NetApp

Learn the basics

Set up and administration

NetApp
April 04, 2023

Table of Contents

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 SaaS platform includes storage and data 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

The BlueXP platform provides four main pillars of data management: storage, mobility, protection, and analysis and control.

Storage

Discover, deploy, and manage storage, whether it's in AWS, Azure, Google Cloud, or on premises.

- Set up and use Cloud Volumes ONTAP for efficient, multi-protocol data management across clouds.
- Set up and use cloud file-storage services:
    - Azure NetApp Files
    - Amazon FSx for ONTAP
    - Cloud Volumes Service for Google Cloud
- Discover and manage on-premises storage:
    - E-Series systems
    - ONTAP clusters
    - StorageGRID systems

Mobility

Move data where it's needed by syncing, copying, tiering, and caching data.

- Cloud Sync
- Cloud Tiering
- Global File Cache

Protection

Use automated protection mechanisms to protect data against data loss, unplanned outages, ransomware, and other cyber threats.

- Cloud Backup
- Replication
- Ransomware Protection
- Kubernetes

Analysis and control

Use tools to monitor, map, and optimize your data storage and infrastructure.

- Cloud Data Sense
- Digital Advisor

Learn more about how you can use BlueXP to help your organization

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 plan to use. Learn about BlueXP pricing

How BlueXP works

BlueXP includes a web-based console that's provided through the SaaS layer, accounts that provide multi-tenancy, and Connectors that manage Cloud Volumes ONTAP and other cloud services.

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 accounts and Connectors.

BlueXP account

When you log in to BlueXP for the first time, you're prompted to create a *BlueXP account*. This account provides multi-tenancy and enables you to organize users and resources in isolated *workspaces*.

Learn more about accounts.

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 the management of resources and processes across your on-premises and cloud environments. It's required to use Cloud Volumes ONTAP and other data services.

Learn more about Connectors.

Restricted mode and private mode

BlueXP is also supported in environments that have security and connectivity restrictions. You can use *restricted mode* or *private mode* to 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, Cloud Sync, Cloud
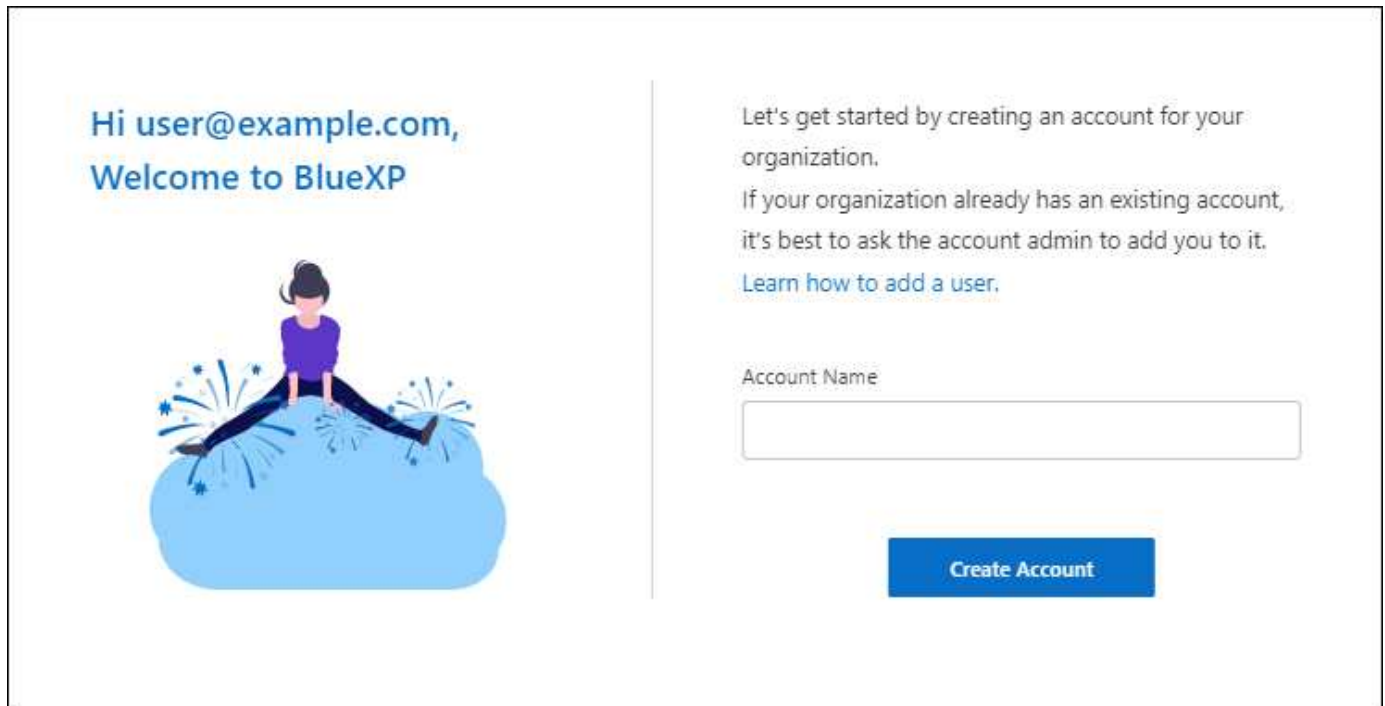
Tiering, Cloud Data Sense, and Cloud Backup (BlueXP platform), and affirmed that they have achieved SOC 2 Type 2 reports based on the applicable Trust Services criteria.

