NetApp

Release notes

NetApp Console setup and administration

NetApp
January 27, 2026

Table of Contents

Release notes

What's new

Learn what's new with NetApp Console administration features: identity and access management (IAM), Console agents, cloud provider credentials, and more.

13 January 2026

Console agent 4.3.0

The 4.3.0 release supports both standard mode and restricted mode.

This release of the Console agent includes security improvements, bug fixes, and the following features:

Ability to validate network connections of Console agents

You can now validate network connections of connected Console agents directly from the NetApp Console. This feature helps verify connectivity and troubleshoot issues with Console agents. This is in addition to the existing ability to run network diagnostics from the Console agent maintenance console command line interface (CLI).

Learn how to run configuration from NetApp Console.

NetApp Console administration

This release includes the following:

Role-Based Access for Federated Groups in NetApp Console

NetApp Console supports assigning roles to federated groups (for example, Active Directory groups), allowing administrators to automate user onboarding and offboarding based on group membership in the organization's identity provider (IdP). This feature reduces administrative overhead, and ensures secure, consistent access by instantly updating Console access as group memberships change.

Learn how to provide access to a federated group to your organization.

Support for federation when NetApp Console is in restricted mode

You can now enable federation for a NetApp Console organization that is in restricted mode. This allows users to log in to the Console using their corporate credentials while maintaining the security benefits of restricted mode.

Read-only mode

You can set a NetApp Console organization to read-only mode. In read-only mode, users can view resources and settings but cannot make any changes. An Org admin or Super admin can enable read-only mode for an organization. When read-only mode is enabled, users with administrative roles must manually elevate their permissions to make changes as needed.

Learn how to enable read-only mode for a Console organization.

Learn how to elevate your role when your organization is in read-only mode.

10 December 2025

Console agent 4.2.0

The 4.2.0 release supports both standard mode and restricted mode.

This release of the Console agent includes security improvements, bug fixes, and the following features:

Support for Google Cloud Infrastructure Manager

NetApp now uses Google Cloud Infrastructure Manager (IM) instead of Google Cloud Deployment Manager to deploy agents and manage agents in Google Cloud. This change was made because Google will be deprecating Cloud Deployment Manager.

- Any new agents 4.2.0 and higher use Infrastructure Manager and you should update both the user account and service account permissions used for deployment. View the permissions change log.

- When you deploy an agent, the system also creates a Google Cloud bucket to store deployment files.

Improved configuration checks for Console agents

- The Console agent now checks for deprecated endpoints when performing a configuration check. If you have not updated to the new endpoint list for 4.0.0 or higher, installations succeed if the system can reach the previous endpoint list. Learn more about the required endpoints for Console agents.

- Run configuration checks on installed Console agents from the Console or Agent maintenance console to verify connectivity and troubleshoot issues. Learn how to run configuration checks on Console agents.

Directly download agent software from NetApp Console

When you need to manually install an agent, you can access agent software directly from the NetApp Console in addition to the NetApp Support site. Learn how to download the Console agent software directly from the NetApp Console.

NetApp Console administration

This release includes the following:

Ability to set notifications for expiring credentials

Set notifications for expiring credentials on service accounts and federations. Choose between seven or 30 days. The Console displays notifications and emails users with the appropriate role. Org admins receive service account notifications. Org admins, Federation admins, and Federation viewers receive federation notifications.

Local logins are not available after enabling federation

After you turn on federation for a Console organization, users cannot use local logins and are sent to federation logins.

Usability enhancements for the Storage management pages

Detailed information about your ONTAP on-premises systems (and FSx for ONTAP) is now easier to view and manage from the Storage management pages.

- The **Discoverable systems** page separates the summary information from the tabbed display of available systems, making it easier to view comprehensive information about discoverable systems.

10 November 2025

Console agent 4.1.0

This release of the Console agent includes security improvements, bug fixes, and the following features:

The 4.1.0 release is available for standard mode and restricted mode.

Renamed Agent status indicators

Renamed the status indicators for the Console agent from **Active** and **Inactive** to **Connected** and **Disconnected** to make their purpose more clear.

Support for Red Hat Enterprise Linux (RHEL) 9.6 and Podman 5.4.0

When manually installing a Console agent, the agent now supports RHEL 9.6 with Podman 5.4.0. In addition, when using RHEL 9 and higher, NetApp supports podman-compose 1.5.0. View operating system requirements.

NetApp Console administration

This release includes the following:

New email address for NetApp Console notifications

The email address that sends NetApp Console notifications has changed to **service@console.netapp.com** from **service@console.bluexp.netapp.com**. NetApp recommends updating any email rules to allow **service@console.netapp.com** to ensure you continue to receive NetApp Console email notifications.

## 06 October 2025

BlueXP is now NetApp Console

The NetApp Console, built on the enhanced and restructured BlueXP foundation, provides centralized management of NetApp storage and NetApp Data Services across on-premises and cloud environments at enterprise grade—delivering real-time insights, faster workflows, and simplified administration that is highly secure and compliant.

Navigation menus and pages

NetApp moved most menu options to the left-navigation pane and reorganized menus for easier navigation in the NetApp Console.

Canvas is replaced by the Systems page

NetApp renamed the Canvas to the **Systems** page. Navigate to the **Systems** page from the **Storage > Management** menu.
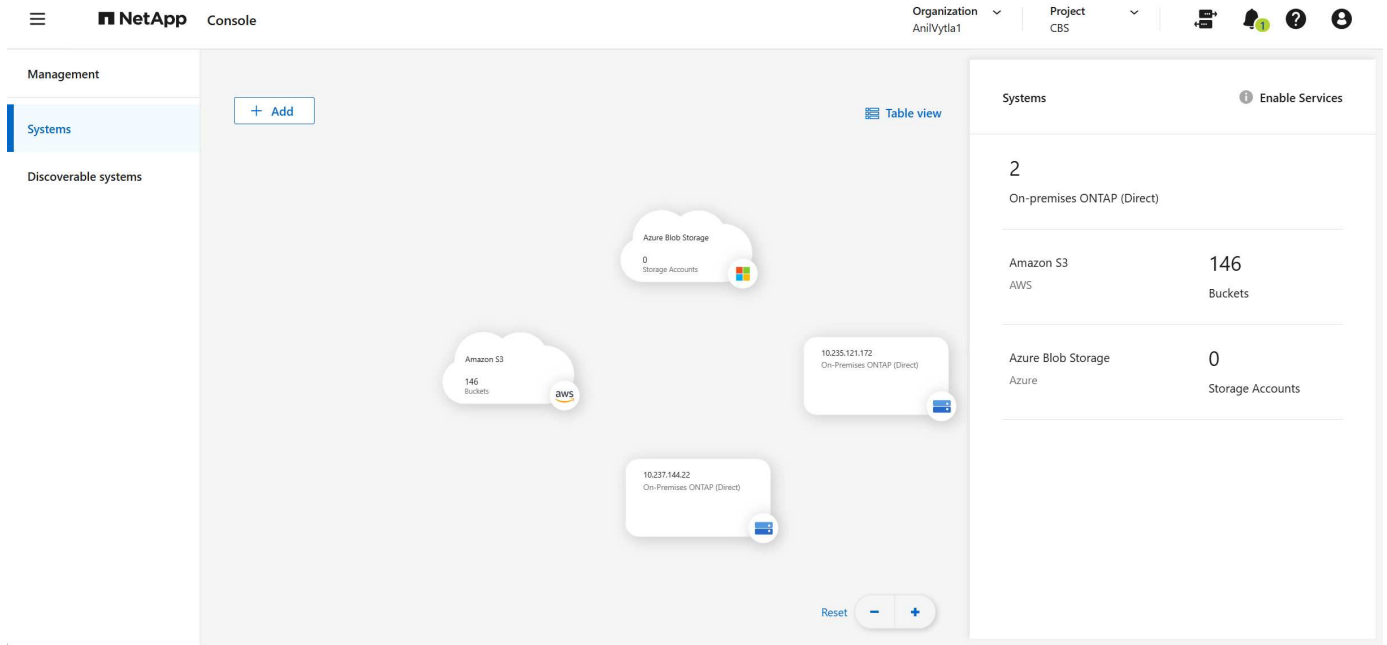
Expanded Storage menu

The **Storage** menu includes **Alerts** to view ONTAP system alerts and **Lifecycle planning** (formerly **Economic efficiency**) to identify unused or underutilized resources.

