on-premises ONTAP clusters
- Manage software updates
- Scan on-premisesONTAP volume data using BlueXP classification
- Monitor license usage with digital wallet
- View storage health information with digital advisor

Copyright information

Trademark information