Use Digital Advisor

Digital Advisor

NetApp
August 14, 2025

This PDF was generated from https://docs.netapp.com/us-en/active-iq/concept_overview_wellness.html on August 14, 2025. Always check docs.netapp.com for the latest.

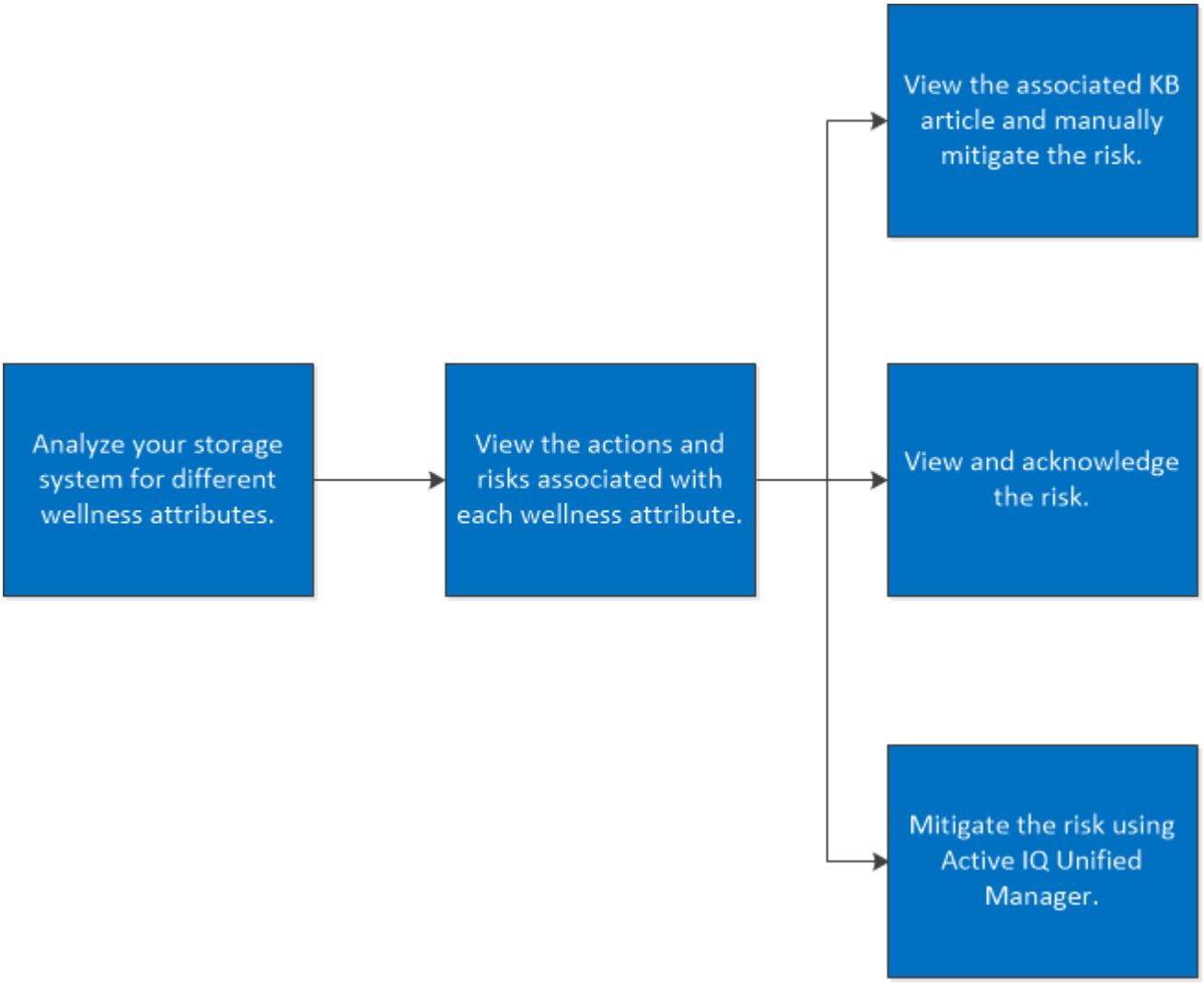
Table of Contents

Use Digital Advisor

Analyze wellness attributes

Understand wellness

Wellness widget provides detailed information about your storage system. It provides information about different attributes of your storage system, such as performance and efficiency, capacity, configuration settings, security vulnerabilities, renewals, and others.



The wellness widget also provides information about the risks and the actions that should be taken to mitigate the risk for each wellness attribute. The following are the types of risks and the associated consequence for each risk:

Risk Type	Consequence
Critical	Data loss, data corruption, cluster data outage, personal safety issue, or potential legal compliance issue.
High	Short-term loss of data access or prolonged loss of node redundancy.

Risk Type	Consequence
Medium	Performance degradation or short-term loss of node redundancy.
Low	Low impact scenarios
Best Practice	Deviations from documented best practices

You can view the following video to understand the importance of the wellness attributes:

View risk and manually take corrective actions

You can analyze the wellness attributes of your storage system by viewing the actions and risks associated with them. You should view the associated corrective actions and manually mitigate the risk.

Steps

1. Click the **Wellness** widget on the dashboard or click **View All Actions** to view the list of all the actions and risks.
2. View the **Actions** and **Risks** associated with the wellness attribute.
3. Click **Actions** to view the risks associated with the actions, click **Risks** to view all the risks, or click **Affected Systems** to view the systems that require attention.
4. Click the risk name to view information about the risk.
5. Click the associated corrective actions and follow the information to resolve the risk.

The steps to mitigate the risks are same for all wellness attributes. You can view the following video to monitor and fix security related issues:

Detect security vulnerability

The NetApp security site is the source of truth for NetApp Product Security: NetApp Product Security

Digital Advisor utilizes telemetry data and published product security advisories to detect security issues for covered* and support-entitled products. Product telemetry data must be transmitted to NetApp via AutoSupport to allow Digital Advisor to detect risks.

For additional NetApp product security information, including products not covered by Digital Advisor, visit NetApp Product Security

*Covered products: ONTAP 9 (on-prem and cloud), SANtricity OS Controller Software, NetApp SolidFire (Element Software), StorageGRID, Active IQ Unified Manager, ONTAP Tools for VMware (OTV)

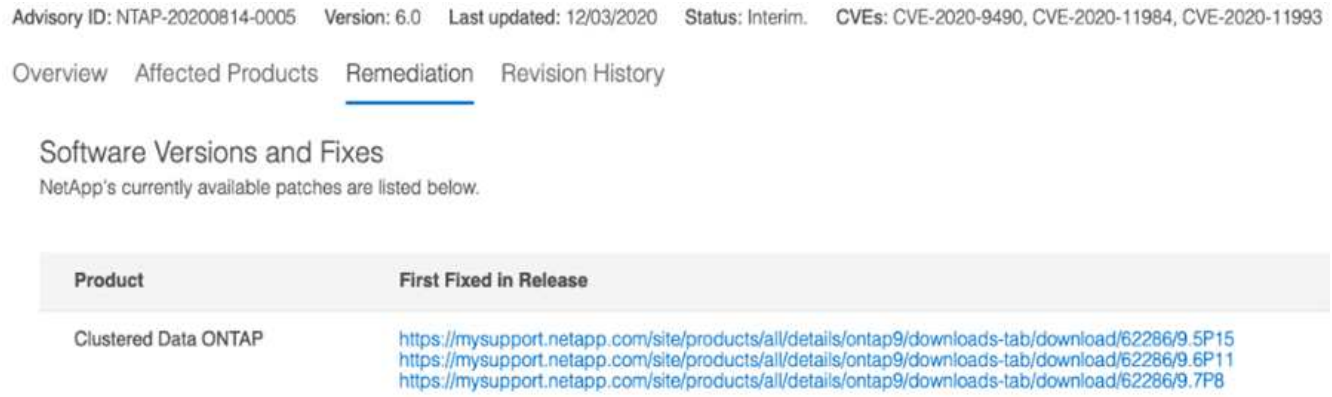
Steps

1. Log in to Digital Advisor.
2. Click **Actions** in the **Security & Ransomware Defense** widget.

3. Clear the **Ransomware Defense** checkbox.

4. For the high-impact security risks, follow the recommended action that is to upgrade the operating system.
5. Click the **Unique Risks** tab, and then click the link in the **Corrective Action** column.

The risk is fixed in ONTAP 9.7P8 and later.



6. The most important step is to plan OS upgrade in the **Upgrade Advisor** in Digital Advisor.

Protect systems against ransomware risks

When you log in to the Digital Advisor, you can view the **Actions** highlighted on the **Security & Ransomware Defense** widget, which shows the risk counts.

You can view the Snapshot creation, retention, and ONTAP FPolicy risks, and then take actions to fix them.

Steps

1. Log in to Digital Advisor.
2. Click **Actions** on the **Security & Ransomware Defense** widget.
3. Clear the **Security Vulnerabilities** checkbox.
4. For the risks that are displayed, check the impact level and follow the recommended actions.
5. Click the Unique Risks tab and link in the **Corrective Action** column.
6. Click the **Affected Systems** tab to view systems with risks.
7. Follow remediation actions that are recommended to protect the systems.

View and acknowledge the risk

You can analyze the wellness attributes of your storage system by viewing the actions and risks associated with them. You should view the corrective actions and manually mitigate the risk.

Steps

1. Click the wellness attribute widget on the dashboard or click **View All Actions** to view the list of all the actions and risks.

2. View the **Actions** and **Risks** associated with the wellness attribute.
3. Click **Actions** to view the risks associated with the actions, click **Risks** to view all the risks, or click **Affected Systems** to view the systems that require attention.
4. Click the risk to view the risk summary.
5. Click **Ack** to acknowledge the risk.

   The detailed risk summary information is provided along with corrective actions that should be manually performed to mitigate the risk.

6. If you do not want to or are unable to mitigate the risk at this time, provide the values for the fields and click **Acknowledge**.

   The risk will be added to acknowledged risks.

If you no longer want a risk to be acknowledged, you can disregard the risk by clicking **Un-Ack** and following the same steps.

View wellness history

You can view system risks occurring in the past three months, so that you can learn how they are faring overtime.

These risks are classified under four types of risks— **Unresolved**, **New**, **Resolved**, and **Acknowledged**. They are represented by different colors. The summary of these risks is represented through a **Risk History** graph.

Steps

1. On the dashboard, in the **Wellness** pane, click **View All Actions**.
2. Click **Wellness History**.
3. In the **Risk History** graph, click the category for which you want to view the risk history.

   When you hover over the colored bars, they display information on the number of risks in each category. Upon clicking the respective risk category, the information gets displayed in the **Risk Information** table.

   You can also download risk summary in an Excel sheet.

View risks that can be automatically mitigated using Unified Manager or Ansible Playbook

You can analyze your storage system by viewing the actions and risks, and mitigate them using Active IQ Unified Manager or Ansible Playbook.

Steps

1. Click **View All Actions** on the dashboard.
2. Click **Actions** to view the risks associated with the actions, click **Risks** to view all the risks, or click **Affected Systems** to view the systems that require attention.

   If the risk can be mitigated using Active IQ Unified Manager, the icon is highlighted and if the risk can be mitigated using Ansible Playbook, the icon is highlighted.

To mitigate the risk using Unified Manager	To mitigate the risk using Ansible Playbook
1. Click the icon. 2. Click **Fix It** to launch Active IQ Unified Manager. 3. Click **Install** to install Active IQ Unified Manager 9.7 or later to use the **Fix It** option. 4. Click **Upgrade** to upgrade to Active IQ Unified Manager 9.7 or later to use the **Fix It** option.	1. Click the icon. 2. Click **Download** to download the AFF and FAS firmware Ansible Automation package.

A SupportEdge Advisor or SupportEdge Expert contract is required to use the **Fix It** option and the Ansible Playbook features.

Avoid downtime and possible data loss

When you log in to the Digital Advisor and notice the red badge on the **Availability and Protection** widget, you can take actions to fix critical risks. Without the firmware fix, these

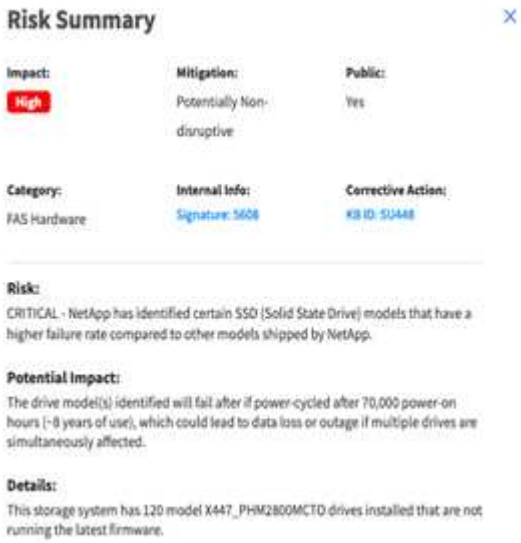
drives are vulnerable to become inoperable after a certain number of hours of being powered on. Fixing this would avoid both the downtime and possible data loss.

Steps

1. Log in to the Digital Advisor.
2. Click **Actions** in the **Availability & Protection** widget.

   For the high-impact security risks, follow the recommended action that is to update disk firmware.

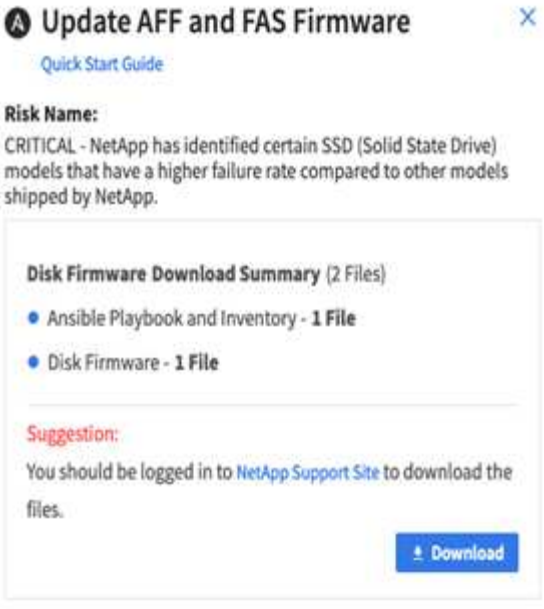
3. Click the **Risk Name** link for viewing risk summary.



4. Click the **Unique Risks** tab, and then click the link in the **Corrective Action** column.

   Digital Advisor generates custom Ansible scripts or playbooks to update the required disk firmware, including the disk firmware files.

5. Click the **Ansible "A"** icon to generate and download the scripts.



Subscribe to wellness review email

You can subscribe to the wellness review email to receive a monthly email that summarizes wellness status, systems that are nearing their renewal dates, systems that require an upgrade for the NetApp products in your installed base.
You will receive a wellness review email so that you can view a monthly summary and take action for your systems.
You also have options to view, edit, share, and delete your subscriptions. At any time, if you decide to not receive the email, you can unsubscribe from getting email as well.

After the subscription is enabled, you should select a start date when adding a subscription.
The monthly email summary provides a view of outstanding wellness, renewal, upgrade, and health check actions. You can confirm the email address and the email is sent to the specified email address.
You also have the option to delete subscriptions.

This feature is available only through NetApp SupportEdge Advisor and SupportEdge Expert service offerings.

Steps

1. From the left pane, click **Wellness Review**.
2. Click **Add Subscription**.
3. Provide the required information in the **Name the Subscription**, **Choose Category**, **Search Customer**, and **Email** fields in the **Add New Subscription** dialog box.
4. Click **Subscribe**.

   Upon successful subscription, you will receive a **Subscription was added** message.

Renew software and hardware of your storage system

You can proactively identify the software and hardware that have expired or are near

expiration in the next 6 months, and send a request to renew the hardware and software.

Steps

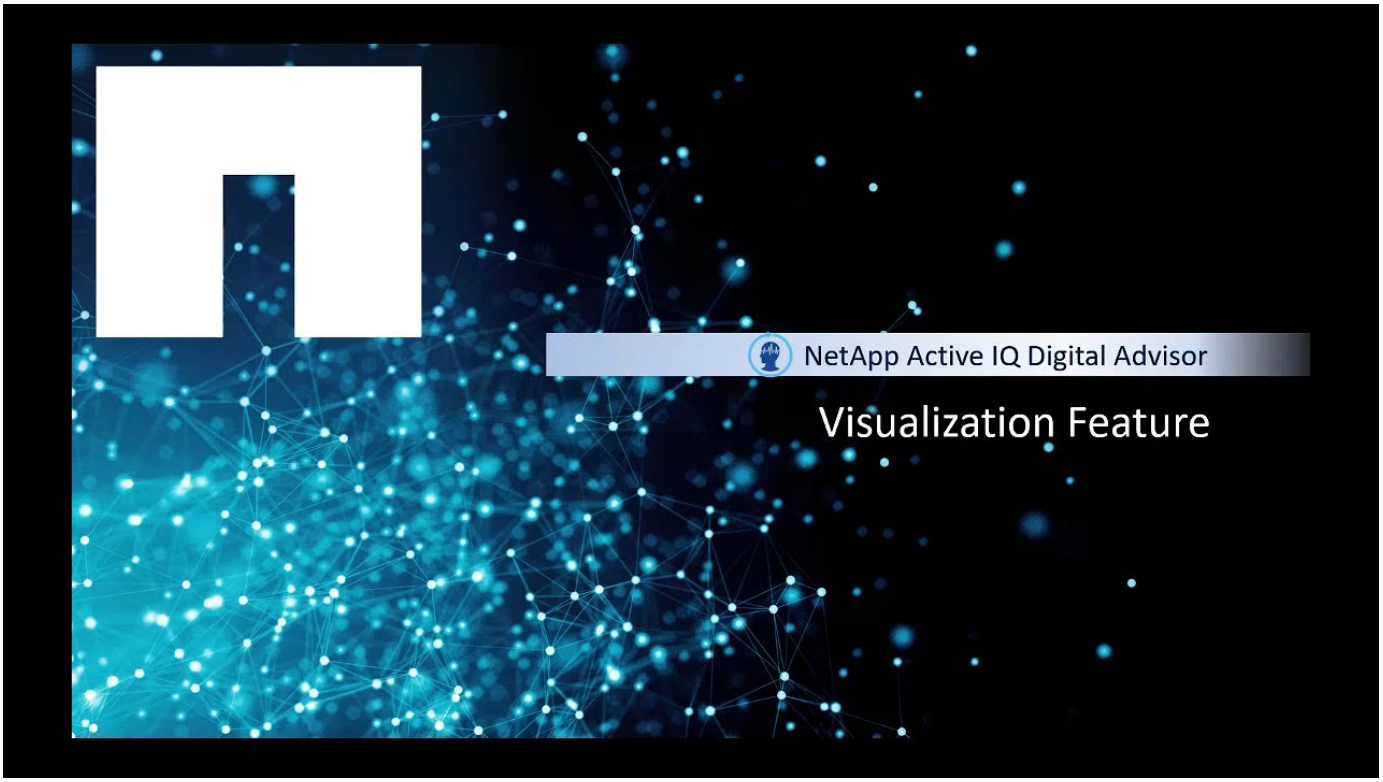
1. Click **Renewals** from the **Planning** widget.
2. Select the systems that you want to renew and click **Renew**.
3. Optionally, provide additional comments.
4. Click **Send**.

