Dell APEX AIOps Infrastructure Observability: A Detailed Review

A Proactive Monitoring and Analytics Application for the Dell Environment

September 2024

H15691.10

White Paper

Abstract

This white paper details Dell APEX AIOps Infrastructure Observability, the cloud-based AIOps proactive monitoring and predictive analytics application for Dell systems. It describes how it uses machine learning and other algorithms, notifications, and recommendations to help you optimize compute, storage, hypercoverged infrastructure, data protection, and network health, performance, and capacity.

DELL Technologies

Copyright

Contents

Executive summary

Overview

With our busy daily lives, it is important to find easier and faster ways to manage IT infrastructure. With APEX AIOps Infrastructure Observability, Dell Technologies seeks to simplify the user experience when it comes to proactively monitoring and providing helpful insights about their Dell environment.

Infrastructure Observability provides a single web-based for monitoring and analyzing Dell's broad portfolio of infrastructure systems which, according to user surveys, yields significant outcomes:

- 2x to 10x faster time to resolution of issues[1]
- One workday saved per week on average[1]

This white paper describes the Infrastructure Observability features that are available in a consolidated user interface through any HTML5 browser. Users can also access Infrastructure Observability on their iOS or Android mobile device.

As a Software-as-a-Service solution, Infrastructure Observability delivers frequent, dynamic, nondisruptive content updates for the user. Infrastructure Observability is built in a secure multitenant platform to ensure that each customer tenant is properly isolated and secure from other customers.

Audience

This white paper is intended for Dell Technologies customers, partners, and employees who are interested in understanding Infrastructure Observability features and how to monitor the following Dell systems:

- APEX Block Storage for Public Cloud
- APEX Cloud Platform for Microsoft Azure
- APEX Cloud Platform for Red Hat OpenShift
- APEX File Storage for Public Cloud
- APEX Hybrid Cloud Services
- APEX Private Cloud Services
- Connectrix
- PowerEdge
- PowerFlex
- PowerMax (including VMAX)
- PowerProtect Data Manager
- PowerProtect DD series appliances (including DDVE)
- PowerScale (including Isilon)

[1] Based on an APEX AIOps Observability User Survey, conducted by Dell Technologies, May-June 2021

- PowerStore
- PowerSwitch
- PowerVault
- SC Series
- Unity XT family (including Dell Unity and Unity XT)
- VxBlock
- VxRail
- XtremIO

Revisions

Date	Part number/ revision	Description
December 2016	—	Initial release
August 2017	—	Updated with additional functionality
June 2019	—	Updated with support for PowerMax/VMAX, SC Series, XtremIO, Connectrix, and VMware
June 2020	H15691	Updated with support for PowerStore, PowerScale, Isilon, PowerVault, and Converged Systems
November 2020	H15691.1	• Updated to reference support.dell.com and cloudiq.dell.com • Updated with details on enabling Dell Trusted Advisors and Partners • Updated with Lifecycle Management for Converged Systems
May 2021	H15691.2	• Updated with support for PowerProtect DD and PowerProtect Data Manager • Updated with support for VxRail • Updated with support for custom tags and custom reports
July 2021	H15691.3	• Updated with support for APEX Offerings • Updated with Cybersecurity
January 2022	H15691.4	• Updated with support for PowerFlex, PowerEdge, and PowerSwitch • Updated with support for Webhooks
January 2022	H15691.5	Updated template

Date	Part number/ revision	Description
July 2022	H15691.6	Updated with REST API Updated with Virtualization View Updated with VxRail multisystem update Updated with support for Secure Connect Gateway Updated with Cybersecurity support for PowerEdge and templates Updated with support for PowerProtect DD performance Updated with support for PowerSwitch performance Deprecated Hosts from Inventory tab Deprecated Metrics Browser Updated with Report Browser metrics per device type Updated with Connectrix Optics support Converted Advanced role to DevOps
January 2023	H15691.7	New navigation menu and consolidated multisystem views Dell Security Advisories in cybersecurity Component level tagging VMware support under Virtualization PowerStore appliance, volume group, and volume details PowerScale node and quota details Powered off VMs in Reclaimable Storage Performance Impacts for PowerScale Subscribed and physical capacity views for APEX Data Storage Services Performance forecasting for Unity Updated Connectivity View PowerProtect DD capacity forecasting and custom reports PowerProtect DD and PowerProtect DM system updates VxRail modified Inventory View and additional performance metrics
July 2023	H15691.8	Updated: • Terminology table (Observability Collector and SupportAssist definitions) • Connectrix and PowerSwitch details (Introduction section) • Administration (Collectors section)

Date	Part number/ revision	Description
October 2023	H15691.9	Port performance metrics for PowerSwitch Performance forecasting for Dell Unity XT and PowerEdge Anomaly charts in custom reporting Support for PowerFlex hosts and alerts PowerEdge maintenance and firmware update actions PowerEdge Dell Security Advisories Home Page customization Single sign-on for AIOps Infrastructure Observability Carbon footprint analysis Service Requests VxBlock health score for storage Licenses and entitlements
September 2024	H15691.10	Rebrand to APEX AIOps Infrastructure Observability Add support for APEX Block Storage for Public Cloud, APEX File Storage for Public Cloud, APEX Hybrid Cloud Services, and APEX Private Cloud Services, APEX Cloud Platform for Microsoft Azure, and APEX Cloud Platform for Red Hat OpenShift Removed references to APEX Data Storage Services Knowledge Base Articles Cybersecurity support for PowerProtect DD Ransomware Incidents Webhooks for Cybersecurity VxBlock CI Code Compare Server Compliance Reports Job scheduling for PowerEdge firmware updates Updated available metrics in Report Browser PowerVault supports Data Protection category in health score More file system details for PowerStore Support for PowerSwitch systems running SONiC More support in mobile app Carbon Footprint support for PowerScale systems Updated custom report wizard Remove references to Secure Remote Services Pools status added on PowerFlex Capacity page Support for SSO Groups Support for Dell XC Appliances

We value your feedback

Dell Technologies and the authors of this document welcome your feedback on this document. Contact the Dell Technologies team by email.

Author: Derek Barboza

Contributors: Susan Sharpe, Frederic Meunier, David Hayward

Note: For links to other documentation for this topic, see the Data Storage Essentials Info Hub.

Terminology

The following table provides definitions for some of the terms that are used in this document.

Table 1. Terminology

Term	Definition
Observability Collector	A small virtual machine distributed as a vApp that enables collection of VMware, Connectrix, and PowerSwitch. The Collector retrieves information from the target objects (vCenter or switches) and sends the collected data back to Infrastructure Observability using Secure Connect Gateway. For VMware, the Collector communicates to vCenter using the VMware API and requires a user with read-only privileges. For Connectrix and PowerSwitch devices, the Collector communicates to the individual switches using REST API and uses a nonprivileged user. A single collector can be used for both VMware, Connectrix, and PowerSwitch.
SupportAssist	Remote connectivity technology that enables SC Series, PowerStore, PowerFlex, and PowerVault systems to connect to Infrastructure Observability and send associated data packets for performance, capacity, and health monitoring. SupportAssist allows Dell to securely transfer files, such as alerts, performance stats, capacity, and configuration information from the systems.
Secure Connect Gateway	Remote connectivity technology replacing Secure Remote Services and SupportAssist Enterprise. It allows Dell devices to securely transfer files such as logs and system telemetry to Dell Support and Infrastructure Observability. It can exist as a centralized stand-alone server or deployed within management platforms as Embedded Service Enabler.
OpenManage Enterprise	Management console for PowerEdge servers. The CloudIQ Plugin and Embedded Service Enabler are required to collect and sent telemetry back to Infrastructure Observability.
Unisphere	The graphical management interface that is built into Dell storage systems for configuring, provisioning, and managing the systems' features. For Unity XT family, and PowerMax/VMAX systems, Unisphere connects to Infrastructure Observability using Secure Connect Gateway; for SC Series, it connects using SupportAssist.
PowerVault Manager	The graphical management interface for PowerVault storage systems. Connectivity to Infrastructure Observability is established in the Settings section of PowerVault Manager using SupportAssist.
PowerStore Manager	The graphical management interface for PowerStore storage systems. Connectivity to Infrastructure Observability is established in the Settings section of PowerStore Manager using Embedded Service Enabler or external Support Connect Gateway.

Term	Definition
Web UI	The graphical management interface for XtremIO storage arrays. Web UI is part of XMS – XtremIO Management Server, which connects to Infrastructure Observability using Secure Connect Gateway.
DD System Manager	The graphical management interface for PowerProtect DD systems. Connectivity to Infrastructure Observability is established in the Maintenance section of DD System Manager using Secure Connect Gateway.
VxRail Manager	A plug-in for VMware vCenter that enables users to manage VxRail clusters including life-cycle management and the hardware platform. Connectivity to Secure Connect Gateway and Infrastructure Observability is established under the Support tab in VxRail Manager.

APEX AIOps Infrastructure Observability overview

Introduction

APEX AIOps Infrastructure Observability is a cloud-based AIOps application that provides for simple and proactive monitoring and troubleshooting of your Dell IT infrastructure including integration with VMware. It leverages machine learning to proactively monitor and measure the overall health of servers, storage, converged, hyperconverged, data protection, and network devices through intelligent, comprehensive, and predictive analytics. Infrastructure Observability is available at no additional charge for products with a valid ProSupport (or higher) contract. Observability is hosted on Dell Technologies Private Cloud, which is highly available, fault-tolerant, and guarantees a 4-hour Disaster Recovery SLO.

Observability provides each customer an independent, secure portal and ensures that customers will only be able to see their own environment. Each user can only see those systems in Observability which are part of that user's site access as defined in Dell Service Center. Customers register their systems with their Site ID. For SC Series and PowerVault systems, a new site ID is created, named after the system ID, for each system selected to be viewed in Observability.

The discussion below elaborates on the various features and functionality in Observability. Some details will vary by product type. For specific details about the product type and the latest features, consult **Online Help**, which is updated with each new feature added into Infrastructure Observability.

Key values of Infrastructure Observability

Reduce Risk – Infrastructure Observability makes daily IT administration tasks easier by helping you identify potential vulnerabilities before they impact your environment. Leveraging a suite of advanced analytics, Observability helps answer key questions IT Administrators deal with regularly using features such as: Proactive Health Scores, Performance Impact Analysis and Anomaly Detection, and Workload Contention Identification. It also identifies cybersecurity configuration risks, applicable Dell Security Advisories, and potential ransomware incidents.

Plan Ahead – Infrastructure Observability helps you stay ahead of business needs with short-term Capacity Full Prediction, Capacity Anomaly Detection, and longer-term Capacity Forecasting. Performance forecasting shows trends for key performance metrics and provides indications when resources will become saturated. SAN optical failure forecasting helps users plan ahead to replace failing components and avoid performance degradation and outages. Energy consumption and carbon footprint calculations let users meet their organization's sustainability goals.

Improve Productivity – Infrastructure Observability helps users improve the productivity of your IT resources, staffing, and equipment by:

- Providing a single monitoring interface for Dell infrastructure for data centers and edge locations including VMware visibility, and extending to Dell data protection systems in public clouds
- Sending notifications for health issue changes, job status changes, cybersecurity misconfigurations, and ransomware incidents

- Supporting customizable reports that can be scheduled and shared
- Enabling Dell and Dell partner Trusted Advisor access for added oversight
- Delivering immediate time-to-value with easy, web-based access and a mobile app
- Integrating with existing IT tools and processes with Webhooks and REST API

Infrastructure Observability requirements

Infrastructure Observability is available to all customers with the following Dell Technologies systems under a ProSupport or higher contract:

Type of data	Product models	Minimum code version
APEX	Block Storage for Public Cloud AWS systems Cloud Platform for Microsoft Azure Cloud Platform for Red Hat OpenShift File Storage for Public Cloud AWS systems Hybrid Cloud Services systems Private Cloud Services systems	N/A
Connectrix B-Series	Connectrix Brocade	FOS 8.2.1a and later
Connectrix MDS Series	Connectrix Cisco	NX-OS 8.2(2) and later, except for NX-OS v8.3(1)
Converged Infrastructure	Vblock 340, 350, 540, 740 VxBlock 340, 350, 540, 740, 1000	VxBlock Central 2.5 and later VMware 6.5 and later
PowerEdge	C Series, FC Series sleds and chassis, R Series, T Series, XE Series, XR and XR2 Series, FX Modular chassis, MX Modular sleds and chassis, M Modular compute sleds and chassis, VRTX Series sleds and chassis, XC appliances	OpenManage Enterprise 3.7 and later[2, 3]
PowerFlex	PowerFlex software and Ready-Nodes PowerFlex Rack and PowerFlex Appliance	V 3.6.x and later PowerFlex Manager 3.7 and later
PowerMax/VMAX	VMAX 10K, 20K, 40K, 100K, 200K, 400K, 250F, 450F, 850F, 950F PowerMax 2000, 8000, 2500, 8500	Unisphere 9.0.2.10 and later[4]
PowerProtect Data Manager	-	PowerProtect Data Manager 19.0 and later
PowerProtect DD series	DD9910, DD9900, DD9410, DD9400, DD6900, DD3300, DD9800, DD9500, DD9300, DD6800, DD6300, DD7200, DD4500, DD4200, Data Domain Virtual Edition (DDVE)	DDOS 7.4.0.5 and later[5]

[2] OpenManage Enterprise 3.9 or higher required for Cybersecurity support and modular chassis support.

[3] OpenManage Enterprise 3.10 or higher with CloudIQ Plugin 1.2 or higher required for maintenance and firmware update operations.

[4] Cybersecurity requirements: For host-based Unisphere, v9.2.1 or higher is required. For embedded Unisphere, v9.2.1 or higher and operating system 5978.711.711 or higher are required.

[5] DDOS v7.6 or higher is required for performance metrics.

Type of data	Product models	Minimum code version
PowerScale/Isilon	Gen 5, Gen 6, and Gen 6.5	OneFS 8.2 and later[6]
PowerStore	PowerStore T and PowerStore Q	PowerStoreOS 1.0 and later[7]
PowerSwitch	N3248TE-ON, S3048-ON, S4048T, S4112F-ON, S4112T-ON, S4128F-ON, S4128T-ON, S4148F-ON, S4148T-ON, S4148U, S5296F-ON, S5248F-ON, S5232F-ON, S5224F-ON S5212F-ON, S5448F-ON, Z9100, Z9264F-ON, Z9332F-ON, Z9432F-ON, Z9664F-ON, E3224F-ON	OS10 v10.5.3 and later[8,9]
PowerSwitch	N3248PXE-ON, N3248X-ON, N3248TE-ON, E3248P-ON, E3248PXE-ON, S5248F-ON, S5296F-ON, S5448F-ON, S5232F-ON, S5224F-ON, S5212F-ON, Z9664F-ON, Z9264F-ON, Z9332F-ON, Z9432F-ON	Enterprise SONiC 4.1.x and later
PowerVault	PowerVault ME4 PowerVault ME5	Firmware GT280R004 and later for ME4 All versions of ME5
SC Series	SC All Flash and SC Hybrid	7.3.1 and later
Unity XT family	XT, All Flash, Hybrid, and UnityVSA – Professional Edition	Dell Unity OE 4.1 and later
VMware	-	ESXi 5.5 and higher (some metrics available at 6.0+)
VxRail	-	7.0 and later
XtremIO	X1 and X2	XMS 6.2.0 and later

Infrastructure Observability data collection

Details on configuring Dell infrastructure, Connectrix, and VMware for Infrastructure Observability can be found in Appendix A: Enabling Infrastructure Observability at the system. After the Dell systems or Connectrix switches have established a connection to Observability, data will be collected and available to the user in the Observability user interface. Dell systems are connected through Secure Connect Gateway or SupportAssist. Observability receives Connectrix, VMware, and PowerSwitch data through a local Observability Collector that sends the data through Secure Connect Gateway to Observability.

The frequency with which data is updated in Observability varies based on the type of information and the type of system. The following table shows the types of data and the frequency with which Observability updates this information for Unity XT family systems; collection for other systems is comparable:

Type of data	Sample update frequency

[6] PowerScale 9.4.0.0 or later required for performance impact detection. Monitoring PowerScale backend switches is not supported.

[7] Cybersecurity requirements: PowerStoreOS 2.0 or higher.

[8] OS10 v10.5.3.2 or later required for error, utilization, and CPU utilization metrics.

[9] OS10 v10.5.4 or later is required for memory utilization metrics.

Type of data	Sample update frequency
Alerts	5 minutes
Performance	5 minutes
Capacity[10]	1 hour
Configuration[2]	1 hour
Data Collection[11]	Daily

Observability maintains up to 2 years of historical data for systems that are being monitored. The details of the data retention are as follows:

Alerts: 2 years

Configuration: 2 years at hourly intervals

	5 min interval	Hourly interval	Daily interval
System level	100 days	2 years	2 years
Object level	22 days	90 days	2 years

Infrastructure Observability features

Infrastructure Observability makes it faster and easier to analyze and identify issues accurately and intelligently, by delivering:

- Centralized monitoring of performance, capacity, system components, configuration, data protection, and carbon footprint. Observability also provides details about components of Dell storage systems, IP and SAN switches, servers, converged and hyperconverged systems, and data protection appliances – as well as VMware environments.
- Predictive analytics that enable intelligent planning and optimization of capacity and performance utilization.
- Proactive Health Scores for monitored storage systems, servers, hyperconverged systems, data protection appliances, and network devices. Observability identifies potential issues in the infrastructure and offers practical recommendations based on best practices and risk management.
- Cybersecurity feature that monitors and implements security assessments for Dell systems by comparing configurations to a set of security-related evaluation criteria, notifying users of security misconfigurations. Identification of applicable Dell Security Advisories and associated Common Vulnerability and Exposures (CVEs). Cybersecurity ransomware incidents detect potential ransomware attacks by learning the expected behavior of reducible data and identifying unexpected anomalies.

[10] Connectrix, VMware, and PowerStore collect at 5-minute intervals.

[11] Daily “all-in” collection.

- Multisystem update feature is implemented for VxRail and PowerEdge, allowing users to perform update pre-checks, code downloads, and system updates from Observability.

Centralized monitoring

Infrastructure Observability allows you to improve your system health by providing instant insight into your Dell IT environment without the maintenance of installed software. The Home Page summarizes key aspects of the environment so that users can quickly see what needs to be addressed and provides hyperlinks to easily open more detailed views. Some examples of these summaries include Proactive Health Scores, Capacity Predictions, Performance Anomaly and Impact Detection, and Reclaimable Storage. These features and others are discussed in detail below.

Predictive analytics

Infrastructure Observability advanced predictive analytics differentiate it from other monitoring and reporting tools.

Performance anomaly and impact detection

Using machine learning and analytics, Infrastructure Observability identifies performance anomalies (supported across all storage platforms, networking devices, and PowerEdge servers). It compares current performance metrics with historical values to determine when the current values deviate outside of normal ranges. This feature provides timely information about the risk level of the storage systems with insights into conditions and anomalies affecting performance.

Besides detecting performance anomalies, Observability goes one step further and identifies performance impacts (supported for PowerMax or VMAX, PowerStore, VxRail, Unity XT family, PowerScale, and PowerFlex systems). Observability analyzes increases in latency against other metrics such as IOPS and bandwidth to determine if an increase in latency is caused by a change in workload characteristics or competing resources. In the case where an impact is identified, Observability also identifies the most likely storage objects causing the workload contention. By differentiating between changes in workloads characteristics and workload contention, Observability enables users to narrow the focus of troubleshooting on when actual impacts to performance may have occurred.

Capacity trending and predictions

Infrastructure Observability provides historical trending and both short- and longer-term future predictions to provide intelligent insight on how capacity is being used, and what future needs may arise.

- Short-term Capacity Full Prediction: Observability uses a daily analysis of capacity usage to help users avoid short-term data unavailability events by starting to predict, within a quarter, when capacity is expected to reach full.
- Capacity Anomaly Detection: Observability uses an hourly analysis of capacity usage to identify a sudden surge of capacity utilization that could result in data unavailability. This anomaly detection helps to avoid the 2:00am phone call resulting from a sudden capacity utilization spike due to a potentially runaway query or rogue actor in the environment.

- Longer-term Capacity Forecasting: Observability helps users more intelligently project capacity utilization so that they can plan future capacity requirements and budget accordingly.

Proactive Health Score

The Proactive Health Score is another key differentiator for Infrastructure Observability, relative to other monitoring and reporting tools. Observability proactively monitors the critical areas of each system to quickly identify potential issues and provide recommended remediation solutions. The Health Score is a number ranging from 100 to 0, with 100 being a perfect Health Score.

The Health Score is based on the five categories shown in the following table. Some examples of how Proactive Health mitigates risk are:

Category		Sample Health Issues
	Components	Physical components with issues: for example, faulty cables and fans
	Configuration	Non-HA host connections
	Capacity	Pools or clusters that are oversubscribed and reaching full capacity
	Performance	Storage groups not meeting their SLO
	Data Protection	Native replication and snapshot schedules are not being met

Cybersecurity

Cybersecurity is a set of features in Infrastructure Observability that identifies potential security violations. System configurations are continuously monitored and compared to a user-configurable evaluation plan at which point a risk level is assigned to each system. Users can quickly get a visual representation of system security risks by seeing the identified misconfigurations and can address security violations using the recommended remediations. Dell Security Advisories and associated Common Vulnerabilities and Exposures (CVEs) are reported against any applicable systems. This provides users with a notification of the vulnerability and an in-context link to the associated knowledge base article for remediation. Cybersecurity ransomware incidents identify potential ransomware attacks in near real-time. By learning the expected behavior of reducible data, Observability can identify anomalies in this behavior that provide indications of possible encryption attacks.

Multisystem updates

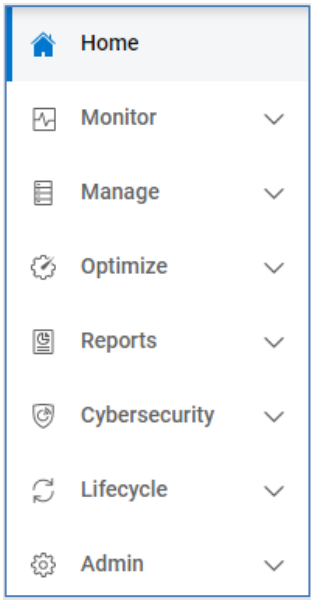
The multisystem update feature pertains to VxRail clusters and PowerEdge servers. Users can initiate VxRail cluster update pre-checks, software downloads, and system updates from the Infrastructure Observability UI. Users can also initiate PowerEdge firmware updates across their server fleet. This feature provides more operational efficiency while maintaining security and consistency.

Infrastructure Observability UI layout

This section discusses the layout of the user interface.

Navigation pane

The left navigation bar is designed to provide clear visibility into Infrastructure Observability functionality to streamline access to information. The top-level menu selections are task-oriented, directing the user to the appropriate section of the user interface to access the necessary information.



The navigation bar consists of the following selections:

Home – Access the home page that provides high-level summary information and some detailed information about various key aspects of the environment, allowing users to quickly identify potential risks. This information includes the Proactive Health Score, predictions on when pools and clusters will reach full capacity and system performance impacts.

Monitor - View the multisystem pages for Storage, Networking, Converged, Hyperconverged, Server, and Data Protection. A drop-down menu allows the user to switch between Health, Inventory, Capacity, and Performance.

- Health – Shows the proactive health scores across the environment.
- Inventory – Shows the system code version, location, site, and contract status. This category is where VxBlock converged system information is displayed.
- Capacity – Includes the usable, used, and free capacity metrics. For switches, capacity is displayed in terms of ports.
- Performance – Shows system level performance KPIs for all systems and switches.

Note: Items in gray indicate that the selected product type or category is not applicable.

The Virtualization View provides users a more traditional VMware tree-style navigation similar to what administrators are familiar with in vCenter. The Virtualization view supports VxRail, storage, and PowerEdge based virtual machines.

The Carbon Footprint page provides insights on energy and carbon emissions at the system and workload level. This includes reporting on both year to date and forecast metrics.

The Service Requests page provides a status of open service requests applicable to the systems monitored by Observability.

There are also views to see aggregated lists of all pools, health issues, and alerts.

Manage – View available system updates for storage, networking HCI, and data protection. Perform VxRail update pre-checks, software downloads, cluster updates, and PowerEdge firmware updates.

Optimize – Access the Reclaimable Storage listing and relevant knowledge base articles for systems.

Reports – Create and view custom reports**.** Reports can consist of both tables and line charts. They can be exported on demand or scheduled and emailed to a specified list of recipients.

Cybersecurity – View security risk levels, active and resolved security issues, and configure security evaluation policies for cybersecurity-enabled systems. View applicable security advisories. Configure and view cybersecurity ransomware incidents for supported platforms.

Lifecycle – View service contracts and life-cycle milestones for the components in VxBlock Converged Systems. This view includes timelines that display the following milestone dates: General Availability, End of Life, End of Support, End of Renewal, End of Service Life. Perform CI code comparisons to identify gaps between running software and firmware versions and target code levels.

Admin – Includes links to various administrative tasks.

The Identity Management section allows Observability administrators to set access controls for standard Observability users and initiate the single sign-on process federating Observability with the customer's Identity Provider.

The Settings menu is used to configure access for User Community and Customer Support and email notification settings. The Settings section also allows users to set filters on which systems they want to see in both the Observability user interface and the mobile app.

The Customization section allows users to temporarily pause connectivity health checks for hosts connected to Unity XT family and SC Series systems and capacity health checks for Unity XT file systems. The Integrations section provides access to Webhooks and REST API settings.

The Integrations page allows users with the DevOps role to configure Webhooks and obtain an authorization key to access the Observability REST API.

The Licenses page shows system license and entitlement details including entitlement type and expiration date for PowerFlex systems, PowerScale virtual edition, and APEX Navigator.

The Connectivity page shows the connectivity status of all Observability capable systems and allows users to onboard SC Series, PowerVault, and VxBlock Converged systems.

The Collectors section is where users can download the Observability Collector for VMware, Connectrix, and PowerSwitch and see the status of all installed Collectors.

The Jobs page shows the status of VxRail and PowerEdge tasks initiated from Observability.

The HCI Settings page allows users to enable access controls and enter credentials to vCenter for system updates.

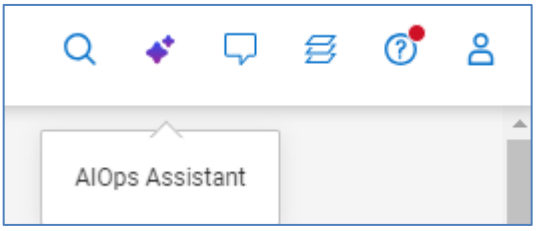
The Tags page allows users to manage tags to assign custom meta data to systems and components.

Global Search

The Global Search feature helps users quickly find Systems, Hosts, Pools, Storage Resource Pools, Storage Groups, LUNs/Volumes, File Systems, Virtual Machines, and MTrees/Storage Units. Users can specify a few keywords and get a summarized list of top matches. From there, users can click an item to access its details or go to an expanded view with all matches.

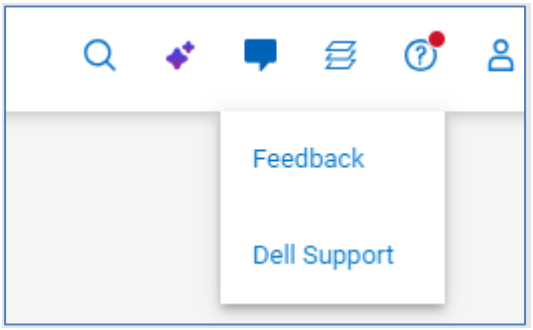
AIOps Assistant

Access and chat with the GenAI-powered virtual assistant to answer questions about product support. At the time of this publication, the AIOps assistant is in tech preview and available through entitlement.



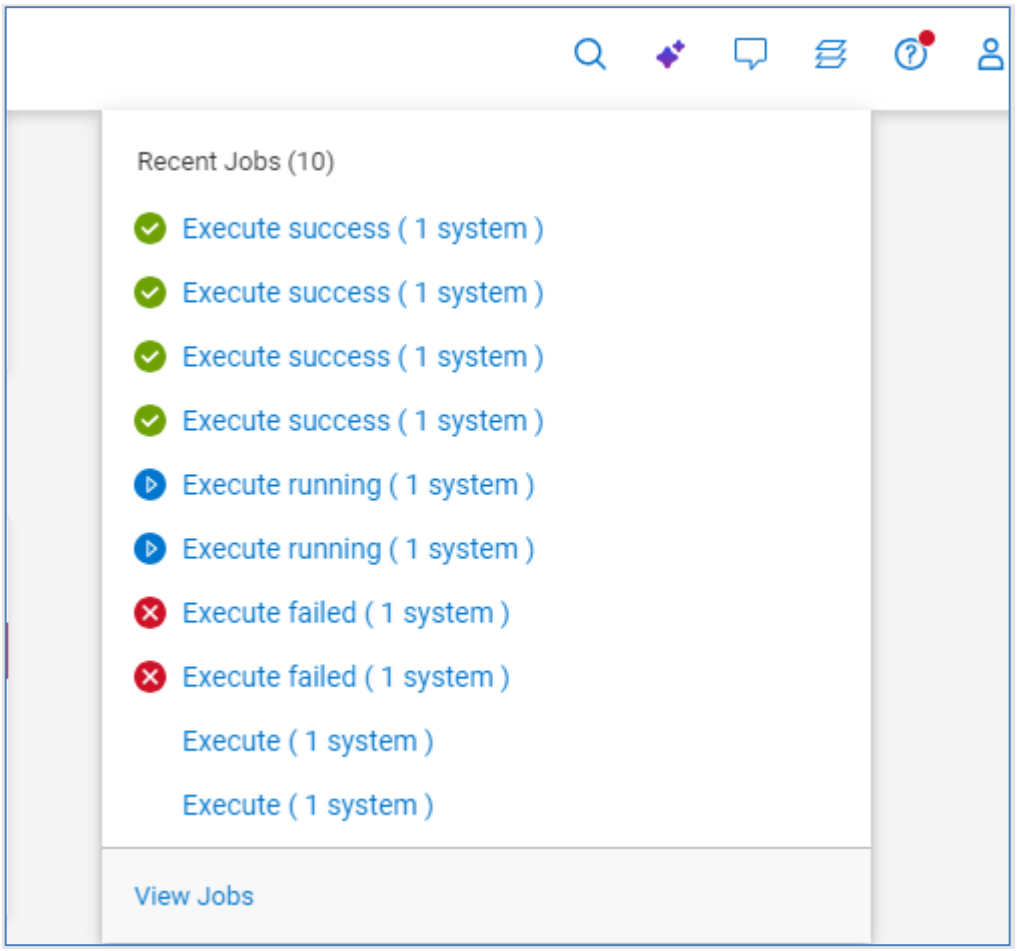
Feedback and Dell Support

Selecting the comment icon allows the user to submit feedback to the Infrastructure Observability product team or open the Dell Support website.



Jobs

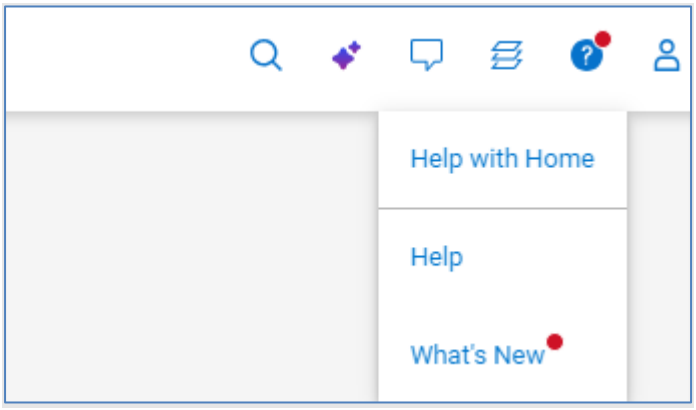
The Jobs icon opens a window showing recent jobs and status and a link to the Jobs page.