NetApp has moved Keystone to the **Storage** menu, where you can manage your NetApp Keystone subscriptions and view your usage.

Administration menu

Use the centralized **Administration** menu to manage the NetApp Console, support cases, licenses, and subscriptions (previously called digital wallet).

Home

Storage

Protection

Governance

Health

Workloads

Mobility

Administration

Licenses and subscriptions
Manage and monitor data service marketplace subscriptions, direct licenses, and billing.

Support
Submit and manage support cases.

Identity and access
Manage users, roles, permissions and authentications methods.

Agents
Provision cloud-scale networking and compute, with flexibility and ease of management access.

Credentials
Add and manage organizational-level and user-level credentials.

**Notification settings**
Manage how notifications are sent and when.

Audit
Audit user and API actions taken in your NetApp organization.

Health menu

An efficient **Health** menu includes **Software updates** where you can manage ONTAP software updates, **Sustainability** where you can monitor your environmental impact, and **Digital Advisor** where you can get proactive recommendations to optimize your storage environment.
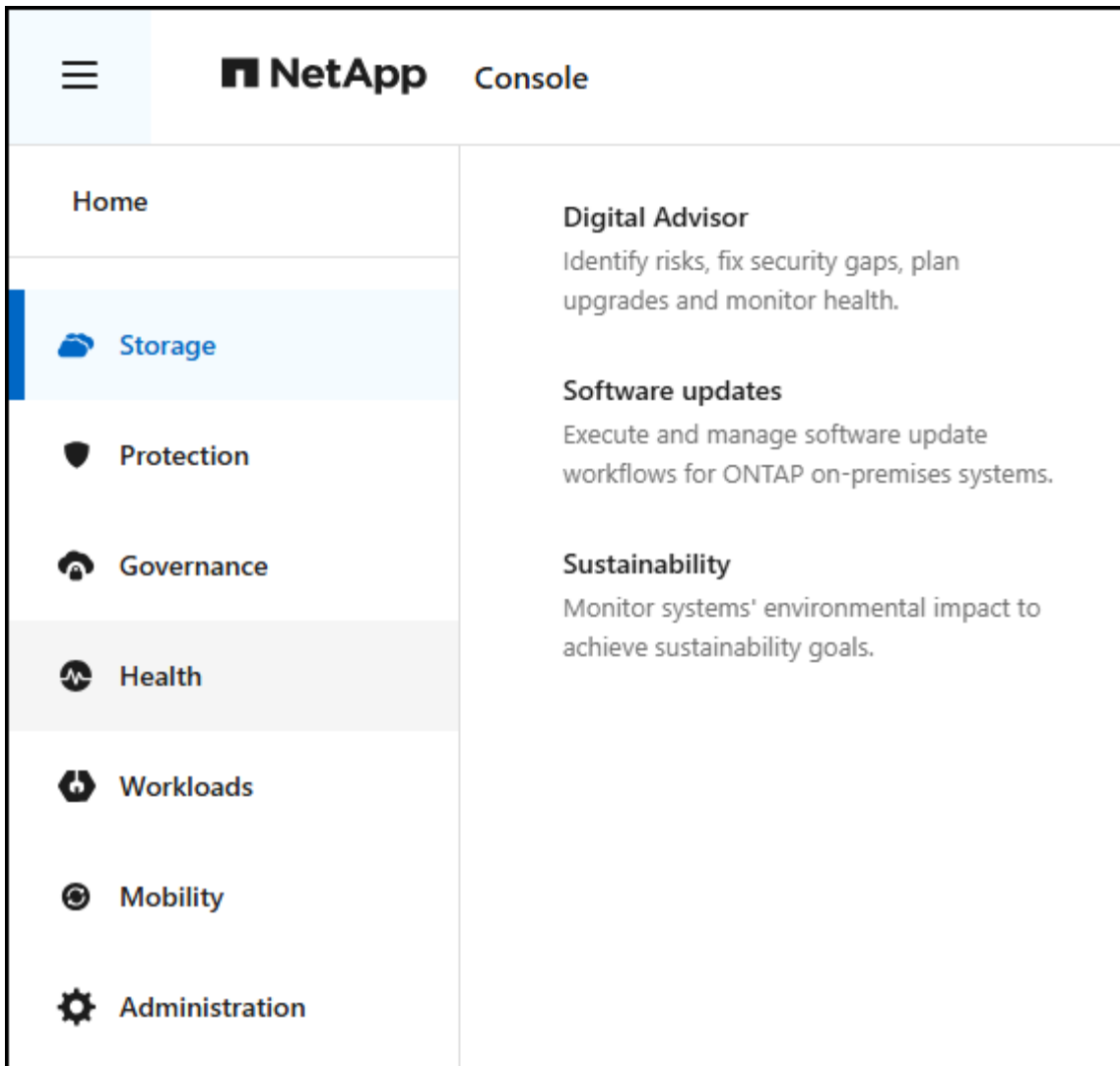
Governance menu