Analyze wellness of clusters and nodes

You can analyze the wellness of your clusters and nodes using ClusterViewer, a one-stop source for information on the physical and logical configuration of your clusters and nodes.

ClusterViewer provides information, such as stack diagrams of your nodes, storage usage and efficiency, headroom in hardware capacity, and so on, that helps you take informed decisions to improve the wellness of your clusters and nodes.

You can view visualizations or graphical representations of the physical configuration of your nodes at cable, stack, and RAID Disk levels. You can also download the visualizations in SVG format.



Steps

1. In the **Inventory** widget, select the cluster or node (host) that you want.
2. At the cluster or node level, click **ClusterViewer** next to the **Configuration** widget.
3. Click the **Visualization** tab to view a graphical representation of the cluster.

Analyze the sustainability of your storage system

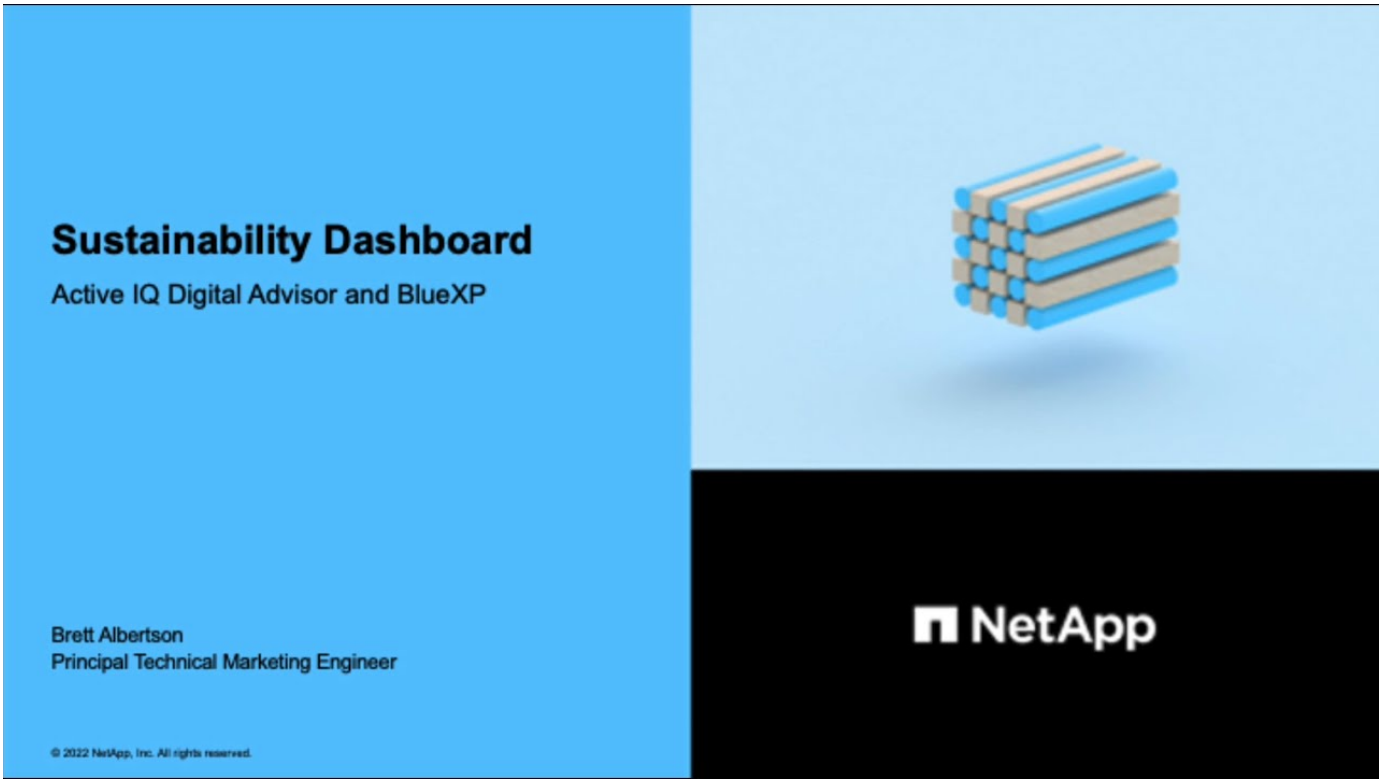
Learn about sustainability

Sustainability, as a service, allows you to reduce the energy consumption and enables you to work towards your environmental goals. This enables you to align your storage systems with eco-friendly practices and achieve the sustainability targets.

You can view the sustainability score, and projected usage of power, direct carbon, and heat from the Sustainability dashboard. You can adjust the carbon mitigation percentage for specific sites. You can also view the sustainability score at the cluster level. Based on the sustainability score, you can assess the sustainability posture and implement NetApp's recommended actions to improve the score. To learn more about the Sustainability dashboard, go to Sustainability dashboard overview.

Sustainability is supported on Cloud Volumes ONTAP, AFF systems (A-Series and C-Series), E-Series, FAS, and StorageGRID systems.

You can view the following video to understand the Sustainability dashboard:



Benefits of sustainability

Sustainability offers the following benefits:

- Accelerate performance by reducing the number of storage devices to store the same amount of data.
- Lower storage costs by optimizing storage systems utilization.
- Reduce carbon footprints by using renewable energy at data centers.
- Improve energy efficiency by implementing energy-efficient policies.

Get started with Sustainability dashboard

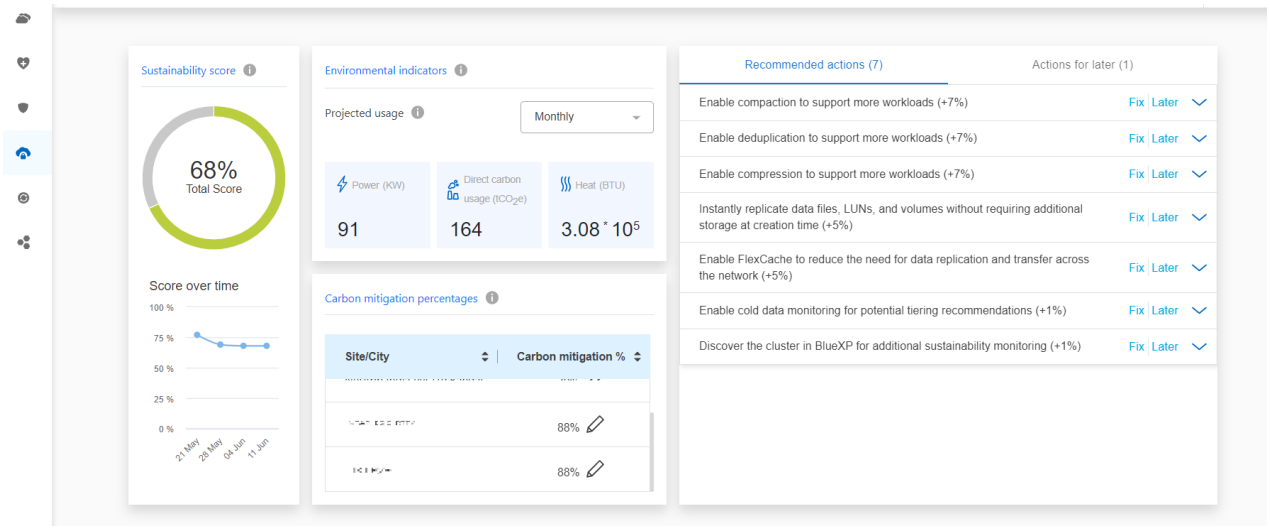
Sustainability dashboard provides AIOps-enabled reporting and scoring with actionable insights to improve your sustainability posture. You can access the Sustainability dashboard through NetApp BlueXP or Digital Advisor.

BlueXP

To log in to BlueXP, you can use your NetApp Support Site credentials or you can sign up for a NetApp cloud login using your email and a password. Learn more about logging in to BlueXP.

Steps

1. Open a web browser, and go to the BlueXP console.
   The NetApp BlueXP login page appears.
2. Log in to BlueXP.
3. From the BlueXP left navigation, select **Governance** > **Sustainability**.
   The Sustainability dashboard appears.



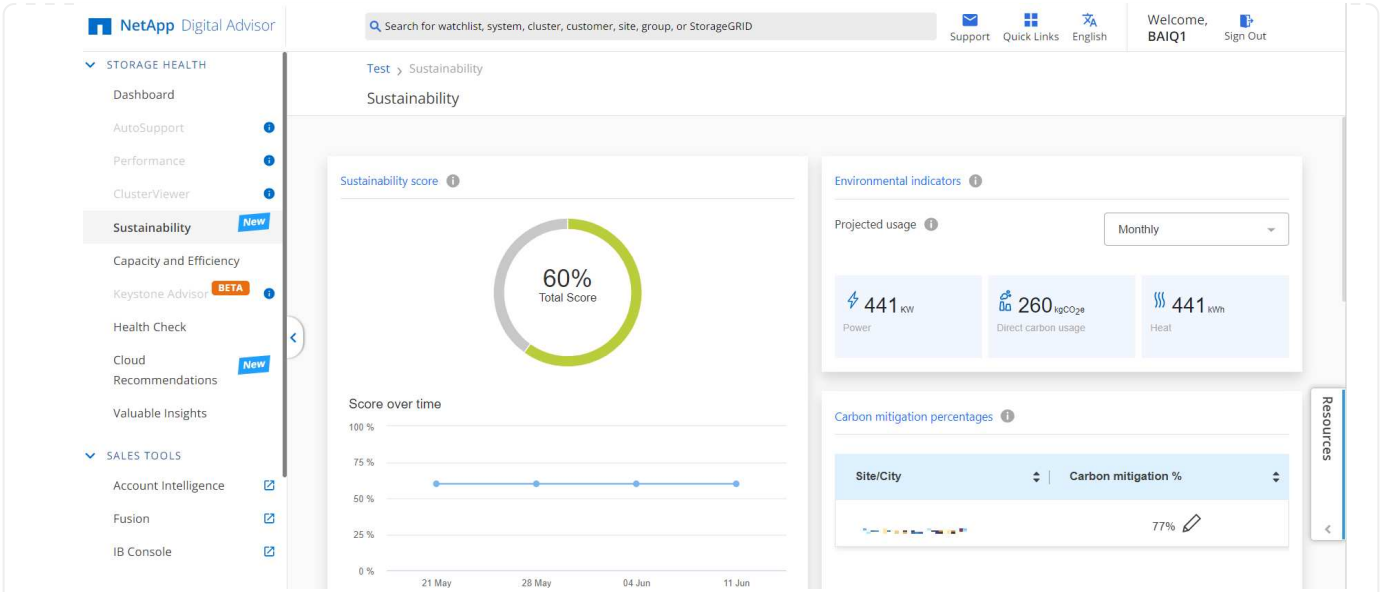
If the Sustainability dashboard is not set up, the option **Add NSS account** appears. Provide your NetApp Support Site (NSS) credentials to view your Sustainability dashboard and the systems associated with your account.

Digital Advisor

To log in to Digital Advisor, you can use your NetApp Support Site credentials.

Steps

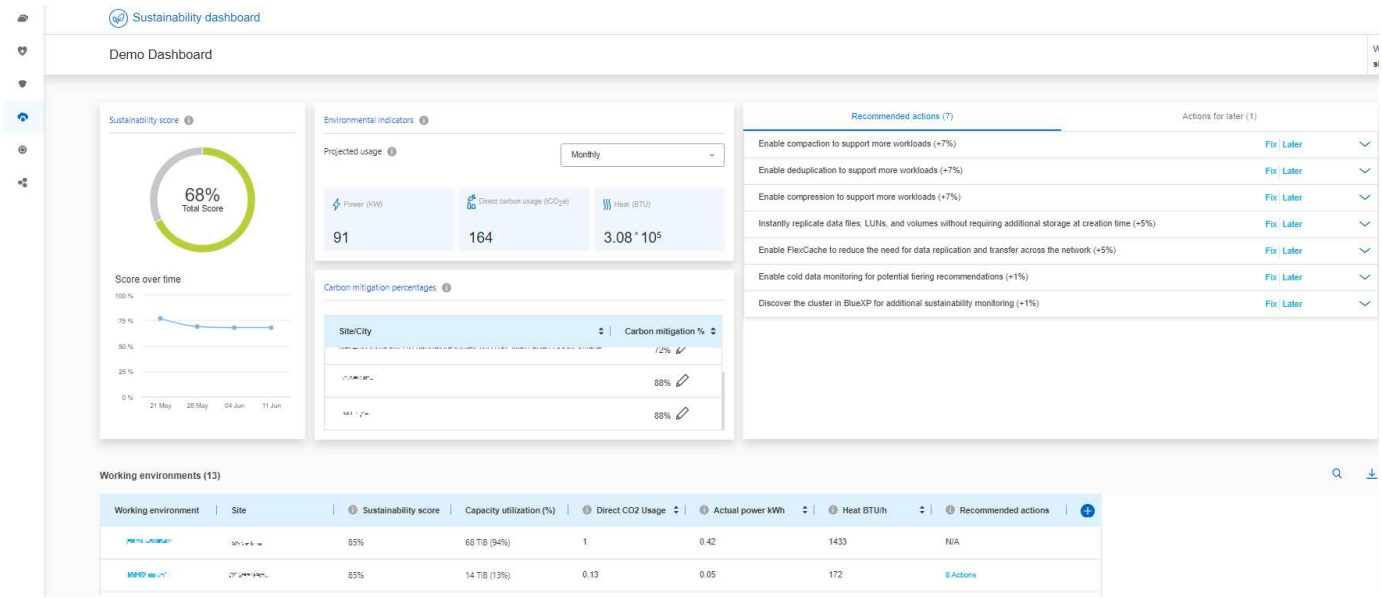
1. Open a web browser, and go to the Digital Advisor login page.
2. Provide your username and password and click **Sign In**.
3. From the left navigation, select **STORAGE HEALTH** > **Sustainability**.



The **Sustainability** option is disabled if the watchlist is not configured. To enable it, you can either create a watchlist or perform a search using customer name, site name, group name, StorageGRID, hostname, cluster, serial number, or system ID. Learn more about watchlist.

Sustainability dashboard overview

Sustainability dashboard provides an environmental assessment of your storage systems and actionable insights for improvement in the form of NetApp's recommended actions.

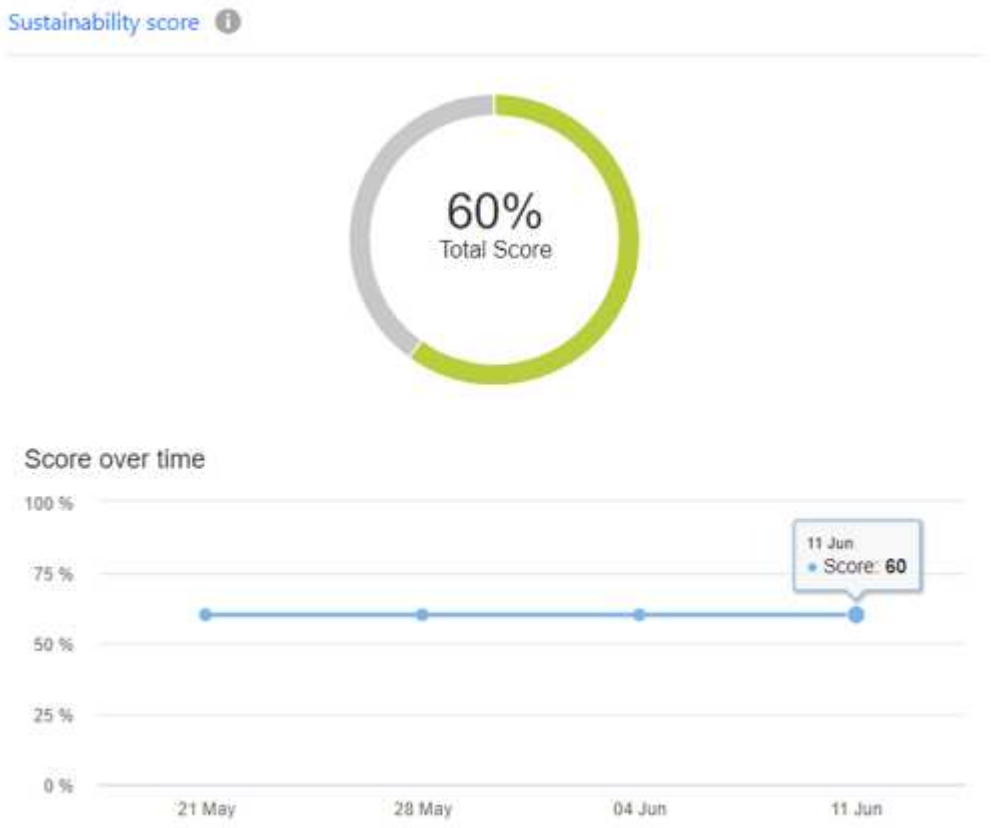


AutoSupport should be enabled for accurate calculation of the sustainability score.