Help and What's New in APEX AIOps Observability

Infrastructure Observability is updated frequently to deliver helpful new content to users. Use the Observability Simulator (https://cloudiq.dell.com/simulator) to view the latest features which may not be documented in this paper.

New features can be seen by clicking the icon on the top menu bar.



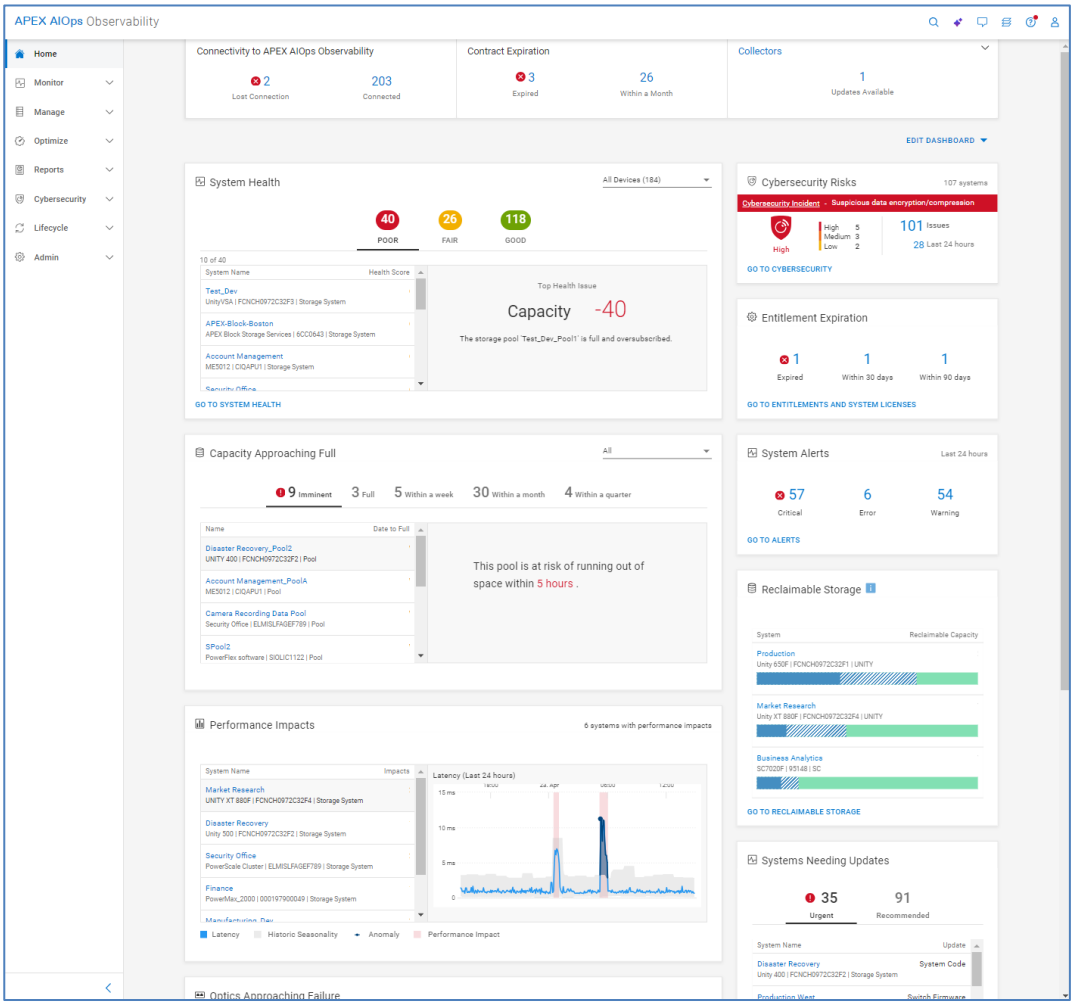
The “What’s New in APEX AIOps Observability” window will appear showing recent changes and enhancements. Clicking **View All Enhancements** displays a historical list of all the updates. The most recent information is presented first, and users can scroll down the list to see the monthly evolution of Observability since its introduction. This display can be turned off by sliding the **Don’t show again until the next update** button.

Selecting the user icon allows the user to switch companies if they have access to multiple sites and sign out of the UI.

Home page

The **Home** page provides a consolidated view of the Dell environment. This page is the highest-level summary of the environment providing users with a roll-up of the key factors to understand the overall health and operation of the IT infrastructure. The tiles on the home page can be reorganized to each user’s preference using the **Edit Dashboard** button. Users can also select **Reset to Default** to revert to the default home page layout.

There are three tiles along the top of the Home page (minimized in image of the Home page below, but shown in a following image).



Connectivity to APEX AIOps Observability – Shows the connectivity status for all systems registered in Observability and the Observability Collector. Systems are displayed in the following four categories:

- **Install Base Issues**: Observability cannot display due to Install Base configuration issues.
- **Lost Connection**: Systems that have lost connection and are no longer sending data to Observability.
- **Not Set Up**: Systems that are not set up to send data through Secure Connect Gateway to Observability.
- **Connected**: Systems that are successfully sending data to Observability.

Selecting each category redirects the user to the Connectivity Page and displays a filtered list of systems and collectors corresponding to that connectivity status.

Contract Expiration – Shows the number of systems with contracts that are:

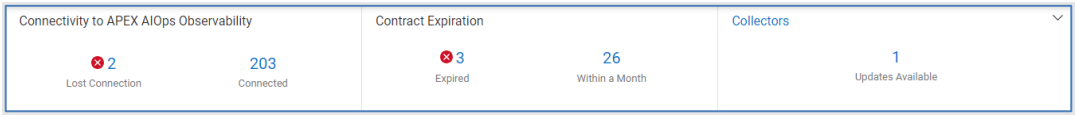
- Expired
- Expire within a month
- Expire within a quarter

The user can select the number to open a window with the list of systems that meets the expiration criteria. Systems whose contracts have expired will be removed from other standard Observability views.

Collectors – Displays the number of Observability Collectors that have:

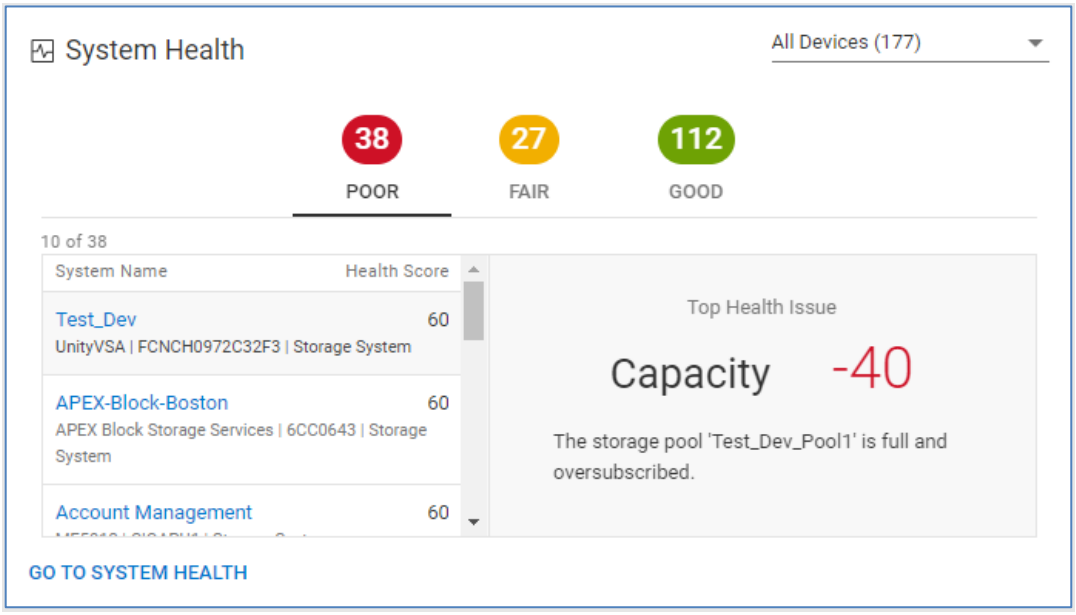
- Issues that need to be resolved
- Available Updates

The user can select the number in each category to view a filtered list of collectors from the Collectors view.



System Health – Categorizes all monitored products into three ranges of health scores:

- **Poor**: 0-70
- **Fair**: 71-94
- **Good**: 95-100
- **Unknown**: List of systems whose health score cannot be calculated. This situation could indicate a connection issue.

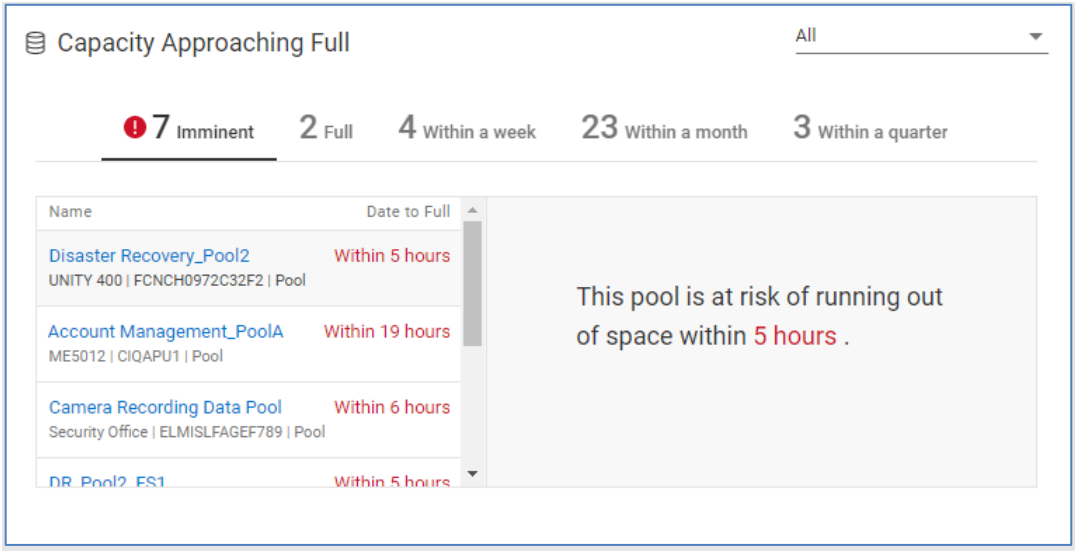


Selecting a range's number along the top of the tile displays the system names and health scores for that range, sorted from low to high. The chart is interactive allowing the user to select a system in the list to display its Top Health Issue in the right pane. This window displays the most impactful issue affecting the health score. Selecting the system name hyperlink directs the user to the Health Score tab of the systems details page. There is also a filter that allows the user to filter this tile on the following product types:

- Storage Systems
- Networking Systems
- HCI Systems
- Data Protection Systems
- Servers

Capacity Approaching Full – Leverages predictive analytics to identify the storage pools, clusters, file systems, appliances, and subscriptions running out of space. The chart is interactive allowing the user to select each object to display a trend line and forecasting chart of the used capacity. The estimated time range until each entity will be full is shown as:

- Imminent (predicted to run out of space within 24 hrs.)
- Full
- Within a week
- Within a month
- Within a quarter

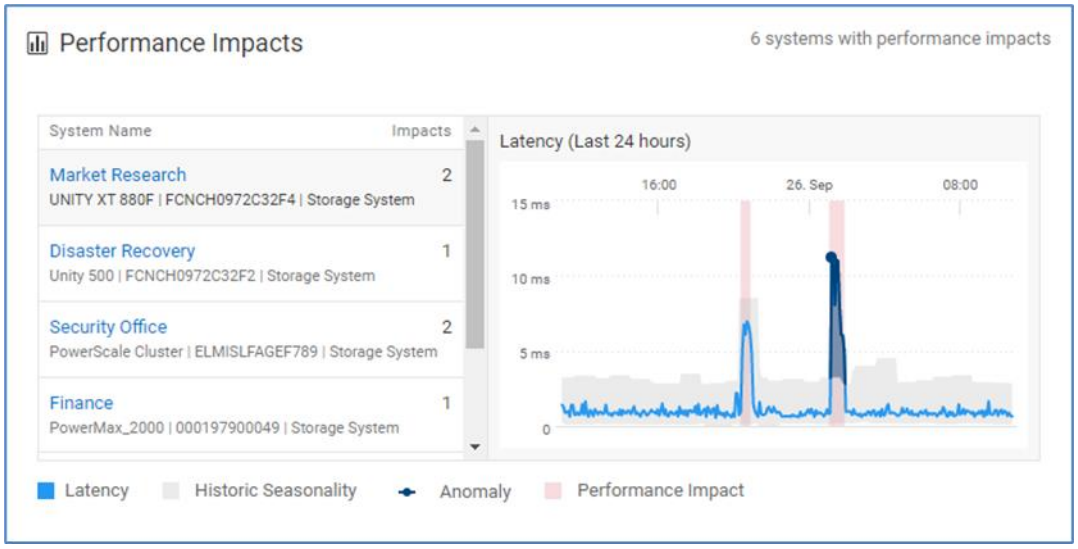


There is a drop-down menu that allows the user to filter the tile based on object type: Appliances, File Systems, Pools, Clusters, or Subscriptions.

The Imminent risk category is supported for APEX Hybrid Cloud Services, APEX Private Cloud Services, Unity XT family, PowerVault, PowerMax/VMAX, PowerStore, PowerScale, and VxRail systems.

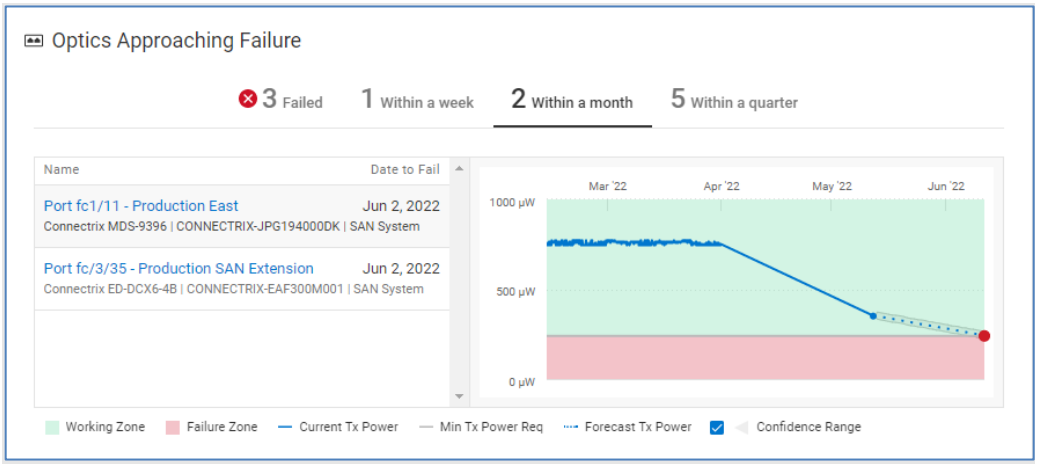
Selecting the object name hyperlink directs the user to the Capacity tab on the object details page.

Performance Impacts – Supported for APEX Hybrid Cloud Services, APEX Private Cloud Services, PowerMax/VMAX, PowerStore, PowerFlex, PowerScale, and Unity XT family systems. Utilizes Observability analytics to identify when there are performance impacts on a system due to a possible workload contention. It will also identify the existence of performance anomalies where the current system workload is outside of expected boundaries based on historical workloads. The chart is interactive allowing the user to select an impacted system and see the latency of that system over the last 24 hours in the right pane. Both performance impacts and performance anomalies are highlighted in the chart. Selecting the system name hyperlink directs the user to the Performance tab of the system details page where the user can see more detailed performance information for the system.

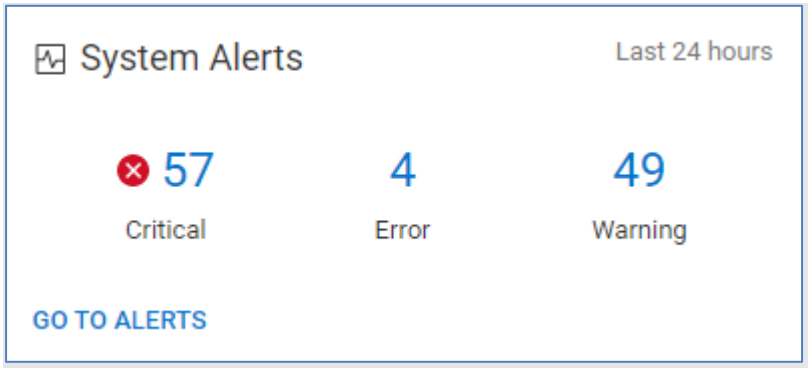


Optics Approaching Failure – Uses predictive analytics to provide a list of Connectrix ports with impending optic failures. The measured and predicted Tx power is analyzed and charted along with the working and failure zones. The estimated time to failure is categorized in each of the following timeframes:

- Failed
- Within a week
- Within a month
- Within a quarter



System Alerts – Summarizes the alerts sent to Observability over the last 24 hours across the Critical, Error, and Warning severity levels. Clicking a number opens a list of alerts in the Alerts window filtered by the selected severity level. Clicking the GO TO ALERTS link navigates the user to a filtered list of alerts, across all severity levels, from the last 24 hours.

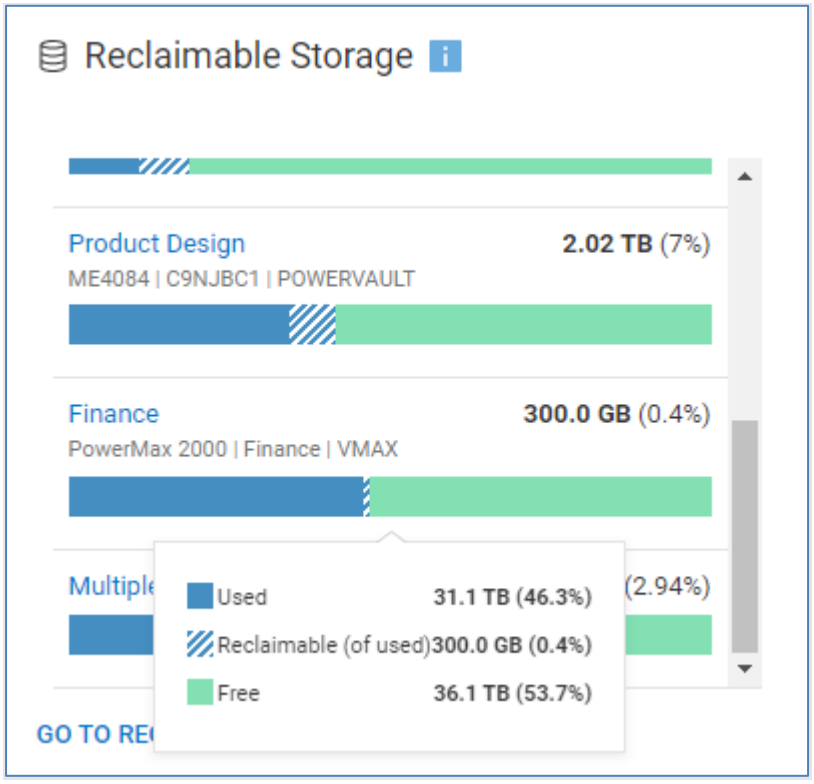


Cybersecurity Risks – Summarizes the active cybersecurity risks in the environment and notifies the user of ransomware incidents. The overall environment has an assigned risk level. A breakdown of the number of systems per risk level is provided as well as total issues and issues identified in the last 24 hours. Links to the System Risk page and the Cybersecurity Issues page are available.

Entitlement Expiration – This tile summarizes the licenses and entitlements that are expired, will expire within 30 days, and will expire within 90 days. This content supports

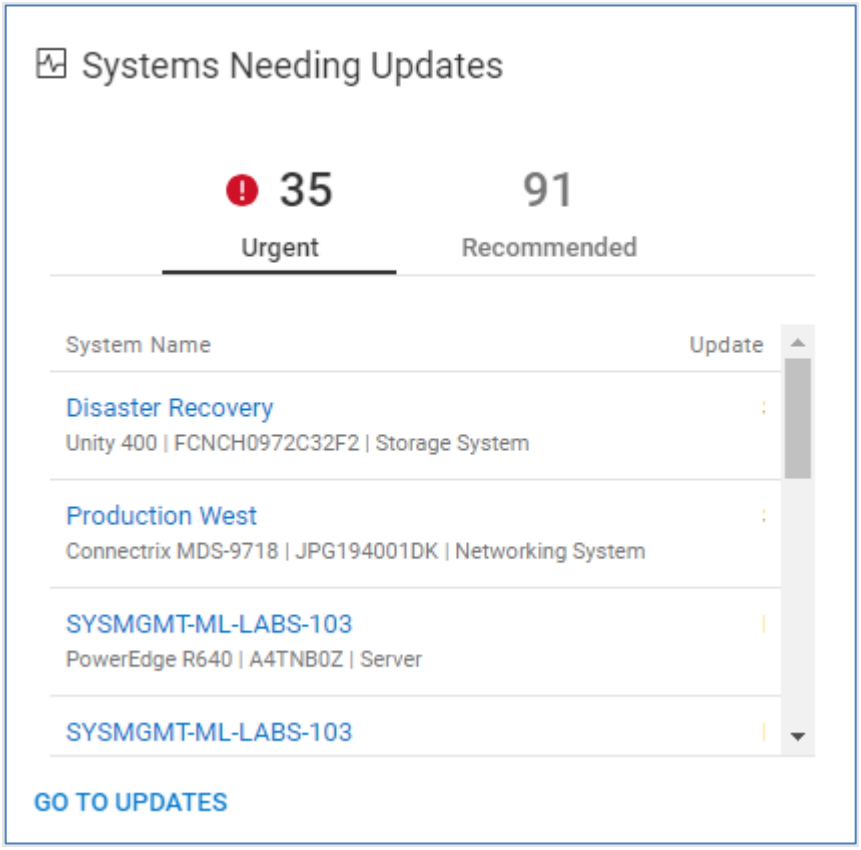
PowerFlex systems, PowerScale Virtual Edition systems, and systems deployed with DELL APEX Navigator for Multicloud Storage. Clicking any of the categories directs the user to the Entitlements and Licenses page and displays the entitlements in the selected category.

Reclaimable Storage – This tile summarizes PowerStore, PowerMax/VMAX, Unity XT family, SC Series, and PowerVault ME systems that have reclaimable storage. Each system with reclaimable storage shows the total amount of used, reclaimable (of used), and free storage. Reclaimable storage includes block and file-based virtual machines that have been shut down for at least the past week. Selecting the system name hyperlink directs the user to the Capacity tab on the system details page.



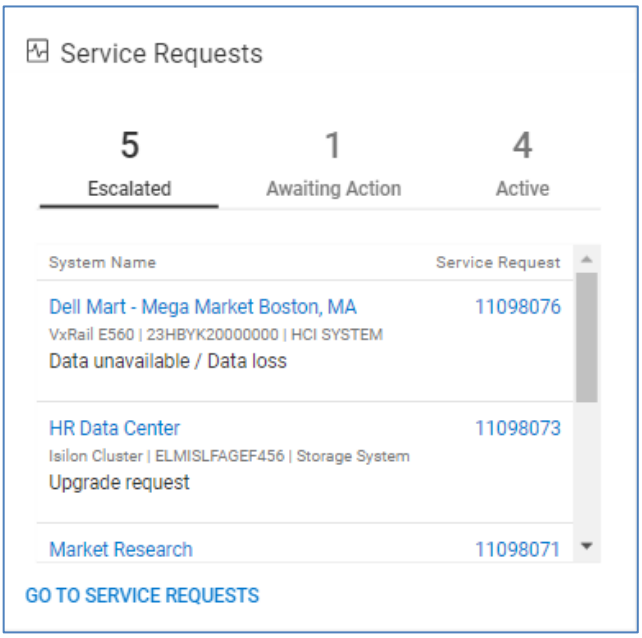
Systems Needing Updates – This tile identifies systems that have either Urgent or Recommended system code, firmware, or management software updates available. It shows the system and the type of update. Selecting the “GO TO UPDATES” link opens the System Updates page. This page shows all available code, firmware, and software

updates across all systems and includes links to download the updates. Selecting the system name hyperlink directs the user to the Inventory tab on the system details page.



Service Requests

The Service Requests tile provides a summary of escalated, awaiting action, and active service requests. Links allow users to go directly to the system details page in Observability or review and update the service request on the Dell support page.



Monitor

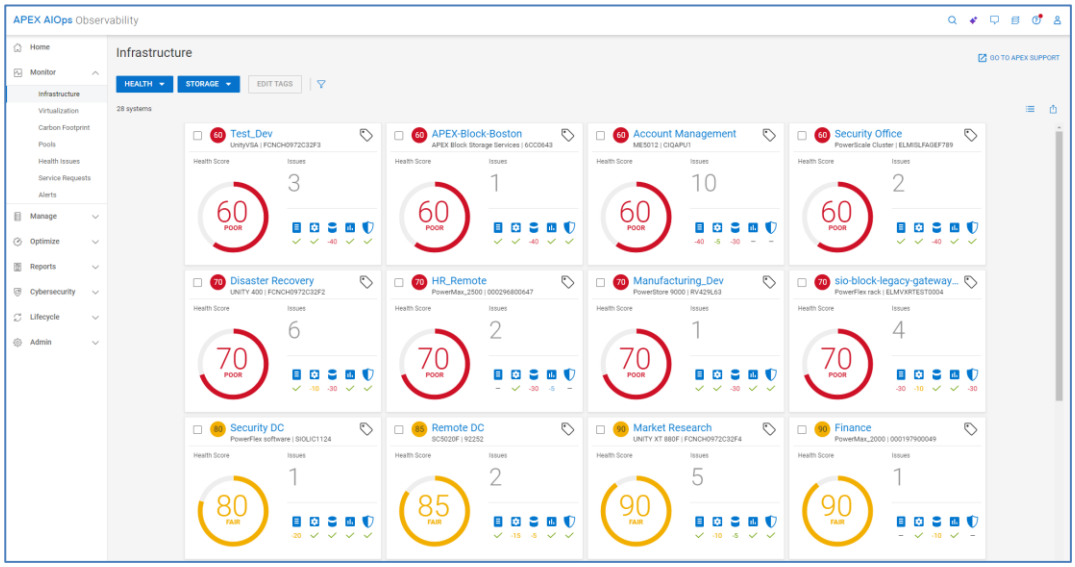
Infrastructure - Health

The Infrastructure page is a consolidated multisystem view that can show Health, Inventory, Capacity, and Performance views for each of the supported Dell platforms. The Health page displays the Proactive Health Score for all systems across all products in a consolidated view. There are up to six available platforms to choose: Converged, Data Protection, HCI, Networking, Servers, and Storage. Users can quickly identify the systems at highest risk, including the number of issues in each category that make up the health score.

Infrastructure Observability uses up to five categories to determine the Proactive Health Score presented on the Infrastructure Health page: Components, Configuration, Capacity, Performance, and Data Protection.

Note:

- PowerMax and VMAX systems do not include health issues in the Components or Data Protection categories. Observability displays a dash (—) for these categories.
- PowerVault systems do not include the Performance or Data Protection categories. Observability displays a dash (—) for these categories.
- VxRail systems, APEX Hybrid Cloud Services, and APEX Private Cloud Services do not include the Data Protection category.
- Connectrix, PowerSwitch, and PowerEdge use only the Components category.
- Converged provides the health score for the storage in the VxBlock system.

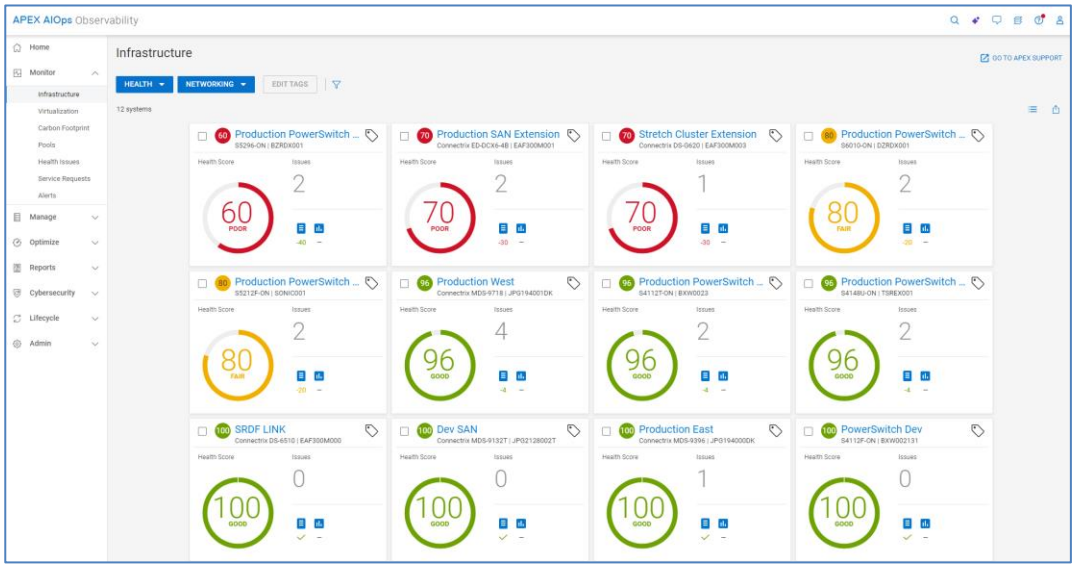


Each system has a health score displayed in the circle (ranging from 100 to 0) which is calculated as 100 minus the issue with the greatest impact. Each of the five categories has either a green check mark, a negative number, or a dash. The green check indicates no issues are present for that category. A negative number represents the deduction for the most impactful issue in the category. A dash indicates that the category is not supported for that system type. This approach is intended to help users focus on the most significant issue for the system, so that they can resolve the issue to improve the health score.

The Health Score range is as follows:

- **Good** = 95–100 (Green)
- **Fair** = 71–94 (Yellow)
- **Poor** = 0–70 (Red)

The Health Score is displayed in the color that corresponds to the range. Blue coloring with a dash instead of a number indicates a system that has recently been added to Observability and does not yet have a calculated health score. Gray coloring with a number indicates a connectivity issue which leads to an uncertain health score. In this case, the user should check the system connectivity.



The **Card** view, shown previously for both Storage and Networking, is the default view for this page. Users can choose the **List** view by selecting the List View Icon ( ) in the upper right of the window. The list view is shown on the next page for Storage. This view may be more useful for larger environments because it allows for a more condensed view of the information and the ability to sort columns. Users can view and edit custom tags from either the Card view or the List view. Custom tags are covered in detail in the Custom Tags section.

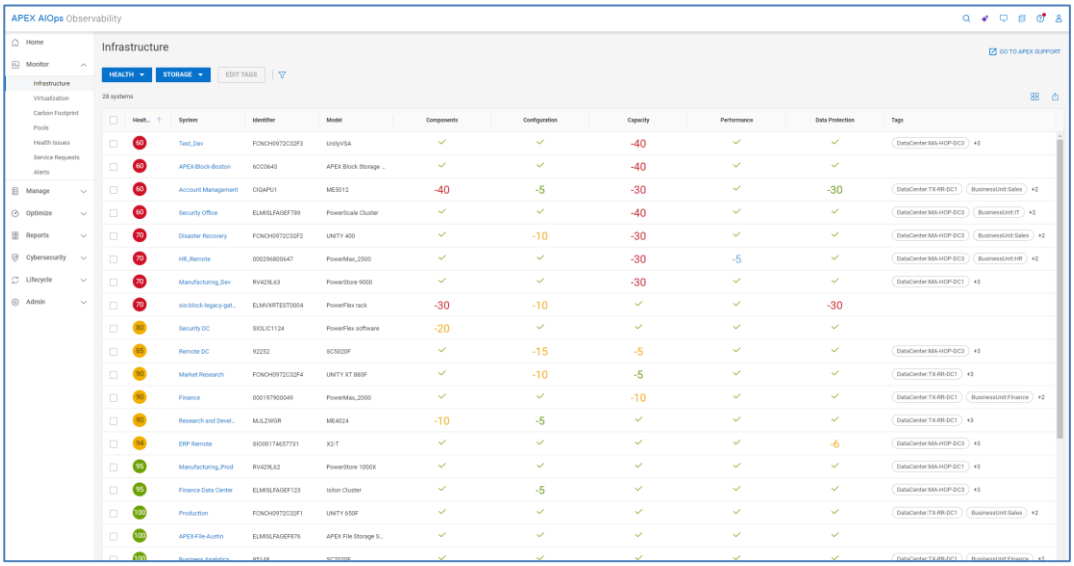
Users can also export the data from many of the views in Observability to a CSV file by selecting the Export CSV icon in the upper right of the view. Exporting the data from any of the multisystem views exports the data from the Health, Inventory, Capacity, and Performance pages.