The **Governance** menu includes **Data Classification** where you can manage data classification and compliance and the **Automation hub** where you can create and manage automation workflows.
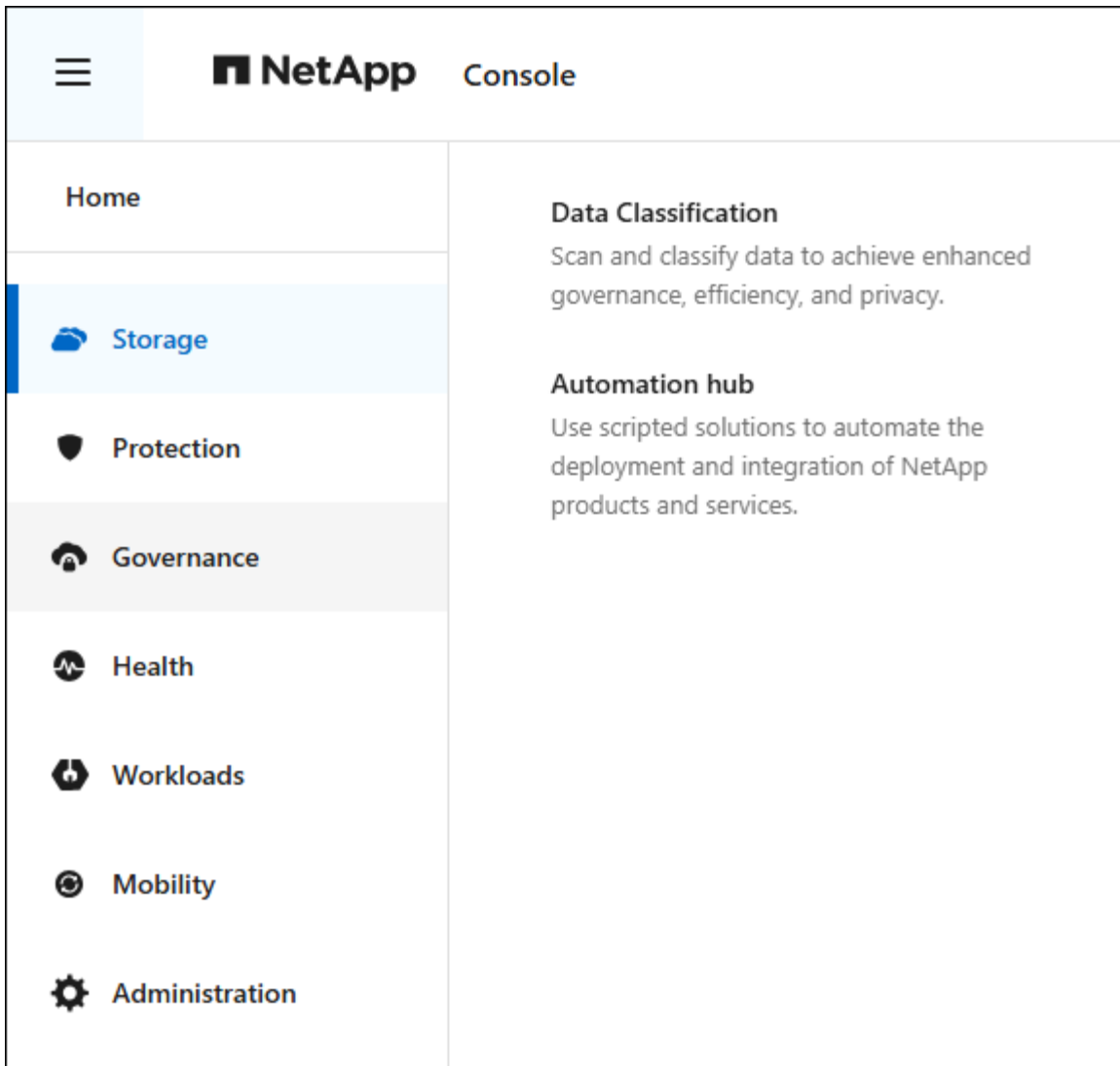
More intuitive naming of elements, data services, and features

NetApp renamed several elements, data services, and features to clarify their purpose. Key changes include:

Previous name	NetApp Console name
Connectors	Console agents. View, add, and manage your agents from the **Administration > Agents** menu.
Timeline page	Audit page View audit Console activity from the **Administration > Audit** menu.
Working environments	Systems View, add, and manage your systems from the **Storage > Management** menu.

Previous name	NetApp Console name
BlueXP Ransomware protection	NetApp Ransomware Resilience. Ransomware Resilience helps you protect your data and recover quickly from a ransomware attack.
BlueXP Economic Efficiency	Lifecycle planning. Lifecycle planning helps you optimize your storage costs by identifying unused and underutilized resources. Access Lifecycle planning from the **Storage > Lifecycle planning** menu.
BlueXP digital wallet	Licenses and subscriptions Access your licenses and subscriptions from the **Administration > Licenses and subscriptions** menu.

Console agents

Access and manage your Console agents from the **Administration > Agents** menu. NetApp has changed how to select a Console agent for the **Systems** page (formerly the Canvas). NetApp has replaced the Connector menu name with an icon , allowing you to select the Console agent that you want to view systems for.
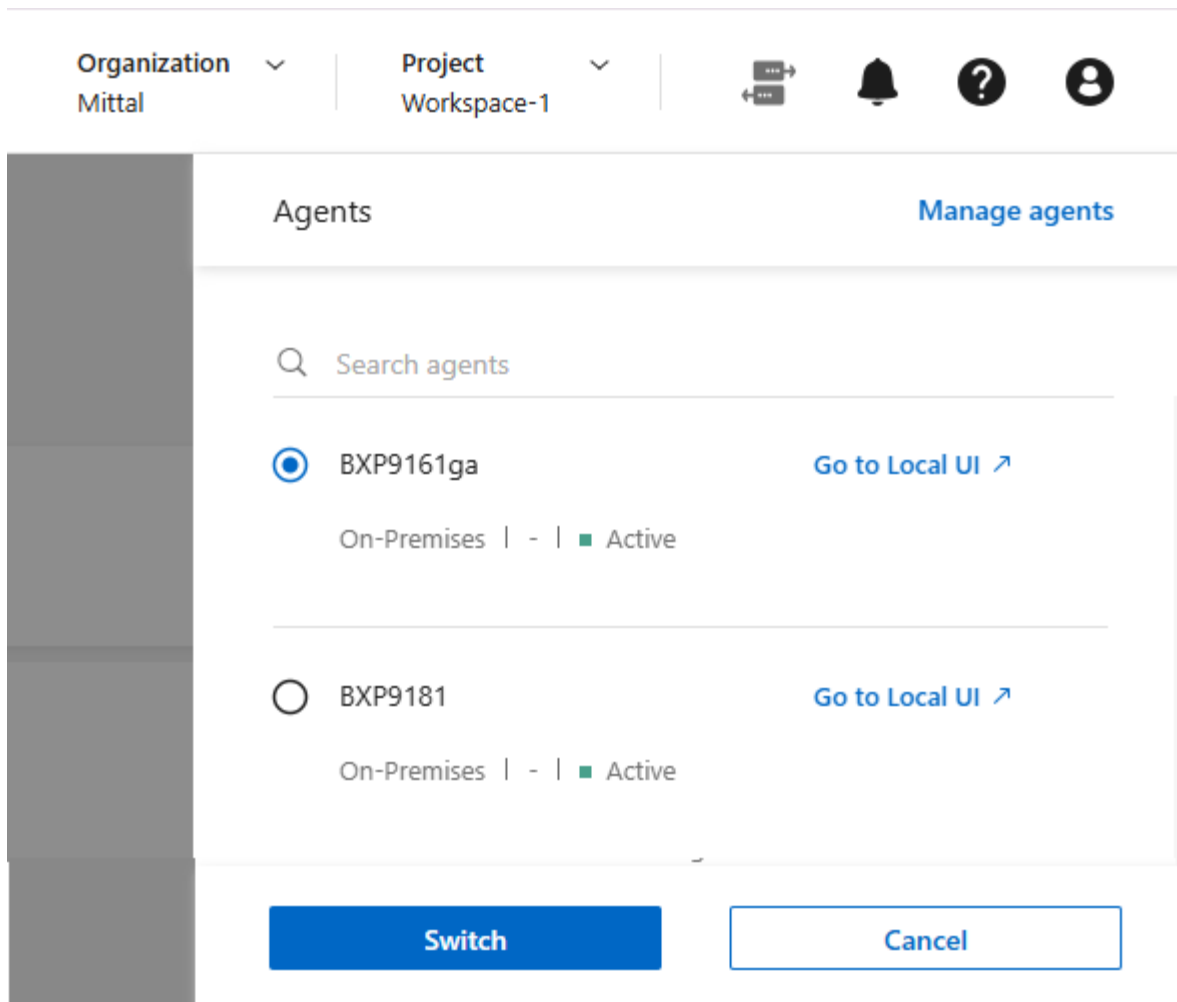
You can also manage your agents from the **Administration > Agents** menu.