Sustainability score: Displays the total score indicating the environmental sustainability of your storage systems. You can assess the sustainability level of your storage systems based on the following range:

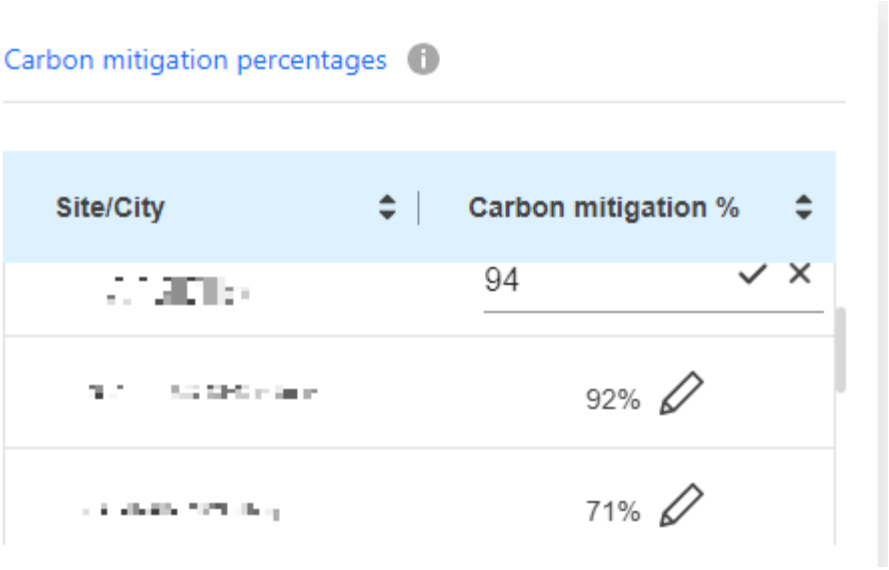
- 76 - 100: Indicates that sustainability is a top priority.
- 51 - 75: Indicates a high level of investment in sustainability initiatives.
- 26 - 50: Indicates good progress towards sustainability initiatives.
- Less than 25: Indicates the need for improvement in sustainability practices.

You can see the graphical representation of the score for up to 5 weeks, which is updated on a weekly basis. You can also see the reason for the increase or decrease in the sustainability score by hovering over the graph.



Environmental indicators: Displays projections for your power, direct carbon usage, and heat emission to evaluate the environmental health of your storage systems. These projections are based on actual power, if unavailable, typical power values. You can view these projections monthly, quarterly, or yearly by selecting the desired option from the drop-down in the top right corner of this section.

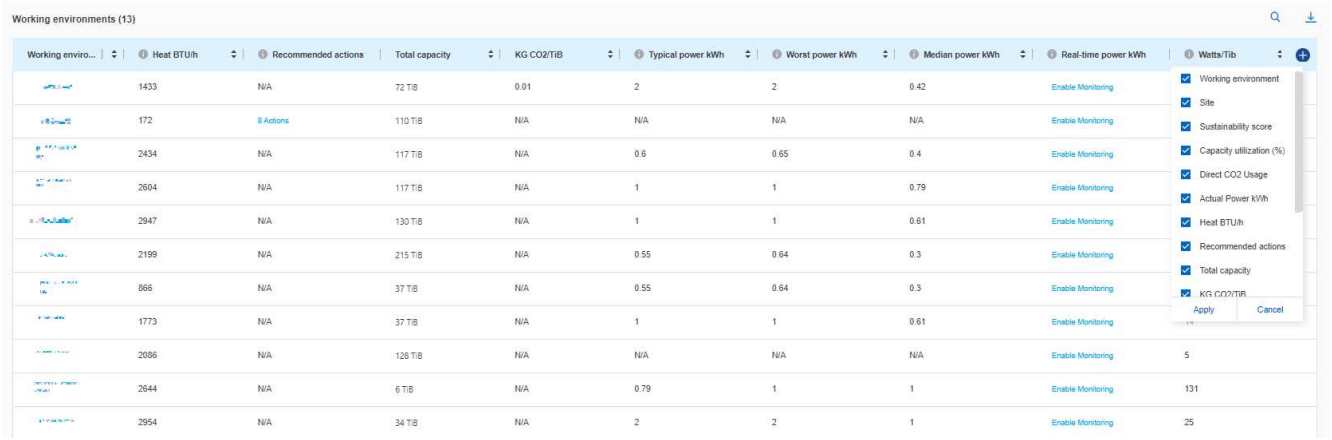
Carbon mitigation percentages: Displays the percentage of carbon mitigation at each site/city, and the presented baseline values are based on your location. You can adjust the carbon mitigation percentage for specific sites by clicking the icon located next to the percentage values, and the carbon numbers will automatically adjust accordingly.



Recommended actions: Displays the list of recommended actions to improve the sustainability score of your storage systems. These actions can be taken immediately, or later.
For more information on how to improve the sustainability score, see Improve sustainability score.

Working environments: Displays environmental parameters in the table that can help in identifying clusters for moving to more efficient storage. From this table, you can:

- View the sustainability score at cluster level, select the cluster name to access **ClusterViewer**, take specific recommended actions to improve the sustainability. For more information, see Improve sustainability score at cluster level.



- Enable monitoring from the **Real-time power** column to view the real-time power details at the cluster level. For more information, see Cloud Insights.

Improve sustainability score

Sustainability dashboard provides recommended actions that you can implement to improve the overall sustainability score and the cluster-level sustainability score.

To get the best results from the dashboard, you must enable AutoSupport. If AutoSupport is not enabled, the data will be based on product specifications. To get real-time power details, you need to enable Cloud Insights. For more information on how to enable Cloud Insights, see Cloud Insights.

Sustainability score computation

The sustainability score is calculated based on a set of rules related to storage systems, with each rule addressing specific risks and providing recommended actions for mitigation. Every rule is given a score to reflect its importance. For example, if there are three rules associated with storage systems: maintaining ambient temperature, ensuring ideal capacity utilization, and using a titanium power supply, with scores of 30, 40, and 30 points, respectively. Adding these scores gives a total of 100 points, which acts as the denominator.

If storage systems meet all criteria perfectly would achieve a sustainability score of 100%. If systems perform at half the optimal level might achieve a score of 50%. The total points serve as a standard, and it is used to compare the actual performance against the ideal performance. You can implement the recommended actions to enhance compliance with these rules, which will improve the sustainability score.

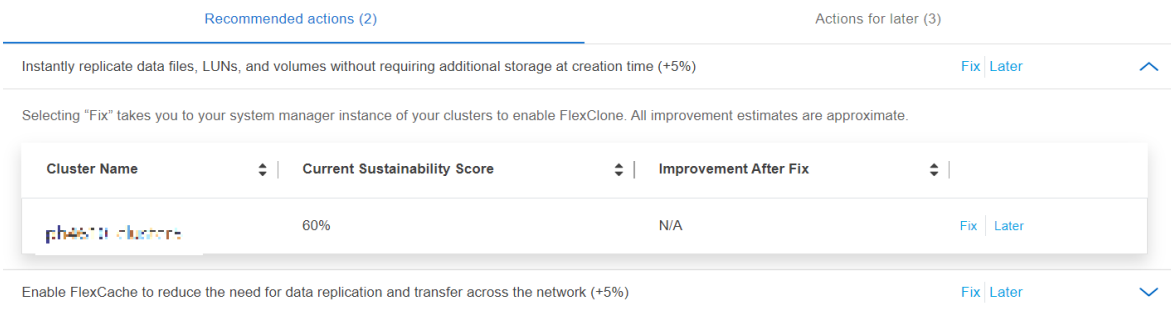
The sustainability score is initially calculated at the cluster level, and then it is aggregated at other levels, such as customer or watchlist level.

Improve overall sustainability score

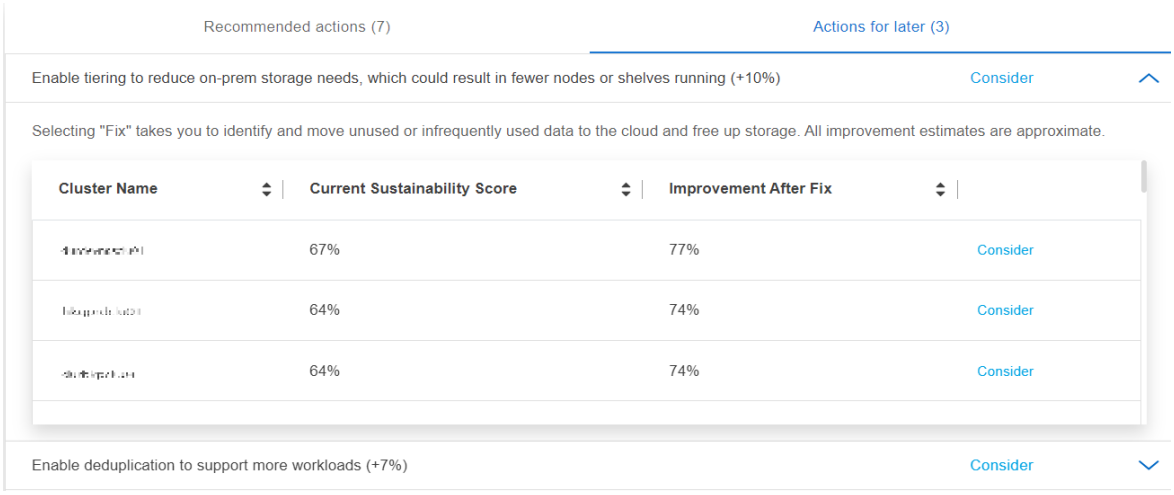
You can follow these steps to improve the overall sustainability score and that focuses on sustainability efforts at company level:

BlueXP

1. Go to **Sustainability** from the **Governance** category available in the BlueXP left navigation.
2. Go to the **Recommended actions** tab.
   - You can select **Fix** to take these actions immediately, or select **Later** to address these actions later.
   - If you plan to address the actions immediately, select **Fix**.
     - It expands the view of the selected recommended action. You can also expand the recommended action view using the down arrow. In the expanded view, you can see the cluster name, the sustainability score, and subsequent increase if you proceed with the **Fix** option.



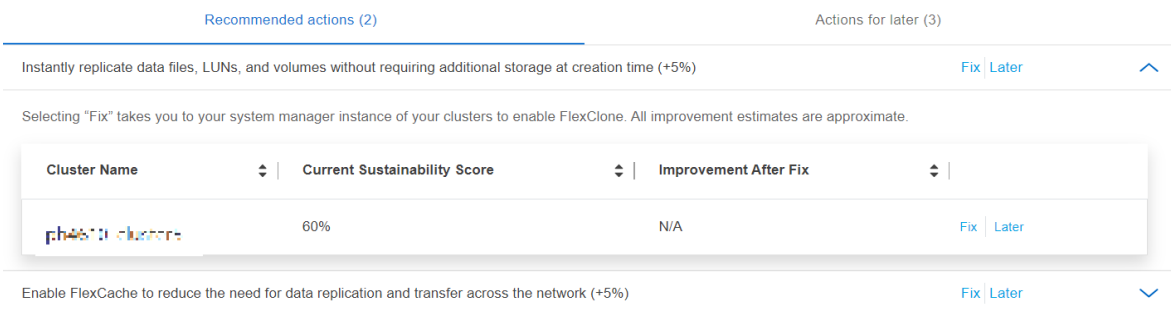
   - If you plan to address the actions later, select **Later**.
     - If you select **Later**, it moves the selected recommended action to the **Actions for later** tab. The selected action will be postponed for 30 days. After 30 days, this action will move to the **Recommended actions** tab.
     - You can also review the postponed actions anytime and can click **Consider** to move them to the **Recommended actions** tab.



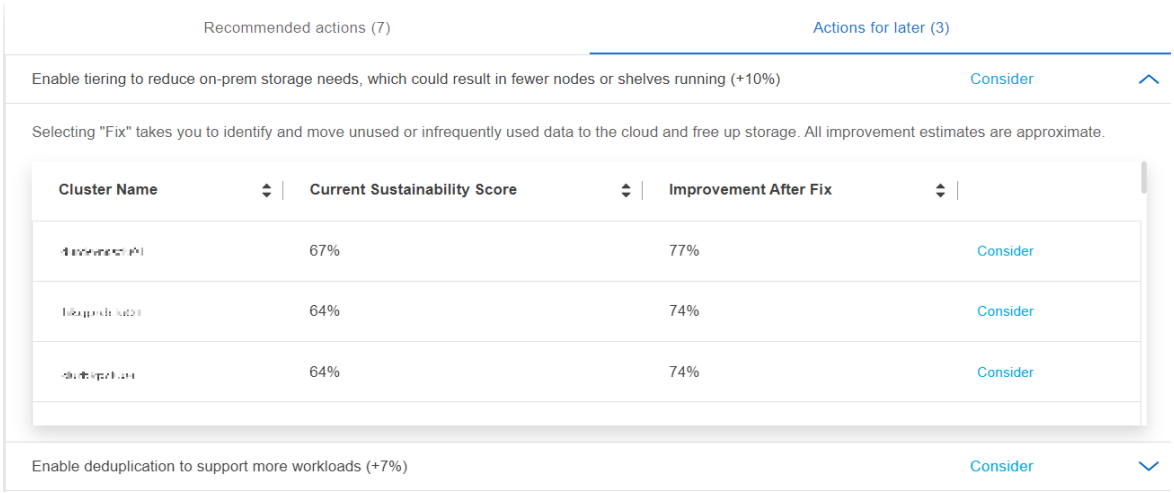
Digital Advisor

1. Go to **Sustainability** from the **STORAGE HEALTH** category available in the left navigation of Digital Advisor dashboard.
2. Go to the **Recommended actions** tab.
   - You can select **Fix** to take these actions immediately, or select **Later** to address these actions later.

- If you plan to address the actions immediately, select **Fix**.
  - The view of the selected recommended action expands. You can also expand the recommended action view using the down arrow. In the expanded view, you can see the cluster name, the sustainability score, and subsequent increase if you proceed with the **Fix** option.



- If you plan to address the actions later, select **Later**.
  - If you select **Later**, it moves the selected recommended action to the **Actions for later** tab. The selected action will be postponed for 30 days. After 30 days, this action will move to the **Recommended actions** tab.
  - You can also review the postponed actions anytime and can click **Consider** to move them to the **Recommended actions** tab.

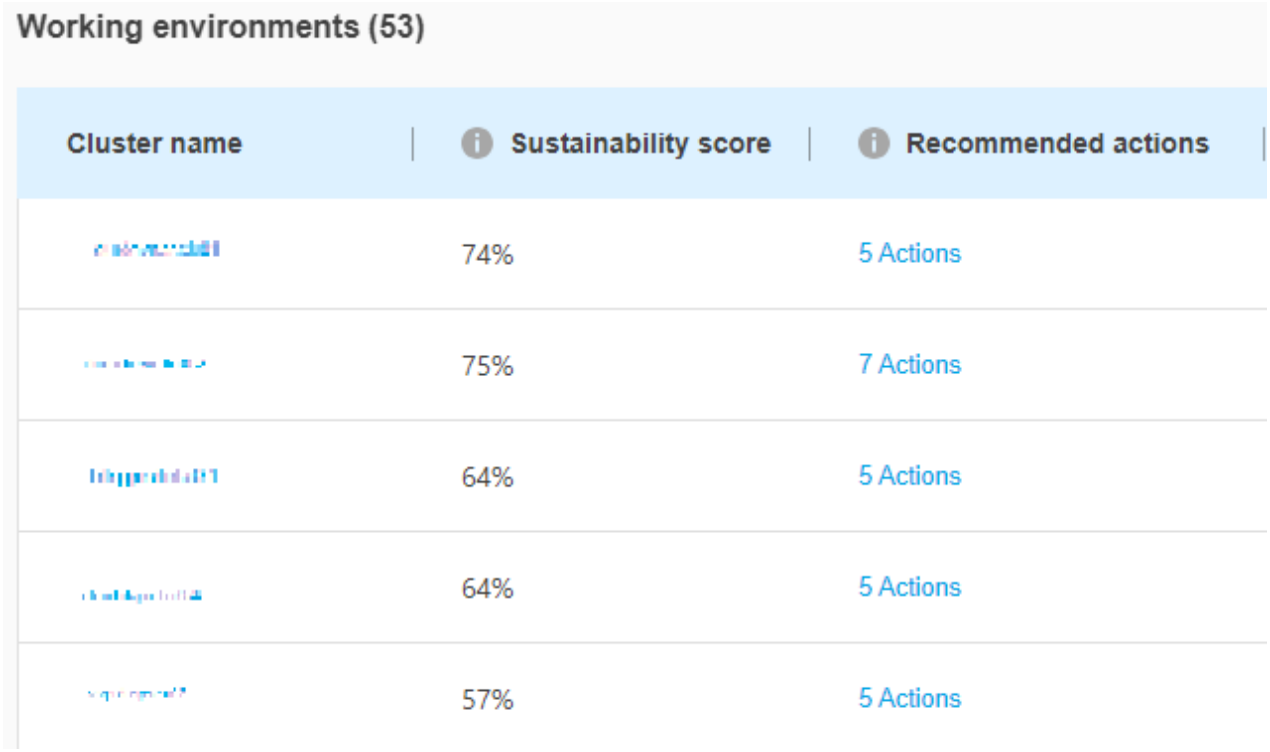


Improve sustainability score at cluster level

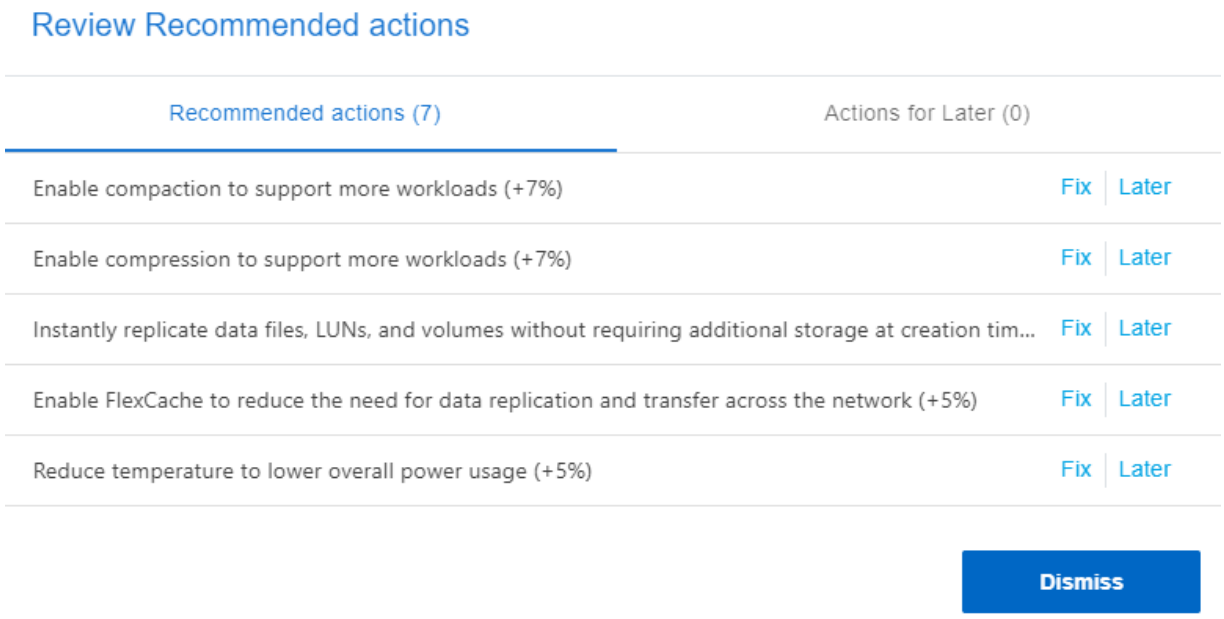
You can follow these steps to improve the cluster-level sustainability score that focuses on improving sustainability for a specific cluster:

BlueXP

1. Go to **Sustainability** from the **Governance** category available in the BlueXP left navigation.
2. Go to the **Working environments** table.
3. Click the number of actions from the **Recommended actions** column for the target cluster.