Users can filter the systems in both the Card View and List View by selecting the **Filter** icon and entering in various criteria. The available criteria vary based on the view, but examples include System Name, Product Type, Heath Score, Custom Tag, Site Name, and Location. The filter settings stay in effect until the user clears the filter or logs out of the UI.

Each view provides the following information:

- **Score** – Proactive Health Score for system
- **Name** – User-defined name of system
- **Model** – Specific model of system
- **Serial number** – Unique serial number or identifier for the system

Selecting an individual system from either the card view or list view navigates the user to the system details page. These pages are discussed for each system type later in this paper.

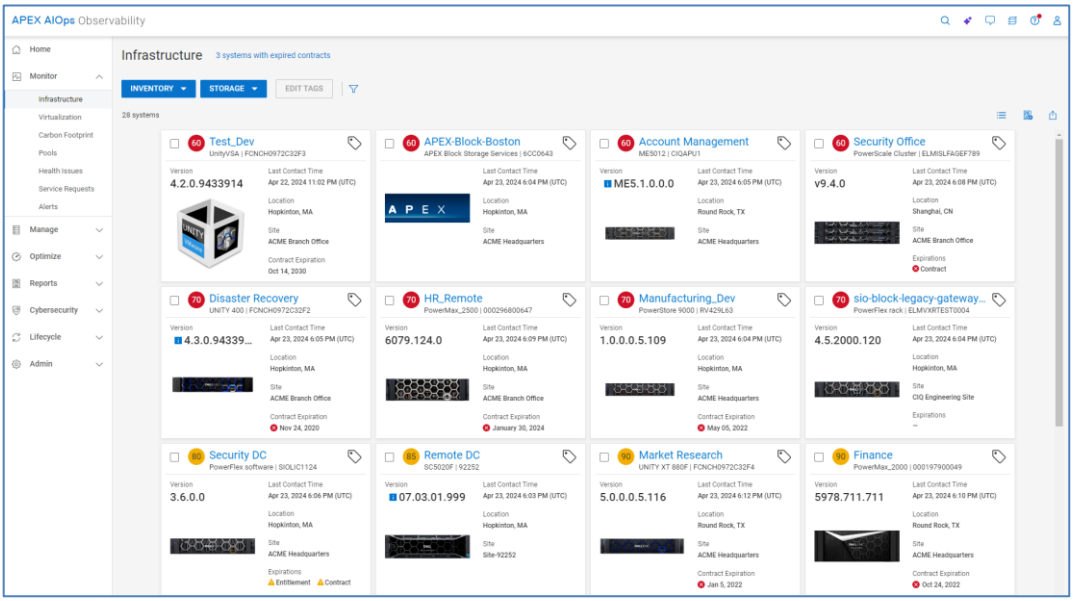


Infrastructure - Inventory

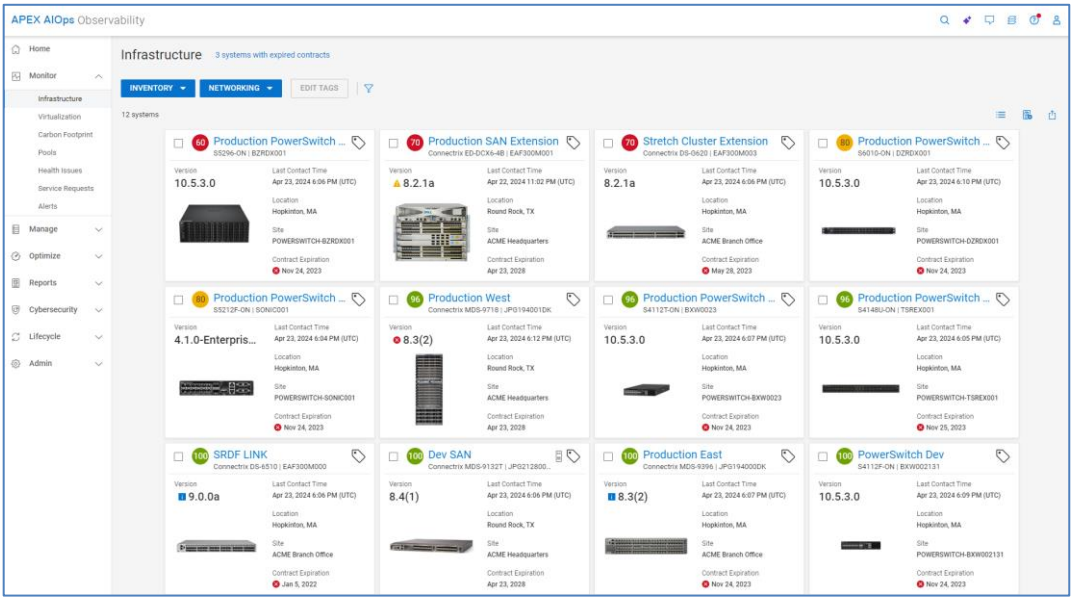
The **Inventory** page is the multisystem view showing the configuration information for all systems in the environment. There can be up to six types of platforms from which to choose: Converged, Data Protection, HCI, Networking, Servers, and Storage. The information displayed on the Systems pages includes:

- **Version** (vCenter Version for Converged) – Version of installed software
- **Last Contact Time** – The last time that Infrastructure Observability received data from the system
- **Managed by** (Converged only) – Type of AMP managing the Converged System
- **Location** – Location where the system is installed
- **Site** – Site ID with which the system is associated
- **Contract Expiration** (Warranty Expiration for PowerEdge) – Expiration date for the service contract. Contract expiration is not supported for PowerFlex, PowerVault, SC Series, or PowerProtect DM.

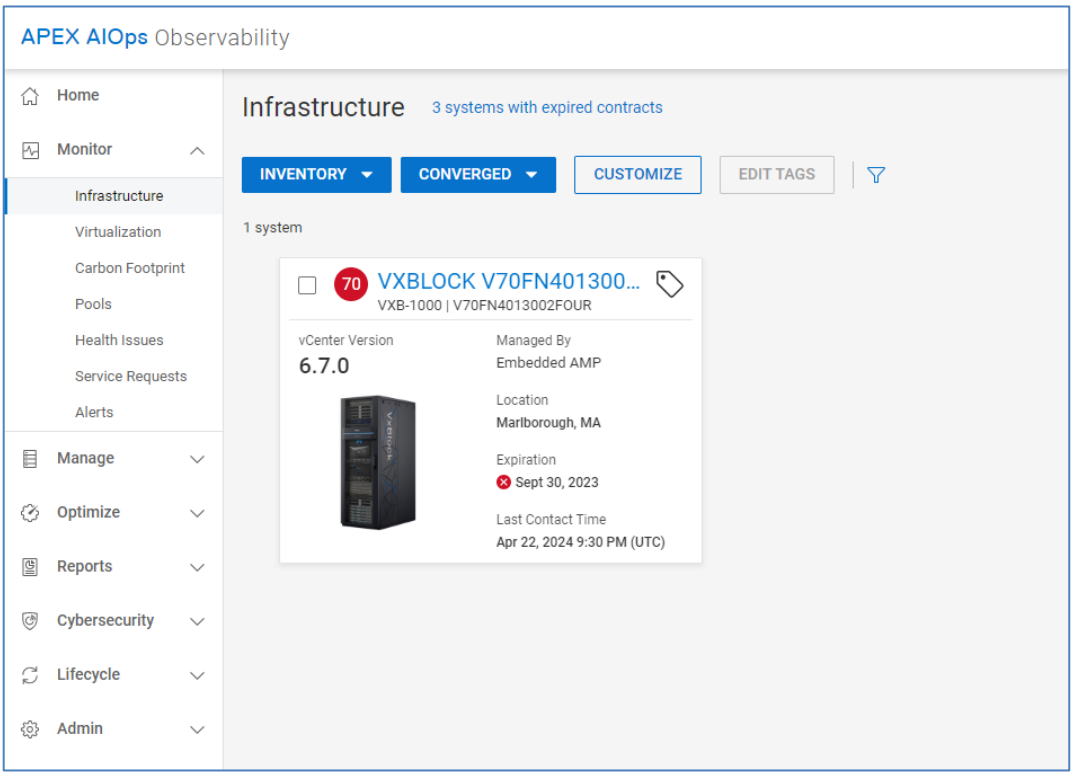
For systems that support the identification of system updates, there will also be an indication when a code update is available. Hovering over the information icon (ⓘ) opens a window showing the update version. Clicking the “Learn More” link from within the window opens a dialog with summary information and links to the Release Notes and the software download. The following shows an example of the Storage page.



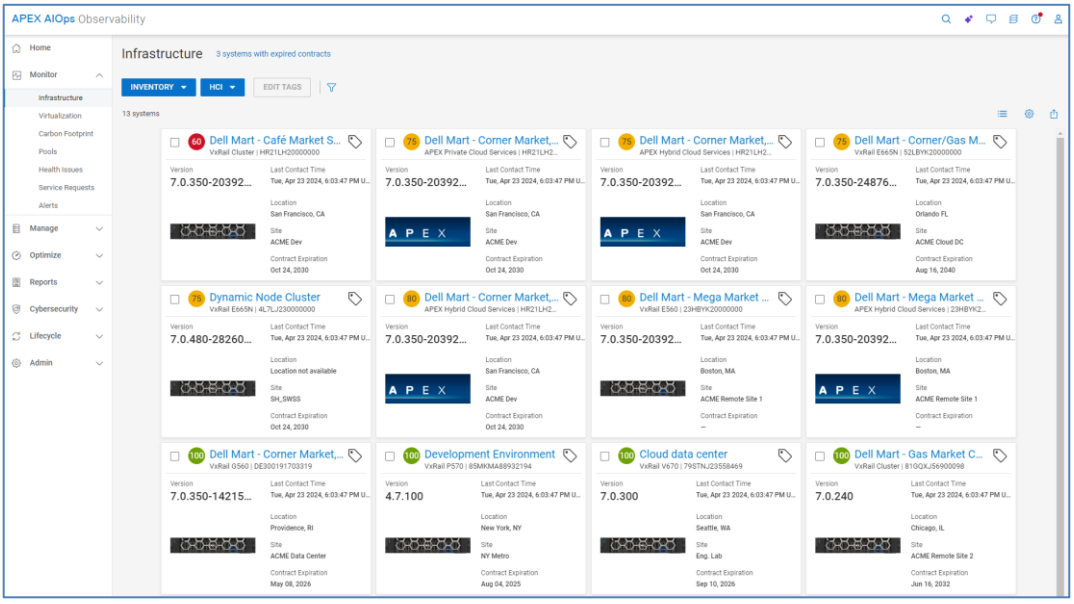
The following example of the Networking page shows similar attributes to those displayed in the Storage page.



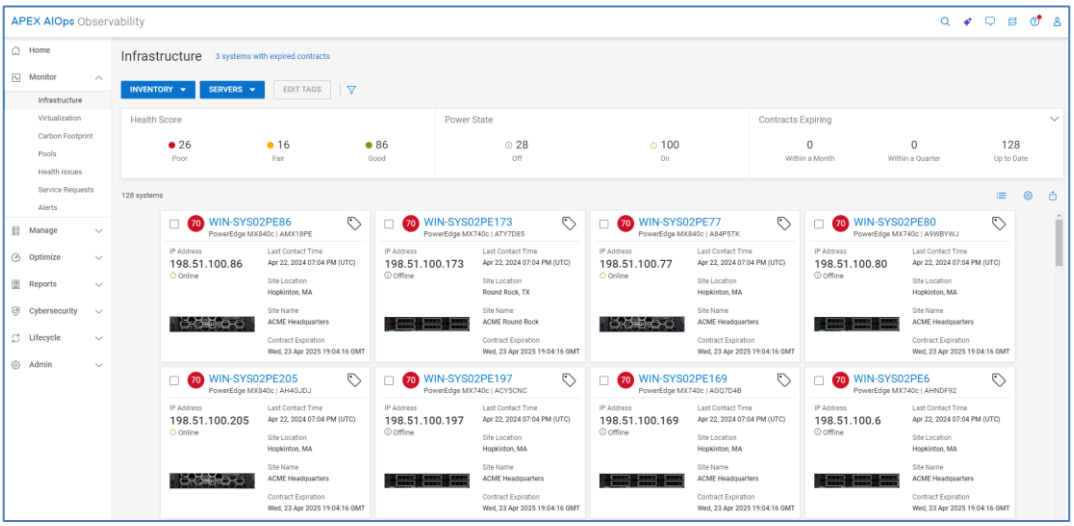
The following is an example of the **CONVERGED** page. The user can edit the system name in the card to provide a more user-identifiable name and differentiate it when multiple systems are being monitored. Users can also use the Customize button to display different attributes in the card view.



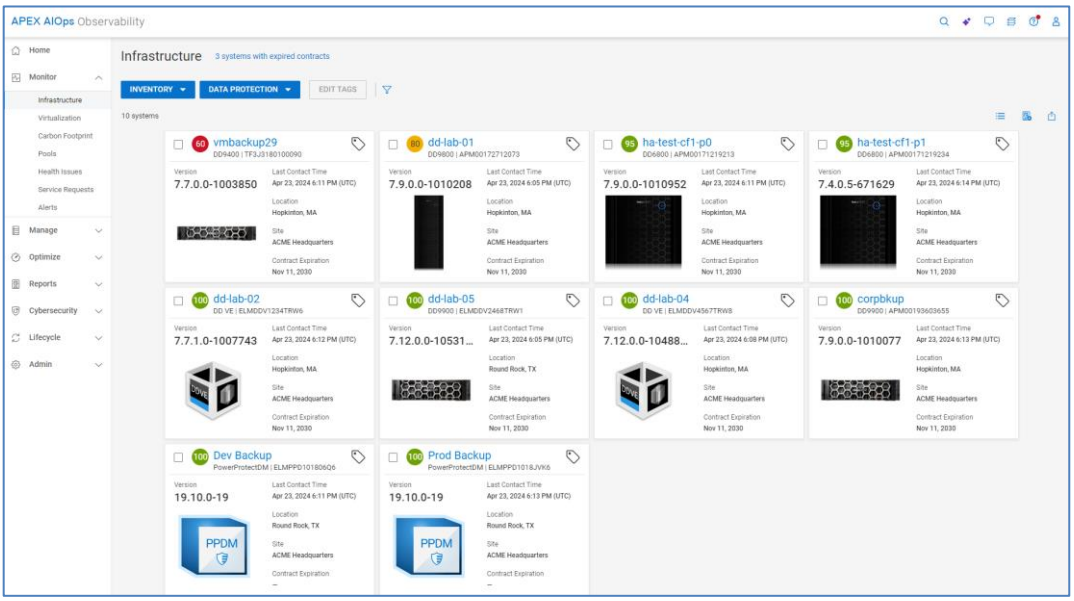
The following example of the HCI page displays the inventory of VxRail systems, APEX Hybrid Cloud Services, and APEX Private Cloud Services.



The following shows an example of the SERVERS page. There is a top banner summarizing the total number of servers by Health Score, Power State, and Contracts Expiring. This banner is provided for compute because of the potential for a large number of servers in Observability.



The following example of the Data Protection tab shows both PowerProtect DD systems and PowerProtect Data Manager instances monitored by Observability.



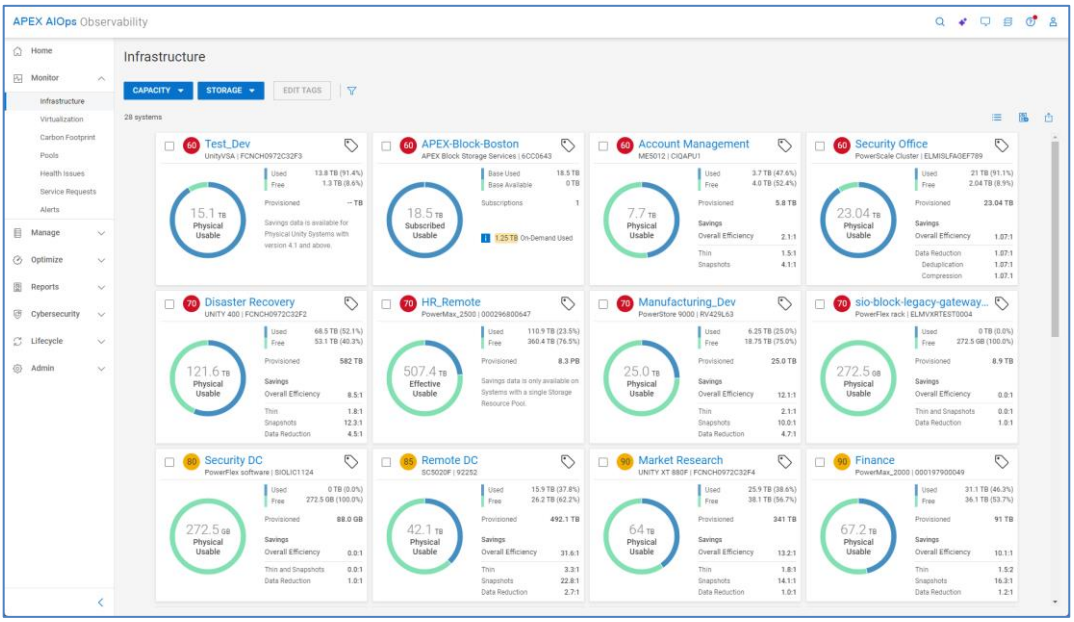
Infrastructure - Capacity

The **Infrastructure Capacity** view displays the system level storage capacity for traditional storage systems, APEX Hybrid Cloud Services, APEX Private Cloud Services, VxRail hyperconverged systems, and PowerProtect DD systems. For Connectrix and PowerSwitch, it displays port capacity.

The information for traditional storage systems includes:

- **Usable** – Total disk capacity, which is the sum of Used and Free space. For PowerMax 2500 and 8500 models, this represents the effective usable capacity.
- **Used** – Disk capacity that is allocated to an object, such as a LUN, Volume, or file system
- **Free** – Disk capacity provisioned to a storage pool but not yet allocated to an object, such as a LUN, Volume, or file system

- **Provisioned –** Total capacity visible to hosts attached to this system
- **Overall Efficiency** – System-level storage efficiency ratio, based on the following combined savings ratios:
  - **Thin** – Ratio of thin provisioned objects on the system (Unity XT family, PowerStore, SC Series, VMAX/PowerMax, PowerVault ME4)
  - **Snapshots** – Ratio of snapshots on the system (Unity XT family, PowerStore, SC Series, VMAX/PowerMax, PowerVault ME4)
  - **Thin and Copy** – Ratio of thin provisioned objects (XtremIO volumes, including snapshots)
  - **Data Reduction** – Ratio of data that has data reduction applied, using compression or deduplication. (Not supported for PowerVault ME4)
  - **Deduplication** – Ratio gained by savings from deduplication (PowerScale/Isilon only)

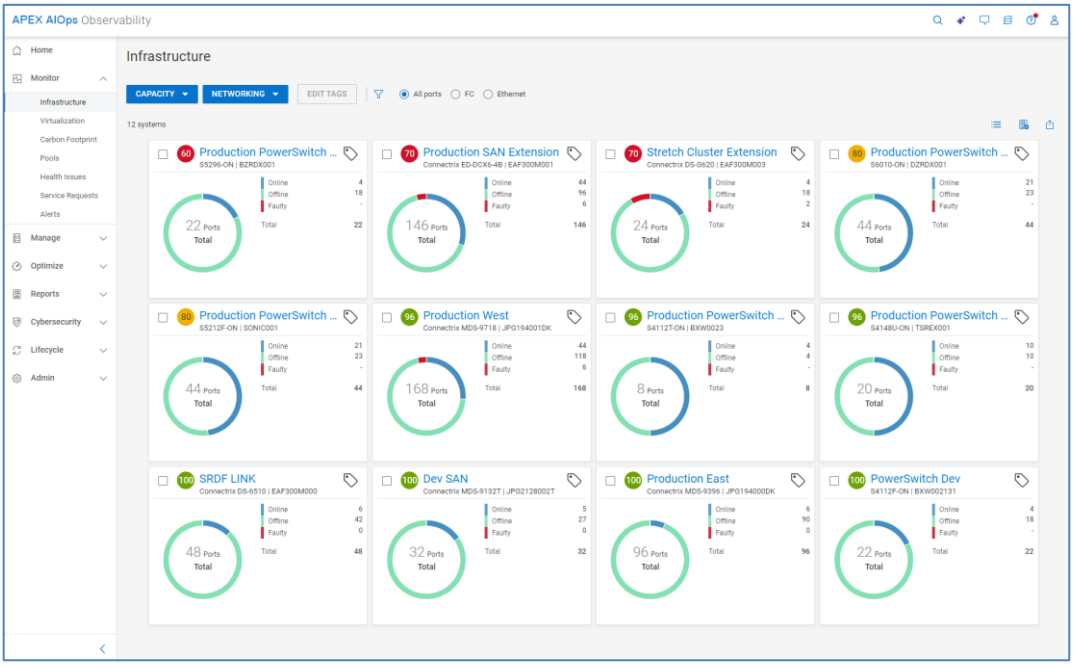


Note: For Unity XT family systems running version 4.3 and higher and SC Series running version 7.3 and higher, Data Reduction includes Compression or Deduplication.

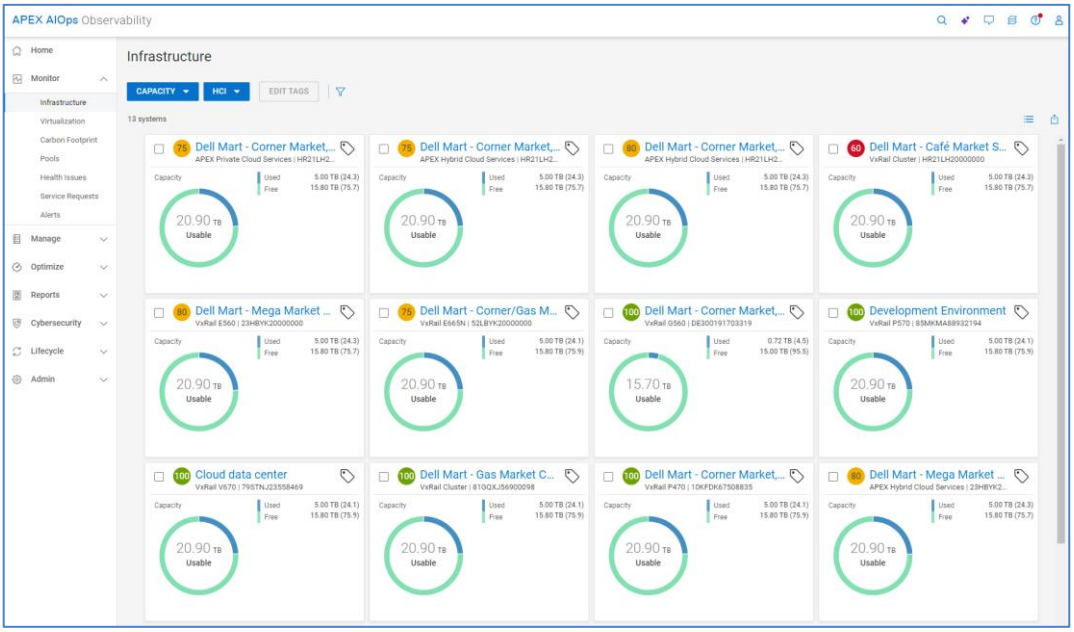
For switches, the user can filter the view to show All ports, FC ports, or Ethernet ports. For each selection, the displayed information includes:

- **Total Ports** – Total number of ports (All ports, FC ports, or Ethernet ports depending on previous selection)
- **Online** – Number of ports in an online state

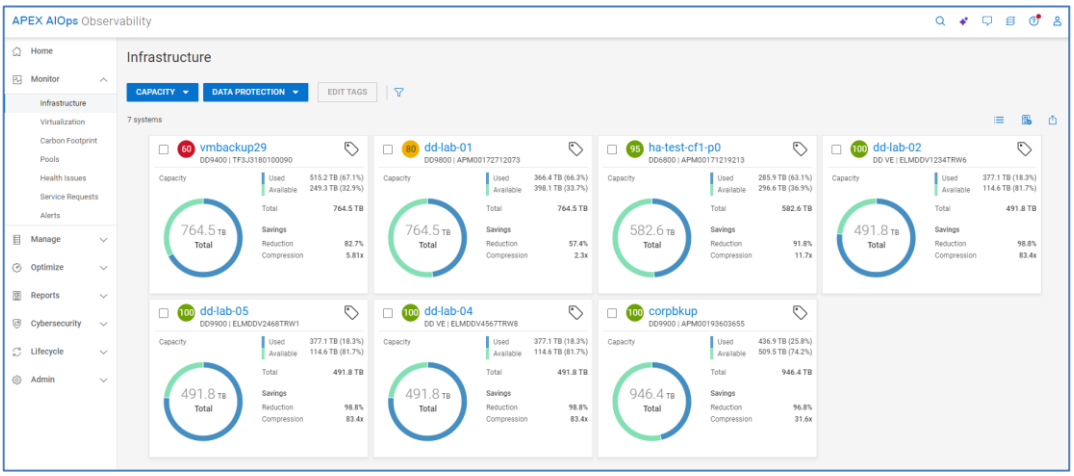
- **Offline** – Number of ports in an offline state
- **Faulty** – Number of ports with one or more faults



For VxRail systems, APEX Hybrid Cloud Services, and APEX Private Cloud Services, Observability displays Usable and a breakdown of Used and Free capacity.



The **Data Protection** view summarizes the capacity for DD systems. Total storage is broken down to Used and Available. Savings due to Reduction and Compression is also provided for each system.



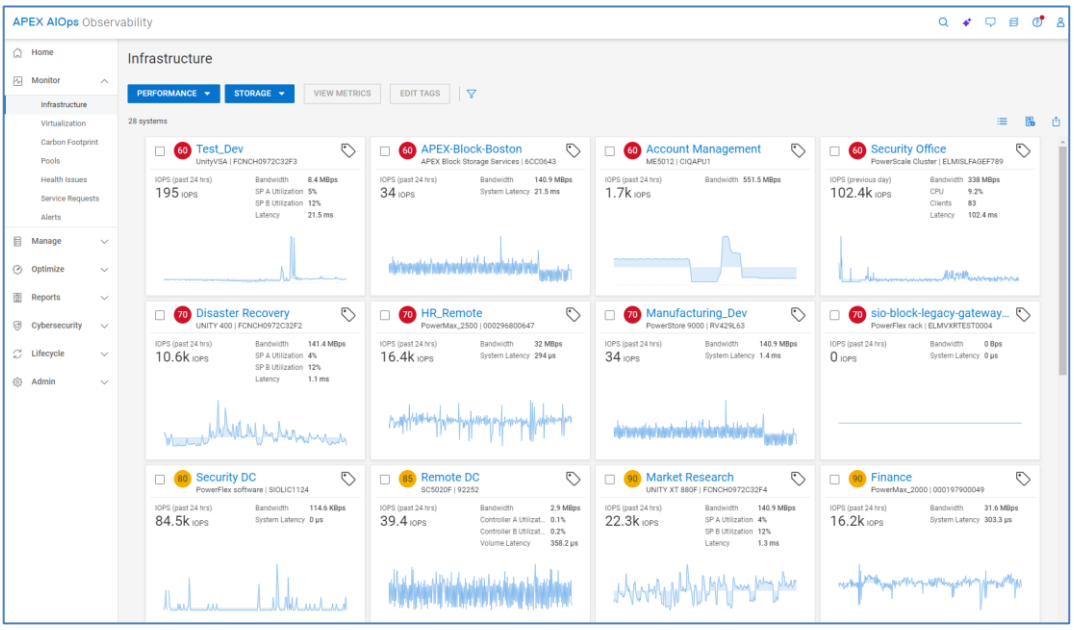
Infrastructure - Performance

The **Infrastructure Performance** view displays system-level performance metrics across all systems.

The information displayed for storage systems includes:

- **IOPS** – Average I/O requests per second over the last 24-hour period.
- **Bandwidth** – System bandwidth showing average host bytes per second over the last 24-hour period.
- **Utilization (Card View Only)** – Average percent of time the Storage Processors (Unity XT family) or Controllers (SC and XtremIO) are busy over the last 24-hour period.
- **Latency** – The average time required for a packet to travel from the host to the object over the last 24-hour period. For PowerMax and VMAX, displays the response time for read and write I/O requests for the system.
- **Clients (Card View Only)** – Number of clients connected to the PowerScale cluster.

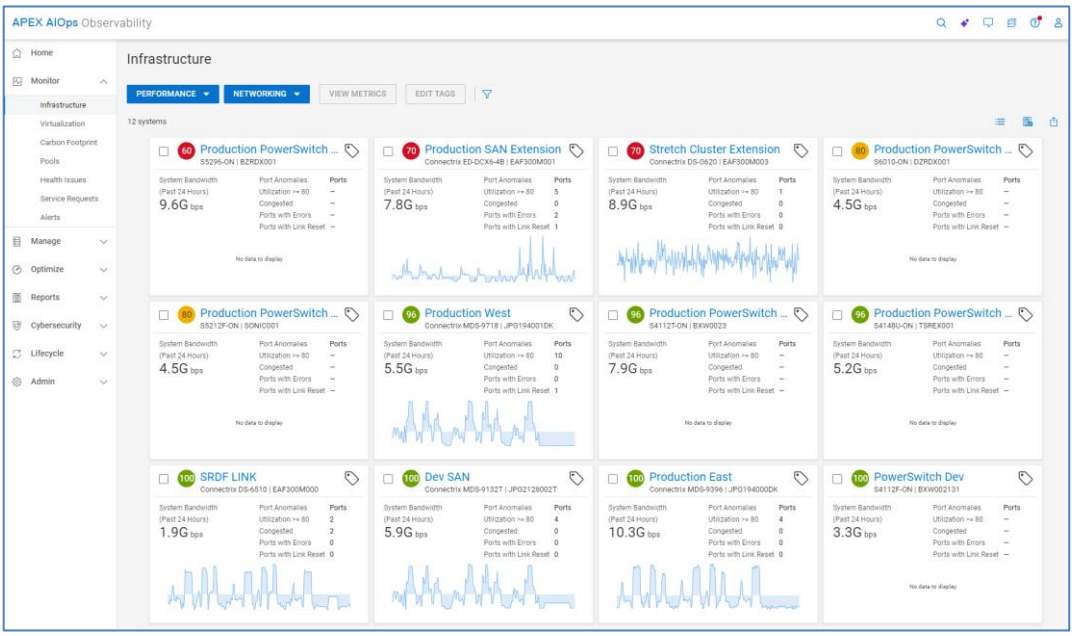
Performance Trend graph – Chart showing IOPS over the past 24 hours with a data point on every update (varies slightly per product type).



