Monitor data protection

BlueXP backup and recovery

NetApp
July 15, 2024

Table of Contents

Monitor data protection

Report on data protection coverage

With BlueXP backup and recovery reports, you can ensure that critical data is protected according to your organization's defined policies and provide audits for compliance needs.

BlueXP backup and recovery reports help you accomplish the following:

- **Operations visibility**: Monitor your service level agreements regarding data protection, backup success rate, and backup window alignment to business needs.
- **Compliance and auditing**: Use operational and inventory reports in your internal and external audit processes for ongoing monitoring of compliance.

Report activities are monitored in the Job Monitoring log so that you can audit all activities. Learn about Job Monitoring.

Reports scope

The BlueXP backup and recovery reports provide information about the following aspects:

- **Connector location**: On-premises or the cloud
- **Source**: Cloud Volumes ONTAP volumes, on-premises ONTAP volumes, applications, or Kubernetes persistent volumes
- **Destination**: Any of the cloud providers, NetApp StorageGRID, or ONTAP S3
- **ONTAP versions**: 9.13.0

Create a Backup Inventory report

From the BlueXP backup and recovery Reports tab, you can create the Backup Inventory report and filter its contents. With the Backup Inventory report, you can see all your backups for a specific account, working environment, or SVM inventory.

The Backup Inventory report shows the following information and more:

- Account, working environment, and SVM
- Protected and non-protected volumes
- Backup target
- Applied backup policy
- Encryption style (provider-managed key or user-managed key)
- DataLock and Ransomware protection status (governance, compliance, or none)
- Archive enabled status
- Count of backup copies
- Backup type (scheduled or user-initiated ad-hoc backup)

- Storage class
- Snapshot label

The Backup Inventory report doesn't include expired or failed backup information.

The top of the report includes a graph that shows the following information:

- Count of volumes in scope with at least one backup
- Total of inactive volumes plus active volumes

The Backup Inventory report shows the following charts:

- **Volume backup status**: Shows protected compared to non-protected volumes for the selected scope.
- **Volumes by backup count**: Groups volumes by the number of available backup copies for this volume.

Steps

1. From the top menu, select **Reports**.
2. Select **Backup inventory**.
3. Select **Create report**.
4. Select the account, working environment, and SVM.

   You can select multiple working environments and SVMs.

5. Select the timeframe: last 24 hours, week, or month.
6. Review the report sections (Snapshot Policies, Replication Policies, or Backup Policies), depending on your report selections.
7. (Optional) Filter the results by job status.
8. (Optional) Export the report contents in .CSV format by selecting **Download CSV**.

Create a Data Protection Job Activity report

Proactive monitoring can reduce effort required to monitor all resources in your ecosystem. Beginning with ONTAP 9.13.0, the Data Protection Job Activity report provides information about snapshot, backup, clone, and restore operations that you can use with your SLA monitoring and track backup and recovery rates.

The report applies to BlueXP backup and recovery operations for Cloud Volumes ONTAP, on-premises, applications, and Kubernetes data.

The Data Protection Job Activity report shows the following information and more:

- Account, working environment, and SVM
- Job type (backup or restore)
- Resource name (volume or application)
- Job status
- Start and end times and duration
- Policy name for backup jobs

- Snapshot label for backup jobs

The charts at the top of the page show the following information:

- Jobs by type
  - Count of ONTAP volumes backup and restore jobs
  - Count of application backup and restore jobs
  - Count of virtual machine backup and restore jobs
  - Count of Kubernetes backup and restore jobs
- Daily job activity

Steps

1. From the top menu, select **Reports**.
2. Select **Data protection job activity**.
3. Select **Create report**.
4. Select the account, working environment, and SVM.
5. Select the timeframe: last 24 hours, week, or month.
6. (Optional) Filter the results by job status, job types (backup or restore), and resource.
7. (Optional) Export the report contents in .CSV format by selecting **Download CSV**.

Monitor the status of backup and restore jobs

You can monitor the status of local Snapshots, replications, and backup to object storage jobs that you initiated, and restore jobs that you initiated. You can see the jobs that have completed, are in progress, or failed so you can diagnose and fix problems. Using the BlueXP Notification Center, you can enable notifications to be sent by email so you can be informed of important system activity even when you're not logged into the system. Using the BlueXP Timeline, you can see details of all actions initiated via the UI or API.