- You can select **Fix** to take these actions immediately, or select **Later** to address these actions later.



- If you select **Later**, it moves the selected recommended action to the **Actions for later** tab. The selected action will be postponed for 30 days. After 30 days, this action will move to the

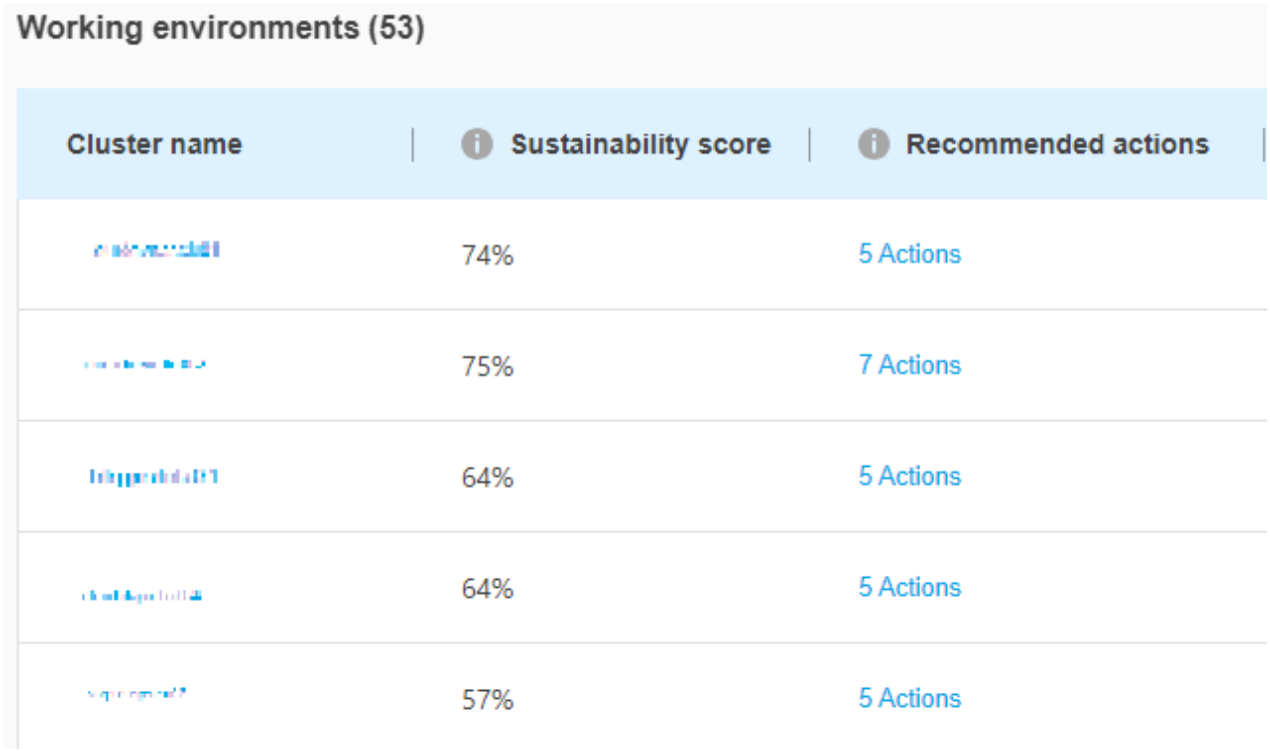
Recommended actions tab.

- You can also review the postponed actions anytime and can click **Consider** to move them to the **Recommended actions** tab.

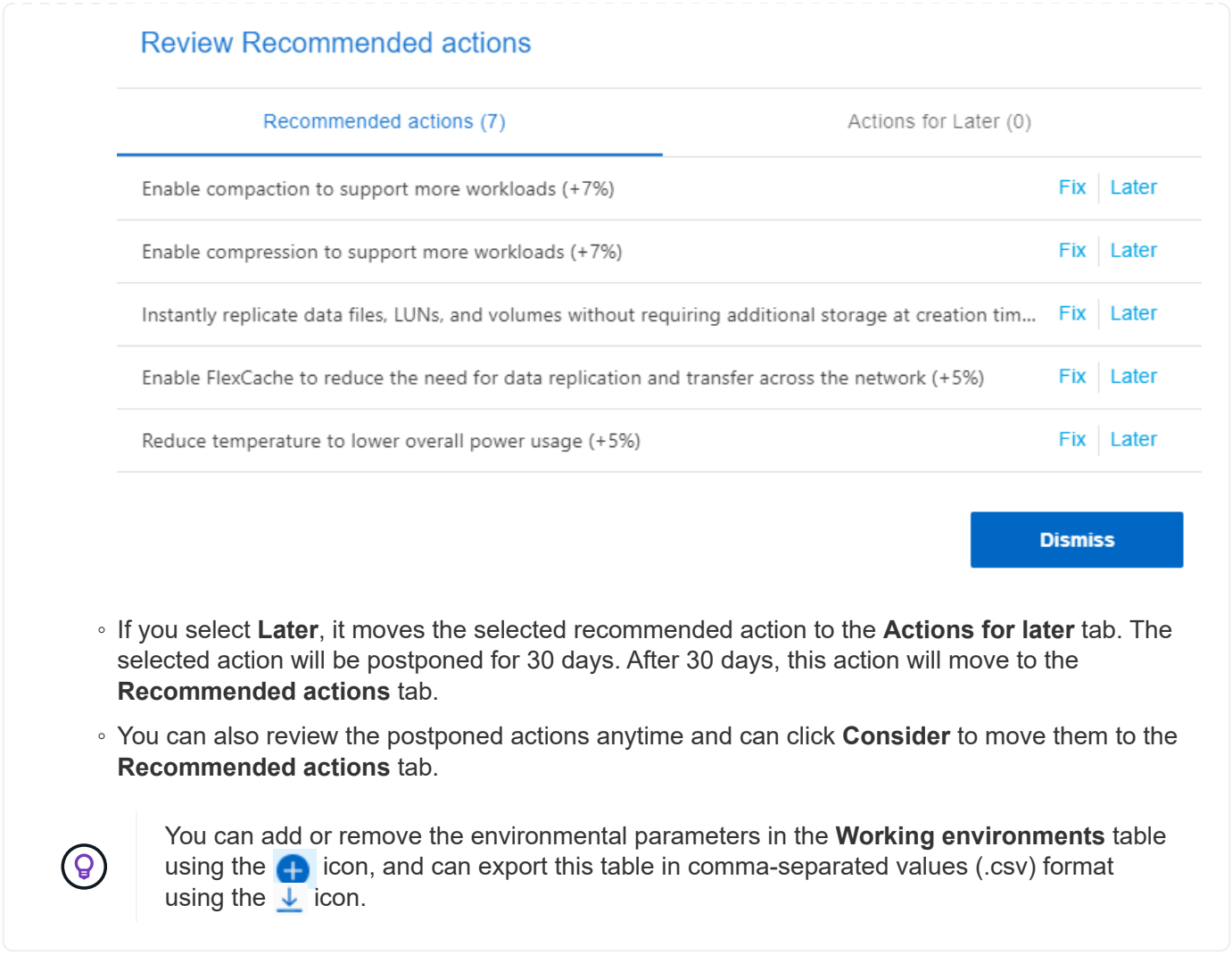
You can add or remove the environmental parameters in the **Working environments** table using the icon, and can export this table in comma-separated values (.csv) format using the icon.

Digital Advisor

1. Go to **Sustainability** from the **STORAGE HEALTH** category available in the left navigation of Digital Advisor dashboard.
2. Go to the **Recommended actions** tab.
3. Go to the **Working environments** table.
4. Click the number of actions from the **Recommended actions** column for the target cluster.



- You can select **Fix** to take these actions immediately, or select **Later** to address these actions later.



- If you select **Later**, it moves the selected recommended action to the **Actions for later** tab. The selected action will be postponed for 30 days. After 30 days, this action will move to the **Recommended actions** tab.
- You can also review the postponed actions anytime and can click **Consider** to move them to the **Recommended actions** tab.

You can add or remove the environmental parameters in the **Working environments** table using the icon, and can export this table in comma-separated values (.csv) format using the icon.

Generate an upgrade plan

Overview

Upgrade Advisor enables you to generate an upgrade plan that includes detailed and step-by-step information required for a successful ONTAP upgrade or revert.

You can generate automated nondisruptive upgrade plans for a single cluster and multiple clusters. You can view upgrade recommendations for a single cluster, which includes a list of risks associated with a cluster, a pre-upgrade check report containing a list of upgrade blockers and warnings, and information about new features and enhancements. The upgrade recommendations are unavailable for multiple clusters. To learn more, see Generate an upgrade plan for single cluster and multiple clusters.

For each cluster in a MetroCluster configuration, generate an individual upgrade plan for complete upgrade instructions.

Before generating an upgrade plan, you should prepare for an ONTAP upgrade. Proper preparation helps in identifying and mitigating potential upgrade risks or blockers before you begin the upgrade process. To learn more, see Prepare for an ONTAP upgrade.

Generate an upgrade plan for single cluster and multiple clusters

You can use Upgrade Advisor to view the list of clusters that are eligible or ineligible for an upgrade. You can view upgrade recommendations for an eligible cluster and generate an upgrade plan. You can fix the issues with an ineligible cluster to make it eligible for an upgrade.

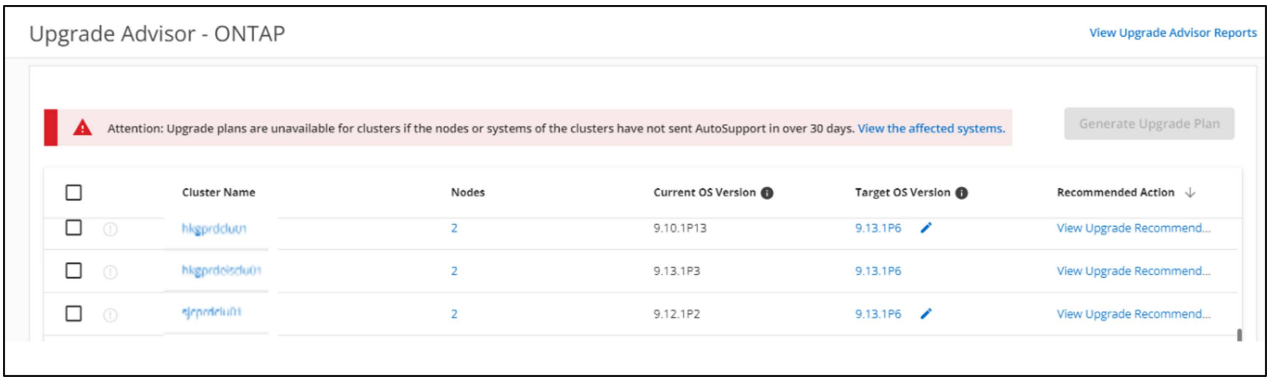
You can follow these steps to generate an upgrade plan for a single cluster and multiple clusters:

Single cluster

1. On the dashboard, click number of clusters in the **Upgrade Advisor** widget.

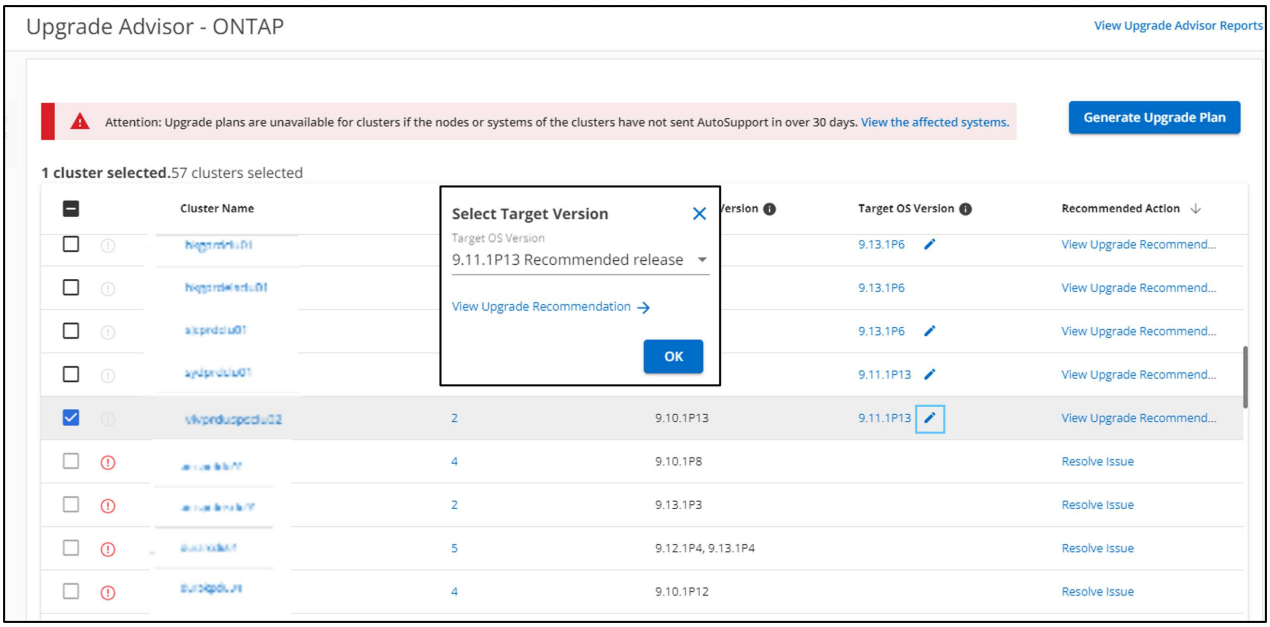
   The **Upgrade Advisor-ONTAP** page appears.

2. You can view a list of eligible and ineligible clusters for an upgrade.

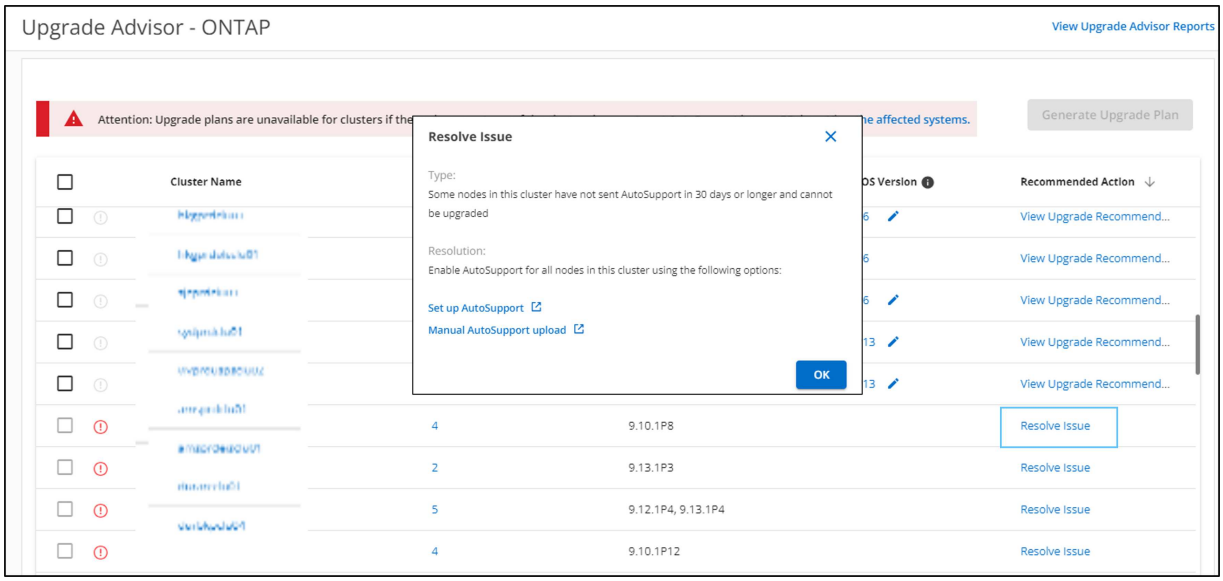


3. Select a cluster for an upgrade.

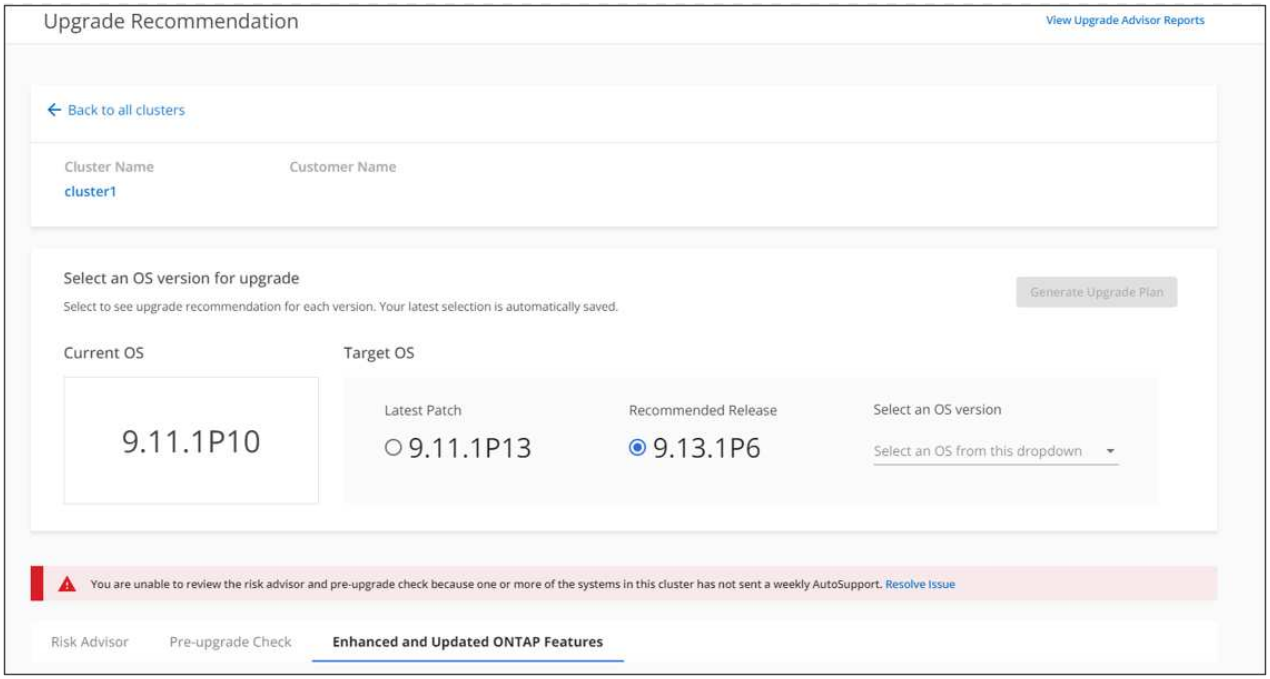
   The **Target OS Version** column displays the recommended target OS version. You can click the icon to select another target OS version of a cluster.