Console agent 4.0.0

This release of the Console agent includes security improvements, bug fixes and the following new features.

The 4.0.0 release is available for standard mode and restricted mode.

Consolidation and reduction of required network endpoints

NetApp has reduced the required network endpoints for the Console and Console agents, enhancing security and simplifying deployment. Importantly, all deployments prior to version 4.0.0 continue to be fully supported. While previous endpoints remain available for existing agents, NetApp strongly recommends updating firewall rules to the current endpoints after confirming successful agent upgrades.

- Learn how to update your endpoint list and view a comparison.
- Learn more about required endpoints.

Support for VCenter deployment of Console agents

You can deploy Console agents in VMware environments using an OVA file. The OVA file includes a pre-configured VM image with Console agent software and settings to connect to the NetApp Console. A file download or URL deployment is available directly from the NetApp Console. Learn how to deploy a Console agent in VMware environments.

The Console agent OVA for VMware offers a pre-configured VM image for quick deployment.

Validation reports for failed agent deployments

When you deploy a Console agent from the NetApp Console, you now have the option to validate the agent configuration. If the Console fails to deploy the agent, it provides a downloadable report to help you troubleshoot.

Improved troubleshooting for Console agents

The Console agent has improved error messages that help you better understand issues. Learn how to troubleshoot Console agents.

NetApp Console

NetApp Console administration includes the following new features:

Home page dashboard

The NetApp Console's Home page dashboard provides real-time visibility into storage infrastructure with metrics for health, capacity, license status, and data services. Learn more about the Home page.

NetApp assistant

New users with the Organization admin role can use the NetApp assistant to configure the Console, including adding an agent, linking a NetApp Support account, and adding a storage system. Learn about the NetApp assistant.

Service account authentication

The NetApp Console supports service account authentication using either a system-generated client ID and secret or customer-managed JWTs, allowing organizations to select the approach that best fits their security requirements and integration workflows. Private Key JWT Client Authentication uses asymmetric cryptography, providing stronger security than traditional client ID and secret methods. Private Key JWT Client Authentication uses asymmetric cryptography, keeping the private key secure in the customer's environment, reducing credential theft risks, and improving the security of your automation stack and client applications. Learn how to add a service account.

Session timeouts

The system logs out users after 24 hours or when they close their web browser.

Support for partnerships between organizations

You can create partnerships in the NetApp Console that let partners securely manage NetApp resources across organizational boundaries, making collaboration easier and security stronger. Learn how to manage partnerships.

Super admin and Super viewer roles

Added the **Super admin** and **Super viewer** roles. **Super admin** grants full management access to Console features, storage, and data services. **Super viewer** provides read-only visibility for auditors and stakeholders. These roles are useful for smaller teams of senior members where broad access is common. For improved security and auditability, organizations are encouraged to use **Super admin** access sparingly and assign fine-

grained roles where possible. Learn more about access roles.

Additional role for Ransomware Resilience

Added the **Ransomware Resilience user behavior admin** role and the **Ransomware Resilience user behavior viewer** role. These roles allow users to configure and view user behavior and analytics data, respectively. Learn more about access roles.

Removed support chat

NetApp has removed the support chat feature from the NetApp Console. Use the **Administration > Support** page to create and manage support cases.

11 August 2025

Connector 3.9.55

This release of the BlueXP Connector includes security improvements, and bug fixes.

The 3.9.55 release is available for standard mode and restricted mode.

Japanese language support

The BlueXP UI is now available in the Japanese language. If your browser language is Japanese, BlueXP displays in Japanese. To access documentation in Japanese, use the language menu on the documentation website.

Operational resiliency feature

The Operational resiliency feature has been removed from BlueXP. Contact NetApp support if you encounter issues.

BlueXP Identity and Access Management (IAM)

Identity and Access Management in BlueXP now provides the following feature.

New access role for operational support

BlueXP now supports an Operational support analyst role. This role grants a user permissions to monitor storage alerts, view the BlueXP audit timeline, and enter and track NetApp Support cases.

Learn more about using access roles.

31 July 2025

Private mode release (3.9.54)

A new private mode release is now available to download from the NetApp Support Site

The 3.9.54 release includes updates to the following BlueXP components and services.

Component or service	Version included in this release	Changes since the previous private mode release
Connector	3.9.54, 3.9.53	Go to the what's new in BlueXP page and refer to the changes included for versions 3.9.54 and 3.9.53.
Backup and recovery	28 July 2025	Go to the what's new in BlueXP backup and recovery page and refer to the changes included in the July 2025 release.
Classification	14 July 2025 (version 1.45)	Go to the what's new in BlueXP classification page.

For more details about private mode, including how to upgrade, refer to the following:

- Learn about private mode
- Learn how to get started with BlueXP in private mode
- Learn how to upgrade the Connector when using private mode

21 July 2025

Support for Google Cloud NetApp Volumes

You can now view Google Cloud NetApp Volumes in BlueXP. Learn more about Google Cloud NetApp Volumes.

BlueXP Identity and Access Management (IAM)

New access role for Google Cloud NetApp Volumes

BlueXP now supports using an access role for the following storage system:

- Google Cloud NetApp Volumes

Learn more about using access roles.

14 July 2025

Connector 3.9.54

This release of the BlueXP Connector includes security improvements, bug fixes, and the following new features:

- Support for transparent proxies for Connectors dedicated to supporting Cloud Volumes ONTAP services. Learn more about configuring a transparent proxy.
- Ability to use network tags to help route Connector traffic when the Connector is deployed in a Google Cloud environment.
- Additional in-product notifications for Connector health monitoring, including CPU and RAM usage.

At this time, the 3.9.54 release is available for standard mode and restricted mode.

BlueXP Identity and Access Management (IAM)

Identity and Access Management in BlueXP now provides the following features:

- Support for IAM in private mode, allowing you to manage user access and permissions for BlueXP services and applications.
- Streamlined management of identity federations, including easier navigation, clearer options for configuring federated connections, and improved visibility into existing federations.
- Access roles for BlueXP backup and recovery, BlueXP disaster recovery, and federation management.

Support for IAM in private mode

BlueXP now supports IAM in private mode, allowing you to manage user access and permissions for BlueXP services and applications. This enhancement enables private mode customers to leverage role-based access control (RBAC) for better security and compliance.

Learn more about IAM in BlueXP.

Streamlined management of identity federations

BlueXP now offers a more intuitive interface for managing identity federation. This includes easier navigation, clearer options for configuring federated connections, and improved visibility into existing federations.

Enabling single sign-on (SSO) through identity federation lets users log in to BlueXP with their corporate credentials. This improves security, reduces password use, and simplifies onboarding.

You'll be prompted to import any existing federated connections to the new interface to gain access to the new management features. This allows you to take advantage of the latest enhancements without having to recreate your federated connections. Learn more about importing your existing federated connection to BlueXP.

Improved federation management allows you to:

- Add more than one verified domain to a federated connection, allowing you to use multiple domains with the same identity provider (IdP).
- Disable or delete federated connections when needed, giving you control over user access and security.
- Control access to federation management with IAM roles.

Learn more about identity federation in BlueXP.

New access roles for BlueXP backup and recovery, BlueXP disaster recovery, and federation management

BlueXP now supports using IAM roles for the following features and data services:

- BlueXP backup and recovery
- BlueXP disaster recovery
- Federation

Learn more about using access roles.