The System Performance information displayed for switches includes:

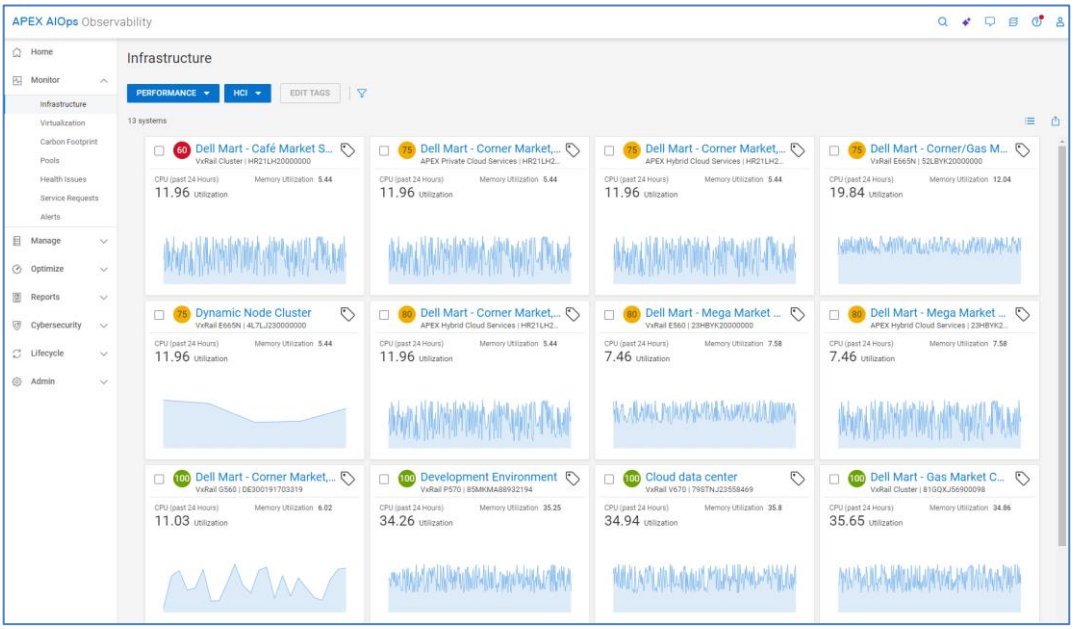
- **System Bandwidth** – Average bandwidth for the switch over the last 24-hour period.[12]
- **Utilization >= 80%** – Number of ports with utilization greater than or equal to 80%[4]
- **Congested** – (Connectrix only) Number of ports with congestion
- **Errors** – Number of ports with errors[1]
- **Link Reset** – (Connectrix only) Number of ports with link resets

[12] PowerSwitch OS10 v10.5.3.2 or later required



Note: The 24-hour bandwidth chart is displayed for Connectrix only.

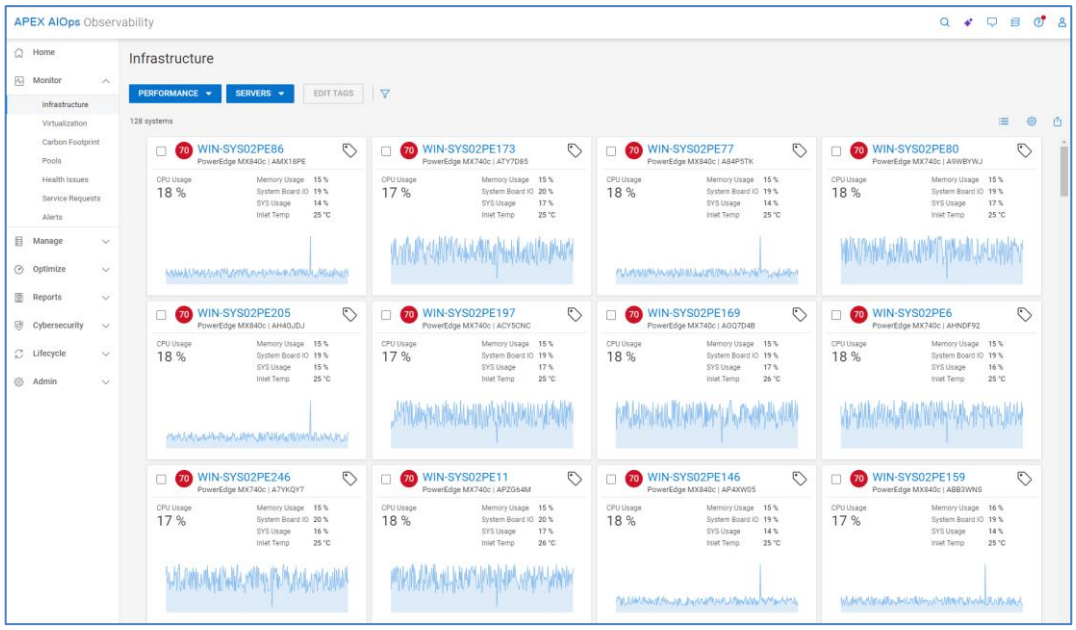
VxRail, APEX Hybrid Cloud Services, and APEX Private Cloud Services display a 24-hour chart of CPU utilization and the 24-hour average for CPU and Memory Utilization.



PowerEdge servers show the following performance metrics:

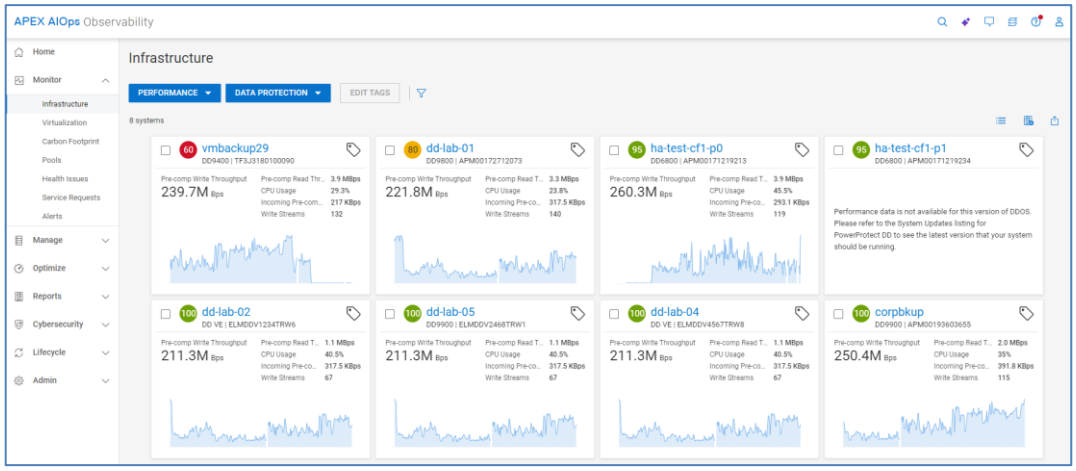
- **CPU Usage** – Percentage of CPU consumed by the server
- **Memory Usage** – Percentage of RAM the server uses based on what is allocated
- **System Board IO**
- **SYS Usage**

- **Inlet Temp** – Temperature reading in Celsius



PowerProtect DD systems show the 24-hour averages for the following metrics:

- Pre-compressed Write throughput
- Pre-compressed Read throughput
- CPU Usage
- Incoming Pre-compressed Replication
- Write Streams



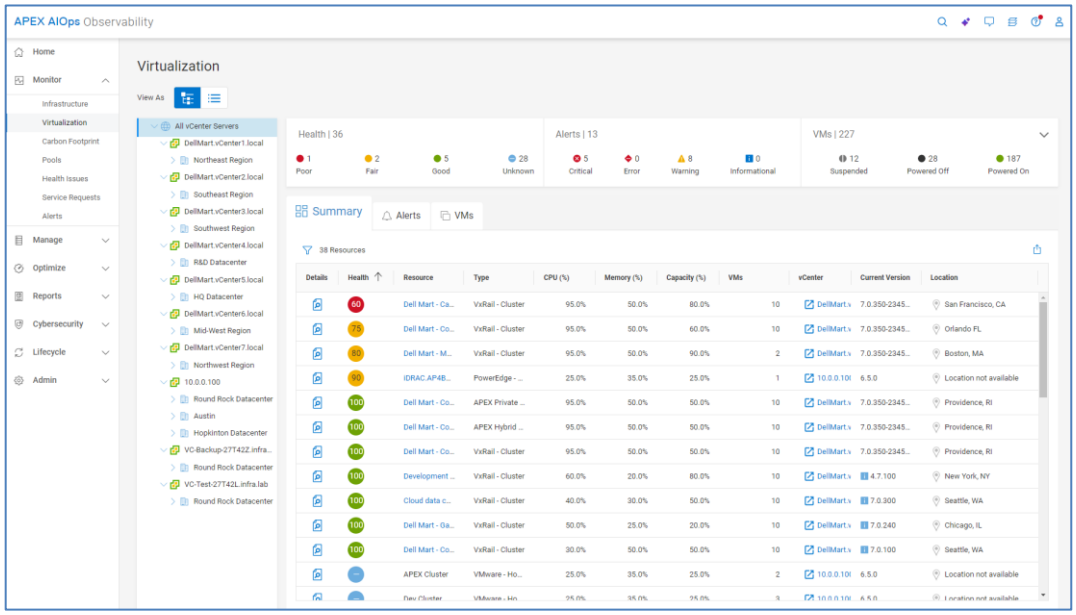
Virtualization

The **Virtualization** view allows users to view VMware related information in a hierarchical navigation model similar to vCenter. It is supported for VxRail clusters and storage-based VMs collected from the Observability Collector.

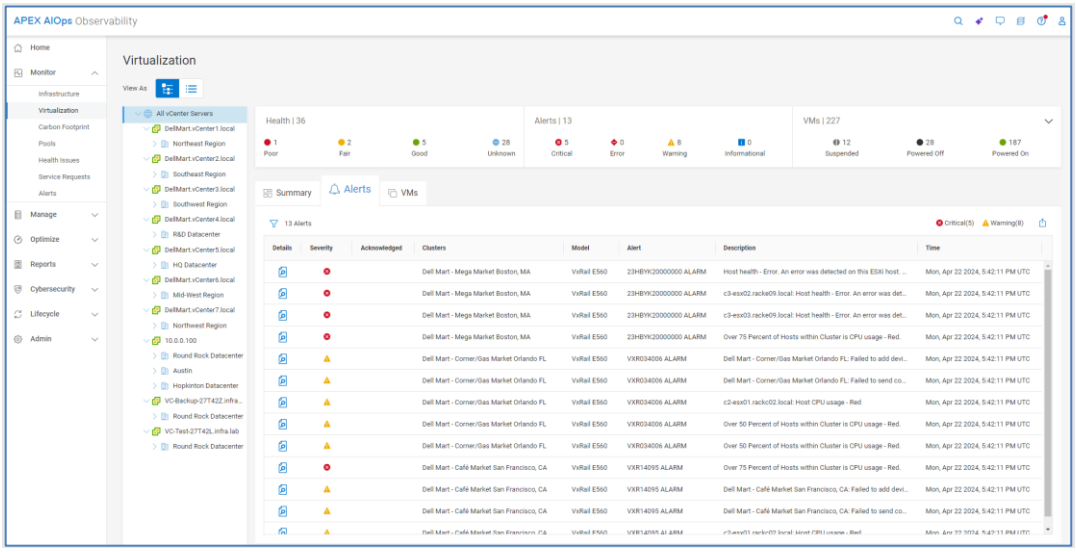
The left side of the screen shows the vCenter servers, the VMware datacenters, and the VxRail clusters or ESXi clusters. The upper right side provides a banner with a summary of clusters in each health category, a summary of alerts by severity, and a summary of

VM status. ESXi clusters show up with a health score of Unknown. The Alerts summary is only applicable to VxRail Clusters. The summary is based on the selected object in the left tree. For example, if the **All vCenter Servers** row is selected, the banner shows all the clusters, alerts, and VMs in the environment. If an individual vCenter is selected, the banner summarizes only those clusters, alerts, and VMs in that vCenter.

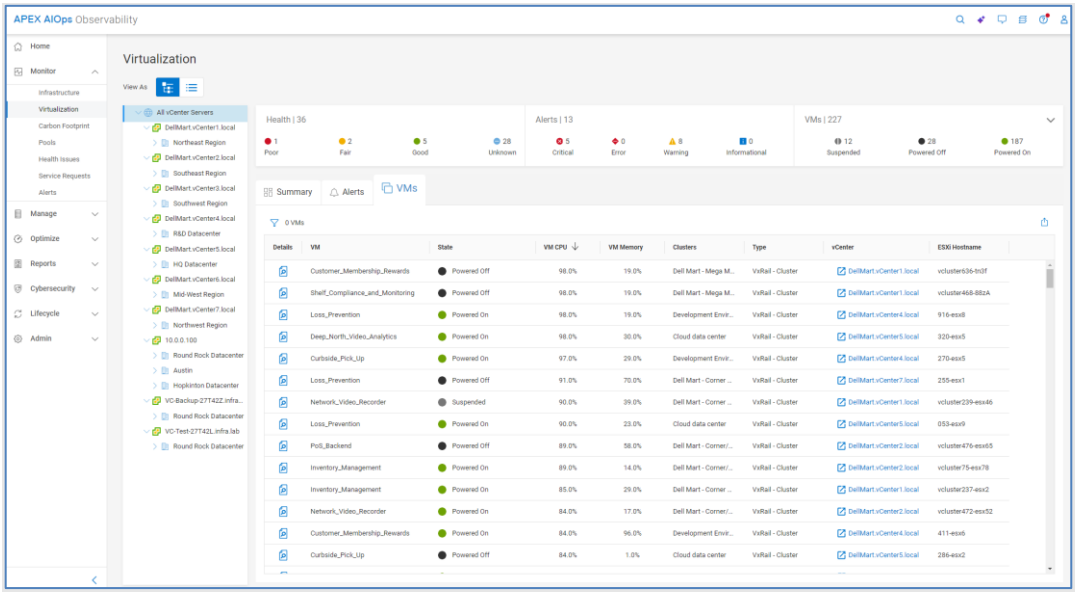
The bottom-right side has three tabs: Summary, Alerts, and VMs. The Summary tab provides the health score (VxRail and PowerEdge), CPU, Memory, Capacity, number of VMs on each cluster, current version, location (VxRail), and a link to launch vCenter. The details icon opens a window with more details for the cluster and health issue details for VxRail clusters.



The Alert tab lists the associated alert information including the description and timestamp. The Details icon opens the alert details window which includes the recommended action.



The VMs tab lists the virtual machines with their state, CPU and Memory metrics, associated cluster, cluster type, vCenter, and ESXi server. The Details icon opens the VM details window which shows more specific capacity, CPU, and Memory metrics. For storage-based VMs, the storage path is provided showing datastore, type, storage object, and storage system.

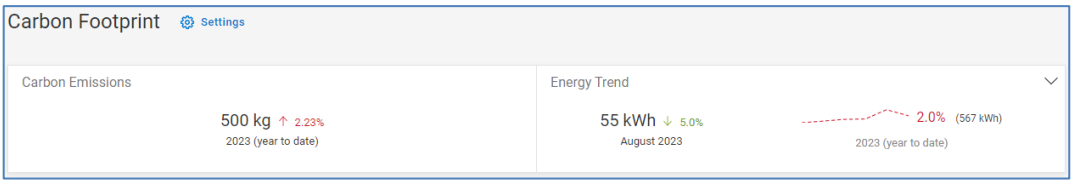


Carbon Footprint

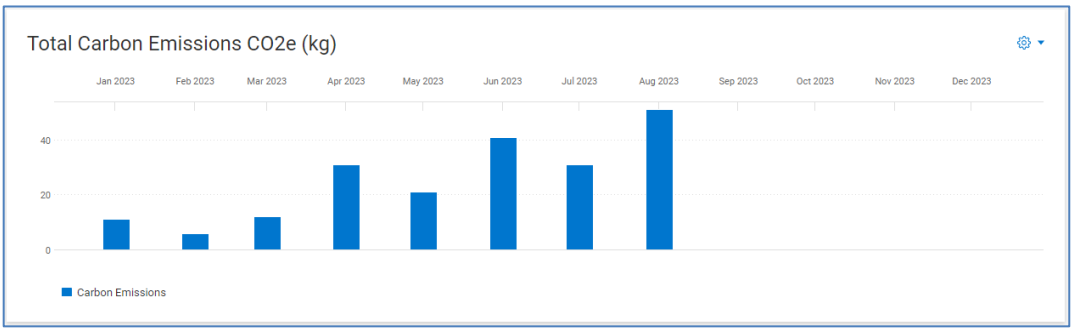
The **Carbon Footprint** page provides summary, system, and workload level metrics for carbon emissions and energy usage. Sustainability has become a key topic in data center infrastructure considerations as companies strive to reach new environmental goals. Infrastructure Observability's carbon emissions feature gives users insights to make the best sustainability decisions for workload consolidation, IT footprint reduction, and energy-efficient technology refresh.

Initial products supported include PowerEdge, PowerScale, VxRail, Connectrix, and Unity XT. The top banner provides totals of carbon emissions and energy usage for all systems. Carbon emissions calculations are based on location-specific emission factors provided

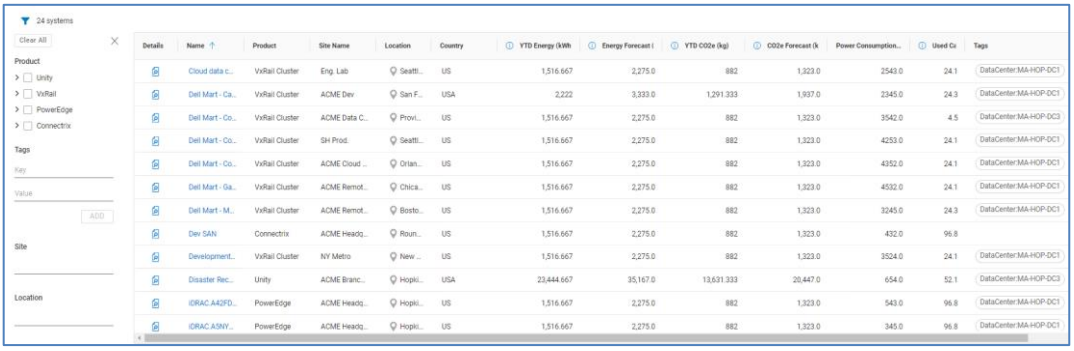
by the International Energy Agency (IEA) and industry average Power Utilization Effectiveness (PUE) values. Users with the Admin role can override these default values by clicking the Settings button.



The Total Carbon Emissions chart provides a one-year trend of total carbon emissions based on monthly values. The chart can be displayed as a bar chart or a line chart.

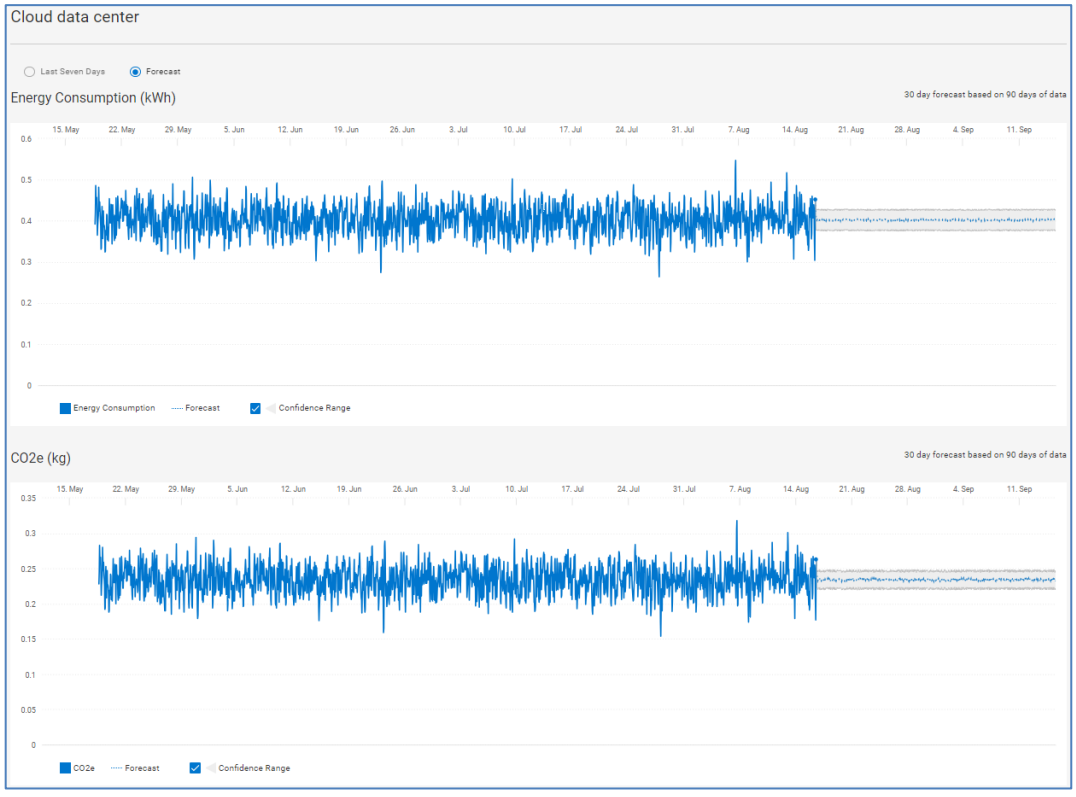


The bottom of the page is a table listing each system, location, YTD energy usage, energy forecast, YTD carbon emissions usage, carbon emissions forecast, and daily power consumption. The system used capacity percentage indicates which systems have available capacity for additional workloads. The filter lets users display systems based on product type, custom tags, site, and location.



Clicking the details icon for a system displays seven-day charts for energy consumption and carbon emissions. The actual value is shown along with the historic seasonality (the expected range) that highlights any anomalies or changes in patterns.

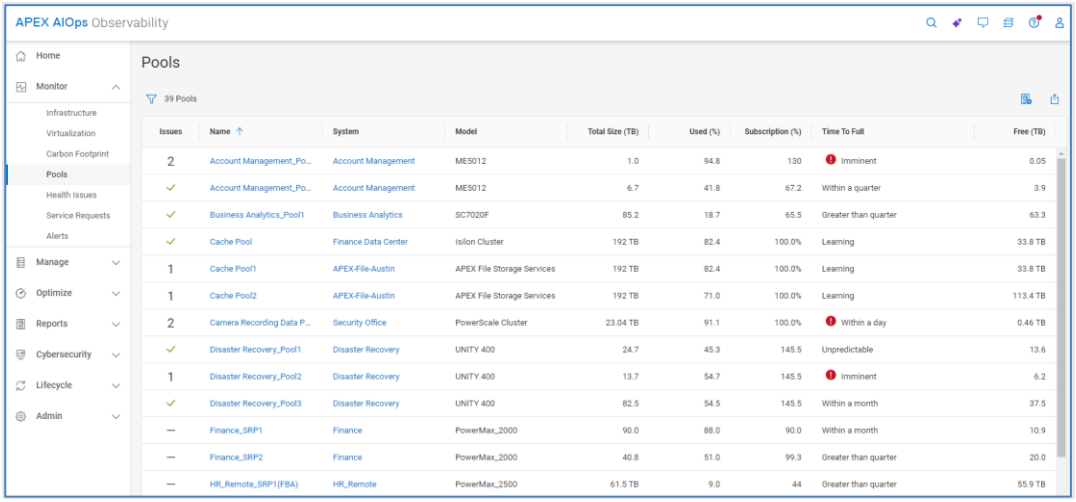
Clicking the Forecast button shows trend and forecast data for each of these charts.



Pools

The **Pools** page provides an aggregated listing of storage pools including PowerMax storage resource pools. The Issues column displays the number of health issues associated with any pool or storage object in that pool or a green check mark for items with no associated issues. Issues can be calculated for Unity XT family, SC Series, PowerScale/Isilon, PowerVault, and PowerFlex. The pool name and system name are hyperlinks to the details for the item.

The Pools listing represents the raw storage on the system that is available to be provisioned as either block storage or file storage. This listing provides the Total Size (TB), Used and Subscription percentages, and Free (TB) storage within the pool that has not been provisioned for storage objects. The Time to Full range is also shown. Time to Full is based on the storage consumption measurements. The longer the pool is configured, the more accurate the prediction of Time to Full. This Time to Full measurement identifies pools that are at greatest risk of running out of storage space, and that require attention.



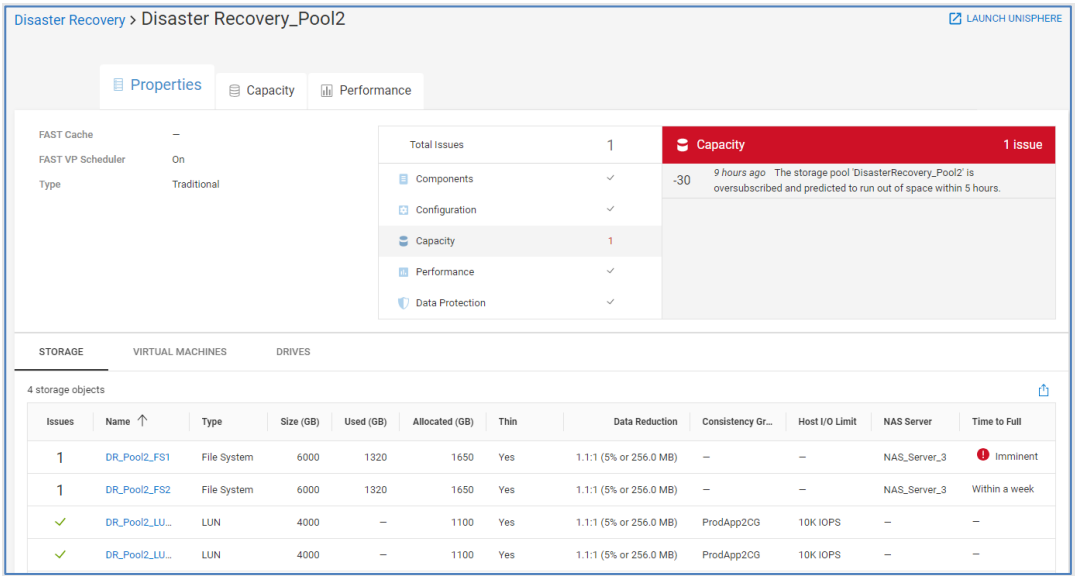
Pool details – Properties

The information in the **Properties** tab for a pool varies depending on the array type. It provides various pool attributes and any health issues associated with the pool. Expanding the issue will provide a suggested resolution. Where supported, there is a hyperlink in the upper right of the window to launch the associated element manager. The bottom of the Pool details page has different tabs of information depending on array type.

The following series of screenshots show the information for each array type.

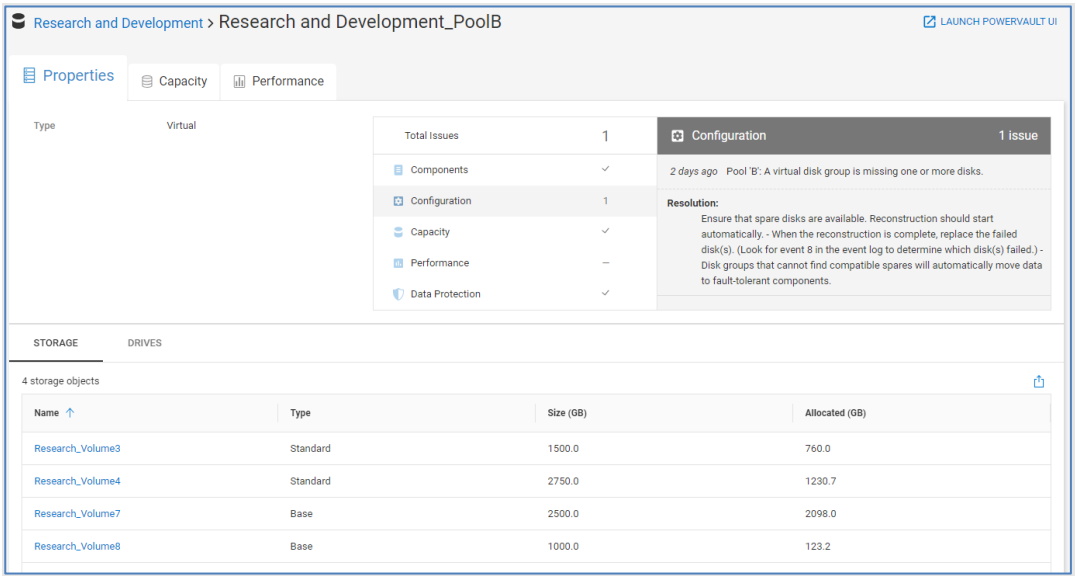
Unity XT family and SC Series:

- Storage
- Virtual Machines
- Drives



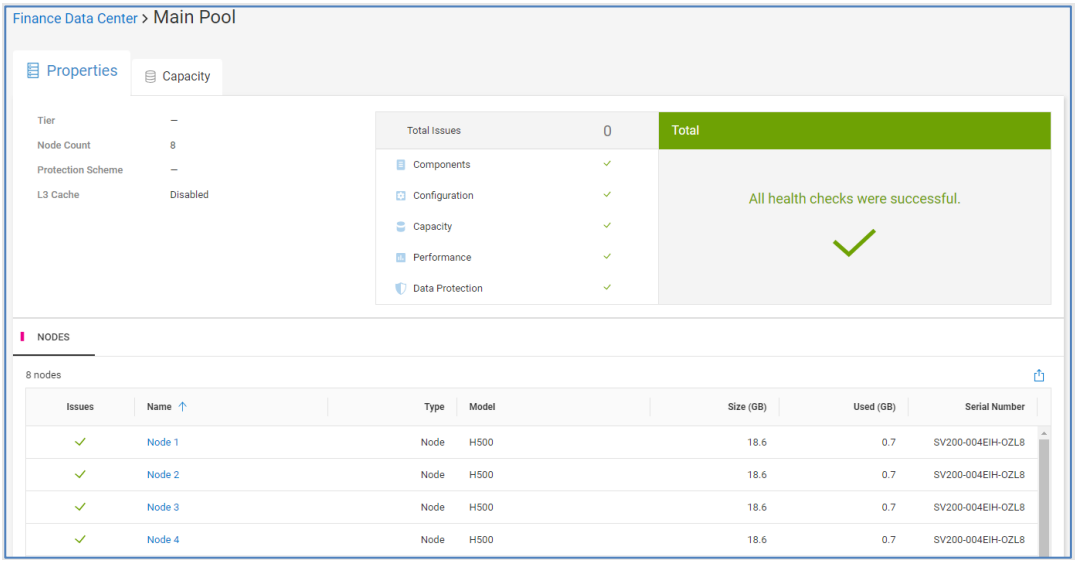
PowerVault:

- Storage
- Drives



PowerScale and Isilon:

- Nodes

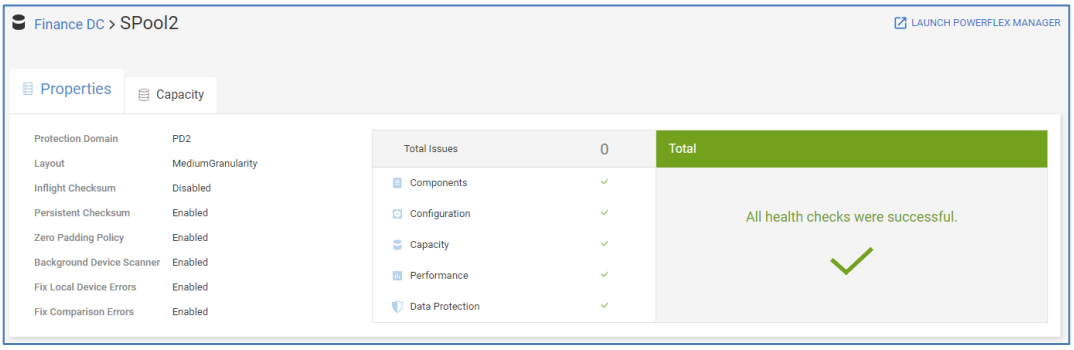


PowerMax:

- No tabs

PowerFlex

- No tabs



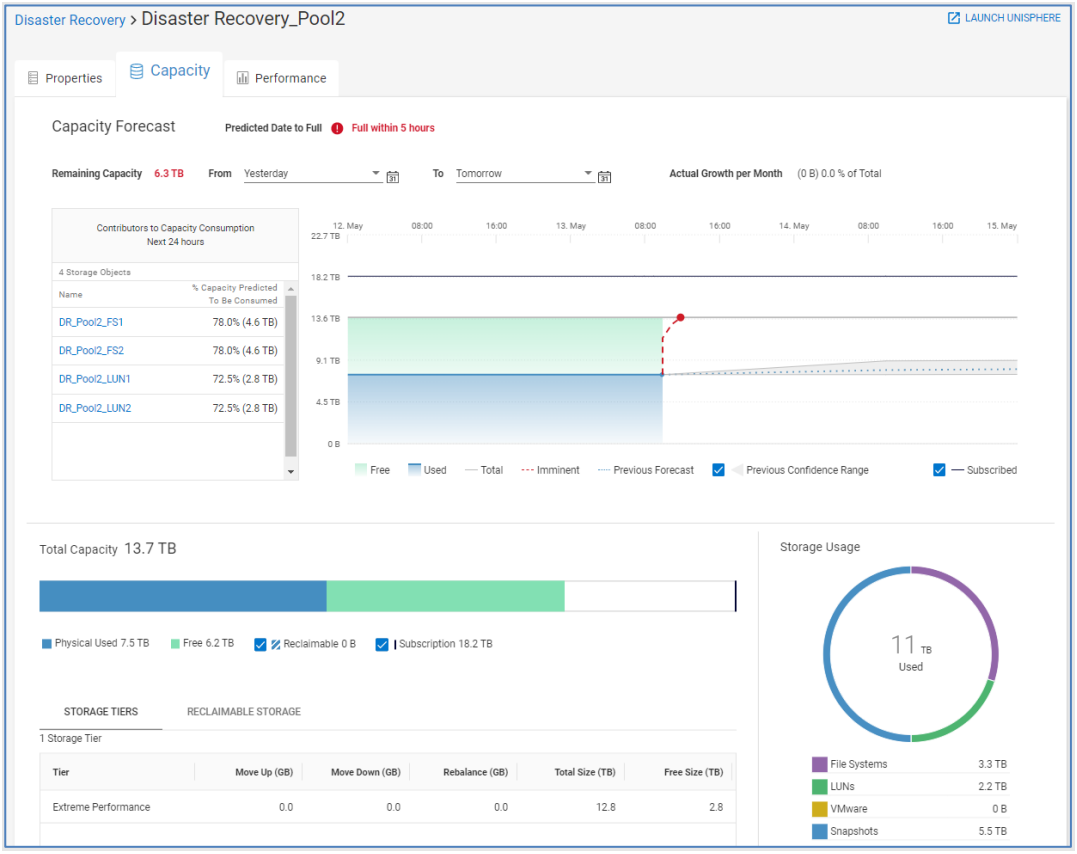
Pool details – Capacity

The **Capacity** tab for a pool varies based on array type.