- You can click the number of nodes in the **Nodes** column to see the node summary of a cluster.
- You can click **Resolve Issues** from the **Recommended Action** column to fix the issues with an ineligible cluster to make it eligible for an upgrade.

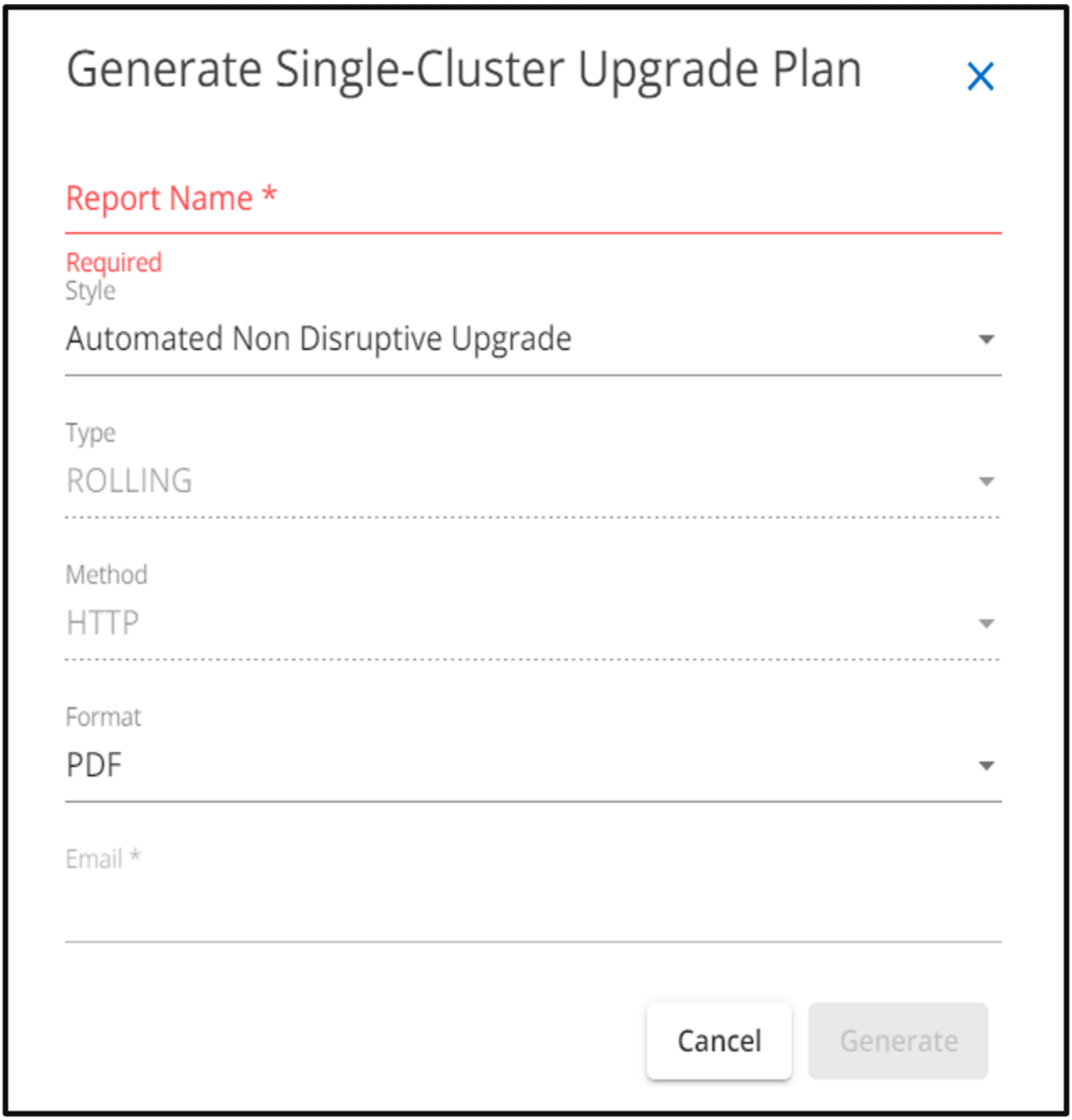


4. Click **Generate Upgrade Plan**.
   You will be redirected to the **Upgrade Recommendation** page.
5. On the **Upgrade Recommendation** page, you can view the details of the risks associated with a cluster through the **Risk Advisor** tab. You can view the upgrade blockers, upgrade warnings, and required actions through the **Pre-upgrade Check** tab, and information about the new features and enhancements that are relevant to the selected target OS version through the **Enhanced and Updated ONTAP Features** tab.



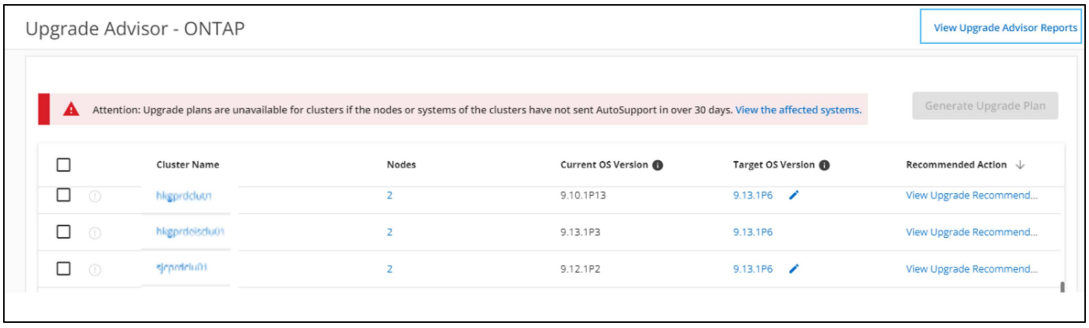
- You can select another target OS version and view the risk summary, pre-upgrade check report, and information on new features and enhancements related to that target OS version.
- You can click the Export icon to export the risk summary to an Excel sheet.

6. Click **Generate Upgrade Plan** from the **Upgrade Recommendation** page.
7. Provide the details in the displayed pop-up.



8. Click **Generate**.
   You will be redirected to the **Reports** page.
9. You can download the upgrade plan from the **Reports** page once it is available.

You can click **View Upgrade Advisor Reports** to go to the **Reports** page.



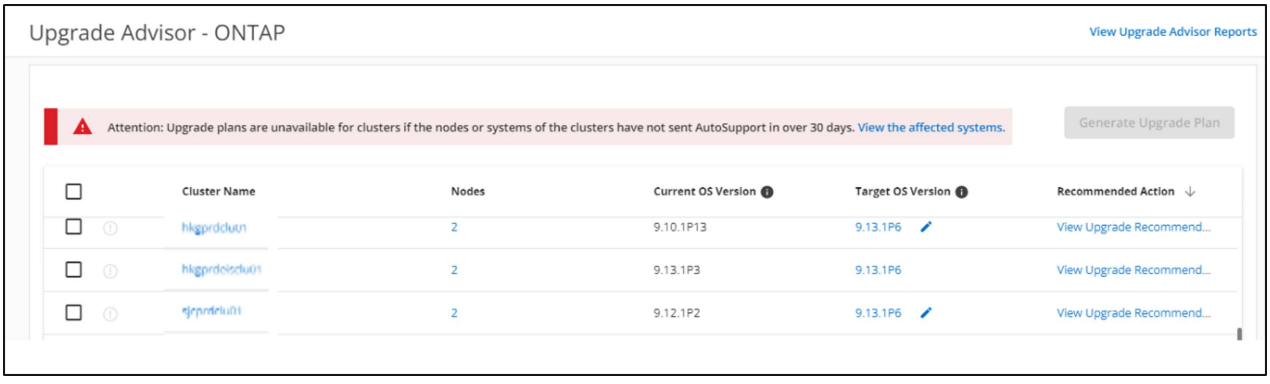
There are some tasks you should perform to confirm the readiness of the cluster after you upgrade ONTAP. To learn more, see What to do after an ONTAP upgrade.

Multiple clusters

1. On the dashboard, click number of clusters in the **Upgrade Advisor** widget.

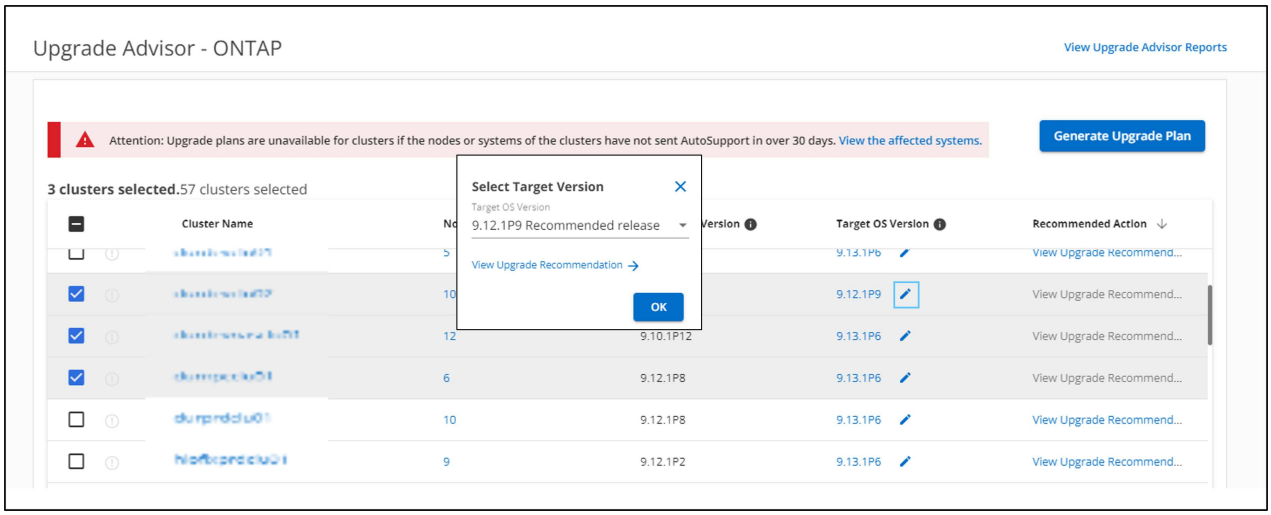
   The **Upgrade Advisor-ONTAP** page appears.

2. You can view a list of eligible and ineligible clusters for an upgrade.

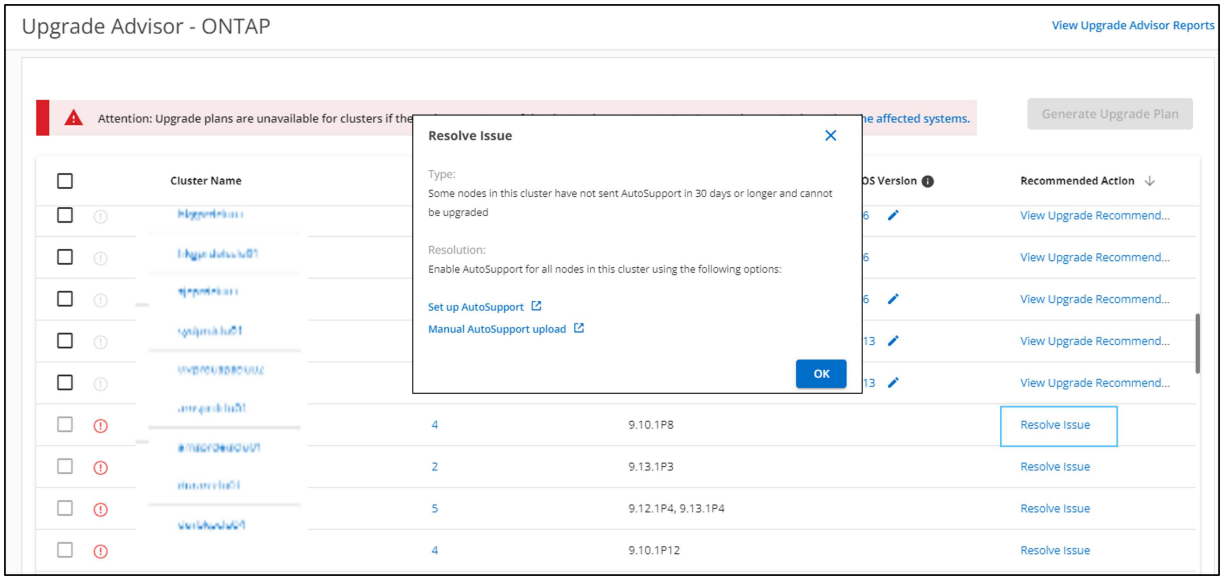


3. Select clusters for an upgrade.

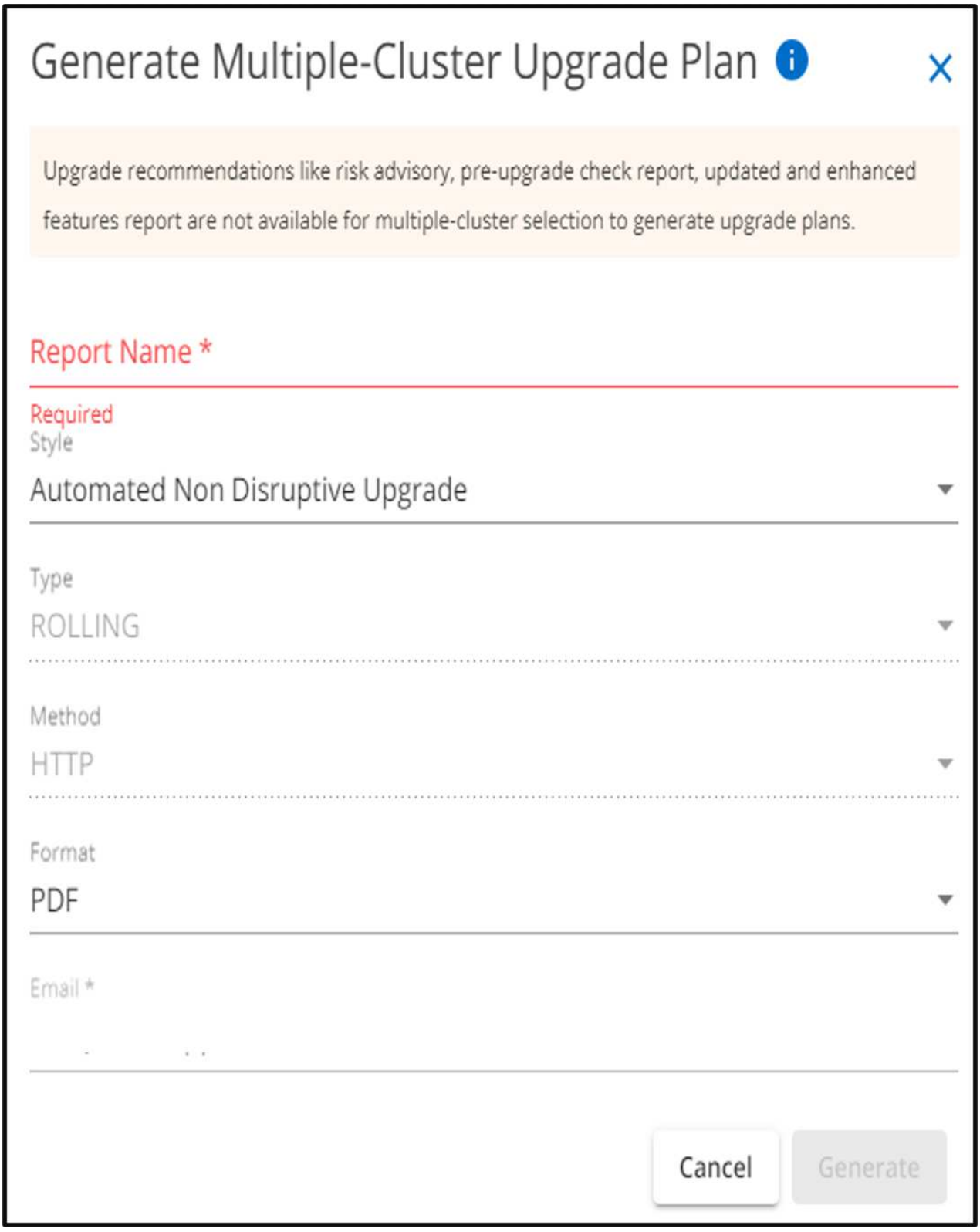
   The **Target OS Version** column displays the recommended target OS version.You can click the icon to select another target OS version of a cluster.



- You can click the number of nodes in the **Nodes** column to see the node summary of a cluster.
- You can click **Resolve Issues** from the **Recommended Action** column to fix the issues with ineligible clusters to make them eligible for an upgrade.