09 June 2025

Connector 3.9.53

This release of the BlueXP Connector includes security improvements and bug fixes.

The 3.9.53 release is available for standard mode and restricted mode.

Disk space usage alerts

The Notifications Center now includes alerts for disk space usage on the Connector. Learn more.

Audit improvements

The Timeline now includes login and logout events for users. You can see when login activity, which can help with auditing and security monitoring. API users who have the Organization administrator role can view the email address of the user who logged in by including the `includeUserData=true`` parameter as in the following: `/audit/<account_id>?includeUserData=true`.

Keystone subscription management available in BlueXP

You can manage your NetApp Keystone subscription from BlueXP.

Learn about Keystone subscription management in BlueXP.

BlueXP Identity and Access Management (IAM)

Multi-factor authentication (MFA)

Unfederated users can enable MFA for their BlueXP accounts to improve security. Administrators can manage MFA settings, including resetting or disabling MFA for users as needed. This is supported in standard mode only.

Learn about setting up multi-factor authentication for yourself.
Learn about administering multi-factor authentication for users.

Workloads

You can now view and delete Amazon FSx for NetApp ONTAP credentials from the Credentials page in BlueXP.

29 May 2025

Private mode release (3.9.52)

A new private mode release is now available to download from the NetApp Support Site

The 3.9.52 release includes updates to the following BlueXP components and services.

Component or service	Version included in this release	Changes since the previous private mode release
Connector	3.9.52, 3.9.51	Go to the what's new in BlueXP connector page and refer to the changes included for versions 3.9.52 and 3.9.50.

Component or service	Version included in this release	Changes since the previous private mode release
Backup and recovery	12 May 2025	Go to the what's new in BlueXP backup and recovery page and refer to the changes included in the May 2025 release.
Classification	12 May 2025 (version 1.43)	Go to the what's new in BlueXP classification page and refer to the changes included in the 1.38 to 1.371.41 releases.

For more details about private mode, including how to upgrade, refer to the following:

- Learn about private mode
- Learn how to get started with BlueXP in private mode
- Learn how to upgrade the Connector when using private mode

12 May 2025

Connector 3.9.52

This release of the BlueXP Connector includes minor security improvements and bug fixes, as well as some additional updates.

At this time, the 3.9.52 release is available for standard mode and restricted mode.

Support for Docker 27 and Docker 28

Docker 27 and Docker 28 are now supported with the Connector.

Cloud Volumes ONTAP

Cloud Volumes ONTAP nodes no longer shutdown when the Connector is out of compliance or down for more than 14 days. Cloud Volumes ONTAP still sends Event Management messages when it loses access to the Connector. This change is to ensure that Cloud Volumes ONTAP can continue to operate even if the Connector is down for an extended period of time. It does not change compliance requirements for the Connector.

Keystone administration available in BlueXP

The beta for NetApp Keystone in BlueXP has added access to Keystone administration. You can access the sign-up page for the NetApp Keystone beta from the left navigation bar of BlueXP.

BlueXP Identity and Access Management (IAM)

New storage management roles

The Storage admin, System health specialist, and Storage viewer roles are available and can be assigned to users.

These roles enable you to manage who in your organization can discover and manage storage resources, as well as view storage health information and perform software updates.

These roles are supported for controlling access to the following storage resources:

- E-Series systems

- StorageGRID systems

- On-premises ONTAP systems

You can also use these roles to control access to the following BlueXP services:

- Software updates

- Digital advisor

- Operational resiliency

- Economic efficiency

- Sustainability

The following roles have been added:

- **Storage admin**

  Administer storage health, governance, and discovery for the storage resources in the organization. This role can also perform software updates on storage resources.

- **System health specialist**

  Administer storage health and governance for the storage resources in the organization. This role can also perform software updates on storage resources. This role cannot modify or delete working environments.

- **Storage viewer**

  View storage health information and governance data.

Learn about access roles.

14 April 2025

Connector 3.9.51

This release of the BlueXP Connector includes minor security improvements and bug fixes.

At this time, the 3.9.51 release is available for standard mode and restricted mode.

Secure endpoints for Connector downloads now supported for Backup and recovery and Ransomware protection

If you are using Backup and recovery or Ransomware protection, you can now use secure endpoints for Connector downloads. Learn about secure endpoints for Connector downloads.

BlueXP Identity and Access Management (IAM)

- Users without the Org admin or Folder or project admin must be assigned a Ransomware protection role to have access to Ransomware protection. You can assign a user one of two roles: Ransomware protection admin or Ransomware protection viewer.

- Users without the Org admin or Folder or project admin must be assigned a Keystone role to have access to Keystone. You can assign a user one of two roles: Keystone admin or Keystone viewer.

Learn about access roles.

- If you have the Org admin or Folder or project admin role, you can now associate a Keystone subscription with an IAM project. Associating a Keystone subscription with an IAM project allows you to control access to Keystone within BlueXP.

28 March 2025

Private mode release (3.9.50)

A new private mode release is now available to download from the NetApp Support Site

The 3.9.50 release includes updates to the following BlueXP components and services.

Component or service	Version included in this release	Changes since the previous private mode release
Connector	3.9.50, 3.9.49	Go to the what's new in BlueXP connector page and refer to the changes included for versions 3.9.50 and 3.9.49.
Backup and recovery	17 March 2025	Go to the what's new in BlueXP backup and recovery page and refer to the changes included in the March 2024 release.
Classification	10 March 2025 (version 1.41)	Go to the what's new in BlueXP classification page and refer to the changes included in the 1.38 to 1.371.41 releases.

For more details about private mode, including how to upgrade, refer to the following:

- Learn about private mode
- Learn how to get started with BlueXP in private mode
- Learn how to upgrade the Connector when using private mode

10 March 2025

Connector 3.9.50

This release of the BlueXP Connector includes minor security improvements and bug fixes.

- Management of Cloud Volumes ONTAP systems is now supported by Connectors that have SELinux enabled on the operating system.

  Learn more about SELinux

At this time, the 3.9.50 release is available for standard mode and restricted mode.

NetApp Keystone beta available in BlueXP

NetApp Keystone will soon be available from BlueXP and is now in beta. You can access the sign-up page for the NetApp Keystone beta from the left navigation bar of BlueXP.

06 March 2025

Connector 3.9.49 update

ONTAP System Manager access when BlueXP uses a Connector

A BlueXP administrator (users with the Organization admin role) can configure BlueXP to prompt users to enter their ONTAP credentials in order to access ONTAP system manager. When this setting is enabled, users need enter their ONTAP credentials each time as they are not stored in BlueXP.

This feature is available in Connector version 3.9.49 and higher. Learn how to configure credentials settings..

18 February 2025

Private mode release (3.9.48)

A new private mode release is now available to download from the NetApp Support Site

The 3.9.48 release includes updates to the following BlueXP components and services.

Component or service	Version included in this release	Changes since the previous private mode release
Connector	3.9.48	Go to the what's new in BlueXP connector page and refer to the changes included for versions 3.9.48.
Backup and recovery	21 February 2025	Go to the what's new in BlueXP backup and recovery page and refer to the changes included in the February 2025 release.
Classification	22 January 2025 (version 1.39)	Go to the what's new in BlueXP classification page and refer to the changes included in the 1.39 release.