Unity XT family, PowerScale, Isilon, PowerVault

The graph along the top displays the historical pool capacity data and the Predicted Date to Full date (Unity XT family, PowerVault, PowerScale/Isilon, and PowerFlex). The graph shows Free, Used, Total, Forecast Used, Confidence Range, and Subscribed. The Confidence Range represents the confidence level in predicting the date to full; the wider the range, the lower the confidence level. When an imminent full condition exists, the graph also shows the Previous Forecast and Previous Confidence Range. It also shows the top storage objects predicted to contribute to capacity consumption over the next 24

hours as shown below. If the pool is in a Learning, Full, or Unpredictable state, only the historical trend graph is displayed.



The beginning of the chart is based on the selection in the “From:” field. By default, the setting is set to “3 months ago.” For pools at imminent risk, the “From:” field is set to yesterday. The following times are available from the pull-down:

- Yesterday
- 1 week ago
- 1 month ago
- 3 months ago (default)
- 6 months ago
- 1 year ago
- 2 years ago
- Custom

The end of the chart is based on the selection in the “To:” field. By default, the setting is set to “Predicted Full.” The following times are available in the pull-down:

- Today (Only historical data is shown)
- Tomorrow
- 1 week from today

- 1 month from today
- 3 months from today
- 6 months from today
- Predicted Full (default)
- Custom

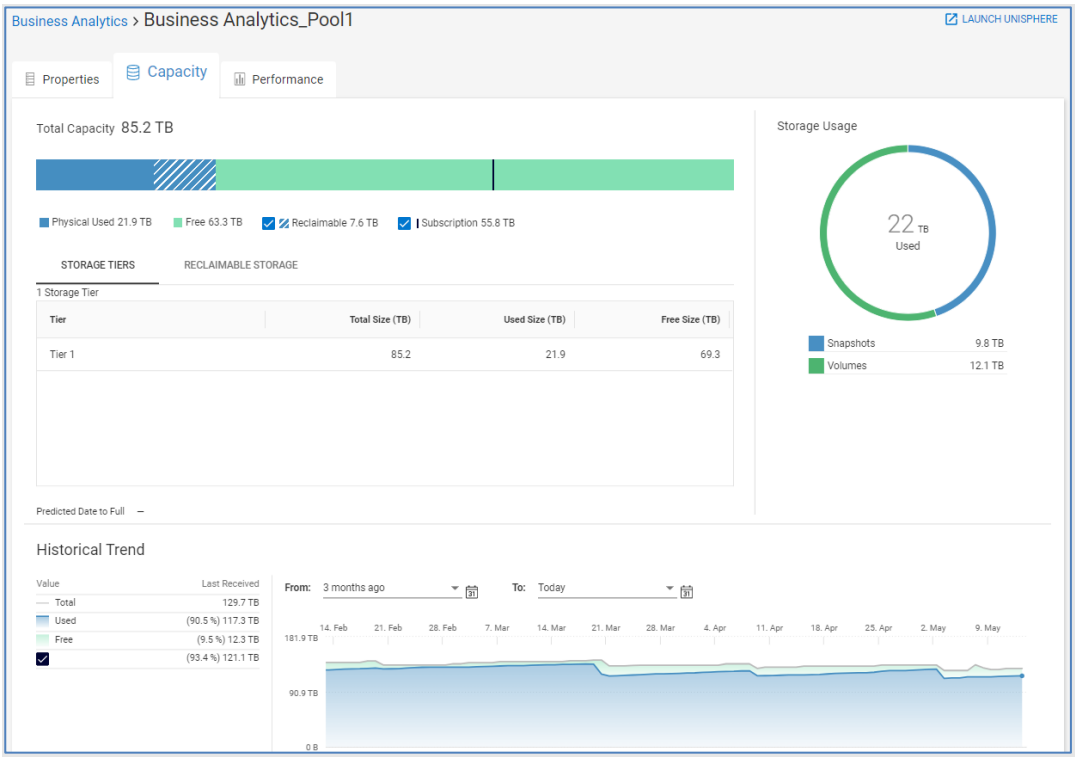
The **Subscribed** checkbox enables the user to view or hide the pool subscription data on the graph.

The **Confidence Range** checkbox enables the user to view or hide the upper and lower confidence range forecasts.

The bottom of the Pools Capacity tab provides details for the pool capacity, showing Used, Free, Reclaimable, and Subscribed. The Storage Usage ring shows how the used storage is configured.

SC Series

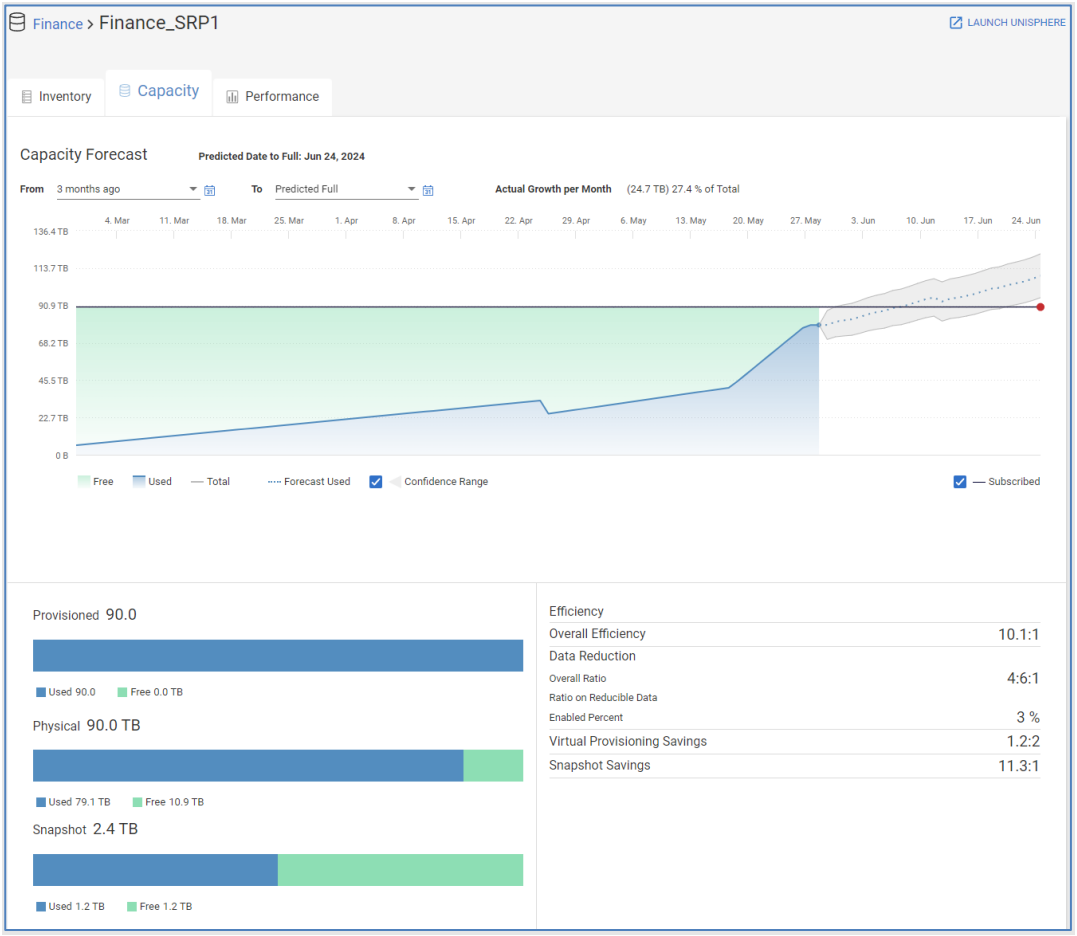
For SC Series, the historical trend of Total, Used, Free, and Subscribed storage is provided along with a Predicted Date to Full. However, the chart does not display forecasting data.



PowerMax 2000, 8000, and VMAX3

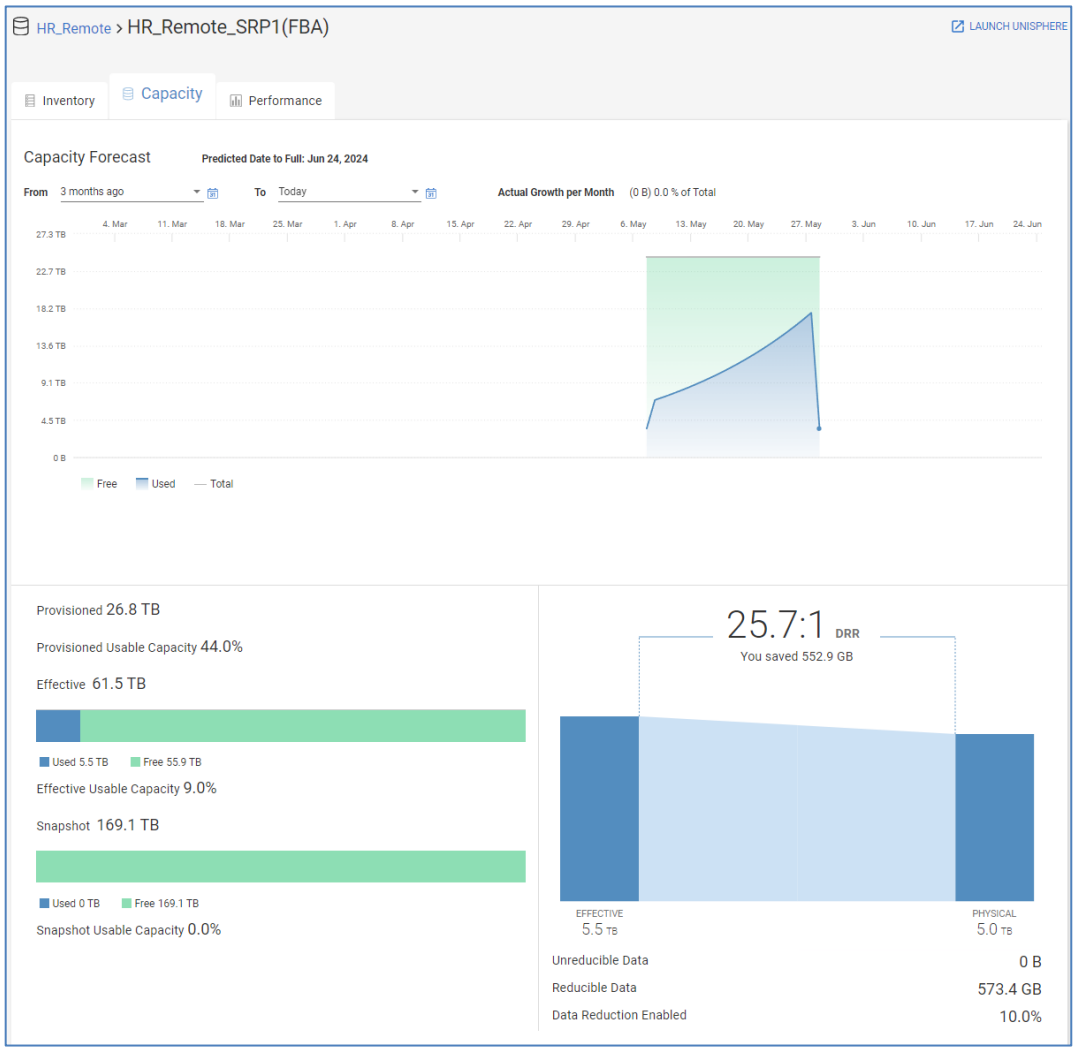
For PowerMax 2000, 8000, and VMAX3 arrays, the Capacity tab displays a capacity forecast chart for storage resource pools. The bottom half of the page shows Used and Free storage in bar charts for Subscribed, Snapshot, and Usable space. It also displays the Overall Efficiency ratio. This ratio is calculated as the sum of all TDEVs plus snapshot sizes (based on 128 K track size) divided by the physical used storage (based on the

compressed track size). Data Reduction ratio and enabled percentage, Virtual Provisioning savings, and Snapshot savings are also displayed.



PowerMax 2500 and 8500

For PowerMax 2500 and 8500 systems, the effective capacity is reported as it provides a more realistic measure of available space considering all data reduction components.

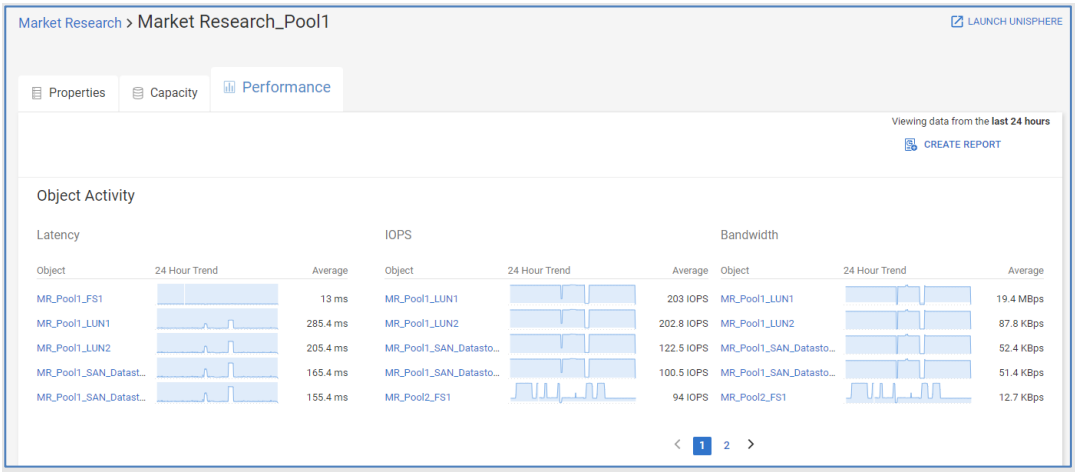


Pool details – Performance

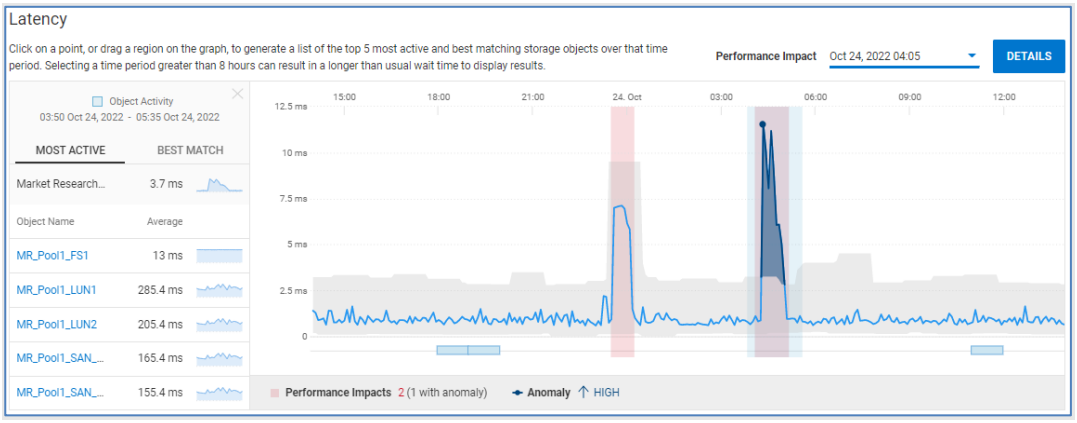
The **Performance** tab for pools is available for Unity XT family, SC Series, PowerMax/VMAX, and PowerVault systems. The information under the Performance tab differs slightly for each supported array type.

Unity XT

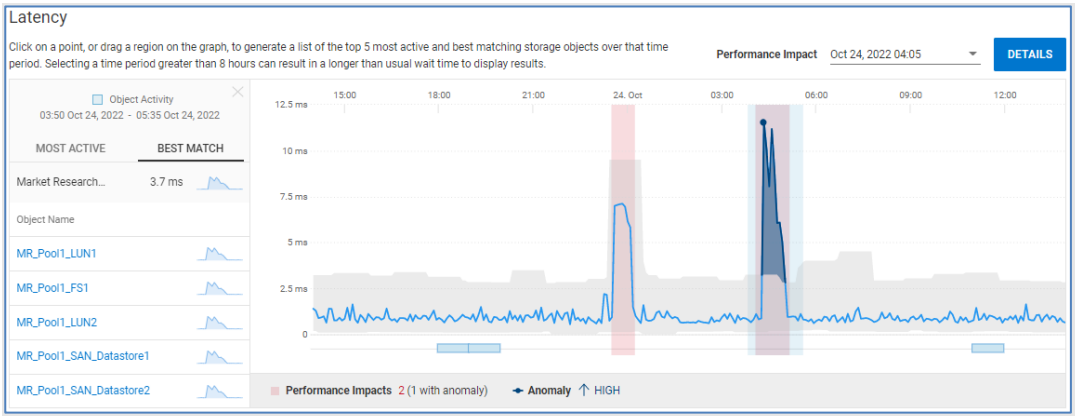
For Unity XT pools, the top of the page displays 24-hour trend lines and a 24-hour average for Latency, IOPS, and Bandwidth for both block objects and file systems. Observability presents the top five objects associated to the pool. The user can scroll to see additional objects.



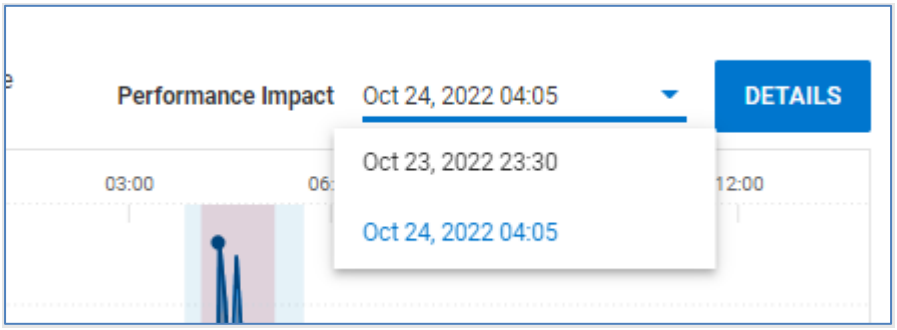
Scrolling down this view provides the user with detailed performance graphs for Latency, IOPS, Bandwidth, and Backend IOPS (one chart per tier). Observability identifies and highlights not only performance anomalies on the Latency chart, but also performance impacts. Performance anomalies are highlighted in dark blue while performance impacts are highlighted in pink. Highlighting an area on the Latency, IOPS or Bandwidth performance graphs identifies up to the top five most active objects contributing to that metric over the highlighted period.



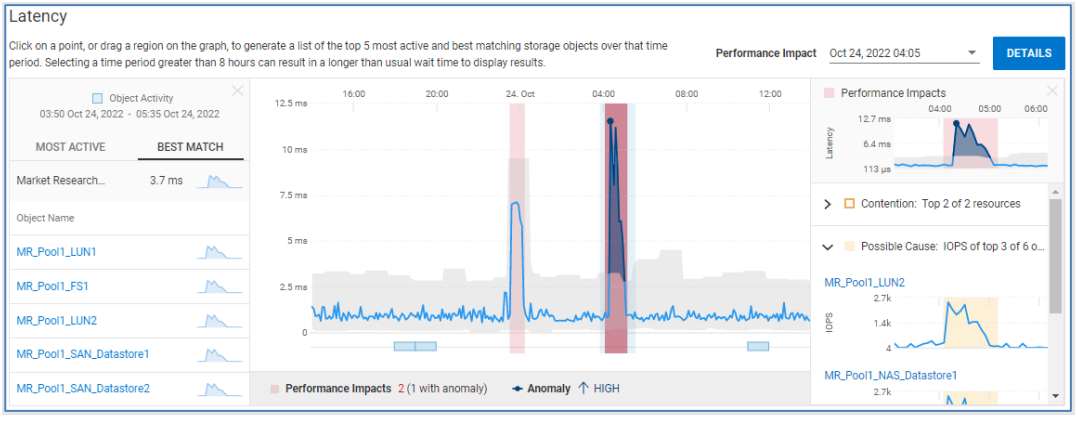
When the user selects Best Match on the left side of the chart, Observability identifies up to five objects that have the highest correlation to the selected period. Best Match is available on the Block Latency, IOPS, and Bandwidth performance charts.



When there are performance impacts detected by Observability, the user can view details of them by selecting the Details button in the upper right of the chart. If there are multiple performance impacts displayed on the chart, the user can select which impact to investigate by selecting the drop-down menu next to the date.

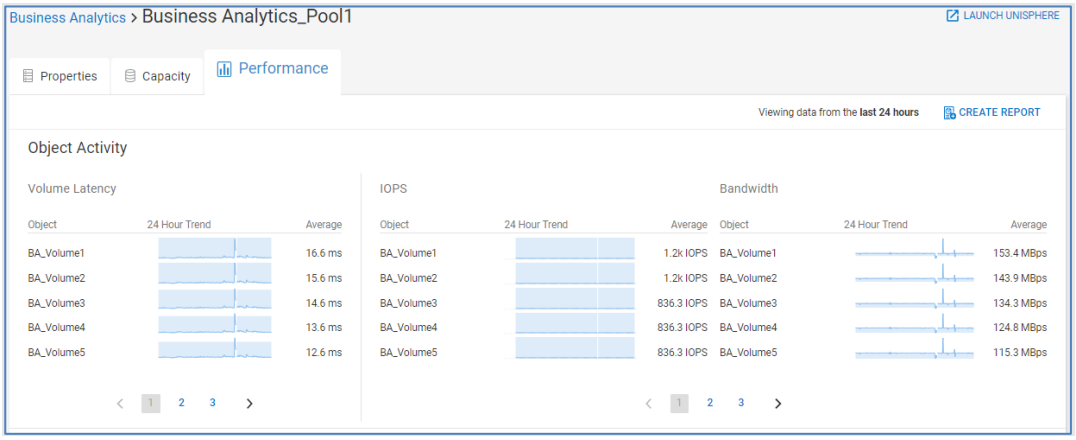


The following shows the results of the details of a performance impact. The right side of the chart shows the time of the selected performance impact and identifies the most likely causes (competing workloads) for the impact and if there is any resource contention for SPs, Cache, Disk, or Ports.

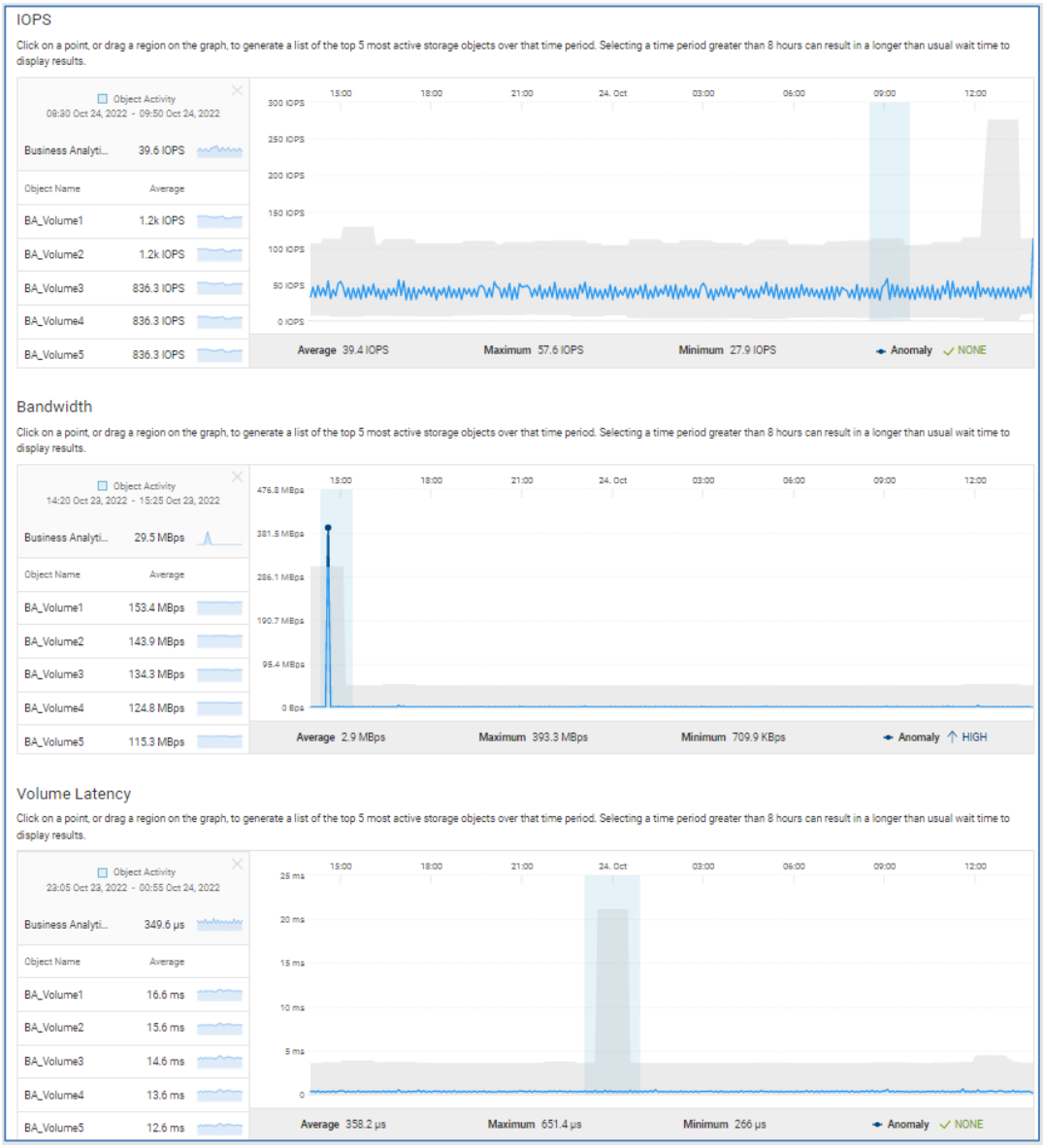


SC Series

Similar to the Unity XT family, the top half of the Performance tab for SC Series pools displays 24-hour trend lines and a 24-hour average for Latency, IOPS, and Bandwidth.

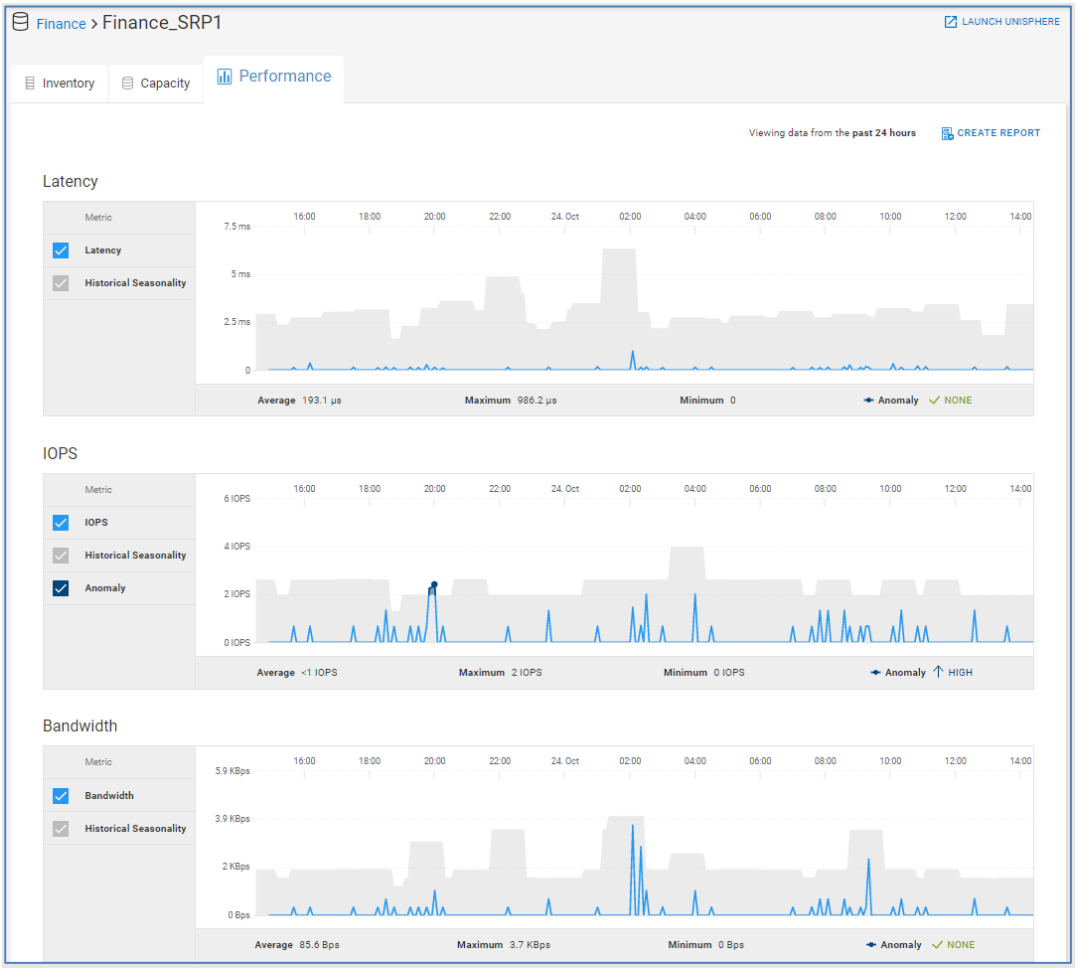


Scrolling down provides displays 24-hour performance graphs for IOPS, Bandwidth, and Volume Latency. Observability identifies and highlights performance anomalies on each performance chart for SC Series pools. Highlighting an area in any of these graphs identifies the top volumes contributing to that metric during the highlighted period.