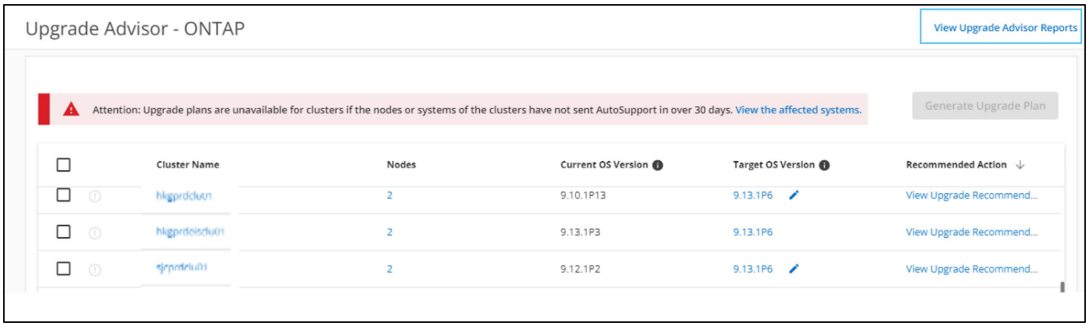


4. Click **Generate Upgrade Plan**.
5. Provide the details in the displayed pop-up.



6. Click **Generate**.
   You will be redirected to the **Reports** page.
7. You can download the upgrade plan from the **Reports** page once it is available.

You can click **View Upgrade Advisor Reports** to go to the **Reports** page.



There are some tasks you should perform to confirm the readiness of the cluster after you upgrade ONTAP. To learn more, see What to do after an ONTAP upgrade.

View firmware update recommendations

Customers can now save time and effort by allowing Control Tower to automatically update their systems with the latest firmware versions, eliminating the need for manual intervention or scheduling. This update reduces the risk of encountering issues due to outdated or incompatible firmware versions, ensuring optimal system performance, stability, and security.

Customers will receive timely notifications and alerts about the status of the firmware updates, with options to enable AutoSupport and auto-update settings.

Steps

1. On the dashboard page, click **Other recommendations** in the **Upgrade Advisor** widget.
2. Click **View recommendations** to view the list of recommendations.
3. In the **Update Status** column, click **See progress** to view the clusters that are eligible for an update.
4. In case of any issues, click on the respective links to view the steps to mitigate the issues.

View system details

View inventory details

The **Inventory** widget provides you with a rollup of the total systems and the support entitled switches that you own. This includes both Digital Advisor enabled and non-enabled products.

You can also generate the report of the selected watchlist and email the report to a maximum of 5 recipients.

View system details

Steps

1. In the **Inventory** widget, click **Systems** to view the system information of all platforms or click the platform type and then click **Systems** to view systems specific to that platform.
2. Click the node or cluster to view detailed information about the system.
3. Download the **Inventory** report to view the system details in .xls format.
4. Download the **Ansible Inventory** report to view the system details in the .yml and .ini formats at the region or site level.

   The Ansible Inventory files can be used with customized Ansible Playbook files to make infrastructure configuration changes.

View support entitled switch details

Steps

1. In the **Inventory** widget, click **Support Entitled Switches** to view information about all the support entitled switches.

Integrating with Cloud Insights to view virtual machines details

Digital Advisor is now integrated with Cloud Insights Basic version to provide a full stack inventory and interoperability checks to customers.

The benefits of this integration are:

- Simplified SaaS monitoring of ONTAP

- Visibility into VMware full-stack monitoring
- Productivity savings for customers through automated interoperability checks to help with ONTAP upgrade planning. This results in smoother ONTAP upgrades and reduces risks of incompatibility with hosts.

This feature is available only for SupportEdge Advisor, SupportEdge Expert, and Digital Advisor Upgrade contracts.

Steps

1. In the **Inventory** widget, click **Virtual Machines** to view the data available in Cloud Insights.
2. Click the **Virtual Machine Overview** tab.
3. Click the **Count of ESX Hosts** to view information about the host.
4. Click the **ESX Name** to navigate to Cloud Insights to view more information.

View valuable insights

The **Valuable Insights** widget provides information about the number of support cases, pending software upgrades, storage efficiency savings, risks mitigated, and others. It also proactively lists the risk notifications from the **Wellness** attribute.

Steps

1. In the **Inventory** widget, click **Systems** to view the system information of all platforms or click the platform type and then click **Systems** to view systems specific to that platform.
2. Click the node or cluster to view detailed information about the system.

   The **Valuable Insights** widget is available on the dashboard.

3. Review the information in the widget to understand the business and technical value received from your

support contract.

View capacity utilization with NetApp Keystone subscription

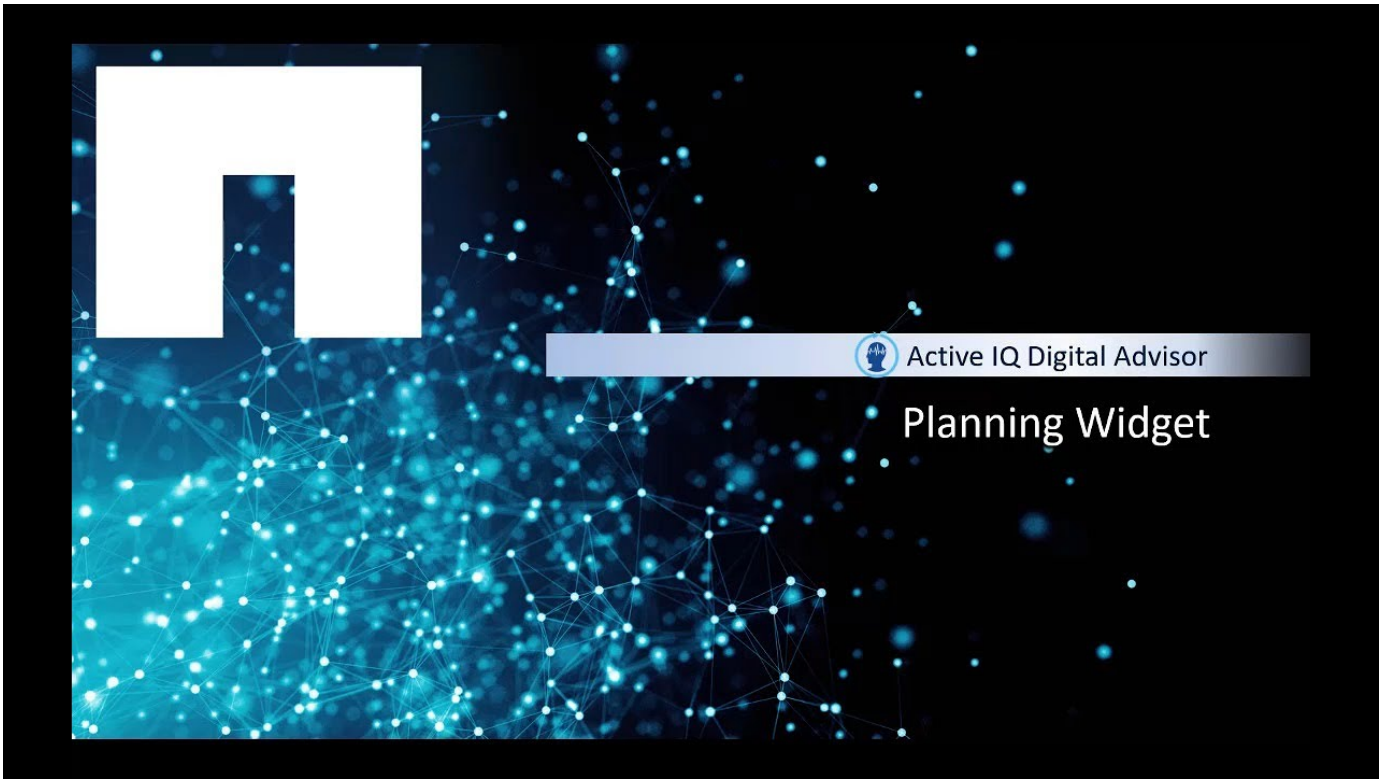
If you are subscribed to NetApp Keystone STaaS services, you can view the Keystone Subscription widget on the Digital Advisor Dashboard.

The Keystone Subscription widget provides you a summary of the capacity usage for your account. It consists of capacity utilization charts with respect to the physical capacity. For more information about the various levels of subscription data and usage information, see Keystone and Digital Advisor.

Identify system requirements proactively

Understand planning

The **Planning** widget helps customers identify capacity requirements that have exceeded 90% capacity or are nearing 90% capacity and identify the software and hardware that have expired or are near expiration in the next 6 months. You can send a request to increase the capacity of your storage system and to renew the hardware and software.



Identify systems reaching capacity limits

Proactively identify systems reaching capacity limits and send a request to increase the capacity of your storage system.

For ONTAP, you can view systems that have exceeded 90% capacity or are to exceed 90% capacity in 1, 3, and 6 months. For StorageGRID, you can view systems that have exceeded 70% capacity or are to exceed 70% capacity in 1, 3, and 6 months.

Steps

1. In the **Planning** widget, click **Capacity Additions**.

   By default, the ONTAP systems that have exceeded 90% capacity or are nearing 90% capacity are displayed.

2. Click **StorageGRID** tab to view the StorageGRID systems that have exceeded 70% capacity or are nearing 70% capacity.
3. Select the systems for which you want to increase capacity.
4. Click **View Capacity Forecast** to view the capacity forecast for the next 6 months.
5. Click **Request to Add Capacity**.
6. Optionally, provide any comments.
7. Click **Send** to send the request to the NetApp storage team to assist with the capacity addition for the selected systems.

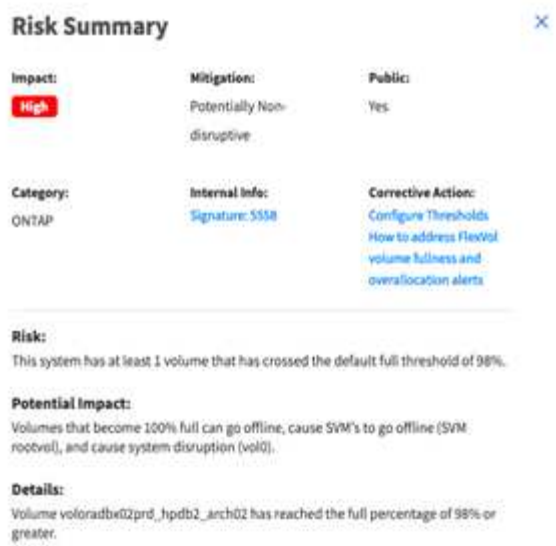
Avoid a volume filling up to prevent an outage

When you log in to Digital Advisor and notice the red badge on the **Configuration** widget. Upon clicking the widget, you see that the volume is 98% full and this might cause an outage. Fixing this issue would avoid a volume filling up, which would make it go read-only resulting in applications accessing it crash and fail.

Steps

1. Log in to Digital Advisor.
2. Click **Actions** in the **Configuration** widget.

3. Click the **Unique Risks** tab. Upon clicking the **Corrective Action** link, you can either change the warning thresholds or allocate more space to the volume.



Evaluate a technology refresh

If you want to identify whether a technology refresh is recommended for your Tech Support contract or hardware, you can use the tech refresh option.

> You can access this feature either through BlueXP economic efficiency (**Governance > Economic efficiency > Tech refresh**) or through NetApp Digital Advisor (**Dashboard > Planning widget > Tech Refresh**).

For more information about this feature, see Evaluate a technology refresh in the BlueXP documentation.

Renew software and hardware of your storage system

You can proactively identify the software and hardware that have expired or are near expiration in the next 6 months, and send a request to renew the hardware and software.

Steps

1. Click **Renewals** from the **Planning** widget.
2. Select the systems that you want to renew and click **Renew**.
3. Optionally, provide additional comments.
4. Click **Send**.

Make informed decisions based on cloud recommendations

Digital Advisor constantly analyzes your system and provides recommendations to improve the performance, efficiency, and health of your system.

> Digital Advisor navigates you to BlueXP to implement the recommendations.

Migration

Provides information about the different types of workloads available within your storage system and identify the workloads that are cloud-ready. Moving workloads to the cloud result in cost savings and provide cloud disaster recovery.

The volumes that meet the following criteria are recommended for migration to Cloud Volumes ONTAP (CVO) and Cloud Volumes Service (CVS):

- Volumes should be using NFS, SMB, CIFS, FCP, or iSCSI protocol
- Root volumes are excluded
- Workloads in the volume are tagged as ORACLE, SAP, SAP HANA, MSSQL, MYSQL, SHAREPOINT, FILESHARE, VIRTUALIZATION and TRIDENT
- System age is greater than 1 year
- Support contract is ending in 6 months

Steps

1. From the left pane, click **Cloud Recommendations**.
2. Click on any one link in the **Migration** pane.
3. Click **Migrate to Cloud** to launch **BlueXP**.

Tiering

Provides information about inactive local tier (aggregate) data, inactive volume data, tiered data, and unmonitored data. You can reduce your storage footprint and associated costs by monitoring and tiering your cold or inactive data to low-cost object storage tiers.

You can enable Inactive Data Reporting (IDR) to generate a zip file with an Ansible Playbook file. This information is available at customer, site, group, watchlist, cluster, and node levels.

The volumes that meet the following criteria are recommended for tiering:

- Volumes should be using NFS, SMB, or CIFS protocol
- Root volumes are excluded
- Inactive Data is more than 50%
- Aggregate Capacity is more than 50%

Steps

1. From the left pane, click **Cloud Recommendations**.
2. Click on any one link in the **Tiering** pane.
3. Click **Tier Data** to launch **BlueXP**.

To learn more about FabricPool, refer to FabricPool Best Practices.

Backup & Archive

Provides information about the systems that should be backed up to the cloud. You can use NetApp Cloud Backup to secure your systems and restore them back when required.

The volumes that meet the following criteria are recommended for backing up to the cloud:

- Root volumes are excluded
- Source volumes and destination systems and volumes that have SnapVault backup are excluded.

Steps

1. From the left pane, click **Cloud Recommendations**.
2. Click on any one link in the **Backup & Archive** pane.
3. Click **Backup to Cloud** to launch **BlueXP**.

Replication

Provides information about the data that should be replicated to the cloud to help in case of disasters.

The volumes that meet the following criteria are recommended for replication to the cloud:

- Root volumes are excluded
- SnapMirror source volumes are excluded
- SnapMirror destination volumes (volume type LS and DP) are excluded

Steps

1. From the left pane, click **Cloud Recommendations**.
2. Click on any one link in the **Disaster Recovery** pane.
3. Click **Replicate to Cloud** to launch **BlueXP**.

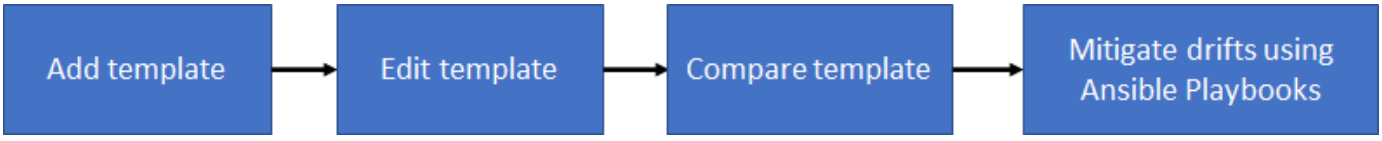
Identify configuration deviation

Understand configuration deviation

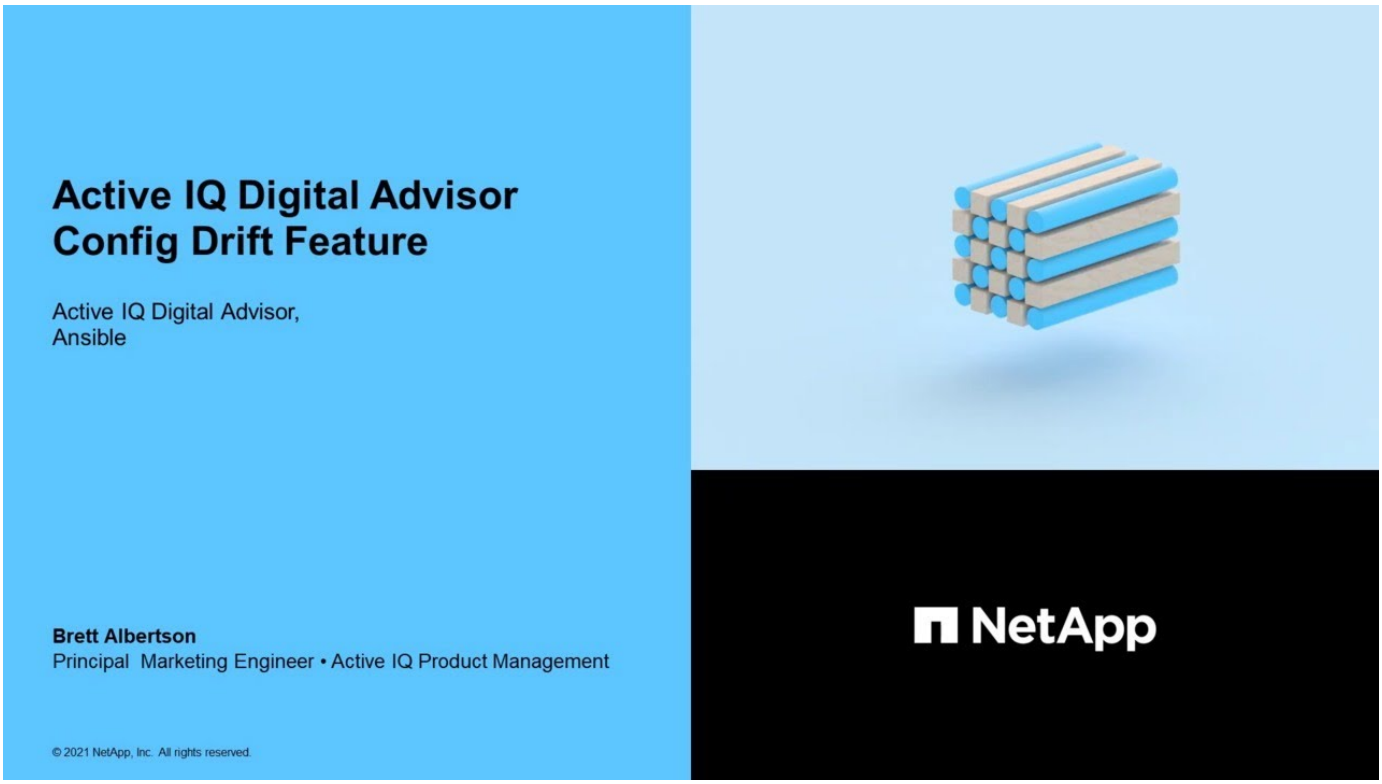
The Config Drift feature identifies configuration deviations by comparing a system template to a “golden” or base system template. You can schedule weekly or monthly drift reports or generate them on-demand. You can mitigate some deviations by using the Ansible Playbooks, which are provided in the config drift report.