10 February 2025

Connector 3.9.49

This release of the BlueXP Connector includes minor security improvements and bug fixes.

At this time, the 3.9.49 release is available for standard mode and restricted mode.

BlueXP identity and access management (IAM)

- Support for assigning multiple roles to a BlueXP user.
- Support for assigning a role on multiple resources of the BlueXP organization (Org/folder/project)
- Roles are now associated with one of two categories: platform and data service.

Restricted mode now uses BlueXP IAM

BlueXP identity and access management (IAM) is now used in restricted mode.

BlueXP identity and access management (IAM) is a resource and access management model that replaces and enhances the previous functionality provided by BlueXP accounts when using BlueXP in standard and restricted mode.

Related information

- Learn about BlueXP IAM
- Get started with BlueXP IAM

BlueXP IAM provides more 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.
- Enhanced resource management enables you to associate a resource with one or more folders or projects.

  For example, you can associate a Cloud Volumes ONTAP system with multiple projects.

- Enhanced access management enables you to assign a role to members at different levels of the organization hierarchy.

These enhancements provide better control over the actions that users can perform and the resources that they can access.

How BlueXP IAM affects your existing account in restricted mode

When you log in to BlueXP, you'll notice these changes:

- Your *account* is now called an *organization*
- Your *workspaces* are now called *projects*
- The names of user roles have changed:
  - *Account admin* is now *Organization admin*
  - *Workspace admin* is now *Folder or project admin*
  - *Compliance viewer* is now *Classification viewer*
- Under Settings, you can access BlueXP identity and access management to take advantage of these enhancements

Note the following:

- There are no changes to your existing users or working environments.
- While the names of the roles have changed, there are no differences from a permissions perspective. Users will continue to have access to the same working environments as before.
- There are no changes to how you log in to BlueXP. BlueXP IAM works with NetApp cloud logins, NetApp Support Site credentials, and federated connections just like BlueXP accounts did.
- If you had multiple BlueXP accounts, you now have multiple BlueXP organizations.

API for BlueXP IAM

This change introduces a new API for BlueXP IAM, but it is backwards compatible with the previous tenancy API. Learn about the API for BlueXP IAM

Supported deployment modes

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

Private mode release (3.9.48)

A new private mode release is now available to download from the NetApp Support Site

The 3.9.48 release includes updates to the following BlueXP components and services.

Component or service	Version included in this release	Changes since the previous private mode release
Connector	3.9.48	Go to the what's new in BlueXP connector page and refer to the changes included for versions 3.9.48.
Backup and recovery	21 February 2025	Go to the what's new in BlueXP backup and recovery page and refer to the changes included in the February 2025 release.
Classification	22 January 2025 (version 1.39)	Go to the what's new in BlueXP classification page and refer to the changes included in the 1.39 release.

13 January 2025

Connector 3.9.48

This release of the BlueXP Connector includes minor security improvements and bug fixes.

At this time, the 3.9.48 release is available for standard mode and restricted mode.

BlueXP identity and access management

- The Resources page now displays undiscovered resources. Undiscovered resources are storage resources that BlueXP knows about but you have not created working environments for. For example, resources that display in digital advisor that do not yet have working environments display on the Resources page as undiscovered resources.
- Amazon FSx for NetApp ONTAP resources aren't displayed on the IAM resources page as you cannot associate them with an IAM role. You can view these resources on their respective canvas or from workloads.

Create a support case for additional BlueXP services

After you register BlueXP for support, you can create a support case directly from the BlueXP web-based console. When you create the case, you need to select the service that the issue is associated with.

Starting with this release, you can now create a support case and associate it with additional BlueXP services:

- BlueXP disaster recovery
- BlueXP ransomware protection

Learn more about creating a support case.

16 December 2024

New secure endpoints to obtain Connector images

When you install the Connector, or when an automatic upgrade occurs, the Connector contacts repositories to download images for the installation or upgrade. By default, the Connector has always contacted the following endpoints:

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

The first endpoint includes a wild card because we can't provide a definitive location. The load balancing of the repository is managed by the service provider, which means the downloads can happen from different endpoints.

For increased security, the Connector can now download installation and upgrades images from dedicated endpoints:

- https://bluexpinfraprod.eastus2.data.azurecr.io

- https://bluexpinfraprod.azurecr.io

We recommend that you start using these new endpoints by removing the existing endpoints from your firewall rules and allowing the new endpoints.

These new endpoints are supported starting with the 3.9.47 release of the Connector. There is no backwards compatibility with previous releases of the Connector.

Note the following:

- The existing endpoints are still supported. If you don't want to use the new endpoints, no changes are required.
- The Connector contacts the existing endpoints first. If those endpoints aren't accessible, the Connector automatically contacts the new endpoints.
- The new endpoints are not supported in the following scenarios:

  - If the Connector is installed in a Government region.
  - If you use the Connector with BlueXP backup and recovery or BlueXP ransomware protection.

  For both of these scenarios, you can continue to use the existing endpoints.

09 December 2024

Connector 3.9.47

This release of the BlueXP Connector includes bug fixes and a change to the endpoints contacted during Connector installation.

At this time, the 3.9.47 release is available for standard mode and restricted mode.

Endpoint to contact NetApp support during installation

When you manually install the Connector, the installer no longer contacts https://support.netapp.com.

The installer still contacts https://mysupport.netapp.com.

BlueXP identity and access management

The Connectors page lists only currently available Connectors. It no longer displays Connectors that you have removed.

26 November 2024

Private mode release (3.9.46)

A new private mode release is now available to download from the NetApp Support Site

The 3.9.46 release includes updates to the following BlueXP components and services.

Component or service	Version included in this release	Changes since the previous private mode release
Connector	3.9.46	Minor security improvements and bug fixes
Backup and recovery	22 November 2024	Go to the what's new in BlueXP backup and recovery page and refer to the changes included in the November 2024 release
Classification	4 November 2024 (version 1.37)	Go to the what's new in BlueXP classification page and refer to the changes included in the 1.32 to 1.37 releases
Cloud Volumes ONTAP management	11 November 2024	Go to the what's new with Cloud Volumes ONTAP management page and refer to the changes included in the October 2024 and November 2024 releases
On-premises ONTAP cluster management	26 November 2024	Go to the what's new with on-premises ONTAP cluster management page and refer to the changes included in the November 2024 release

While the BlueXP digital wallet and BlueXP replication are also included with private mode, there are no changes from the previous private mode release.

For more details about private mode, including how to upgrade, refer to the following:

- Learn about private mode
- Learn how to get started with BlueXP in private mode
- Learn how to upgrade the Connector when using private mode

11 November 2024

Connector 3.9.46

This release of the BlueXP Connector includes minor security improvements and bug fixes.

At this time, the 3.9.46 release is available for standard mode and restricted mode.

ID for IAM projects

You can now view the ID for a project from BlueXP identity and access management. You might need to use the ID when making an API call.

Learn how to obtain the ID for a project.

10 October 2024

Connector 3.9.45 patch

This patch includes bug fixes.

07 October 2024

BlueXP identity and access management

BlueXP identity and access management (IAM) is a new resource and access management model that replaces and enhances the previous functionality provided by BlueXP accounts when using BlueXP in standard mode.

BlueXP IAM provides more 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.
- Enhanced resource management enables you to associate a resource with one or more folders or projects.

  For example, you can associate a Cloud Volumes ONTAP system with multiple projects.

- Enhanced access management enables you to assign a role to members at different levels of the organization hierarchy.