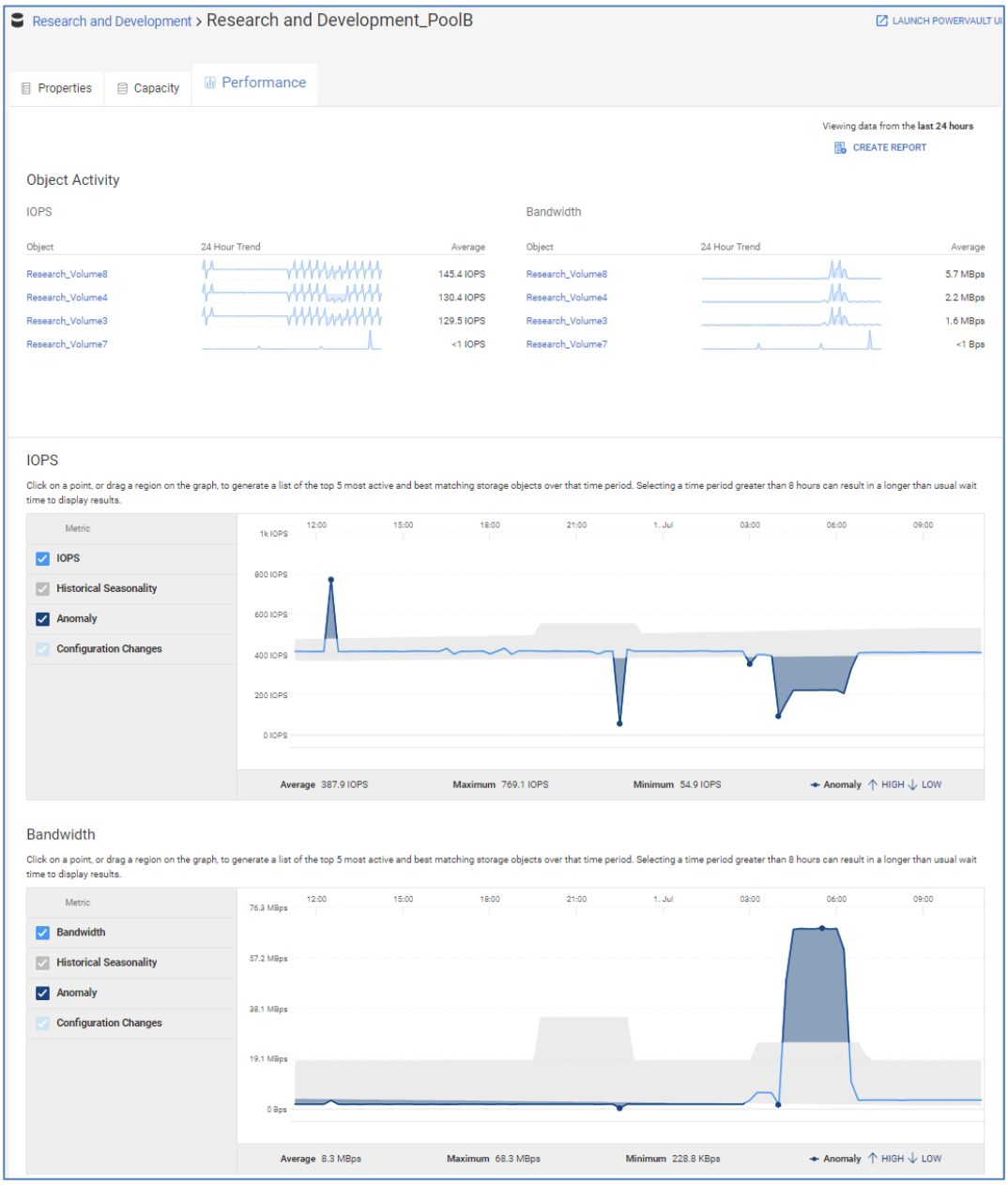
PowerMax

The Performance tab for PowerMax Storage Resource Pools provides 24-hour charts for Latency, IOPS, Bandwidth, %Read, IO Size, and Queue Length. Observability highlights performance anomalies for each chart in the SRP Performance tab. The pool performance charts for PowerMax are not selectable.



PowerVault

The Performance tab for PowerVault pools also displays top object activity on the top half of the page and 24-hour charts at the bottom of the page. Metrics displayed include IOPS and Bandwidth. Selecting an area in the IOPS and Bandwidth charts displays the top volumes contributing to that metric during that time period under the Most Active tab. The Best Match tab shows up to five objects with the highest correlation to the selected period.



Note: The Performance tab is not yet supported for PowerScale/Isilon or PowerFlex pools.

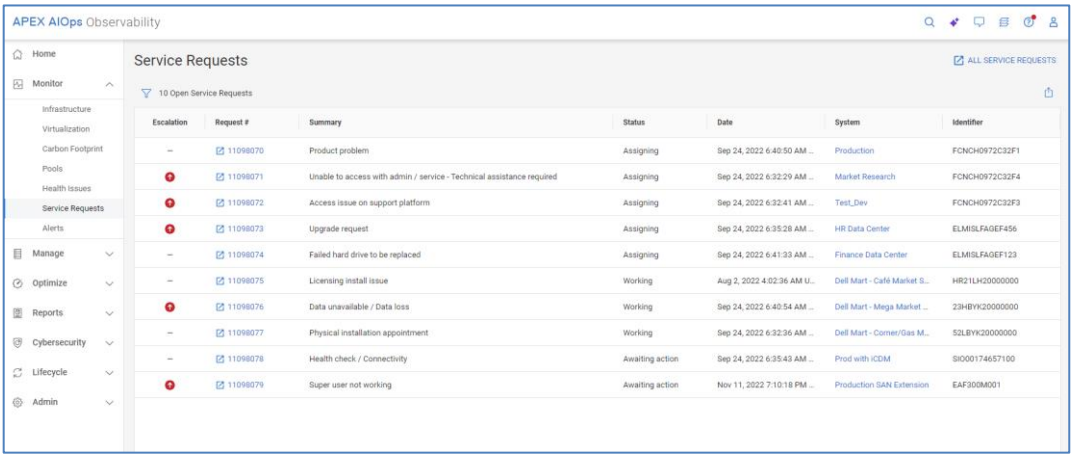
Health Issues

The Health Issues page displays a comprehensive view of all current health issues across the environment grouped by system. Issues can be grouped by system or not grouped. When grouped by system is selected, expanding the system shows all health issues on the system. The Details icon opens a details window that includes the recommended remediation.

The user can click the Filter icon to show a subset of systems based on the system name, product type, site, and location. When the user starts typing the name of the system, a prepopulated list of system names is displayed that contains the entered text.

Service Requests

The **Service Requests** page lists all service requests open against systems monitored by Infrastructure Observability. The table identifies escalated service requests, service request number, status, creation date, and affected system. Clicking the hyperlink in the **Request #** column directs the user to the service request on the Dell support page.



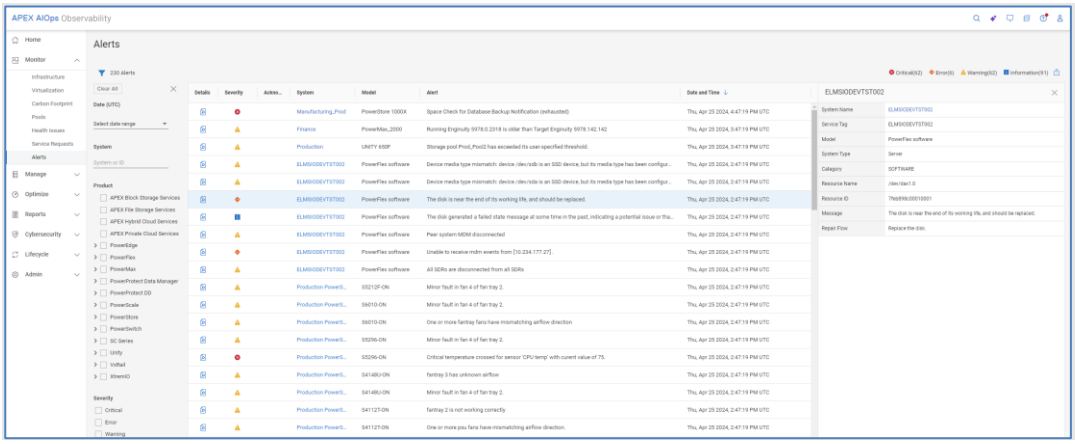
Alerts

The **Alerts** page displays all alerts associated with the monitored systems. The Filter icon allows the user to filter alerts based on the following criteria:

- **Date** – Date range
- **System** – System Name or ID
- **Product** – Product type
  - APEX Cloud Platform
  - APEX Hybrid Cloud Services
  - APEX Private Cloud Services
  - PowerEdge
  - PowerFlex
  - PowerMax
  - PowerProtect Data Manager
  - PowerProtect DD
  - PowerScale
  - PowerStore
  - PowerSwitch
  - SC Series
  - Unity XT family
  - VxRail
  - XtremIO

- **Severity**
  - Critical – Event that has significant impact on the system and needs to be remedied immediately
  - Error – Event that has a minor impact on the system and needs to be remedied
  - Warning – Event that administrators should be aware of but has no significant impact on the system
  - Information – Event that does not impact the system functions
- **Acknowledged**
  - Acknowledged – Event that has been reviewed and acknowledged on the system
  - Unacknowledged – Event that has not been acknowledged on the system

Selecting the Details icon opens a window on the right side of the page with additional alert details.



Note:

- Alerts shown in Infrastructure Observability originate from the system and can only be acknowledged, unacknowledged, and cleared on the system.
- Alerts for PowerVault, Connectrix, and VxBlock systems are not yet supported.

Manage

System Updates

The **System Updates** page has up to five tabs: Storage, Networking, HCI, Data Protection, and Server.

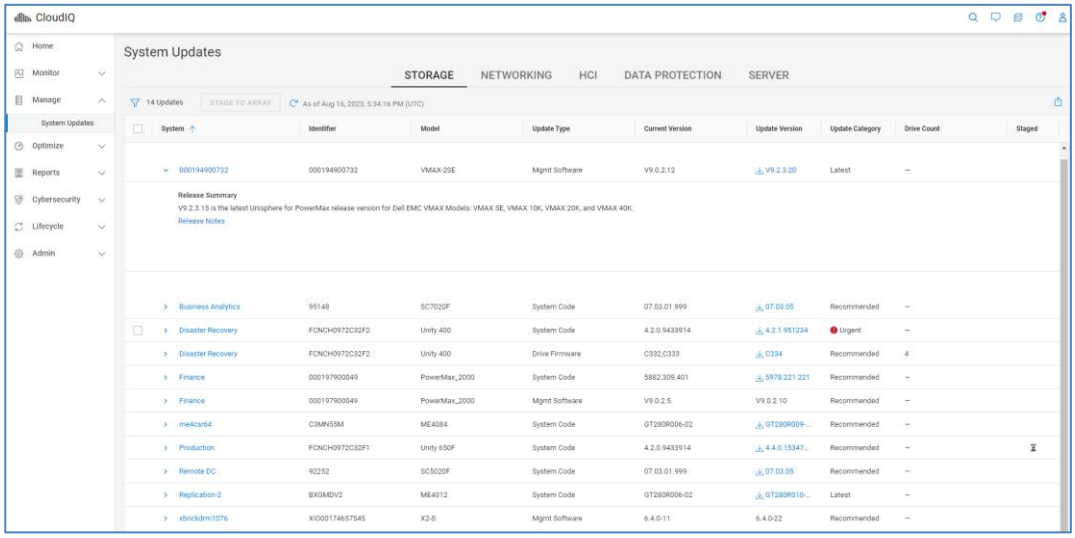
Storage

The **Storage** tab displays a list of all available system code, management software, and drive firmware updates across all supported systems. It includes the system name, update category, update type, the current version, and recommended version. The Recommended Update column is a hyperlink to the code allowing the user to quickly access the update code. Selecting the “>” icon expands the row to display the Release

Summary with more details about the update and a link to the release notes for the system update.

This page also allows users to stage Unity XT code updates to the array. By selecting the Unity XT family arrays and the Stage to Array button, the code in the Recommended Update column is downloaded to the arrays. The user can log in to Unisphere and initiate the code upgrade at an appropriate time.

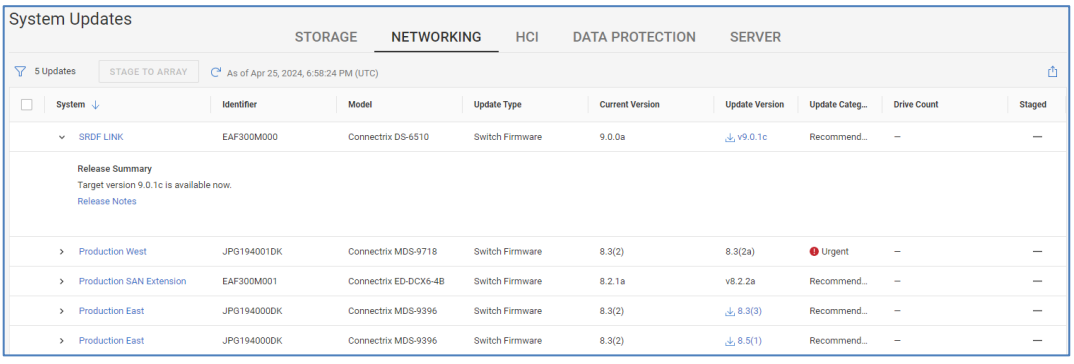
The user can filter the results by selecting the Filter icon, sort any of the columns and export the list to a CSV file.



Note: The System Updates listing in Infrastructure Observability does not support PowerScale/Isilon, PowerFlex, and PowerSwitch.

Networking

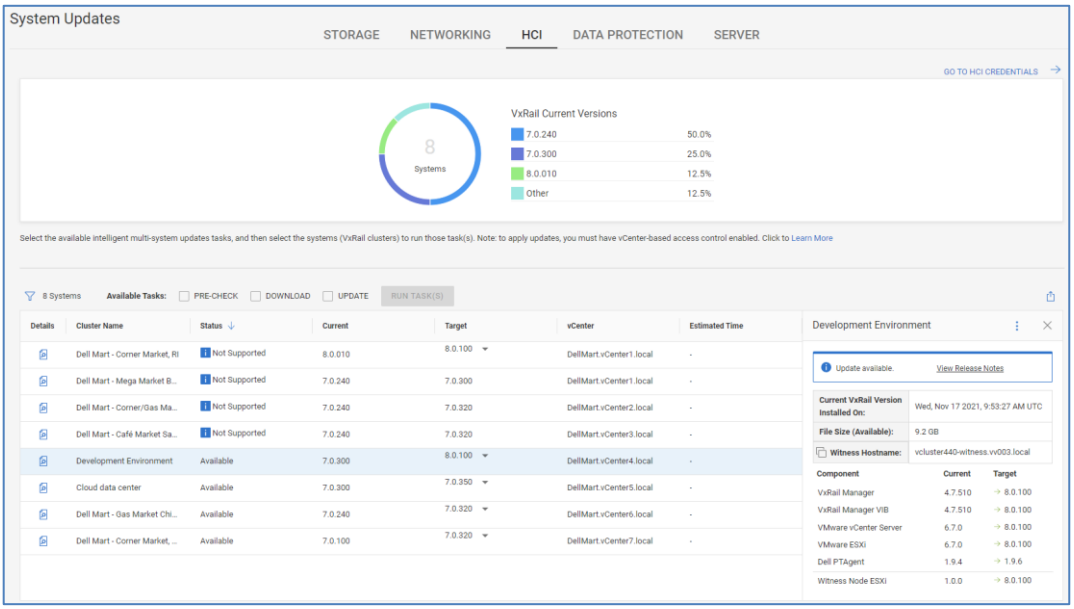
The **Networking** tab provides a list of recommended switch firmware updates for Connectrix switches.



HCI

The **HCI** tab allows users to initiate multisystem updates from Infrastructure Observability. Users can run pre-check, code download, and system update tasks on their VxRail clusters. The top of the page provides a chart with the VxRail software distribution for all

monitored VxRail clusters. The bottom of the page lists each cluster along with various information such as current version, target version, and vCenter hostname. Observability intelligently provides a list of all possible target versions based on the current cluster version. Selecting the details icon provides additional information about the current installation timestamp, the update file size, and the component current and target versions.



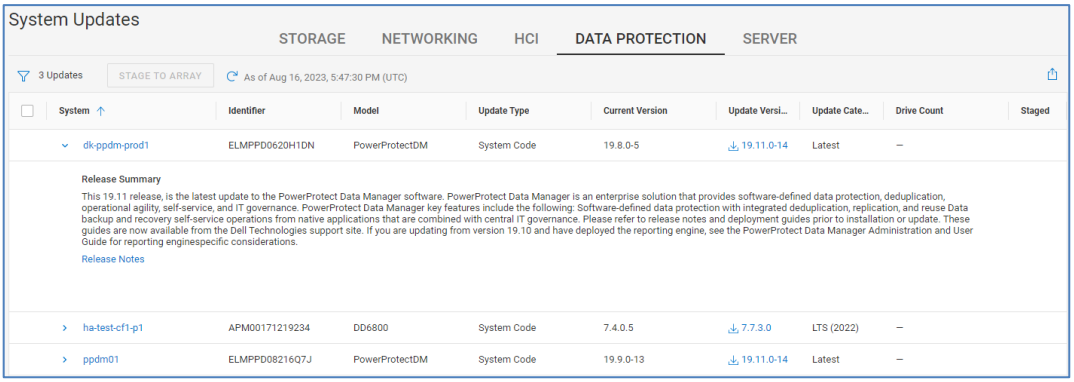
When preparing for a cluster update, users can run the Pre-check task. The Pre-check task determines the cluster's readiness for a system update and includes the checks found in VxVerify. The Pre-check task produces a pass/fail status with a job report that lists the details of each check. If a check fails, the job report provides a link to a knowledge base article that users can review to help remediate the issue before proceeding with a code download and system update. This is covered in more detail in the Infrastructure Observability administration section of this paper.

The Download task downloads and stages the update bundle onto the VxRail Manager VM of the cluster. This operation performs a change analysis between the existing software version running on the cluster and the selected target version. It then identifies and bundles only the necessary component files needed for the system update. This intelligent bundling can significantly reduce file transfer size and download times for all clusters, and particularly for those clusters at remote sites with limited bandwidth.

Once the Pre-check and Download tasks are successful, users can confidently run the Update task. Users can select a combination of tasks at once. For example, instead of running each task individually, they could select both the Pre-check and Download tasks and then come back and initiate the Update task. They could also select all three tasks. If a task failure occurs, the remaining tasks will not run.

Data Protection

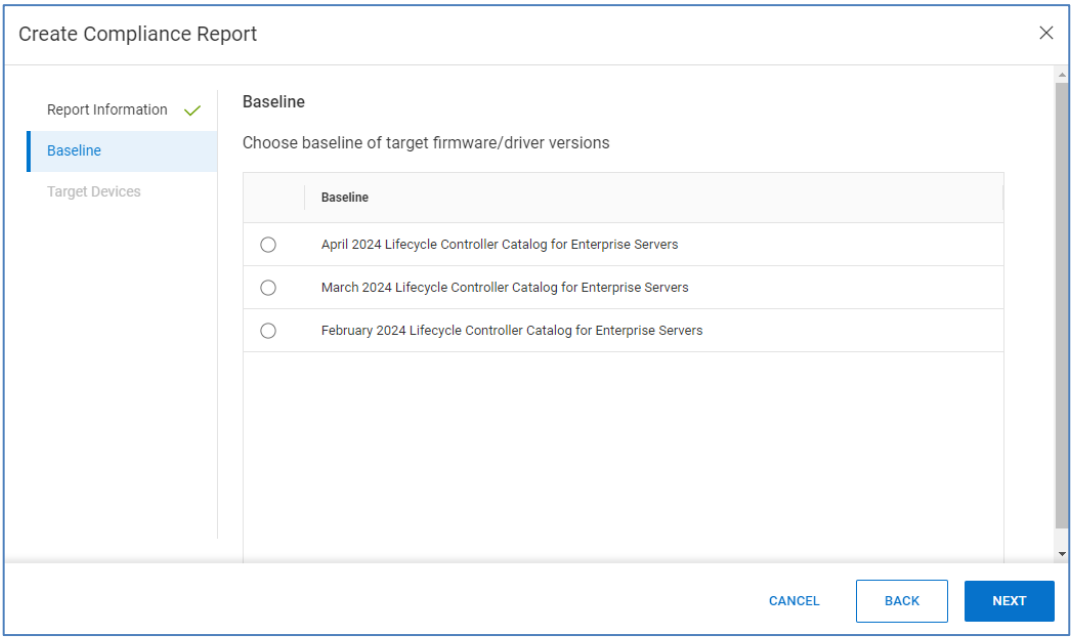
The **Data Protection** tab lists recommended updates for PowerProtect DM instances and PowerProtect DD series appliances.



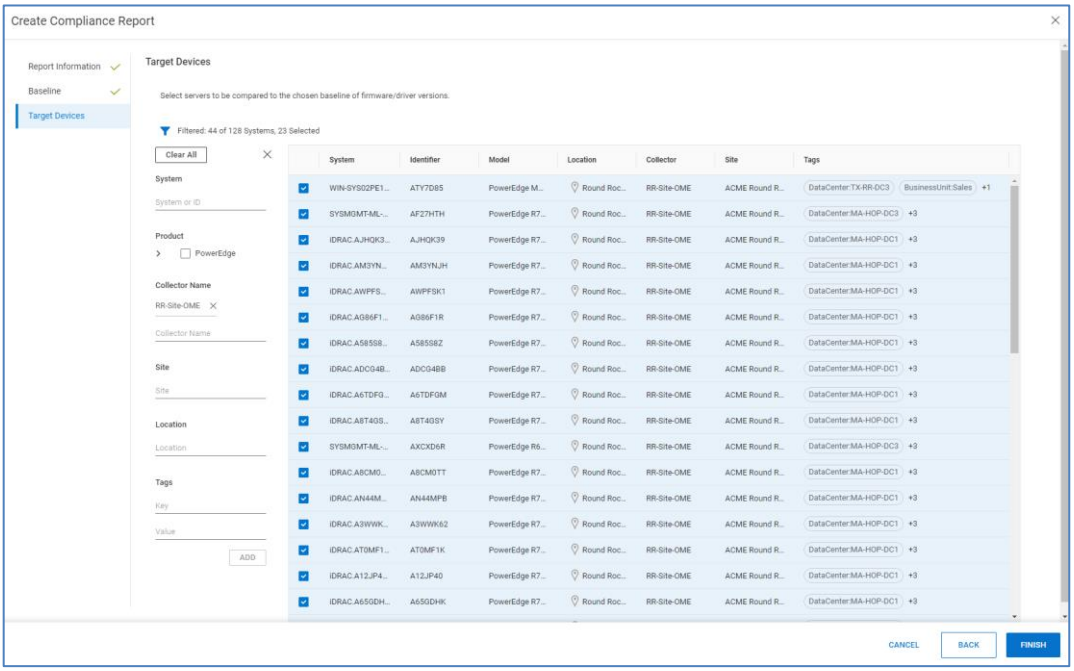
Server

The **Server** tab lets users initiate BIOS and firmware updates for their PowerEdge servers and chassis. OpenManage Enterprise v3.10 or later with CloudIQ Plugin v1.2 or later are required and the Remote Management option must be enabled in the CloudIQ Plugin in OpenManage Enterprise. Also, users must have the Server Admin role in Observability to initiate updates. See Identity Management for more information about Observability roles.

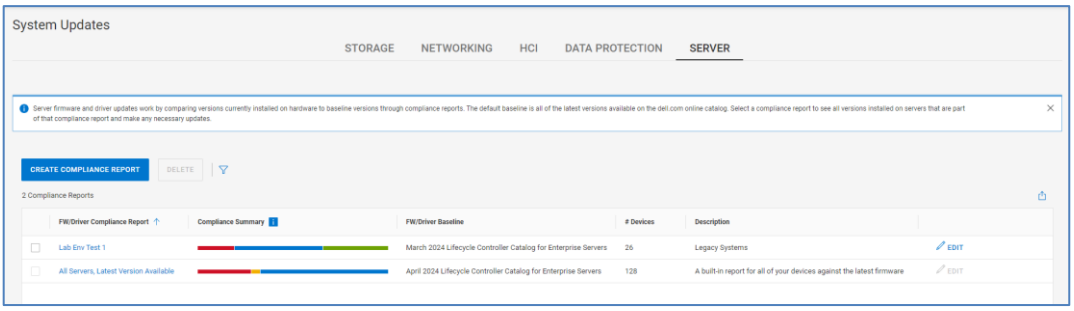
The user first creates a compliance report choosing a baseline of target firmware and driver versions based on the latest or recent Lifecycle Controller Catalogs for Enterprise Servers. By default, a compliance report is created for all servers against the latest available versions exists and cannot be edited or deleted.



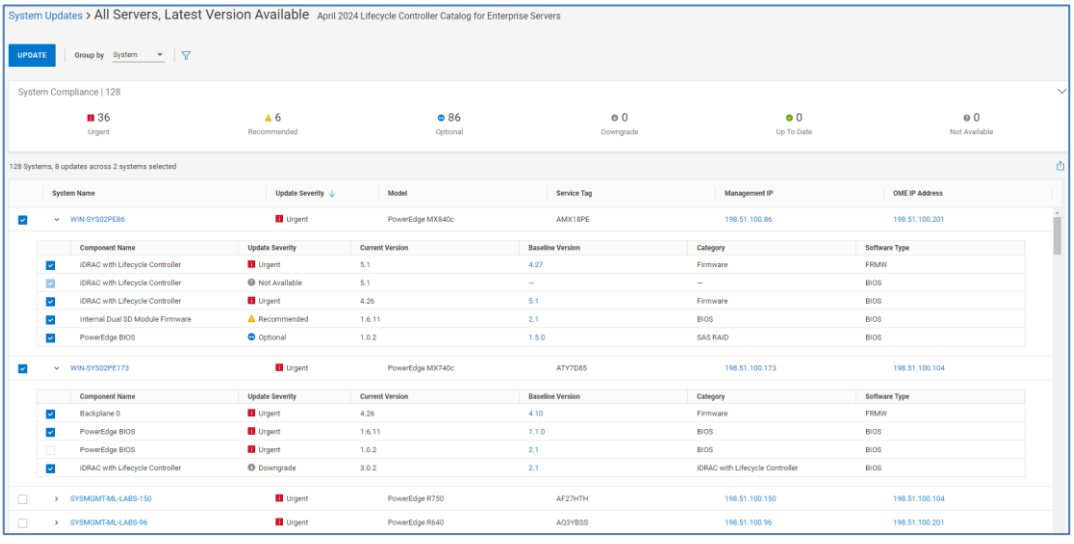
After selecting the baseline, the user chooses a set of target devices. To simplify the selection process, a filter is available to choose target devices based on System name, Product, OpenManage Enterprise Collector, Site, Location, and Custom Tags.



Once the compliance report is created, the user can see a bar chart showing a summary of urgent, recommended, optional, and up to date upgrades.

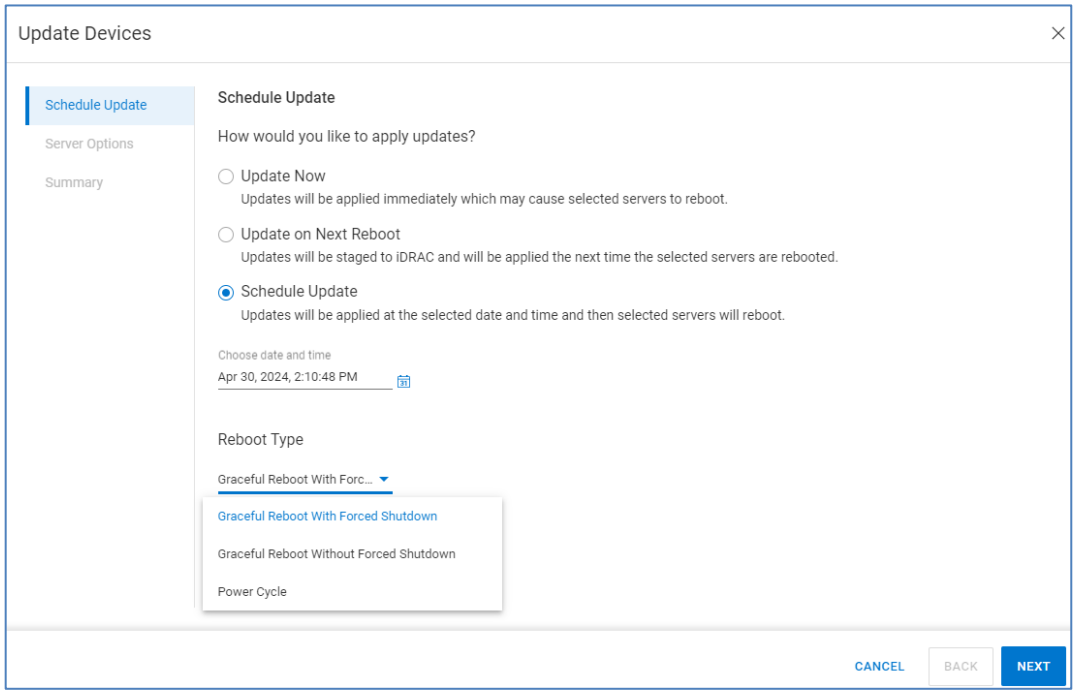


Clicking the name opens the compliance report. The Group by pull-down menu lets the user group the updates by System or by none. When they are not grouped, they are ordered by severity and then service tag. After the user selects which updates they want to perform, the Update button becomes selectable.



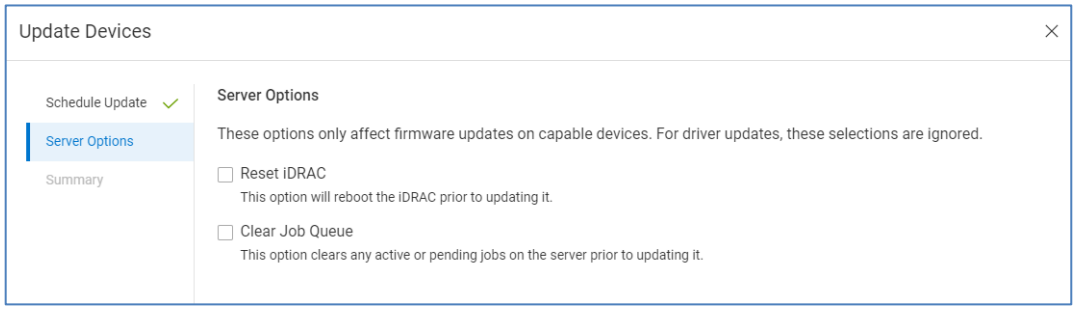
When the user clicks the **Update** button, they select various options. Under the **Schedule Update** section, users can choose to apply the updates now, on the next reboot, or schedule them. If they choose to apply the update now or schedule them, they then choose the reboot type:

- Graceful reboot with forced shutdown
- Graceful reboot without forced shutdown
- Power cycle



Under the **Server Options** section, the user chooses each of the following for firmware updates. The selections are ignored for driver updates.

- Reset iDRAC
- Clear job queue



The Summary page provides a summary of the devices and components being updated. Clicking Finish sends the update request to the appropriate OpenManage Enterprise server. Users can monitor the update on the Jobs page.