This feature is available to systems with Advisor and Expert Support contracts only.

You can look at the following diagram to understand the workflow to identify configuration deviations and generate the report.



You can view the following video to generate and run an Ansible Playbook to fix the configuration deviations:



Add a config drift template

You should add a template to compare the system and cluster configurations and detect the configuration deviations in near real time. The config drift templates are added using systems running AutoSupport data.

About this task

The attributes in a config drift template are editable, and the following groups of the template support regular expressions for some sections:

Group	Section	Attribute
AGGREGATE	AGGR-INFO.XML	name
CLUSTER	CLUSTER-INFO.XML	cluster-name
LUN	LUN.XML	name
VSERVER	VSERVER-INFO.XML	vserver
NETWORK	NETWORK-INTERFACE.XML	vif
DNS	DNS.XML	domains
VOLUME	VOLUME.XML	vol

Using a regular expression, a user can create a config drift report that includes drifts arising from naming inconsistencies of volumes, aggregates, clusters, and so on. For instance, if a regular expression **aggr-name*** is mentioned for the attribute **Name** for the section **AGGR-INFO.XML** in the group **AGGREGATE**, then the values of the attribute without the prefix **aggr-name** are marked as a drift when the config drift report is generated.

Steps

1. From the left pane, click **Config Drift**.
2. Click **Add Template**.
3. Provide the requested values.
4. Optional: You can customize the template by editing the groups or deleting the non-required groups for a template.
5. Click **Add Template**.

Compare a config drift template

You can compare the system and cluster configurations and detect the configuration deviations in near real time.

Steps

1. From the left pane, click **Config Drift**.
2. Select one of the existing templates or click **Add Template** to add a new template.
3. Generate a config drift report

   You can generate a report immediately or you can schedule the report to be generated on a weekly or monthly basis.

To generate a report immediately	To schedule the report to be generated on a weekly or monthly basis
1. Select a category and provide the requested values for the report. 2. Select **Include only drifts** option to download only the configuration deviation changes. 3. Click **Submit**. 4. Download and view the config drift report. 5. Run Ansible Playbook (included as part of the config drift report) to mitigate the drifts.	1. Click the **Schedule Report** tab. 2. Select a category and provide the requested values for the report. 3. Select **Include only drifts** option to download only the configuration deviation changes. 4. Select the frequency of the report. 5. Select the start date and end date for the report. 6. Click **Submit**. 7. Download and view the config drift report. 8. Run Ansible Playbook (included as part of the config drift report) to mitigate the drifts.

An email is sent with the details of the configuration deviation between the selected systems.

Generate a drift timeline report

You can compare the AutoSupport data of the last 90 days and generate a report that provides information about the events and the configuration deviations that have occurred.

Steps

1. From the left pane, click **Config Drift**.
2. Select the **Drift Timeline** report type.
3. Generate a drift timeline report

   You can generate a report immediately or you can schedule the report to be generated on a weekly or monthly basis.

To generate a report immediately	To schedule the report to be generated on a weekly or monthly basis
1. Select a category and provide the requested values for the report. 2. Select **Include only drifts** option to download only the configuration deviation changes. 3. Click **Submit**. 4. Download and view the drift timeline report.	1. Click the **Schedule Report** tab. 2. Select a category and provide the requested values for the report. 3. Select **Include only drifts** option to download only the configuration deviation changes. 4. Select the frequency of the report. 5. Select the start date and end date for the report. 6. Click **Submit**. 7. Download and view the drift timeline report.

Manage a template

You can clone a template, share a template, edit the details of an existing template, and delete a template.

Sharing a template saves the time and effort required to create and customize a template that has already been created by a user. Shared templates can be mutually changed by shared users, allowing several users to make modifications to a single golden template.

About this task

- Access to shared templates can be revoked at any time.
- Shared users can delete this template from their account at any time.

Steps

1. From the left pane, click **Config Drift**.
2. Click  to make a copy of the template.
3. Click  and enter the usernames with whom you want to share the template.

   If you enter the email address of the user instead of the username, the template will not be shared.

4. Click  to update the details of the template.
5.

Click to delete the template.

Improve the efficiency and performance of your storage system

Analyze capacity and storage efficiency savings

You can view the capacity details and the storage efficiency savings of your system and take appropriate actions. The capacity and storage efficiency information can be viewed either at a cluster level or a node level.

This feature is not supported on E-Series systems.

The capacity dashboard displays the capacity details and the capacity forecast of your system. Capacity forecast uses historical capacity information to identify the utilization of each system. Based on the historical data (a year's data, if available) of utilized and allocated capacity, the algorithm considers the current utilization of each system and generates a forecast for the system's utilization over the next 1 through 6 months.

The storage efficiency dashboard displays the data reduction ratio, the logical space used, the physical space used, and the total data saved for storage systems running ONTAP 9.1 and later. The data reduction ratio and savings can be seen with and without Snapshot copies for AFF systems, non-AFF systems, or both. The total data savings across customer storage can be seen per efficiency feature such as volume deduplication, volume compression, compaction, FlexClone volumes, and Snapshot copies. You can view the top 5 storage systems with the best efficiency ratio. You can also view the SAN and NAS efficiency without Snapshot copies at a node level for ONTAP systems including AFF A-Series, AFF C190, All SAN Array, and FAS500 running ONTAP 9.10 and later.

Steps

1. From the left pane, click **Capacity and Efficiency**.

   By default, the **Capacity** tab is selected.

2. View the capacity details at the cluster and node level.
   a. View the capacity forecast at the node level.

      For ONTAP systems, information about RAW capacity is available in ClusterViewer.

   b. Click **Add Capacity** to send a notification to NetApp or your partner to add capacity.
3. View the storage efficiency and the data savings of your storage system.
   a. If the storage efficiency ratio of your storage system is higher than the average storage efficiency ratio, click **Share Your Success Story** to let us know the best practices followed.
   b. If the storage efficiency ratio of your storage system is less than the average storage efficiency ratio, click **Contact Us** to let us know the configurations of your storage system.

For more information about capacity and storage efficiency, see Frequently asked questions about Digital Advisor.

Analyze performance graphs

Performance graphs enable you to analyze the performance of your storage devices. You can view detailed performance graphs for an ONTAP cluster or multiple nodes of an ONTAP cluster and E-Series controllers. These graphs provide historical performance data, which can be used for understanding performance trend and pattern analysis. You can select a date from the calendar to view performance graphs for a day, week, month, two months, and twelve months. You can select multiple nodes to view a particular graph at the same time.

You have an option to set preferences, for example, you can view either one graph for three nodes or two graphs for three nodes.

When the graph is first displayed, a 1-week tab is preselected and it presents data for a 1 week in a graphical format to make it easier to understand large quantities of data and its relationship between different series of data. If you want to reset the date range, for example, you can click 1-month tab and select dates in the calendar.

You also have an option to zoom in performance graph; the individual data points are displayed.

Steps

1. On the Dashboard, click **Performance**.

   For ONTAP systems, you can click the **Node** tab to view the performance of a single node of an ONTAP cluster, click the **Local Tier** tab to view the performance of the local tier, or click the **Volume** tab to view the performance of the volume. By default, the cluster performance is displayed.

   For E-Series systems, you can view the graphs only at a controller level.

2. Select either 1 day, 1 week, 1 month, 2 months, or 12 months, in the calendar, for viewing performance data in a graphical format.

   For example, select 2-months tab to view data for 2 months. This enables you to view specific data for a duration based on your performance requirements.

3. The following performance graphs with required metrics are available for ONTAP clusters and nodes:

For Cluster	For Node	For Local Tier	For Volume
IOPS	CPU Utilization - Peak Performance (Headroom)	Average Throughput	IOPS
Network Throughput	Latency	Average Utilization	Latency
	IOPS		
	Protocol IOPS		
	Network Throughput		

Node latency, local tier (aggregate), and volume performance graphs are supported only on systems that are running ONTAP 9.2 and later.

4. The following performance graphs with required metrics are available for E-Series controllers:
    - CPU Utilization
    - Latency
    - IOPS
    - Throughput

Analyze the health of your storage system

Understand Health Check dashboard

The Digital Advisor Health Check dashboard provides a point-in-time review of your overall environment.

Based on the health check score, you can align your storage systems to the recommended NetApp best practices to facilitate long-term planning. It helps you monitor all the systems running on software and hardware through a centralized user interface. Health Check scores enable you to quickly gain insights about system risks. The key recommendations and best practices help you take actions to improve the health of your installed base.

You can access the Health Check dashboard only through NetApp SupportEdge Advisor and SupportEdge Expert service offerings.

Get started with Health Check dashboard

This dashboard provides an at-a-glance summary of your installed base through the following widgets:

- **AutoSupport Adoption**: Displays the number and percentage of systems with AutoSupport enabled. You can also view systems marked as 'Declined', those with **HTTPS** and **AutoSupport on Demand** enabled, as well as **Loss of Signal** for those systems that have stopped sending AutoSupport data in the last 7 days.
  To view your health check score and information about the systems in your install base, click the **AutoSupport Adoption** widget.
- **Recommended Configuration**: Displays systems that are compliant and non-compliant as per the **Recommended Configuration** widget. It helps you take actions to ensure that your systems are well configured across your installed base. You can view the score provided on the dashboard and take actions based on the key recommendations which are provided in order of priority.
- **Recommended Software**: Displays a consolidated list of all the software and firmware upgrades and currency recommendations. You can view the systems with AutoSupport enabled that should be at either the minimum or latest software or firmware versions.
- **Support & Entitlements**: Displays support contracts that have expired and those that are nearing expiration within 6 to 12 months. It displays end of support platforms, disks, shelves, entitlement compliance, pending expirations, and end of support for platform and hardware is not applicable.
  You can view the health check score provided on the dashboard and take actions based on the key recommendations, which are provided in order of priority.
  To view detailed information about support contracts, click the **Support & Entitlements** widget. You can also renew your support contracts using this widget.
- **Best Practices**: Displays the health check score by assessing the best practices attributes of your storage

system — performance & efficiency, availability & protection, capacity, configuration, and security vulnerabilities. NetApp best practices help sustain system health, which optimizes the performance of your installed base.

- **Technical Cases**: Provides you with a detailed view of your technical case history, by case type and open or closed status, over selectable time ranges. You can drill into case groups as well as view case details through NetApp Support Site or other case portals.

Renew your support contracts

You can view the score and summary of all the active support contracts on the dashboard. You can take actions based on the key recommendations which are provided in order of priority.

Steps

1. On the Health Check Dashboard, click the **Support & Entitlements** widget.
2. If any of your system support contracts have expired or are nearing expiration, then click the **Active Support Contracts** widget.
3. Select the checkboxes and click **Renew** for initiating the renewal process for the selected systems.

Upgrade to optimize your install base

Upgrade the support offering

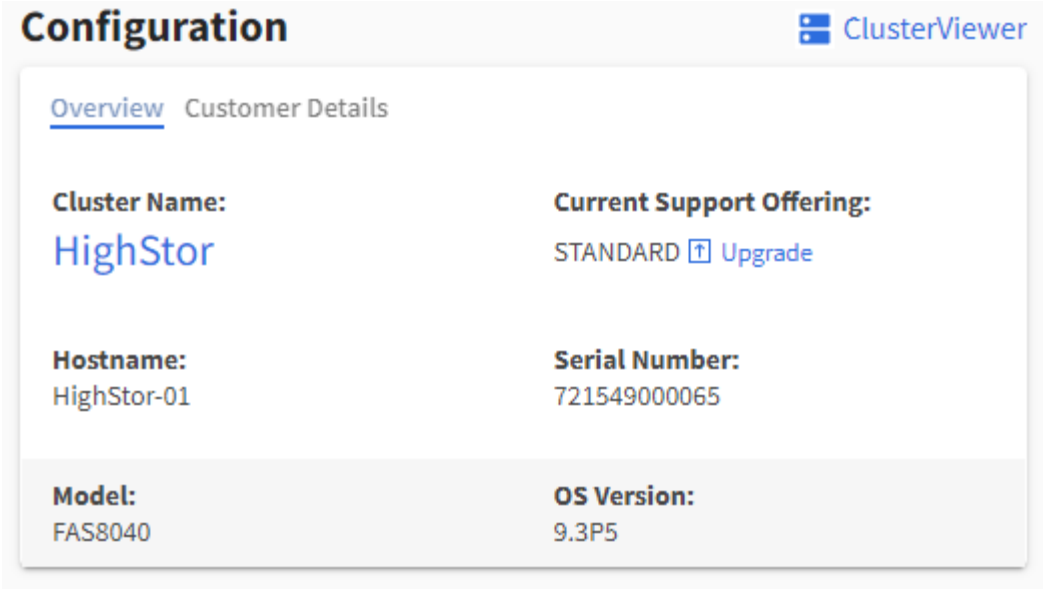
You can purchase an upgrade to the support offering to access more features and functionalities in Digital Advisor.

You can upgrade your current support offering to optimize your install base with the help of recommended practices and fixes, upgrade automation with Ansible playbooks, actionable reports and reviews, personalized support, and so on. The upgrade can be purchased when you renew your support contracts or at any other time from the system (node) dashboard.

You can opt for AIQ Upgrade only if you currently use the SupportEdge Premium or SupportEdge Secure support offerings.

Steps

1. Click **View All Systems** next to the **Inventory** widget.
2. On the Inventory Dashboard, select the node (host) that you want to upgrade.
   You are redirected to the system or node dashboard.
3. Click **Upgrade** in the **Configuration** widget.



4. Optionally, click **Compare Support Offerings** to view the comparison chart and pick the support offering that fits your requirements.
   Alternatively, you can click **Support Offerings** on the left navigation menu to view the comparison chart.
5. Select the type of upgrade that you want.
   a. Add AIQ Upgrade to your SupportEdge Premium or SupportEdge Secure support offerings
   b. Any other upgrade request
6. Add any comments that you have and click **Send**.
   A request to purchase the support offering upgrade is sent to the NetApp Renewals team.

Update your AFF and FAS firmware using Ansible Playbook

Download AFF and FAS firmware Ansible Automation package

You should update the AFF and FAS firmware using Ansible to mitigate the identified risks and keep your storage system up to date.

Before you begin

Before updating AFF and FAS firmware using Ansible, you should:

- Install and set up Ansible on your storage system
- Install Ansible 2.9 with collections on your storage system
- Upgrade your storage system to ONTAP 9.1 or later
- Configure your account with an administrator role

Steps

1. Click any wellness widget on the dashboard or click **View All Actions** to view a list of all the actions and risks.
2. Click **Firmware Upgrade** to view all firmware upgrade risks.
3. Click **Update AFF and FAS Firmware** to view all available update packages or click  next to each risk

to update the package specific to that risk.

4. Click **Download** to download the zip files and update your storage system.

   The zip file contains the following:

   - Ansible Playbook - A YAML file containing the Ansible script to perform the disk, shelf, and service processor firmware updates.
   - Inventory - A YAML file containing the details of the systems that are applicable for firmware updates.
   - Disk, Shelf, and Service Processor/BMC Firmware packages are named as **all.zip**, **all_shelf_fw.zip**, and **<SP/BMC>_<version_number>_fw.zip** respectively.

Manual addition of clusters and controllers to the inventory file is not supported.

Install and execute AFF and FAS firmware Ansible automation package (Experienced Users)

Experienced users can install and execute the AFF and FAS firmware ansible automation package quickly.

Firmware update with Ansible using NetApp Docker Image

Steps

1. Pull the Ansible Docker image to the Linux host:

```
$ docker pull schmots1/netapp-ansible
Using default tag: latest
latest: Pulling from schmots1/netapp-ansible
docker.io/schmots1/netapp-ansible:latest
```

2. Run the docker image as a container on the Linux host:

```
$ docker run -v <downloaded_playbook_path>:/<container_path> -it
schmots1/netapp-ansible:latest /bin/bash
```

The Ansible Playbook and the inventory file should be in the same path.

3. Execute the Ansible Playbook on the Linux host. Firmware updates run in the background for a few hours.

```
$ cd <container_path>
$ ansible-playbook na_ontap_pb_upgrade_firmware.yml

Enter your ONTAP admin username: ****
Enter the password for your ONTAP admin user: ****
Enter the base URL to the firmware package (using HTTP is recommended):
 http://<web-server>/path/
PLAY [ONTAP Firmware Upgrade]
*********************************************************************
```

If the URLs for disk firmware, shelf firmware, and service processor firmware are **http://<web-server>/path/all_shelf_fw.zip**, **http://<web-server>/path/all.zip** and **http://<web-server>/path/<SP/BMC>_<version_number>_fw.zip**, provide **http://<web-server>/path/** as the input for the base URL to the firmware package. If there are a set of clusters with different login credentials, the Ansible Playbook must be run on each cluster. There are no changes required to the inventory file as the Ansible Playbook skips the clusters for which the login has failed.

4. Log in to the cluster as the cluster administrator and verify that the new drive firmware has been installed:

```
::> storage disk show -fields firmware-revision,model
 disk     firmware-revision model
-------------- ----------------- ----------------
1.11.0   NA01              X423_HCOBE900A10
1.11.1   NA01              X423_HCOBE900A10
1.11.2   NA01              X423_HCOBE900A10
1.11.3   NA01              X423_HCOBE900A10
1.11.4   NA01              X423_HCOBE900A10
```

Firmware update if Ansible is already used

Steps

1. Install Python and Ansible and then download the Python packages using PIP:

```
$ pip install netapp-lib requests paramiko

Installing collected packages: netapp-lib, requests, paramiko
Successfully installed netapp-lib-2020.3.12 requests-2.23.0 paramiko-
2.7.2
```

2. Install the NetApp Ansible Collection:

```
To install the collection only for the current user:
$ ansible-galaxy collection install netapp.ontap

For universal installation:
$ ansible-galaxy collection install netapp.ontap -p
/usr/share/ansible/collections
$ chmod -R +rw /usr/share/ansible/collections
```

3. Ensure that the Ansible Playbook and the inventory file are in the same path and then execute the Ansible Playbook. Firmware updates run in the background for a few hours.

```
$ cd <playbook_path>
$ ansible-playbook na_ontap_pb_upgrade_firmware_disk.yml

Enter your ONTAP admin username: ****
Enter the password for your ONTAP admin user: ****
Enter the base URL to the firmware package (using HTTP is recommended):
http://<web-server>/path/
PLAY [ONTAP Firmware Upgrade]
*****************************************************************
```

If the URLs for disk firmware, shelf firmware, and service processor firmware are **http://<web-server>/path/all_shelf_fw.zip**, **http://<web-server>/path/all.zip** and **http://<web-server>/path/<SP/BMC>_<version_number>_fw.zip**, provide **http://<web-server>/path/** as the input for the base URL to the firmware package. If there are a set of clusters with different login credentials, the Ansible Playbook must be run on each cluster. There are no changes required to the inventory file as the Ansible Playbook skips the clusters for which the login has failed.