View job status on the Job Monitor

You can view a list of all the Snapshot, replication, backup to object storage, and restore operations and their current status in the **Job Monitoring** tab. This includes operations from your Cloud Volumes ONTAP, on-premises ONTAP, applications, virtual machines, and Kubernetes systems. Each operation, or job, has a unique ID and a status.

The status can be:

- Success
- In Progress
- Queued
- Warning
- Failed

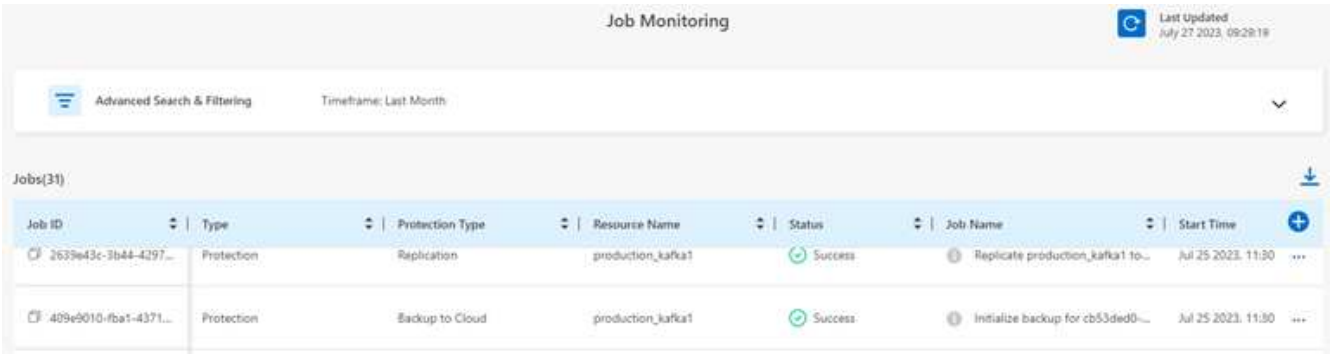
Snapshots, replications, backups to object storage and restore operations that you initiated from the BlueXP

backup and recovery UI and API are available in the Job Monitoring tab.

If you've upgraded your ONTAP systems to 9.13.x and you don't see ongoing scheduled backup operations in the Job Monitor, then you'll need to restart the BlueXP backup and recovery service. Learn how to restart BlueXP backup and recovery.

Steps

1. From the BlueXP menu, select **Protection > Backup and recovery**.
2. Select the **Job Monitoring** tab.



This screenshot shows the default column headings.

3. To show additional columns (Working Environment, SVM, User Name, Workload, Policy Name, Snapshot Label), select .

Search and filter the list of jobs

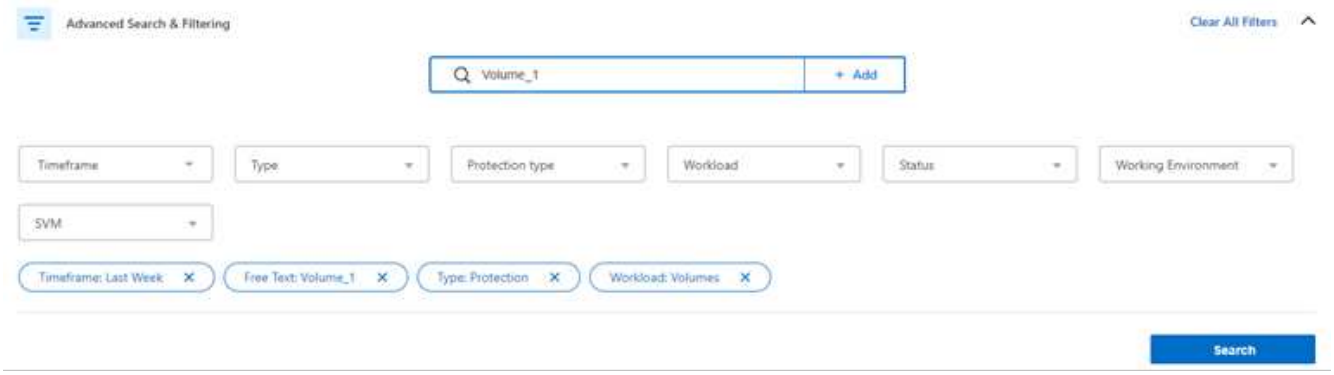
You can filter the operations on the Job Monitoring page using several filters, such as policy, Snapshot label, type of operation (protection, restore, retention, or other) and protection type (local Snapshot, replication, or backup to the cloud).

By default, the Job Monitoring page shows protection and recovery jobs from the last 24 hours. You can change the timeframe using the Timeframe filter.