Optimize

Reclaimable Storage

The **Reclaimable Storage** page shows block and file objects that may no longer be in use. Reclaimable storage is supported for PowerStore, PowerMax or VMAX, PowerVault, the Unity XT family, and SC Series systems. It shows the total number of storage objects and the total amount of potentially reclaimable space across all systems. The following rules are used to identify potentially reclaimable storage:

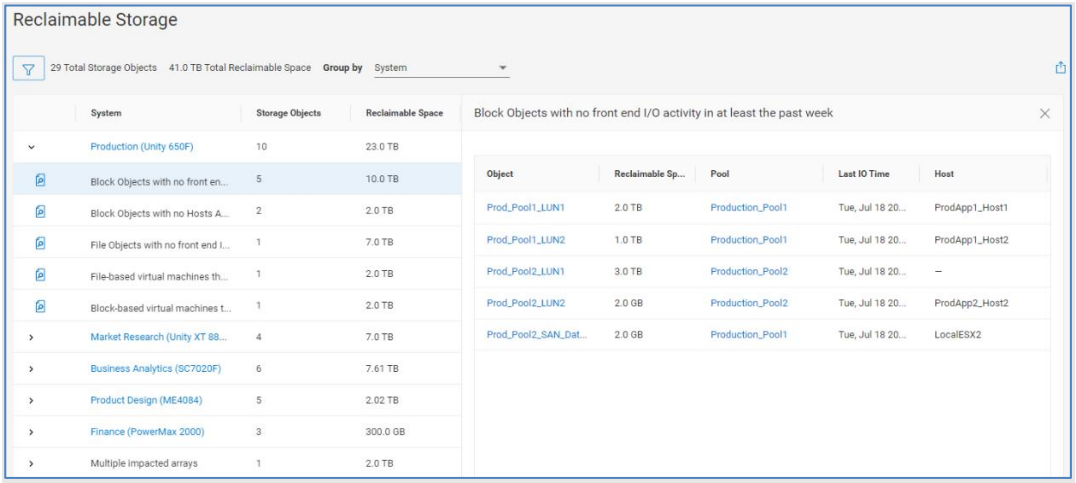
- Block Objects with no frontend I/O activity in the past week or longer
- File Objects with no frontend I/O activity in the past week or longer
- Block Objects with no hosts attached
- Block-based virtual machines that have been shut down for at least a week
- File-based virtual machines that have been shut down for at least a week

Note: The Reclaimable Storage report intelligently filters out objects that are array-based replicas, because those replicas are not attached to hosts and do not have frontend I/O.

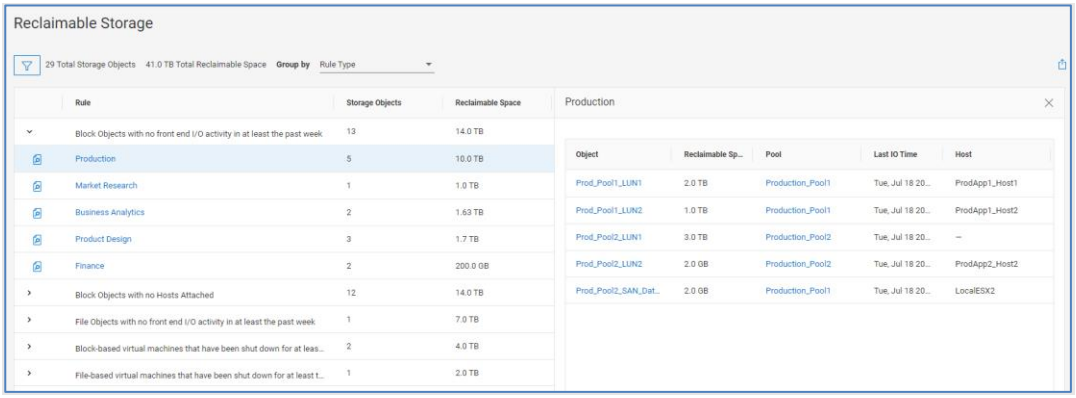
The **Group By** drop-down menu allows the user to group the storage objects by system or by the rule types mentioned above.

Group by System (Default) shows the total number of storage objects and reclaimable space per system. A more detailed view of the objects identified under each rule can be seen by selecting the line item to expand to display the associated details.

The Filter button allows the user to filter the results based on System or Rule Type.

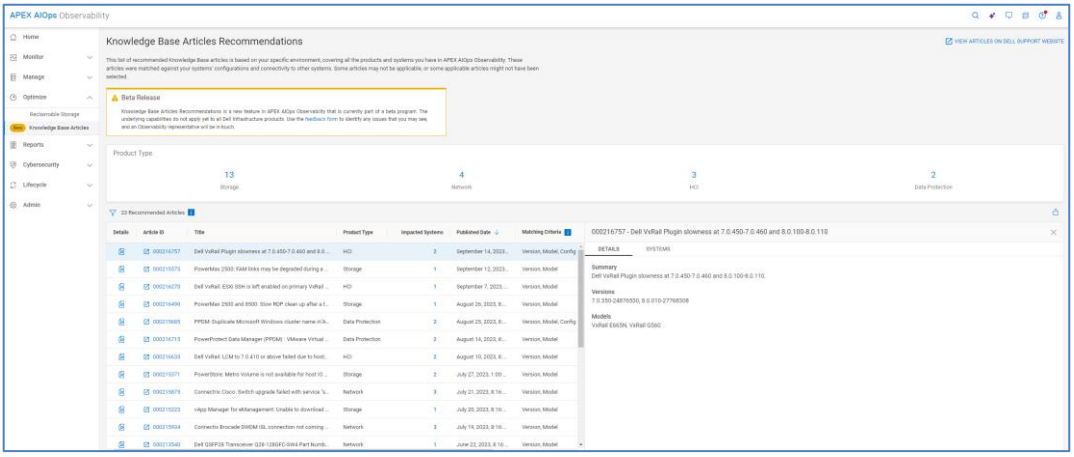


The **Group by Rule Type** shows reclaimable storage for each rule. In this view, the total number of storage objects and reclaimable capacity is summarized for each rule.



Knowledge Base Articles

The Knowledge Base Articles page parses the KB article database and provides details and links to articles that may be applicable to the systems monitored in Infrastructure Observability. Matching criteria could include version, model, and configuration. The Details icon opens a window with details of the issue and the affected versions and models. The Systems tab lists the potentially impacted systems associated with the issue identified in the article. The Article ID is a link to the article on the Dell support page.

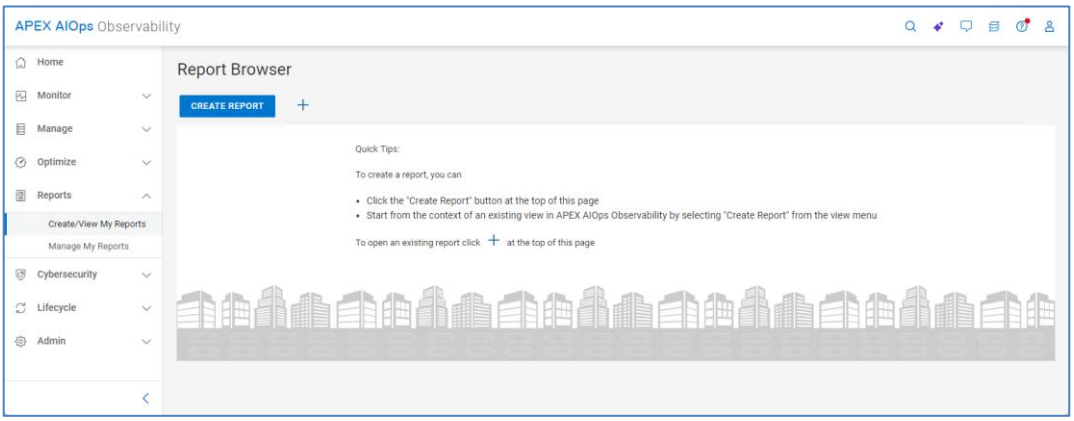


Reports

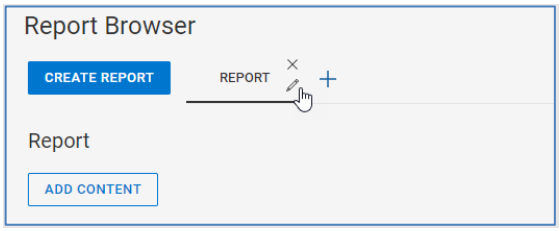
Create/View My Reports

The **Report Browser** is accessed from the Create/View My Reports menu. It acts as a user's reporting workspace and dashboard. It allows users to create, view, and modify reports. Reports can be scheduled, duplicated, bookmarked, and exported in PDF format. Reports can consist of any combination of tables and line charts.

The **CREATE REPORT** button is used to create a report. The plus icon is used to add an existing report to the dashboard.

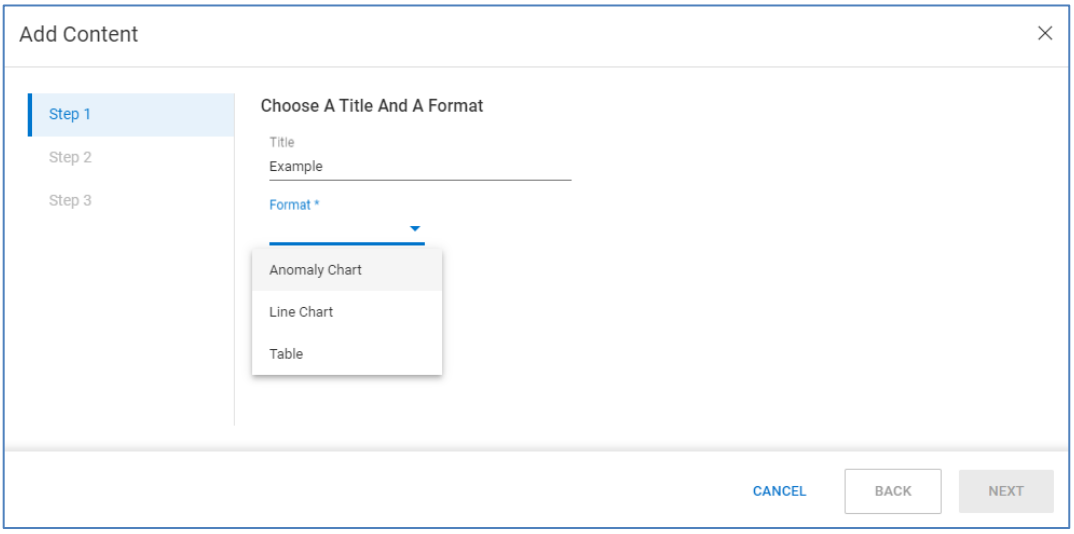


A default name is given to a new report. To edit the name, select the edit icon next to the report name. The icon becomes visible when the mouse is moved over that area. To remove the report from the Report Browser, select the X icon. Removing the report from Report Browser does not delete the report. It is still available from **All Reports** which is discussed in Manage My Reports.



The **ADD CONTENT** button is used to add tables and charts to the report.

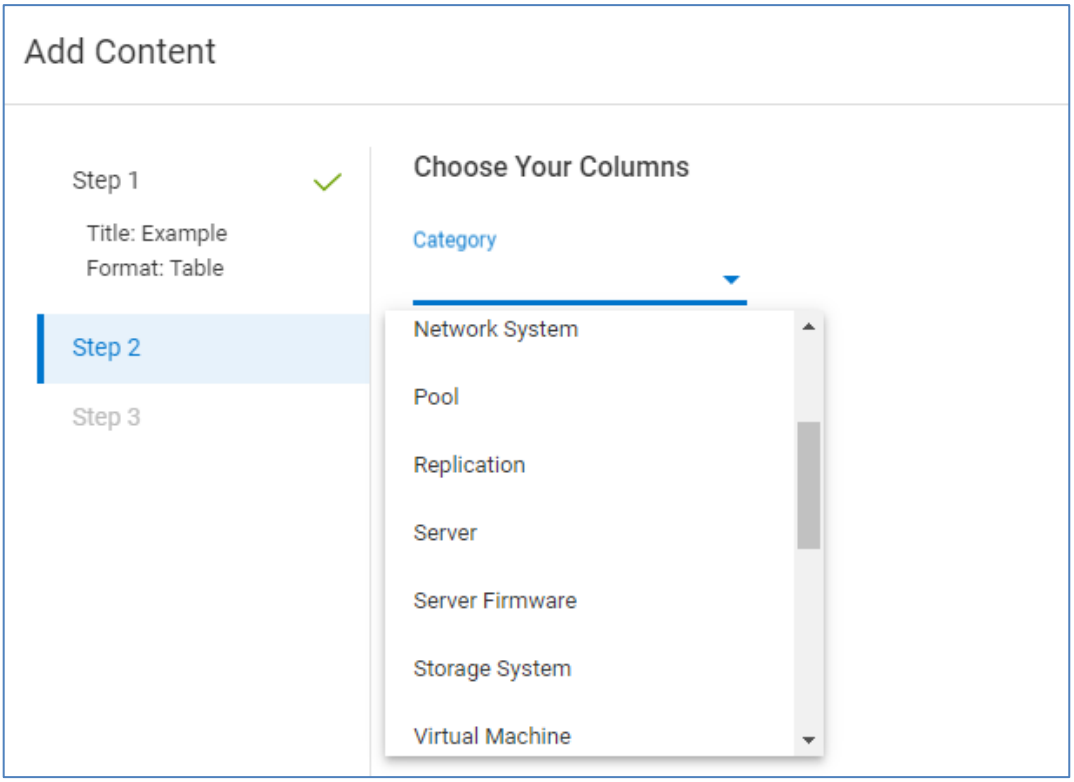
It opens the **Add Content** window shown here. This window presents a series of drop-down menus to define the content including the format. The remaining menus differ based on the selected format.



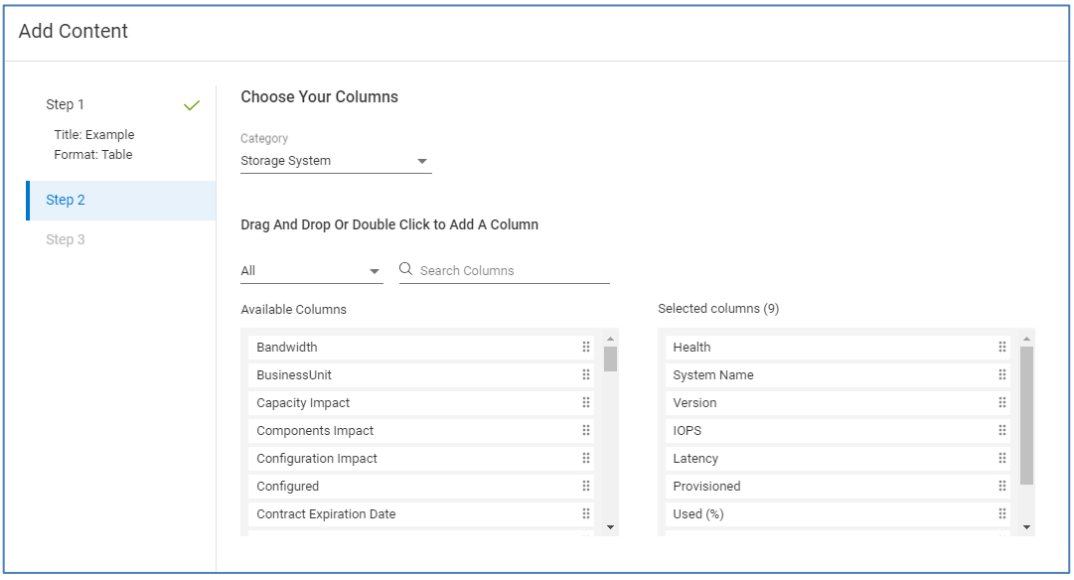
Tables

A table allows the user to select one of the following categories:

- Data Protection System
- Filesystem
- Host
- MTree
- Network System
- Pool
- Replication
- Server
- Server Firmware
- Storage System
- Virtual Machine
- Volume
- Volume Group
- HCI System
- PowerFlex Host
- PowerFlex Protection Domain
- PowerFlex SDS
- PowerFlex Storage Pool
- PowerFlex Device
- PowerFlex Fault Set

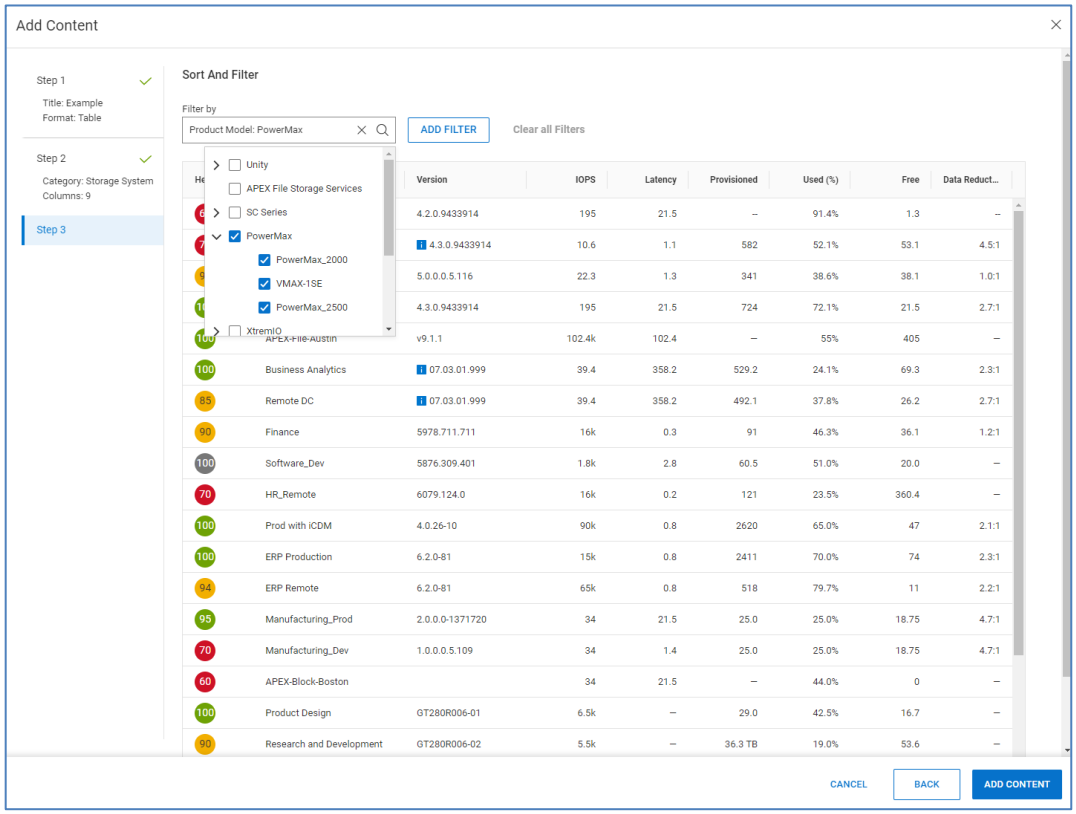


When the user selects the Category, a list of available and selected columns is displayed. Observability prepopulates the report with common columns. The user can either drag and drop or double-click a column name to add or remove it.



The next step shows a preview of the content and allows the user to sort and filter the results. The user can select in the “Filter by” field and scroll through the full list of columns, or they can begin typing to find a specific one. When the column is selected, the

user can choose from an applicable value. The following example shows a filter on the Product Model column and then on all PowerMax systems.



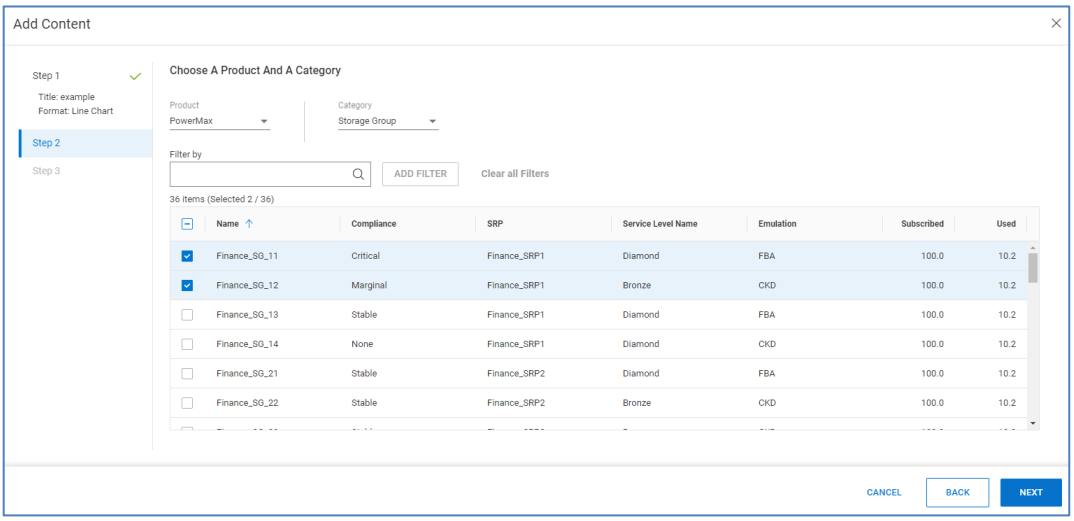
Users can display custom tags in their reports and can use filtering to create reports specific to custom tags such as applications or business units. See the Custom Tags section for more information.

Sorting is performed by clicking the column name on which to sort. Once the user has the table as they want it, clicking Add Content will add the table to the report.

Line charts

A line chart requires the user to select the Product and Category. Once those are selected, a table with available objects in that category is presented.

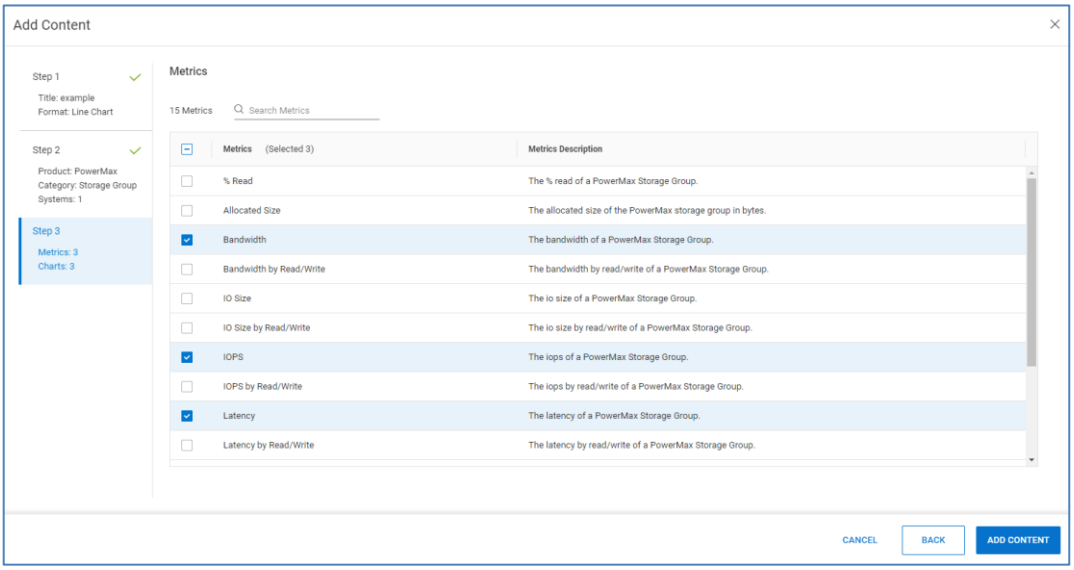
The user chooses which objects to include and clicks Next. The following example shows PowerMax storage groups "Finance_SG_11" and "Finance_SG_12" selected.



After choosing the objects, the final step is to choose the metrics.

The following example shows the Bandwidth, IOPs, and Latency metrics. Clicking Add Content adds the line charts to the reports.

Metrics available for line charts are shown in Appendix D: Report Browser metrics.



Anomaly charts

Anomaly charts are like line charts. The list of supported products is restricted to the following:

- Connectrix
- PowerFlex
- PowerMax
- PowerScale
- PowerStore

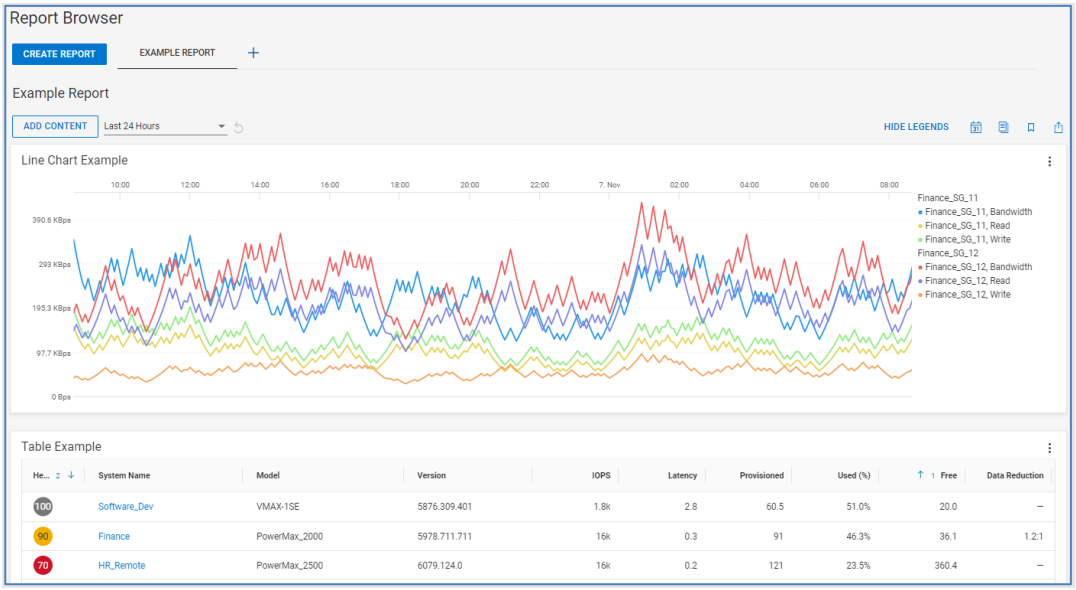
- PowerVault
- SC Series
- Unity XT
- VMware

Anomaly charts provide both the value of the metric and the historic seasonality. By plotting the historic seasonality, users can identify any unexpected anomalies or changes in patterns. Anomaly charts show up to 24 hours of data.

Report options

When a report is created, there are several options that are available for the user at the report level.

- HIDE LEGENDS – For line charts, it provides the option to hide the legend of each object on the right side of the chart. The legend shows the data timestamp and value for each object as the user hovers over the chart. The legend also serves as a filter to remove metrics from the chart.
- Schedule: Schedule the report. Choose an initial runtime and one of the following intervals: Daily, Weekly, Biweekly, Monthly, or Quarterly. Choose a format of PDF or CSV. Enter email addresses for recipients.
- Duplicate: Create a duplicate copy of the report in the Report Browser. This is used to create multiple similar reports where the user wants to make minor changes to a report.
- Bookmark: Add or remove the bookmark on the report. Bookmarks allow the user to easily find and view the report in the Report Browser from the Add Report icon.
- Export PDF: Export the report in PDF format.



The time range of line charts is set to Last 24 Hours by default. It can be changed to another preset value or a custom range using the pull-down.

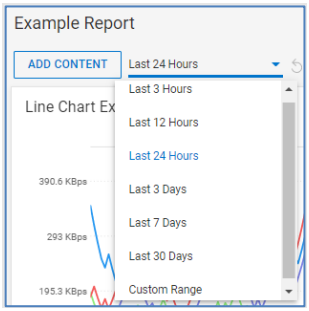
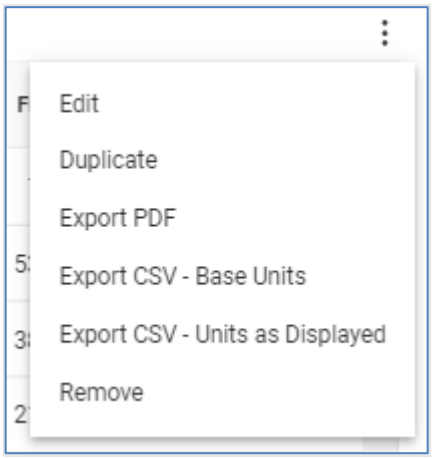


Chart and table options

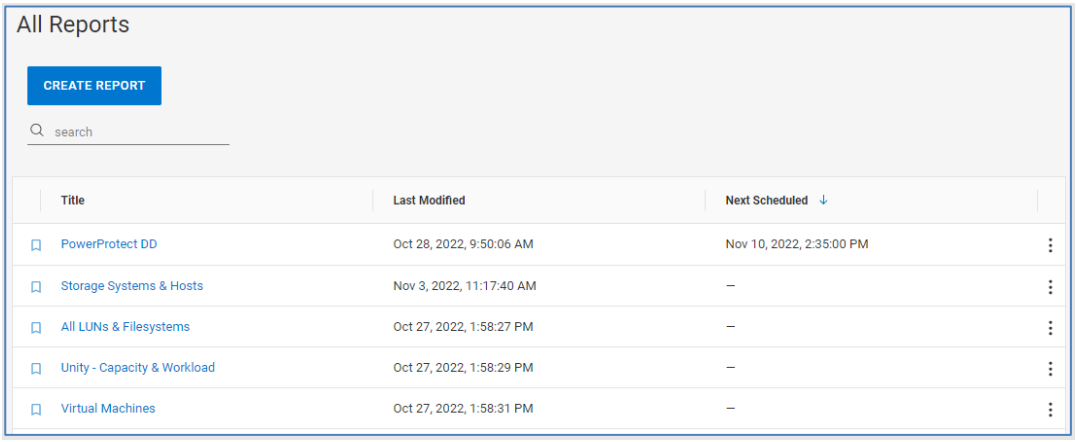
For each individual chart or table, the user is presented with several options after selecting the options icon (⋮).

- Edit – Modify the individual chart or table.
- Duplicate – Create a duplicate chart or table in the same report.
- Export PDF – Export the individual chart or table in PDF format.
- Export CSV – Base Units. Export the individual table in CSV format.
- Export CSV – Units as Displayed. Export the individual chart or table in CSV format using scaled values shown in the table.
- Remove – Delete the chart or table.

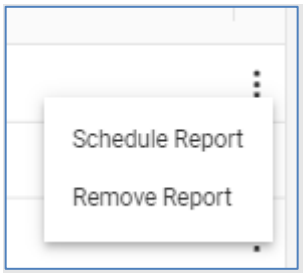


Manage My Reports

All reports are accessible from the **Manage My Reports** menu. Selecting a report from All Reports adds the report to the Report Browser and directs the user to it. In situations where there are many reports, the search field can be used to find a report. The list of reports shows if a report is bookmarked, when it was last modified, and when it is scheduled to run next. The options icon on the right side of each row allows the user to edit the report or delete the report from Observability. The CREATE REPORT button directs the user to the Report Browser to create a report.



Users can schedule and delete a report by selecting the three dots on the right side of the row.



Cybersecurity

Introduction

Cybersecurity is a feature within Infrastructure Observability that adds the ability to monitor Dell resources for security risks. Observability compares configurations and setups to a set of security-related evaluation criteria, notifying users of any deviations from the configured plan. It also provides vulnerability awareness by displaying applicable Security Advisories for supported systems. Cybersecurity is supported for PowerMax, PowerStore, PowerEdge Server and Modular Chassis, and PowerProtect DD systems and will continue to expand coverage to other Dell systems.

Note: To gain access to Cybersecurity, users must be given a Cybersecurity-related role. An Admin user must assign these roles to users, including themselves. See Identity Management and KB#000205045 for additional details.