4. Log in to the cluster as the cluster administrator and verify that the new drive firmware has been installed:

```
::> storage disk show -fields firmware-revision,model
 disk     firmware-revision model
-------------- ----------------- ----------------
1.11.0   NA01              X423_HCOBE900A10
1.11.1   NA01              X423_HCOBE900A10
1.11.2   NA01              X423_HCOBE900A10
1.11.3   NA01              X423_HCOBE900A10
1.11.4   NA01              X423_HCOBE900A10
```

Install and execute AFF and FAS firmware Ansible automation package (beginners)

Host firmware files using web server

After you download the automation package, the firmware files should be hosted on a web server.

The web server can be set up in multiple ways. For instructions to set up a simple web server using Python, refer to Webserver using Python.

Step

1. Save the base URL of the web server. If the URLs for disk firmware, shelf firmware, and service processor firmware are **http://<web-server>/path/all_shelf_fw.zip**, **http://<web-server>/path/all.zip**, and **http://<web-server>/path/<SP/BMC>_<version_number>_fw.zip**, save **http://<web-server>/path/** as the base URL.

The filename is automatically detected by the Ansible Playbook.

Work with inventory file

The inventory file consists of the cluster management LIFs of the systems that are eligible for firmware updates. It contains the list of clusters with disk and shelf firmware filename information wherever applicable.

For service processor firmware update, node hostnames and SP/BMC IP is included in the inventory file.

Inventory file format

The following is a sample inventory file format with both disk and shelf firmware updates:

```
clusters:
  - clustername: <cluster management LIF-1>
    disk_fw_file: all.zip
    shelf_fw_file: all_shelf_fw.zip

  - clustername: <cluster management LIF-2>
    disk_fw_file: all.zip
    sp_nodes:
    - hostname: <node hostname 1>
      sp_fw_file: SP_FW_308-03990_11.5.zip
      sp_fw_type: bmc
      sp_fw_ver: '11.5'
      sp_ip: <BMC IP>
    - hostname: <node hostname 2>
      sp_fw_file: SP_FW_308-03991_5.8.zip
      sp_fw_type: sp
      sp_fw_ver: '5.8'
      sp_ip: <SP IP>
```

In the example, both shelf and disk firmware updates are applicable on cluster-1 and disk and SP/BMC firmware updates are applicable on cluster-2.

Delete a cluster from the inventory file

In case you do not want to apply firmware updates on a particular cluster, you can remove the cluster from the inventory file.

For example, if you do not want to apply disk firmware updates on cluster-2, you can remove it from the inventory file using the following command:

```
clusters:
  - clustername: <cluster management LIF-1>
    disk_fw_file: all.zip
    shelf_fw_file: all_shelf_fw.zip
```

You can observe that all the data for cluster-2 has been deleted.

If you want to apply only disk firmware updates on cluster-1 and not shelf firmware updates, you can do so using the following command:

```
clusters:
  - clustername: <cluster management LIF-1>
    disk_fw_file: all.zip
```

You can see that the *shelf_fw_file* key and value have been removed from cluster-1.

Manual addition of clusters or controllers is not supported.

Execute Ansible Playbook using NetApp Docker image

Before you execute the Ansible Playbook, ensure that the **NetApp_Ansible_***.**zip** file has been extracted and the web server with disk or shelf firmware files is ready.

Before you begin

Before executing Ansible Playbook using NetApp docker, you should:

- Download AFF and FAS firmware Ansible Automation package
- Host the firmware files using the web server
- Work with the inventory file
- Ensure that NetApp Docker is installed.

Steps

1. Set up Docker.
2. Pull the NetApp Docker image from DockerHub by executing the following command:

```
$ docker pull schmots1/netapp-ansible

Using default tag: latest
latest: Pulling from schmots1/netapp-ansible
docker.io/schmots1/netapp-ansible:lates
```

For more information about the docker pull command, refer to the Docker Pull Documentation.

3. Run the Docker image as a container and log in to the container to execute the Ansible Playbook.
4. Copy the path of the folder which contains the extracted Ansible Playbook and inventory files, for example, **downloaded_playbook_path**. The Ansible Playbook and inventory files should be in the same folder for successful execution.
5. Mount the folder as a volume on the Docker container. For example, to mount the folder **container_path**, you should execute the following command:

```
$ docker run -v <downloaded_playbook_path>:/<container_path> -it
schmots1/netapp-ansible:latest /bin/bash
```

The container starts and the console is now at bash shell of the container. For more information about the Docker Run command, refer to the Docker Run Documentation.

6. Execute the Ansible Playbook inside the container using the **ansible-playbook** command:

```
$ cd <container_path>
$ ansible-playbook na_ontap_pb_upgrade_firmware.yml

Enter your ONTAP admin username: ****
Enter the password for your ONTAP admin user: ****
Enter the base URL to the firmware package (using HTTP is recommended):
http://<web-server>/path/
PLAY [ONTAP Firmware Upgrade]
*********************************************************
```

If there are a set of clusters with different login credentials, the Ansible Playbook must be run on each cluster. There are no changes required to the inventory file as the Ansible Playbook skips the clusters for which the login has failed.

For more information about the **ansible-playbook** command, refer to the Ansible Playbook Documentation and to execute the Ansible playbook in check mode (dry run), refer to Ansible: Check mode.

After executing the Ansible Playbook, refer to the Firmware Installation Validations for post-execution instructions.

Execute Ansible Playbook without NetApp Docker image

Steps

1. Install Python and Ansible.
2. Install the required Python packages using **pip**:

```
$ pip install netapp-lib requests paramiko

Installing collected packages: netapp-lib, requests, paramiko
Successfully installed netapp-lib-2020.3.12 requests-2.23.0 paramiko-
2.7.2
```

3. Install NetApp Ansible collection using the **ansible-galaxy** command:

```
To install the collection only for the current user
$ ansible-galaxy collection install netapp.ontap

To do a more universal installation,
$ ansible-galaxy collection install netapp.ontap -p
/usr/share/ansible/collections

$ chmod -R +rw /usr/share/ansible/collections
```

   For more information about the ansible-galaxy command, refer to Ansible Galaxy Documentation and for more information about the NetApp Ansible Collection, refer to the NetApp Ansible Collection page.

4. Execute the Ansible Playbook using **ansible-playbook** command:

```
$ cd <downloaded_playbook_path>
$ ansible-playbook na_ontap_pb_upgrade_firmware.yml

Enter your ONTAP admin username: ****
Enter the password for your ONTAP admin user: ****
Enter the base URL to the firmware package (using HTTP is recommended):
http://<web-server>/path/
PLAY [ONTAP Firmware Upgrade]
*********************************************************************
```

   If there are a set of clusters with different login credentials, the Ansible Playbook must be run on each cluster. There are no changes required to the inventory file as the Ansible Playbook skips the clusters for which the login has failed.

For more information about the **ansible-playbook** command, refer to the Ansible Playbook Documentation and to execute the Ansible Playbook in check mode (dry run), refer to Ansible: Check mode.

After executing the playbook, refer to the Firmware Installation Validations for post-execution instructions.

Validate firmware installation

After the execution of the playbook, log in to the cluster as the cluster administrator.

Validate disk firmware installation

Steps

1. Verify that the drive firmware is installed:

```
::*> storage disk show -fields firmware-revision,model
disk     firmware-revision model
---------------- ----------------- ----------------
1.11.0   NA01              X423_HCOBE900A10
1.11.1   NA01              X423_HCOBE900A10
1.11.2   NA01              X423_HCOBE900A10
1.11.3   NA01              X423_HCOBE900A10
1.11.4   NA01              X423_HCOBE900A10
```

   For more information about the command, refer to storage disk show.

2. Verify that the new NVMe Flash Cache firmware is installed:

```
::*> system controller flash-cache show
```

   For more information about the command, refer to system controller flash-cache show.

Validate shelf firmware installation

Steps

1. Verify that the new shelf firmware is updated:

```
::*> system node run -node * -command sysconfig -v
```

   In the output, verify that each shelf's firmware is updated to the desired level. For example:

```
Shelf 1: IOM6 Firmware rev. IOM6 A: 0191 IOM3 B: 0191
```

   For more information about the command, refer to system node run.

2. Verify that the new ACP firmware is updated:

```
::*> storage shelf acp module show -instance
```

For more information about the command, refer to storage shelf acp module show.

3. Verify that the desired ACP mode is configured:

```
::*> storage shelf acp show
```

For more information about the command, refer to storage shelf acp show.

4. Change the ACP mode (channel):

```
::*> storage shelf acp configure -channel [in-band | out-of-band]
```

For more information about the command, refer to storage shelf acp configure.

Validating SP/BMC Firmware installation

The Ansible Playbook for Service Processor/BMC firmware updates is enabled with an option to verify the installation of latest SP/BMC firmware on the controller. After the verification is complete (the updates could take a maximum time of two hours), the Ansible Playbook applies internal switch firmware updates by connecting to the SP/BMC console.

The failure and success information for SP/BMC firmware and the internal switch firmware installations will be notified at the end of Ansible Playbook execution. Follow the steps mentioned in the Ansible Playbook in case the SP/BMC firmware/internal switch firmware installation fails.

Integrate data using APIs

Understand API Services

Digital Advisor API Services uses automation to add efficiency to your workflows. Inside API Services resides the **API Catalog**, which describes over 100 different API endpoints that are grouped into 20+ different service areas. These APIs are available to you as a NetApp customer and they span different areas of interest, such as system information, storage efficiency, performance, health, and upgrades.

NetApp Digital Advisor is transitioning from REST APIs to GraphQL as its primary API platform to improve performance, flexibility, and scalability. The transition will be phased, with a period of overlap between REST APIs and GraphQL APIs. For each deprecated REST API, a deprecation notice will be published in the Digital Advisor API catalog, and you will have 6 months to migrate that specific endpoint to GraphQL. To review the list of APIs scheduled for deprecation, navigate to **API services → Browse → Deprecated APIs**

APIs are interfaces that enable you to write simple code that can contact Digital Advisor programmatically and bring back data into your compute environment. You can write code in such a way that it contacts Digital

Advisor every day and brings back the latest data in the areas that are of interest to you. You can then use this data to populate your ticketing system or to create your own dashboards, webpages, or reports. The Digital Advisor API Catalog has both code samples and a facility for you to try out the APIs in the browser.

Automation with APIs is a great way to add efficiency and accuracy to daily or weekly tasks. It frees up your resources to perform more complex activities or to automate new workflows. For example, if you have system health risks that need to be fixed, you can automate at least the pullout of those items from Digital Advisor and the push into your ticketing system.

API Catalog

The toggle at the top of the page allows the user to switch between the two modes to view the Catalog. The Code view focuses on the input parameters needed, the content and format of the return data, and code samples to get the user started with putting code in place. The Experiment view offers the user a chance to “try out” the API in the browser using a generated token obtained from the main API Services page.

Either view allows the user to browse through available items using the navigation pane on the left. The items are organized by service in alphabetical order. Within a given service, you can expand the heading to show the individual API Endpoints. Clicking on the service heading or an API Endpoint will take you to that section of the Catalog in the middle pane.

Using the APIs

Once you are authorized and can generate tokens, you can leverage the tokens to make programmatic queries and retrieve data. You can also test out an API from within the API Catalog to see first-hand how the query works and the type of data that is returned. This is a great way to make sure you understand how an API will work prior to building out the code framework in your system.

Generate tokens to use APIs

It is easy to register for API Services and generate tokens.

Steps

1. From the **Quick Links** menu, click **API Services**.
2. Click **Register**.
3. Complete the request for authorization form and click **Submit**.

   Activation is automatic and should be instantaneous. Once you have been authorized to use the Digital Advisor APIs, you can generate tokens to use when making programmatic API calls. You can also use these tokens to execute “try it out” from within the API Catalog. When obtained programmatically, tokens always come in sets of two: An Access Token and a Refresh Token. The Access Token must be passed to successfully use all APIs (except for one - the Refresh Token is used to programmatically obtain a new set of tokens).

4. On the Main API Services page, click **Generate Token** to view and download the access token and refresh token to invoke APIs.

   The portal gives you multiple ways to save one or both tokens in the set. You can copy them to clipboard, download them as a text file, or view them as plain text.

You should download and save the access token and refresh token for later use. Access tokens expire one hour after generation and refresh tokens should be regenerated, manually, every 7 days and installed in the application. To do this, you do not need to log in to the application. However, after 90 days, you need to log in to the application to obtain a new access and refresh token.

Use API Catalog to execute APIs

The API Catalog allows you to browse through categories and the available APIs within each of those categories.

Using a valid Access Token and correct inputs for the required fields, you can make a test call for an API.

Access GraphQL APIs

Steps

1. From the **Quick Links** menu, click **API Services**.
2. Click Browse under the **API Catalog** icon.

   The API Catalog is displayed.

3. Click **GraphQL** and review the documentation.
4. Try out the GraphQL APIs by using the ready-to-run sample queries at Digital Advisor GraphQL Studio.
5. Supply a user token by selecting the authorization field in the Header of the API request
6. Provide the required variables
7. Run the query and review the output

Access REST APIs

Steps

1. From the **Quick Links** menu, click **API Services**.
2. Click Browse under the **API Catalog** icon.

   The API Catalog is displayed.

3. Click **ActiveIQ-Public** and select any API
4. At the top of the page, slide the toggle to “Experiment”.
5. From the left navigation, expand the categories and select any API to view detailed information.
6. Expand the API.
7. Click the **Try it out** button on the right.
8. Provide the required parameters and click **Execute** to view the results.

   You can also examine the **Responses** section of the API to understand the data that will be returned better. You can click on **Example Value** to see the format of the data or click on **Model** and click on the carets to expand the sections to see the definition of each element.

By sliding the toggle to the **Code** view, you can view code samples in various languages.

Generate custom reports

Types of reports

Digital Advisor provides a variety of reporting options that enable you to monitor and manage your system health and operation success.

The following are the types of reports that are available in Digital Advisor:

Report Name	Description	Available in ONTAP	Available in E-Series	Available in Storage GRID
Ansible Inventory	Provides an Ansible inventory file which lists all system inventory details by region or site. This file can be used for automation.	Yes	No	No
Capacity & Efficiency	Provides information about the Capacity and Efficiency details at cluster, customer, site, group, watchlist and node level.	Yes	Yes	Yes
Cloud Recommendations	Provides insights and recommendations for optimizing cloud resources. It includes details on disaster recovery, backup, tiering, and migration.	Yes	No	No
ClusterViewer	Provides information about a single or multiple clusters at a customer and watchlist level. You can generate this report only for watchlist with up to 100 nodes.	Yes	No	No
Config Drift	Allows users to establish a "golden baseline" for system configurations and alerts them when deviations from this baseline occur. It helps identify and address configuration changes that may impact system performance or security.	Yes	No	No
Delivery Logistics	Provides information about the logistics of delivering products and services.	Yes	Yes	No
Health Assessment Executive Summary	Provides information about various Active IQ KPIs in a PowerPoint (PPT) format, with different KPI being described on different slides.	Yes	Yes	No
Inventory	Provides information about the install base for a selected watchlist, customer, site, group levels. This report can be generated either as a direct download from Inventory details page or can be generated from Reports page.	Yes	Yes	Yes
IO Density	IO Density Report provides insights into peak input-output operations for customers in terms of data and meta-data consumption and density.	Yes	No	No

Report Name	Description	Available in ONTAP	Available in E-Series	Available in Storage GRID
Performance	Provides information, at a watchlist level, about the performance of a cluster, node, local tier (aggregate), and volume. You can generate this report only for watchlist with up to 100 nodes.	Yes	Yes	No
Periodic Digest	Summarizes key metrics and insights periodically. It includes data on system performance, capacity, and efficiency.	Yes	No	No
Recommended Configuration	Provides information about the various recommended configuration gaps for Remote Management Configuration, spares and drives, HA Pair, SVM Health, battery status, and recovery guru advisories.	Yes	Yes	No
Support Contracts / Hardware EOS	Provides information about the contract details and the list of controllers, shelves, and disks, that have reached end-of-support (EOS).	Yes	Yes	No
Technical Case Details	Provides a yearly report about all the technical cases and their status.	Yes	Yes	Yes
Upgrade Plan	Offers recommendations for software and firmware upgrades. It includes details on the latest recommended versions, potential issues, and steps for performing upgrades.	Yes	No	No
Upgrade Recommendations (SW & FW)	Multi-tabbed report about the software and firmware currency and recommended versions for each controller or serial in the search criteria.	Yes	Yes	No
Volume Performance	Provides information about the performance details of the volumes at the cluster level.	Yes	No	No
Wellness	Provides information about the outstanding and acknowledged risks, risk details, corrective actions, and affected systems.	Yes	Yes	Yes

Generate reports

You can generate reports immediately or schedule a report to be generated on a weekly or monthly basis. The reports can be generated in different formats. Based on the report selected, the available formats are displayed.

About this task

- You cannot edit the reports in Digital Advisor. You should delete the existing report and create a new report.

Steps

1. From the left pane, click **Reports**.
2. Click **Create Report** to generate a new report.

You can generate a report immediately or you can schedule the report to be generated on a weekly or monthly basis.

To generate a report immediately	To schedule the report to be generated on a weekly or monthly basis
1. Select the type of report and provide the requested values for the report. 2. Select the format of the report. 3. Click **Submit**. The report is saved in Digital Advisor for 3 days.	1. Click the **Schedule Report** tab. 2. Select the type of report and provide the requested values for the report. 3. Select the format of the report. 4. Select the frequency of the report. 5. Select the start date and end date for the report. 6. Click **Submit**. The existing scheduled reports will be replaced when the new reports are generated.

Copyright information

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.