View NetApp's SOC 2 reports

Learn about BlueXP accounts

A *BlueXP account* provides multi-tenancy and enables you to organize users and resources in isolated workspaces from within BlueXP. For example, multiple users can deploy and manage Cloud Volumes ONTAP systems in isolated environments called *workspaces*. These workspaces are invisible to other users, unless they are shared.

When you first access BlueXP, you're prompted to select or create an account. For example, you'll see the following screen if you don't have an account yet:

BlueXP Account Admins can then modify the settings for this account by managing users (members), workspaces, and Connectors:

Learn how to manage your BlueXP account.

Deployment modes

BlueXP offers the following deployment modes for your account: standard mode, restricted mode, and private mode. These modes support environments that have varying levels of security and connectivity restrictions.

Learn more about BlueXP deployment modes.

Members

Members are BlueXP users that you associate with your BlueXP account. Associating a user with an account and one or more workspaces in that account enables those users to create and manage working environments in BlueXP.

When you associate a user, you assign them a role:

- *Account Admin*: Can perform any action in BlueXP.
- *Workspace Admin*: Can create and manage resources in the assigned workspace.
- *Compliance Viewer*: Can only view Cloud Data Sense compliance information and generate reports for systems that they have permission to access.

Learn more about these roles.

Workspaces

In BlueXP, a workspace isolates any number of *working environments* from other users in the account. Workspace Admins can't access the working environments in a workspace unless the Account Admin associates the admin with that workspace.

A working environment represents a storage system. For example:

- A Cloud Volumes ONTAP system
- An on-premises ONTAP cluster
- A Kubernetes cluster

Learn how to add a workspace.

Connectors

A Connector executes the actions that BlueXP needs to perform in order to manage your data infrastructure. The Connector runs on a virtual machine instance that you deploy in your cloud provider or on an on-premises host that you configured.

You can use a Connector with more than one BlueXP service. For example, if you're using a Connector to manage Cloud Volumes ONTAP, you can use that same Connector with another service like Cloud Tiering.

Learn more about Connectors.

Examples

The following examples depict how you might set up your accounts.

> (i) In both example images that follow, the Connector and the Cloud Volumes ONTAP systems don't actually reside *in* the BlueXP account—they're running in a cloud provider. This is a conceptual representation of the relationship between each component.

Multiple workspaces

The following example shows an account that uses two workspaces to create isolated environments. The first workspace is for a production environment and the second is for a dev environment.

Multiple accounts

Here's another example that shows the highest level of multi-tenancy by using two separate BlueXP accounts. For example, a service provider might use BlueXP in one account to provide services for their customers, while using another account to provide disaster recovery for one of their business units.