Steps

1. Select the **Job Monitoring** tab.
2. To sort the results differently, select each column heading to sort by Status, Start Time, Resource Name, and more.
3. If you're looking for specific jobs, select the **Advanced Search & Filtering** area to open the Search panel.

   Use this panel to enter a free text search for any resource; for example "volume 1" or "application 3". You can also filter the jobs list according to the items in the drop-down menus.



This screenshot shows how you would search for all "Volume" "Backup" jobs for volumes named "Volume_1" in the "past week".

Most of the filters are self-explanatory. The filter for "Workload" enables you to view jobs in the following catagories:

- Volumes (Cloud Volumes ONTAP and on-premises ONTAP volumes)
- Applications
- Virtual Machines
- Kubernetes

- You can search for data within a specific "SVM" only if you have first selected a Working Environment.
- You can search using the "Protection type" filter only when you have selected the "Type" of "Protection".

4. To update the page immediately, select the button. Otherwise, this page refreshes every 15 minutes so that you'll always see the most recent job status results.

View job details

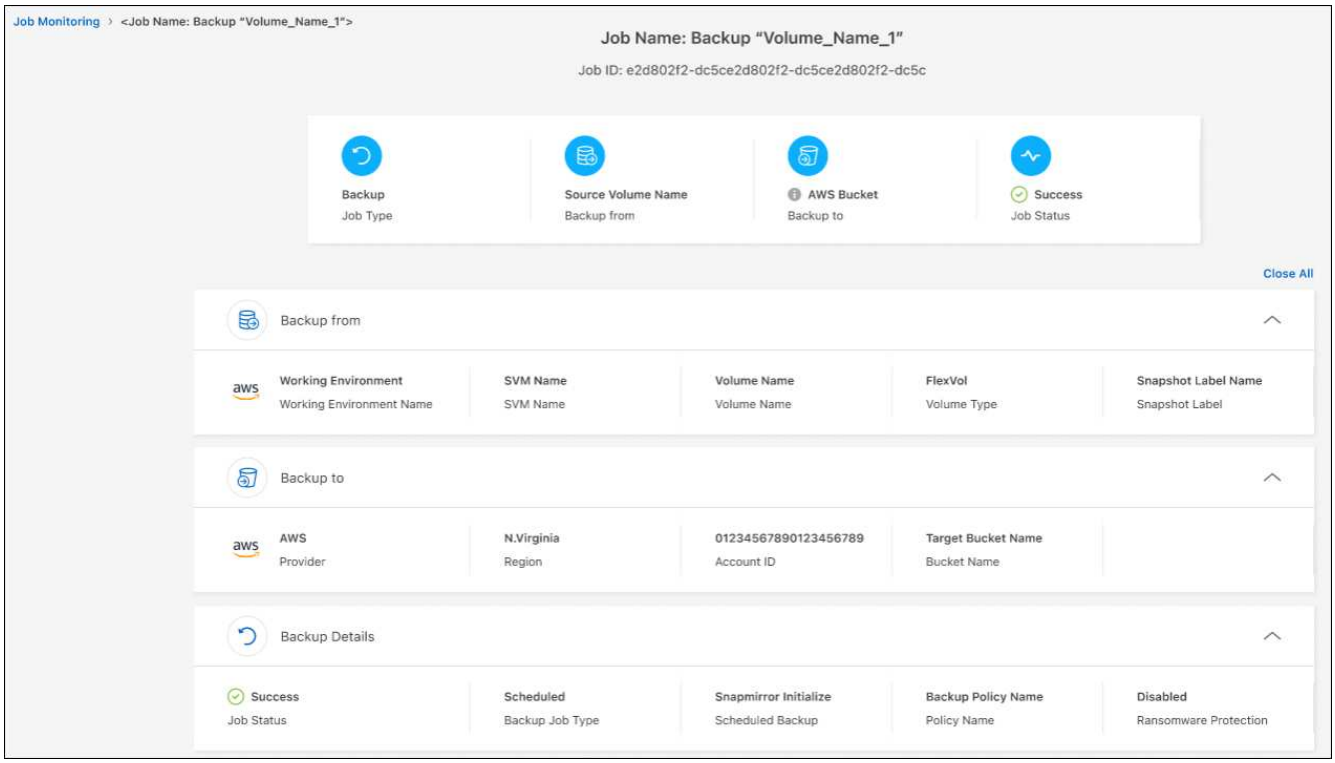
You can view details corresponding to a specific completed job. You can export details for a particular job in a JSON format.