These enhancements provide better control over the actions that users can perform and the resources that they can access.

How BlueXP IAM affects your existing account

When you log in to BlueXP, you'll notice these changes:

- Your *account* is now called an *organization*
- Your *workspaces* are now called *projects*
- The names of user roles have changed:
    - *Account admin* is now *Organization admin*
    - *Workspace admin* is now *Folder or project admin*
    - *Compliance viewer* is now *Classification viewer*
- Under Settings, you can access BlueXP identity and access management to take advantage of these enhancements

Note the following:

- There are no changes to your existing users or working environments.
- While the names of the roles have changed, there are no differences from a permissions perspective. Users will continue to have access to the same working environments as before.
- There are no changes to how you log in to BlueXP. BlueXP IAM works with NetApp cloud logins, NetApp Support Site credentials, and federated connections just like BlueXP accounts did.
- If you had multiple BlueXP accounts, you now have multiple BlueXP organizations.

API for BlueXP IAM

This change introduces a new API for BlueXP IAM, but it is backwards compatible with the previous tenancy API. Learn about the API for BlueXP IAM

Supported deployment modes

BlueXP IAM is supported when using BlueXP in standard mode. If you're using BlueXP in restricted mode or

private mode, then you'll continue using a BlueXP *account* to manage workspaces, users, and resources.

Where to go next

- Learn about BlueXP IAM
- Get started with BlueXP IAM

Connector 3.9.45

This release includes expanded operating system support and bug fixes.

The 3.9.45 release is available for standard mode and restricted mode.

Support for Ubuntu 24.04 LTS

Starting with the 3.9.45 release, BlueXP now supports new installations of the Connector on Ubuntu 24.04 LTS hosts when using BlueXP in standard mode or restricted mode.

View Connector host requirements.

Support for SELinux with RHEL hosts

BlueXP now supports the Connector with Red Hat Enterprise Linux hosts that have SELinux enabled in either enforcing mode or permissive mode.

Support for SELinux starts with the 3.9.40 release for standard mode and restricted mode and with the 3.9.42 release for private mode.

Note the following limitations:

- BlueXP does not support SELinux with Ubuntu hosts.
- Management of Cloud Volumes ONTAP systems it not supported by Connectors that have SELinux enabled on the operating system.

Learn more about SELinux

30 September 2024

Private mode release (3.9.44)

A new private mode release is now available to download from the NetApp Support Site.

This release includes the following versions of the BlueXP components and services that are supported with private mode.

Service	Version included
Connector	3.9.44
Backup and recovery	27 September 2024
Classification	15 May 2024 (version 1.31)
Cloud Volumes ONTAP management	9 September 2024
Digital wallet	30 July 2023

Service	Version included
On-premises ONTAP cluster management	22 April 2024
Replication	18 Sept 2022

For the Connector, the 3.9.44 private mode release includes the updates introduced in the August 2024 and September 2024 releases. Most notably, support for Red Hat Enterprise Linux 9.4.

To learn more about what's included in the versions of these BlueXP components and services, refer to the release notes for each BlueXP service:

- What's new in the September 2024 release of the Connector
- What's new in the August 2024 release of the Connector
- What's new with BlueXP backup and recovery
- What's new with BlueXP classification
- What's new with Cloud Volumes ONTAP management in BlueXP

For more details about private mode, including how to upgrade, refer to the following:

- Learn about private mode
- Learn how to get started with BlueXP in private mode
- Learn how to upgrade the Connector when using private mode

09 September 2024

Connector 3.9.44

This release includes support for Docker Engine 26, an enhancement to SSL certificates, and bug fixes.

The 3.9.44 release is available for standard mode and restricted mode.

Support for Docker Engine 26 with new installations

Starting with the 3.9.44 release of the Connector, Docker Engine 26 is now supported with *new* Connector installations on Ubuntu hosts.

If you have an existing Connector created prior to the 3.9.44 release, then Docker Engine 25.0.5 is still the maximum supported version on Ubuntu hosts.

Learn more about Docker Engine requirements.

Updated SSL certificate for local UI access

When you use BlueXP in restricted mode or private mode, the user interface is accessible from the Connector virtual machine that's deployed in your cloud region or on-premises. By default, BlueXP uses a self-signed SSL certificate to provide secure HTTPS access to the web-based console running on the Connector.

In this release, we made changes to the SSL certificate for new and existing Connectors:

- The Common Name for the certificate now matches the short host name
- The Certificate Subject Alternative Name is the Fully Qualified Domain Name (FQDN) of the host machine

Support for RHEL 9.4

BlueXP now supports installing the Connector on a Red Hat Enterprise Linux 9.4 host when using BlueXP in standard mode or restricted mode.

Support for RHEL 9.4 starts with the 3.9.40 release of the Connector.

The updated list of supported RHEL versions for standard mode and restricted mode now includes the following:

- 8.6 to 8.10
- 9.1 to 9.4

Learn about support for RHEL 8 and 9 with the Connector.

Support for Podman 4.9.4 with all RHEL versions

Podman 4.9.4 is now supported with all supported versions of Red Hat Enterprise Linux. Version 4.9.4 was previously supported with only RHEL 8.10.

The updated list of supported Podman versions includes 4.6.1 and 4.9.4 with Red Hat Enterprise Linux hosts.

Podman is required for RHEL hosts starting with the 3.9.40 release of the Connector.

Learn about support for RHEL 8 and 9 with the Connector.

Updated AWS and Azure permissions

We updated the AWS and Azure policies for the Connector to remove permissions that are no longer required. The permissions were related to BlueXP edge caching and discovery and management of Kubernetes clusters, which are no longer supported as of August, 2024.

- Learn what changed in the AWS policy.
- Learn what changed in the Azure policy.

22 August 2024

Connector 3.9.43 patch

We updated the Connector to support the Cloud Volumes ONTAP 9.15.1 release.

Support for this release includes an update to the Connector policy for Azure. The policy now includes the following permissions:

```
"Microsoft.Compute/virtualMachineScaleSets/write",
"Microsoft.Compute/virtualMachineScaleSets/read",
"Microsoft.Compute/virtualMachineScaleSets/delete"
```

These permissions are required for Cloud Volumes ONTAP support of Virtual Machine Scale Sets. If you have existing Connectors and you want to use this new feature, you'll need to add these permissions to the custom roles that are associated with your Azure credentials.

- Learn about the Cloud Volumes ONTAP 9.15.1 release
- View Azure permissions for the Connector.

8 August 2024

Connector 3.9.43

This release includes minor improvements and bug fixes.

The 3.9.43 release is available for standard mode and restricted mode.

Updated CPU and RAM requirements

To provide higher reliability and to improve the performance of BlueXP and the Connector, we now require additional CPU and RAM for the Connector virtual machine:

- CPU: 8 cores or 8 vCPUs (the previous requirement was 4)
- RAM: 32 GB (the previous requirement was 14 GB)

As a result of this change, the default VM instance type when deploying the Connector from BlueXP or from the cloud provider's marketplace is as follows:

- AWS: t3.2xlarge
- Azure: Standard_D8s_v3
- Google Cloud: n2-standard-8

The updated CPU and RAM requirements apply to all new Connectors. For existing Connectors, increasing the CPU and RAM is recommended to provide improved performance and reliability.

Support for Podman 4.9.4 with RHEL 8.10

Podman version 4.9.4 is now supported when installing the Connector on a Red Hat Enterprise Linux 8.10 host.