Note that account 2 includes two separate Connectors. This might happen if you have systems in separate regions or in separate cloud providers.

Learn about Connectors

A *Connector* is NetApp software running in your cloud network or on-premises network. It executes the actions that BlueXP needs to perform in order to manage your data infrastructure. The Connector constantly polls the BlueXP SaaS layer for any actions that it needs to take. 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.

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 working environment creation

  While a Connector isn't required to create a working environment, it is required to create and manage volumes, replicate data, and integrate FSx for ONTAP with BlueXP services, such as Data Sense and Cloud Sync.

- 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 Cloud Data Sense to scan Azure NetApp Files data.

- Cloud Sync

- Cloud Volumes Service for Google Cloud

- Digital Advisor

- Digital Wallet

  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-prem ONTAP clusters

When a Connector is required

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

- Amazon FSx for ONTAP management features
- Amazon S3 discovery
- Azure Blob discovery
- Cloud Backup
- Cloud Data Sense
- Cloud Tiering
- Cloud Volumes ONTAP
- E-Series systems
- Global File Cache
- Google Cloud Storage discovery
- Kubernetes clusters
- On-premises ONTAP cluster integration with BlueXP data services
- StorageGRID

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, may be
adversely impacted.

Impact on Cloud Volumes ONTAP

A Connector is a key component in the health and operation of Cloud Volumes ONTAP. If a Connector is powered down, Cloud Volumes ONTAP PAYGO systems and capacity-based BYOL systems shut down after losing communication with a Connector for longer than 14 days. This happens because the Connector refreshes licensing on the system each day.

If your Cloud Volumes ONTAP system has a node-based BYOL license, the system remains running after 14 days because the license is installed on the Cloud Volumes ONTAP system.

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

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 create a Connector

A BlueXP Account Admin can create 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
- Quick start for BlueXP in standard mode
- Quick start for BlueXP in restricted mode
- Quick start for 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. There's nothing else that you need to

do.

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

- Standard mode
    - Set up AWS permissions
    - Set up Azure permissions
    - Set up Google Cloud permissions
    - Set up cloud permissions for on-prem deployments
- Set up cloud permissions for restricted mode
- Set up cloud permissions for private mode

To view the exact permissions that the Connector needs, 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

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 and functionalities are dependent on the version of the Connector. That includes Cloud Volumes ONTAP management, on-prem ONTAP cluster management, settings, and help.

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

Operating system and VM maintenance

Maintaining the operating system on the Connector host is your responsibility. For example, you 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 don't need to stop any services on the Connector host when running an OS update.

If you 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

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.

Multiple Connectors

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 multi-cloud environment (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 account to provide services for their customers, while using another account to provide disaster recovery for one of their business units. Each account would have separate Connectors.

When to switch

When you create your first Connector, BlueXP automatically uses that Connector for each additional working environment that you create. Once you create an additional Connector, you'll need to switch between them to see the working environments that are specific to each Connector.

Learn how to switch between Connectors.

Disaster recovery

You can manage a working environment with multiple Connectors at the same time for disaster recovery purposes. If one Connector goes down, you can switch to the other Connector to immediately manage the working environment.

To set up this configuration:

1. Switch to another Connector.
2. Discover the existing working environment.
   - Add existing Cloud Volumes ONTAP systems to BlueXP
   - Discover ONTAP clusters
3. Set the Capacity Management Mode

   Only the main Connector should be set to **Automatic Mode**. If you switch to another Connector for DR purposes, then you can change the Capacity Management Mode as needed.

BlueXP deployment modes

BlueXP offers multiple *deployment modes* that enable you to use BlueXP in a way that meets your business and security requirements. *Standard mode* leverages the BlueXP 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.

Overview

BlueXP offers the following deployment modes for your account. Each mode differs in terms of outbound connectivity requirements, deployment location, installation process, authentication method, available data and storage services, and charging methods.