You can view details such as job type (scheduled or on-demand), SnapMirror backup type (initial or periodic) start and end times, duration, amount of transferred data from working environment to object storage, average transfer rate, policy name, retention lock enabled, ransomware scan performed, protection source details, and protection target details.

Restore jobs show details such as backup target provider (Amazon Web Services, Microsoft Azure, Google Cloud, on-premises), S3 bucket name, SVM name, source volume name, destination volume, Snapshot label, recovered objects count, file names, file sizes, last modification date, and full file path.

Steps

1. Select the **Job Monitoring** tab.
2. Select the name of the job.
3. Select the Actions menu ••• and select **View Details**.



4. Expand each section to see details.

Download Job Monitoring results as a report

You can download the contents of the main Job Monitoring page as a report after you've refined it. BlueXP backup and recovery generates and downloads a .CSV file that you can review and send to other groups as needed. The .CSV file includes up to 10,000 rows of data.

From the Job Monitoring Details information, you can download a JSON file containing details for a single job.

Steps

1. Select the **Job Monitoring** tab.
2. To download a CSV file for all jobs, select the button and locate the file in your download directory.
3. To download a JSON file for a single job, select the Actions menu ••• for the job, select **Download JSON File**, and locate the file in your download directory.

Review retention (backup lifecycle) jobs

Monitoring of retention (or *backup lifecycle*) flows helps you with audit completeness, accountability, and backup safety. To help you track the backup lifecycle, you might want to identify the expiration of all backup copies.

A backup lifecycle job tracks all Snapshot copies that are deleted or in the queue to be deleted. Beginning with ONTAP 9.13, you can look at all job types called "Retention" on the Job Monitoring page.

The "Retention" job type captures all Snapshot deletion jobs initiated on a volume that is protected by BlueXP backup and recovery.

Steps

1. Select the **Job Monitoring** tab.

2. Select the **Advanced Search & Filtering** area to open the Search panel.
3. Select "Retention" as the job type.

Review backup and restore alerts in the BlueXP Notification Center

The BlueXP Notification Center tracks the progress of backup and restore jobs that you've initiated so you can verify whether the operation was successful or not.

In addition to viewing the alerts in the Notification Center, you can configure BlueXP to send certain types of notifications by email as alerts so you can be informed of important system activity even when you're not logged into the system. Learn more about the Notification Center and how to send alert emails for backup and restore jobs.

The Notification Center displays numerous Snapshot, replication, backup to cloud, and restore events, but only certain events trigger email alerts:

Operation type	Event	Alert level	Email sent
Activation	Backup and recovery activation failed for working environment	Error	Yes
Activation	Backup and recovery edit failed for working environment	Error	Yes
Local Snapshot	BlueXP backup and recovery ad-hoc Snapshot creation job failure	Error	Yes
Replication	BlueXP backup and recovery ad-hoc replication job failure	Error	Yes
Replication	BlueXP backup and recovery replication pause job failure	Error	No
Replication	BlueXP backup and recovery replication brake job failure	Error	No
Replication	BlueXP backup and recovery replication resync job failure	Error	No
Replication	BlueXP backup and recovery replication stop job failure	Error	No
Replication	BlueXP backup and recovery replication reverse resync job failure	Error	Yes
Replication	BlueXP backup and recovery replication delete job failure	Error	Yes

Beginning with ONTAP 9.13.0, all alerts appear for Cloud Volumes ONTAP and on-premises ONTAP systems. For systems with Cloud Volumes ONTAP 9.13.0 and on-premises ONTAP, only the alert related to "Restore job completed, but with warnings" appears.

By default, BlueXP Account Admins receive emails for all "Critical" and "Recommendation" alerts. All other users and recipients are set up, by default, not to receive any notification emails. Emails can be sent to any BlueXP users who are part of your NetApp Cloud Account, or to any other recipients who need to be aware of backup and restore activity.

To receive the BlueXP backup and recovery email alerts, you'll need to select the notification severity types "Critical", "Warning", and "Error" in the Alerts and Notifications Settings page.

Learn how to send alert emails for backup and restore jobs.

Steps

1. From the BlueXP menu bar, select the ().
2. Review the notifications.

Review operation activity in the BlueXP Timeline

You can view details of backup and restore operations for further investigation in the BlueXP Timeline. The BlueXP Timeline provides details of each event, whether user-initiated or system-initiated and shows actions initiated in the UI or via the API.

Learn about the differences between the Timeline and the Notification Center.

Copyright information

Trademark information