User validation for identity federation

If you use identity federation with BlueXP, each user who logs in to BlueXP for the first time will need to complete a quick form to validate their identity.

31 July 2024

Private mode release (3.9.42)

A new private mode release is now available to download from the NetApp Support Site.

Support for RHEL 8 and 9

This release includes support for installing the Connector on a Red Hat Enterprise Linux 8 or 9 host when using BlueXP in private mode. The following versions of RHEL are supported:

- 8.6 to 8.10
- 9.1 to 9.3

Podman is required as the container orchestration tool for these operating systems.

You should be aware of Podman requirements, known limitations, a summary of operating system support, what to do if you have a RHEL 7 host, how to get started, and more.

Learn about support for RHEL 8 and 9 with the Connector.

Versions included in this release

This release includes the following versions of the BlueXP services that are supported with private mode.

Service	Version included
Connector	3.9.42
Backup and recovery	18 July 2024
Classification	1 July 2024 (version 1.33)
Cloud Volumes ONTAP management	10 June 2024
Digital wallet	30 July 2023
On-premises ONTAP cluster management	30 July 2023
Replication	18 Sept 2022

To learn more about what's included in the versions of these BlueXP services, refer to the release notes for each BlueXP service.

- Learn about private mode
- Learn how to get started with BlueXP in private mode
- Learn how to upgrade the Connector when using private mode
- Learn what's new with BlueXP backup and recovery
- Learn what's new with BlueXP classification
- Learn what's new with Cloud Volumes ONTAP management in BlueXP

15 July 2024

Support for RHEL 8.10

BlueXP now supports installing the Connector on a Red Hat Enterprise Linux 8.10 host when using standard mode or restricted mode.

Support for RHEL 8.10 starts with the 3.9.40 release of the Connector.

Learn about support for RHEL 8 and 9 with the Connector.

8 July 2024

Connector 3.9.42

This release includes minor improvements, bug fixes, and support for the Connector in the AWS Canada West (Calgary) region.

The 3.9.42 release is available for standard mode and restricted mode.

Updated Docker Engine requirements

When the Connector is installed on an Ubuntu host, the minimum supported version of Docker Engine is now 23.0.6. It was previously 19.3.1.

The maximum supported version is still 25.0.5.

View Connector host requirements.

Email verification now required

New users who sign up to BlueXP are now required to verify their email address before they can log in.

12 June 2024

Connector 3.9.41

This release of the BlueXP Connector includes minor security improvements and bug fixes.

The 3.9.41 release is available for standard mode and restricted mode.

End of support for RHEL 7 and CentOS 7

On June 30, 2024, RHEL 7 reached end of maintenance (EOM), while CentOS 7 reached end of life (EOL). NetApp discontinued support for agents on these Linux distributions on June 30, 2024.

Red Hat: What to know about Red Hat Enterprise Linux 7 End of Maintenance

If you have an existing agent running on RHEL 7 or CentOS 7, NetApp does not support upgrading or converting the operating system to RHEL 8 or 9. You need to create a new agent on a supported operating system.

1. Set up a RHEL 8 or 9 host.
2. Install Podman.
3. Install a *new* agent.
4. Configure the agent to discover the systems that the previous agent was managing.
5. Rediscover the systems.

   Refer to the following pages to rediscover your systems after you deploy a new Console agent.

   - Add existing Cloud Volumes ONTAP systems
   - Discover on-premises ONTAP clusters
   - Create or discover an FSx for ONTAP system
   - Create an Azure NetApp Files systems
   - Discover E-Series systems
   - Discover StorageGRID systems

4 June 2024

Private mode release (3.9.40)

A new private mode release is now available to download from the NetApp Support Site. This release includes the following versions of the BlueXP services that are supported with private mode.

Note that this private mode release does *not* include support for the Connector with Red Hat Enterprise Linux 8 and 9.

Service	Version included
Connector	3.9.40
Backup and recovery	17 May 2024
Classification	15 May 2024 (version 1.31)
Cloud Volumes ONTAP management	17 May 2024
Digital wallet	30 July 2023
On-premises ONTAP cluster management	30 July 2023
Replication	18 Sept 2022

To learn more about what's included in the versions of these BlueXP services, refer to the release notes for each BlueXP service.

- Learn about private mode
- Learn how to get started with BlueXP in private mode
- Learn how to upgrade the Connector when using private mode
- Learn what's new with BlueXP backup and recovery
- Learn what's new with BlueXP classification
- Learn what's new with Cloud Volumes ONTAP management in BlueXP

17 May 2024

Connector 3.9.40

This release of the BlueXP Connector includes support for additional operating systems, minor security improvements, and bug fixes.

At this time, the 3.9.40 release is available for standard mode and restricted mode.

Support for RHEL 8 and 9

The Connector is now supported on hosts running the following versions of Red Hat Enterprise Linux with *new* Connector installations when using BlueXP in standard mode or restricted mode:

- 8.6 to 8.9
- 9.1 to 9.3

Podman is required as the container orchestration tool for these operating systems.

You should be aware of Podman requirements, known limitations, a summary of operating system support, what to do if you have a RHEL 7 host, how to get started, and more.

Learn about support for RHEL 8 and 9 with the Connector.

End of support for RHEL 7 and CentOS 7

On June 30, 2024, RHEL 7 will reach end of maintenance (EOM), while CentOS 7 will reach end of life (EOL). NetApp will continue to support the Connector on these Linux distributions until June 30, 2024.

Learn what to do if you have an existing Connector running on RHEL 7 or CentOS 7.

AWS permissions update

In the 3.9.38 release, we updated the Connector policy for AWS to include the "ec2:DescribeAvailabilityZones" permission. This permission is now required to support AWS Local Zones with Cloud Volumes ONTAP.

- View AWS permissions for the Connector.
- Learn more about support for AWS Local Zones

Known limitations of NetApp Console

Known limitations identify platforms, devices, or functions that are not supported by this release of the product, or that do not interoperate correctly with it. Review these limitations carefully.

These limitations are specific to the set up for the NetApp Console and administration: the agent, the software as a service (SaaS) platform, and more.

Console agent limitations

Possible conflict with IP addresses in the 172 range

The NetApp Console deploys an agent with two interfaces that have IP addresses in the 172.17.0.0/16 and 172.18.0.0/16 ranges.

If your network has a subnet configured with either of these ranges, then you might experience connectivity failures from the Console. For example, discovering on-premises ONTAP clusters in the Console might fail.

See Knowledge Base article Agent IP conflict with existing network for instructions on how to change the IP address of the agent's interfaces.

SSL decryption supported only for Cloud Volumes ONTAP

Transparent proxy servers are supported for agents associated with Cloud Volumes ONTAP only. You cannot use a transparent proxy for an agent if it is used with other NetApp data services. If you use NetApp data services with Cloud Volumes ONTAP, create a dedicated agent for Cloud Volumes ONTAP where you can use a transparent proxy server.

For enhanced security, you have the option to install an HTTPS certificate signed by a certificate authority (CA).

Blank page when loading the local UI

If you load the web-based console that's running on an agent, the interface might fail to display sometimes, and you just get a blank page.

This issue is related to a caching problem. The workaround is to use an incognito or private web browser session.

Shared Linux hosts are not supported

The agent isn't supported on a VM that is shared with other applications. The VM must be dedicated to the agent software.

Third-party agents and extensions

Third-party agents or VM extensions are not supported on the agent VM.