Standard mode

BlueXP is accessible to users as a cloud service from the web-based console. Depending on the BlueXP services that you're planning 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

A BlueXP Connector is installed in the cloud (in a government region, sovereign cloud region, or commercial region) and has limited outbound connectivity to the BlueXP SaaS layer. Users access BlueXP locally from the web-based console that's available from the Connector, not from the 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

A BlueXP Connector is installed 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 BlueXP locally from the web-based console that's available from the Connector, not from the SaaS layer.

A secure region includes AWS C2S and SC2S 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 BlueXP SaaS layer	The Connector

	Standard mode	**Restricted mode**	**Private mode**
Authentication	Through SaaS using auth0, NSS login, or identity federation	Through SaaS using auth0 or identity federation	Local user authentication
Storage and data services	All are supported	Many are supported	Several are supported
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.
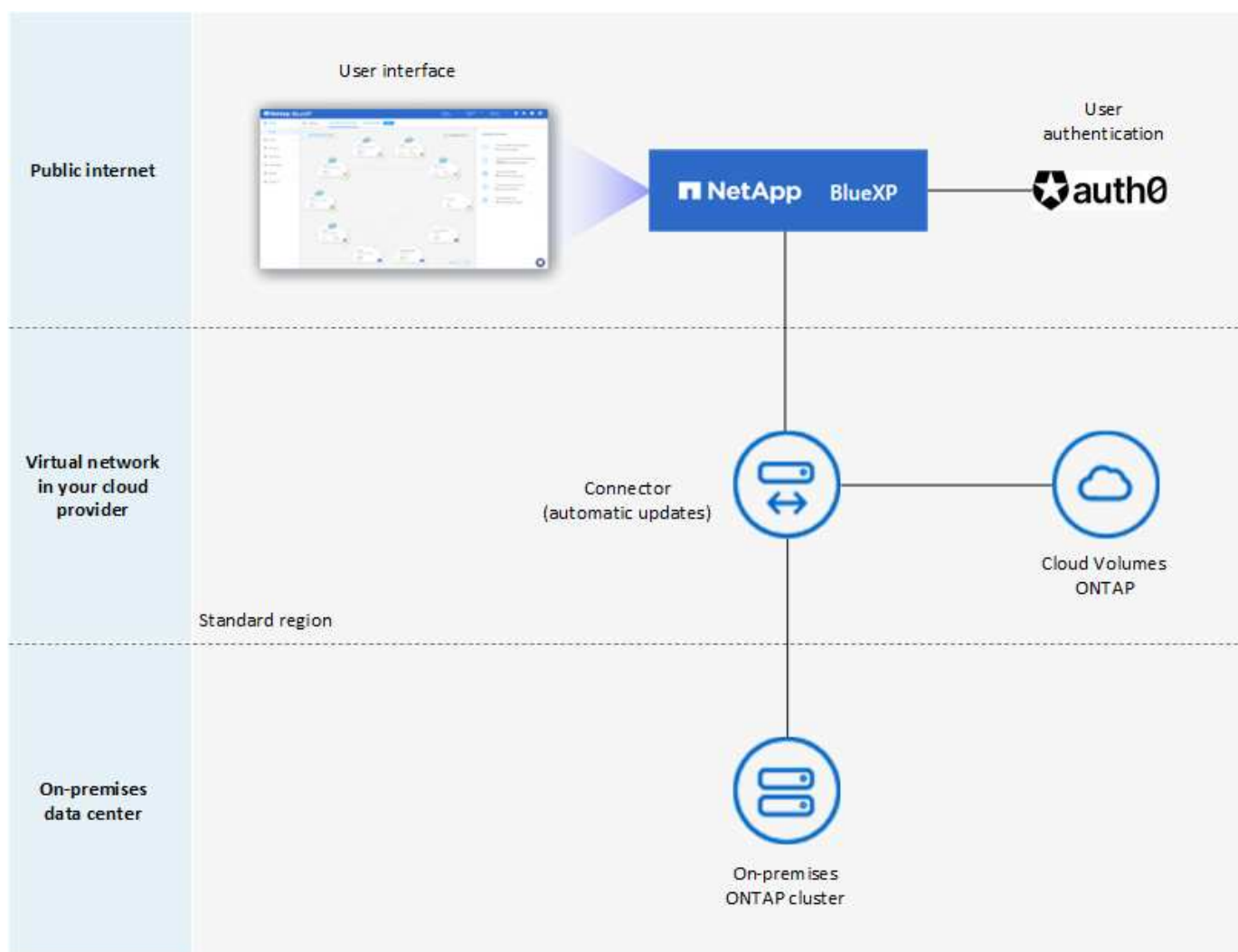
BlueXP works as follows in standard mode:

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

Connector installation is possible from a setup wizard in BlueXP, from the AWS or Azure Marketplace, or using an installer to manually install the Connector on your own Linux host in your data center or in the cloud.

Connector upgrades

Automated upgrades of the Connector software are available from BlueXP 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

Authentication is provided through BlueXP's cloud service using auth0 or through 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.

BlueXP works as follows in restricted mode:

Outbound communication

Outbound connectivity is required from the Connector to the BlueXP SaaS layer to use BlueXP data services, to enable automatic software upgrades of the Connector, to use auth0-based authentication, and to send metadata for charging purposes (storage VM name, allocated capacity, and volume UUID, type, and IOPS).

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

Automated upgrades of the Connector software are available from BlueXP with monthly updates.

User interface access

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

API endpoint

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

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
Amazon FSx for ONTAP	Full support
Azure NetApp Files	Full support
Cloud Backup	Supported in Government regions and commercial regions with restricted mode. Not supported in sovereign regions with restricted mode. The following features are not supported: Applications, Virtual Machines, and Kubernetes.
Cloud Data Sense	Supported in Government regions with restricted mode. Not supported in commercial regions or in sovereign regions with restricted mode. The following limitations apply: • OneDrive accounts, SharePoint accounts, and Google Drive accounts can't be scanned. • Microsoft Azure Information Protection (AIP) label functionality can't be integrated.
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-prem cluster 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 account yet, you'll be prompted to create your account 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.

If you already have an account and you want to create another one, then you need to use the Tenancy API.

Note that you can't change the restricted mode setting after BlueXP creates the account. You can't enable restricted mode later and you can't disable it later. It must be set at time of account creation.

- Learn how to get started with restricted mode.
- Learn how to create an additional BlueXP account.

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.

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.

BlueXP works as follows in private mode:

Outbound communication

No outbound connectivity is required. 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
Cloud Backup	Supported in AWS and Azure commercial regions. Not supported in Google Cloud or in AWS C2S/SC2S or Azure IL6
Cloud Volumes ONTAP	Because there's no internet access, the following features aren't available: automated software upgrades, AutoSupport, and AWS cost information.
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-prem deployments

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

Supported services	Notes
Cloud Backup	Only back up and restore of on-prem ONTAP volumes to StorageGRID systems is supported. Learn how to back up on-prem ONTAP data to StorageGRID

Cloud Data Sense	• 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 will need to manually upload your Cloud Volumes ONTAP licensing file in the Digital Wallet.

Learn how to add licenses to the 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.

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.

BlueXP service or feature	Restricted mode	Private mode
Amazon FSx for ONTAP	Yes	No
Amazon S3	No	No
AppTemplate	No	No
Azure Blob	No	No
Azure NetApp Files	Yes	No

BlueXP service or feature	Restricted mode	Private mode
Cloud Backup	Yes	Yes
Cloud Data Sense	Yes	Yes
Cloud Sync	No	No
Cloud Tiering	No	No
Cloud Volumes ONTAP	Yes	Yes
Cloud Volumes Service for Google Cloud	No	No
Compute	No	No
Digital Advisor	No	No
Digital Wallet	Yes	Yes
E-Series	No	No
Economic efficiency	No	No
Global File Cache	No	No
Google Cloud Storage	No	No
Kubernetes clusters	No	No
On-prem ONTAP clusters	Yes	Yes
Operational resiliency	No	No
Ransomware Protection	No	No
Replication	Yes	Yes
StorageGRID	No	No
Credentials	Yes	Yes
NSS accounts	Yes	No
Notifications	Yes	No
Timeline	Yes	Yes