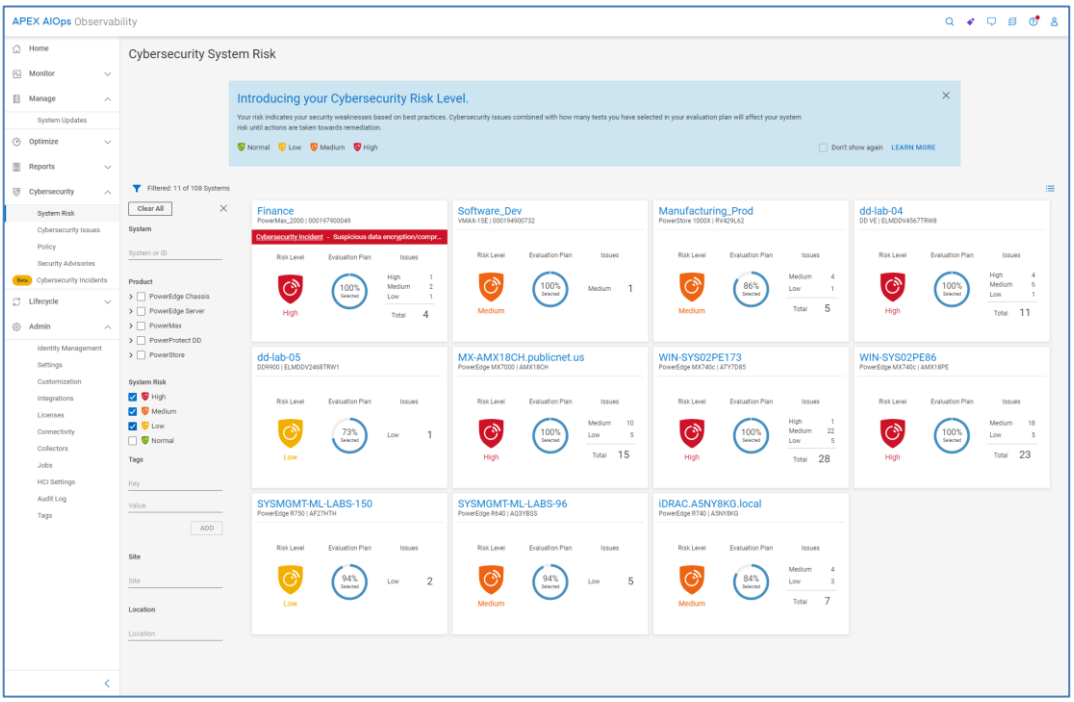
System Risk

The **System Risk** page is the multisystem view for Cybersecurity. It displays all systems that are enabled for Cybersecurity along with the Risk Level, percentage of tests enabled in the Evaluation Plan, and summary of Issues. For systems that have an active ransomware incident, Observability displays a red ransomware incident banner in the card view. The Risk Level provides an overall assessment for the system based on the enabled evaluation tests, and has one of the following values:

- Normal
  - No active Cybersecurity issues.

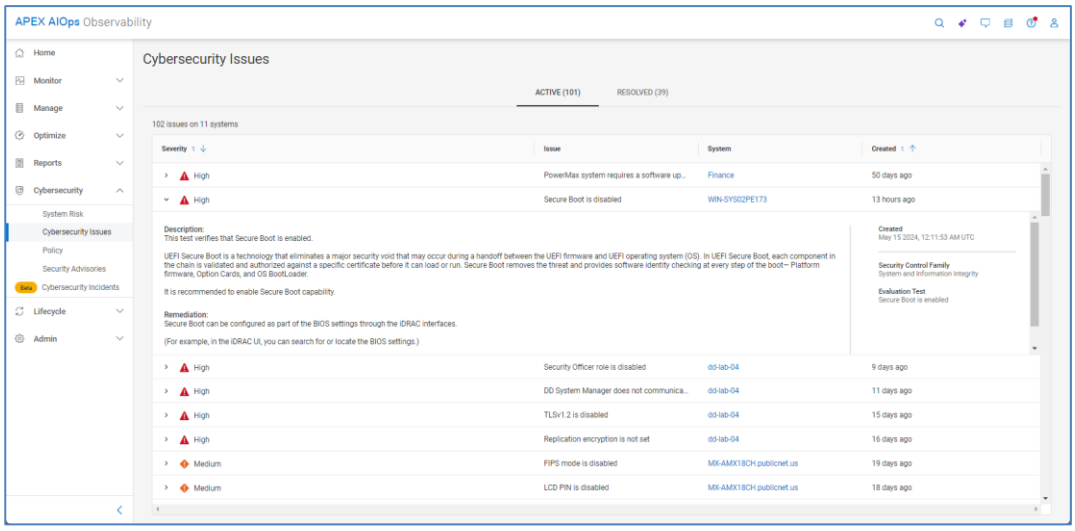
- Low
  - One or two active Low severity Cybersecurity issues.
  - There are at least five enabled tests and the number of enabled tests is greater than 70%.
- Medium
  - One to five active non-High severity Cybersecurity issues with at least one being Medium and number of enabled tests greater than five.
  - Greater than two active Low severity Cybersecurity issues and the number of enabled tests is greater than five.
- High
  - One or more active High severity Cybersecurity issues and the number of enabled tests is greater than five.
  - More than five non-High active issues where at least one issue is Medium severity and the number of enabled tests is greater than five.
- Unknown
  - Evaluation Plan is disabled.
  - The number of enabled tests is less than or equal to five.
  - There are no active Cybersecurity issues and the number of enabled tests is less than 70%.
  - There are one or two active Low severity Cybersecurity issues and the number of enabled tests is less than 70%.

The page can be filtered based on System, Product, System Risk, Custom Tag, Site, or Location.



Cybersecurity Issues

The **Cybersecurity Issues** page provides an overall listing of Cybersecurity issues that have been identified in the environment. The Active tab lists out all active issues and provides the severity, issue name, associated system, and when it was created. Expanding the issue provides the issue description and the recommended remediation, creation timestamp, security control family, and evaluation test. The Resolved tab lists out all issues that have been corrected and the timestamp for when the issue was resolved.



Policy

The **Policy** page is where users enable, disable, and configure the tests in the Evaluation Plan. This can be done by creating individual evaluation plans for each system or by creating a template and applying it to multiple systems. There are two tabs in the Policy page: SYSTEMS and TEMPLATES.

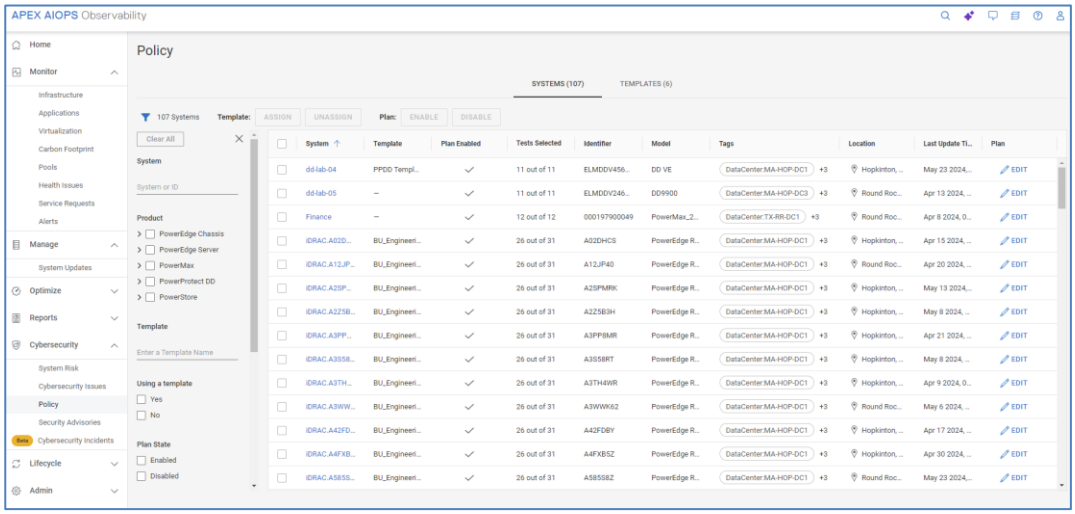
Systems

The Systems tab lists the Cybersecurity enabled systems. It also includes information such as the associated template, status of the evaluation, number of selected tests, custom tags, and the last time the evaluation plan was updated. Cybersecurity Admins can assign or unassign templates to systems, enable or disable the evaluation plan for systems, or edit the evaluation plan for an individual system.

The filter icon allows users to filter the list of systems based on the following:

- System name or ID
- Product type
- Template name
- Systems using or not using a template
- Systems evaluation plan status
- Custom tags
- Site
- Location

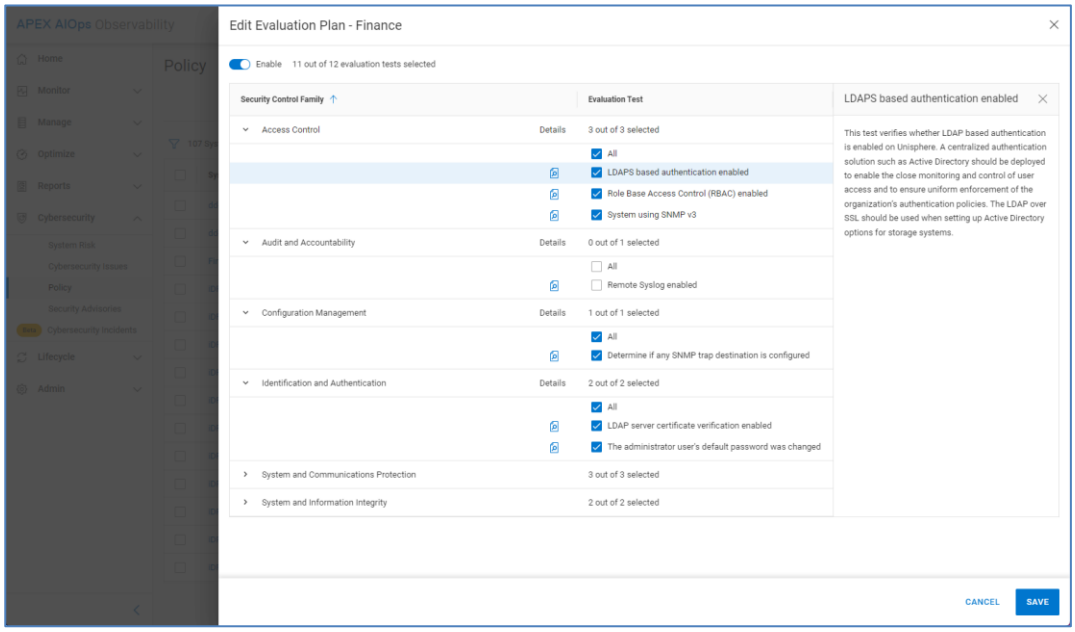
By using the filter mechanism, users can produce a group of systems on which they can perform an action like assign a template or disable the evaluation plan. For example, a user can select all PowerEdge systems from the product category and select “No” under “Using a template”. They can then assign a template to all systems that are not associated with a template.



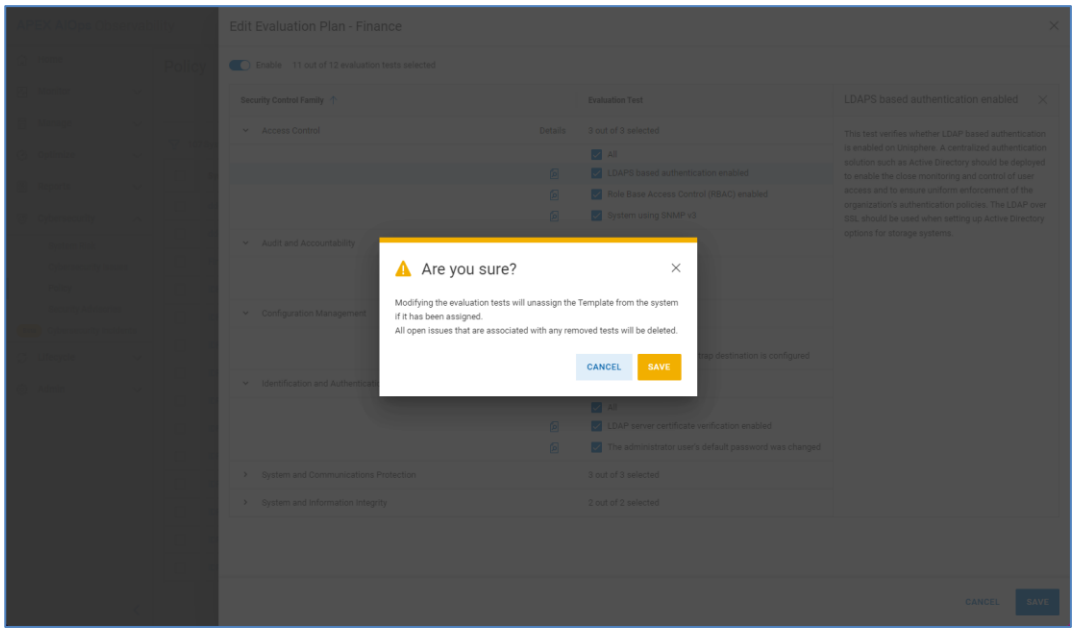
There are a few scenarios that require further explanation. If a user assigns a template to a system that already has a template, the old template is automatically unassigned. If the evaluation plan of a system is disabled, it does not affect the assigned template. The template will remain associated to the system. If the evaluation plan is edited by selecting the Edit icon in the right-side column, the template for that system is unassigned.

Selecting the Edit button opens the Edit Evaluation Plan window for the system and allows the user to set the plan for that individual system. The possible evaluation tests are listed and grouped by Security Control Family (based on NIST 800-53 R5). Each test can

be selected or cleared for inclusion in the Evaluation Plan. Selecting the Details icon provides a detailed description of the test.



When an Evaluation Test is cleared and removed from the Evaluation Plan, any associated active issues for that test will be deleted. The following warning is provided anytime the user removes an Evaluation Test and saves the Evaluation Plan.

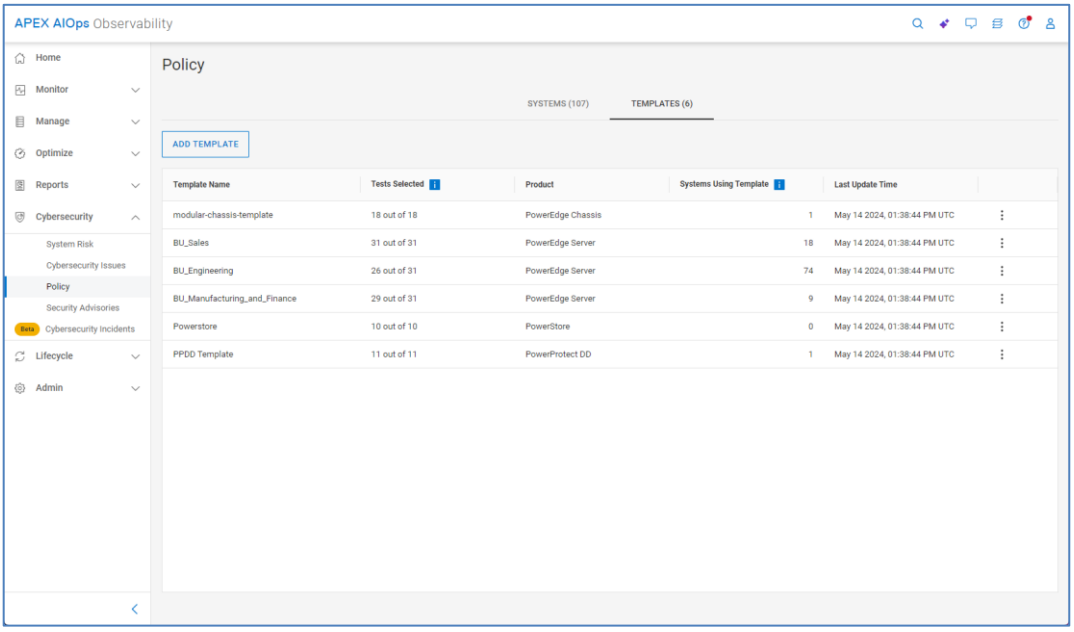


Users will be notified in the What's New section when new tests are added to the product.

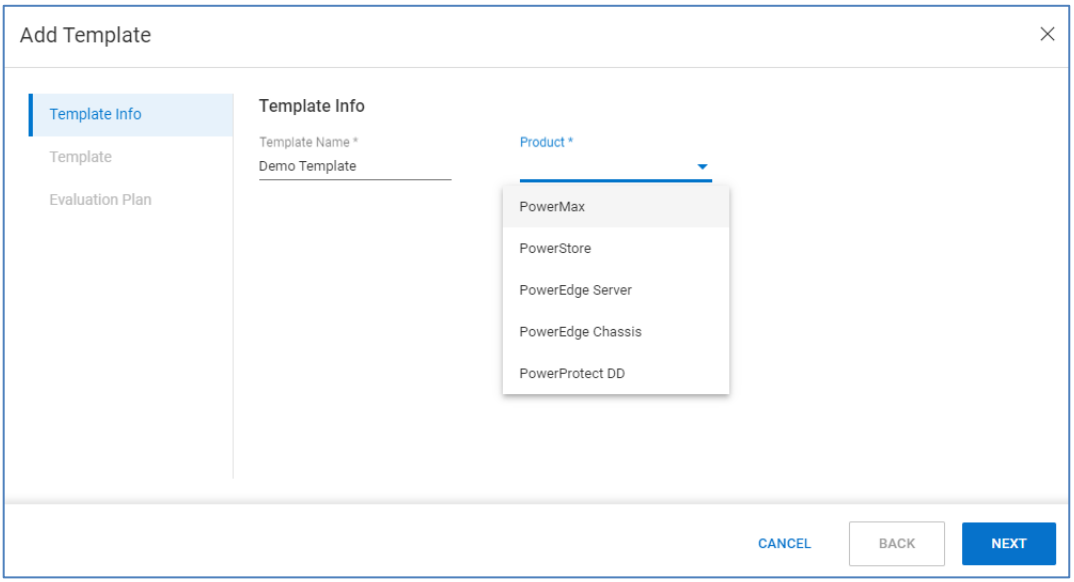
Templates

The **Templates** tab lists the configured templates and allows users to create templates and view, edit, and delete existing templates. A template contains a list of configured tests

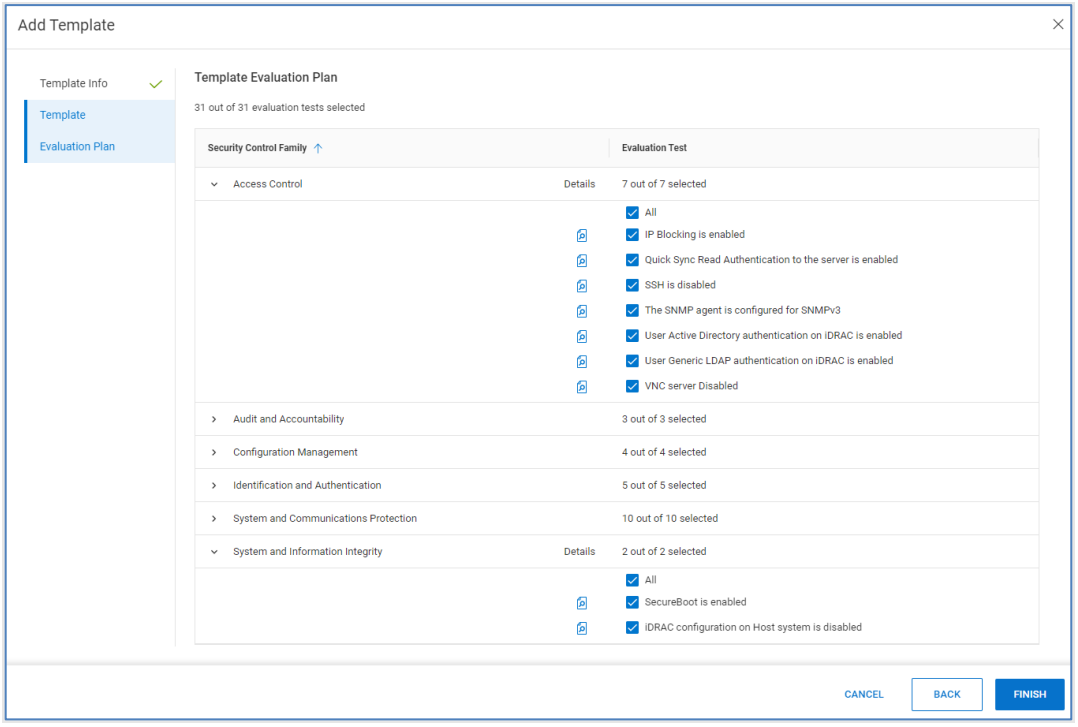
which can be assigned to multiple systems of the same product technology. It allows users to efficiently set a consistent evaluation plan across many systems. A template can only be edited and deleted when there are no systems assigned to it. If a template has an assigned system, it can only be viewed or duplicated.



Selecting Add Template steps the user through the template creation wizard. The user provides a template name and then selects the product type for the template.



Then, the user selects which tests to include in the evaluation plan and then selects Finish to save the template. Then, it is available to assign to systems of that product type.

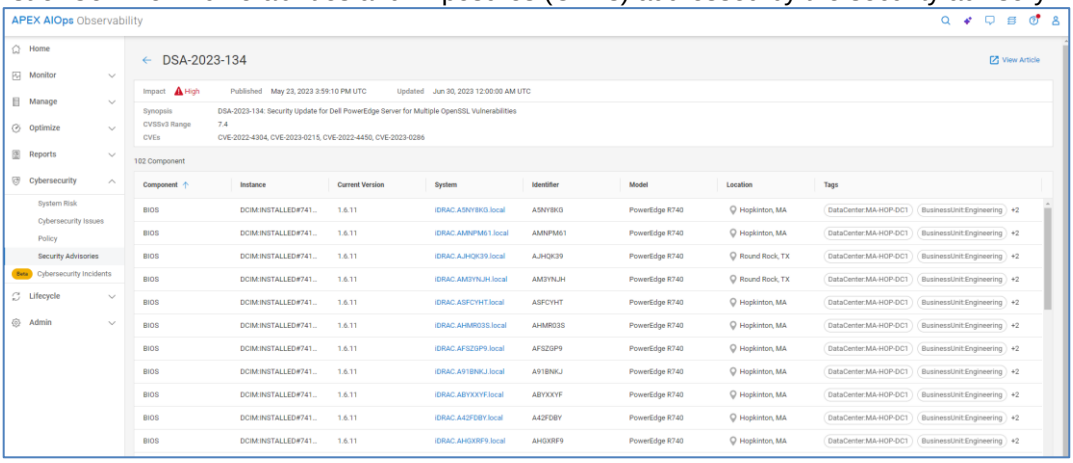


The operations that are available for a template depend on whether there are systems assigned to the template. For templates with assigned systems, the allowable operations are View and Duplicate. Templates with assigned systems cannot be edited or deleted. Templates without assigned systems have the Edit, Duplicate, and Delete operations available.

Security Advisories

The **Security Advisories** page provides a full list of applicable Security Advisories along with their impact, a synopsis, component, number of impacted systems, and publish date. Clicking the **View Article** hyperlink opens the article details on the Dell support page.

Clicking the **Advisory ID** hyperlink opens a window providing a list of all affected systems. This window also shows additional information about the security advisory including the list of Common Vulnerabilities and Exposures (CVEs) addressed by the security advisory.

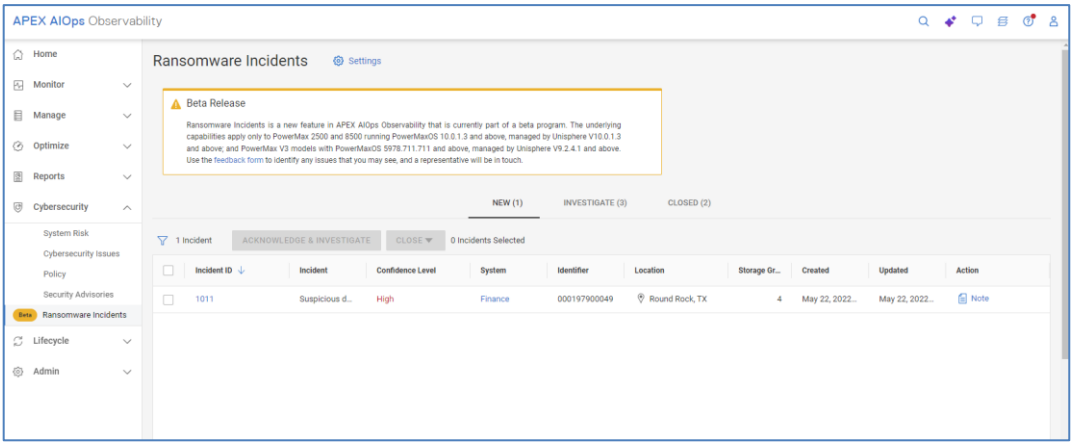


Ransomware Incidents

Ransomware Incidents enables users to monitor for cybersecurity ransomware incidents in near real time. At the time of publication, ransomware incidents is supported on PowerMax systems. Coverage will continue to expand to other platforms. This feature is also considered Beta at the time of this publication, meaning support and feedback for this feature is accomplished through the **Feedback Form** link in the Observability UI.

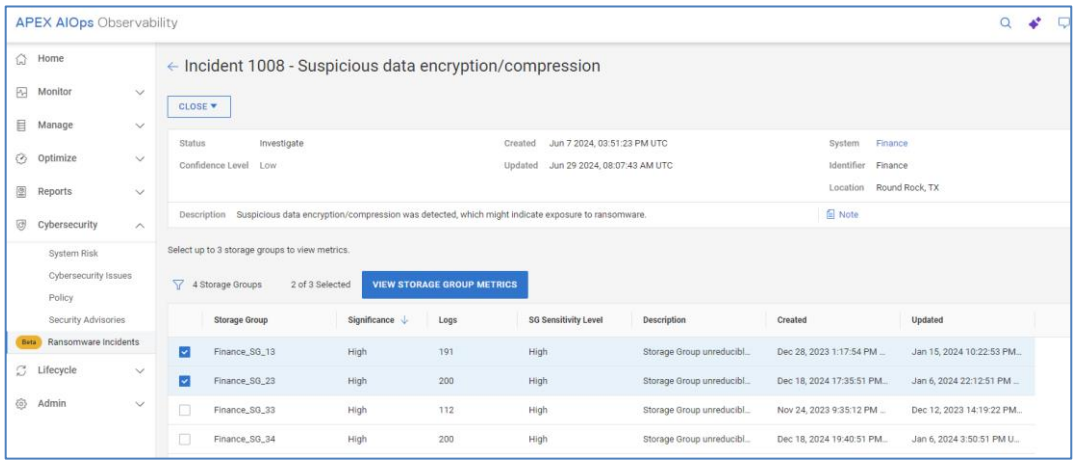
In the event of a ransomware attack, the attackers encrypt the data which requires an encryption key to essentially unlock the data. One of the effects of encryption is that the data becomes uncompressible or irreducible. By establishing an expected range of the reducible data, and then continuously monitoring the level of it, one can identify variances outside of normal patterns which are referred to as anomalies. Through various algorithms and analysis, Observability can then identify potential ransomware incidents in near real time.

The **Ransomware Incidents** page is accessed from the Cybersecurity menu on the left side of the Infrastructure Observability user interface. This page shows all identified incidents and puts them in one of three categories: New, Investigate, or Closed. When an incident is first identified, it appears in the New tab. Each incident has an incident ID, a confidence level, the system identifier, the location, the number of affected storage groups, and the created and updated times. There is also the ability to add notes to each incident. When the incident is ready to be analyzed, the user selects it and clicks **Acknowledge & Investigate**.

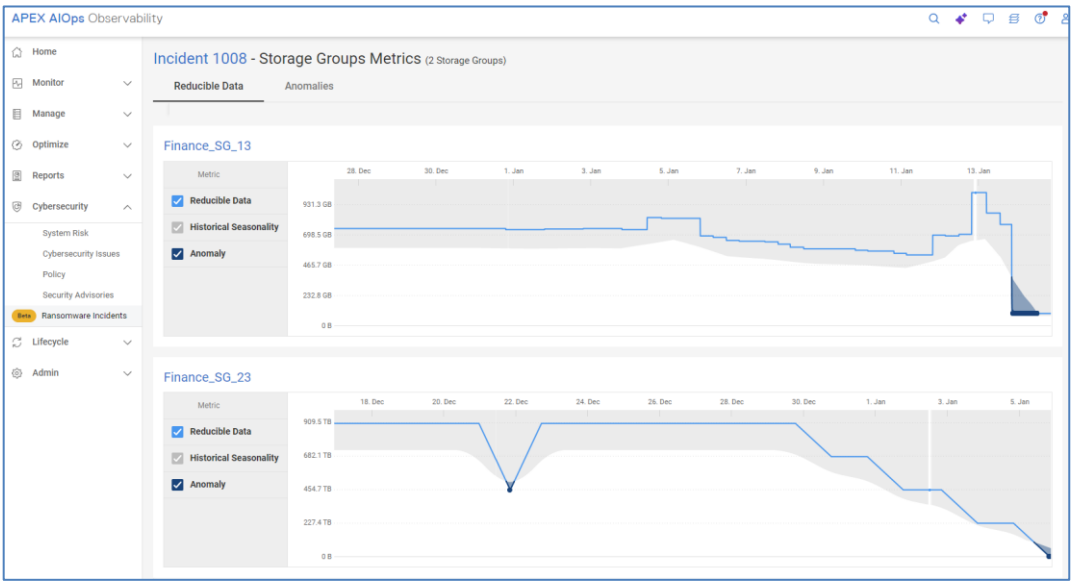


At this point, this incident is “frozen” and moved under the Investigate tab. Any new anomalies will trigger a new incident. While in the investigate state, the user can look at the potentially affected hosts and applications to determine if the incident is a true ransomware attack. If so, they can take appropriate action to isolate and recover.

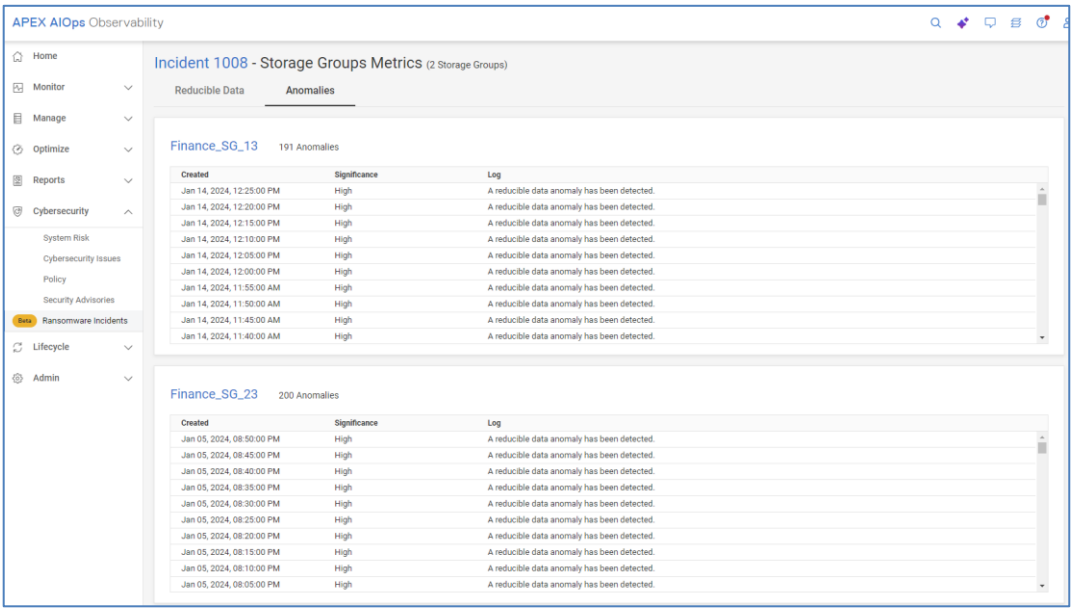
To help investigate, the user can click the incident ID link and see the details of which storage groups experienced anomalies and when the anomalies were created and last updated.



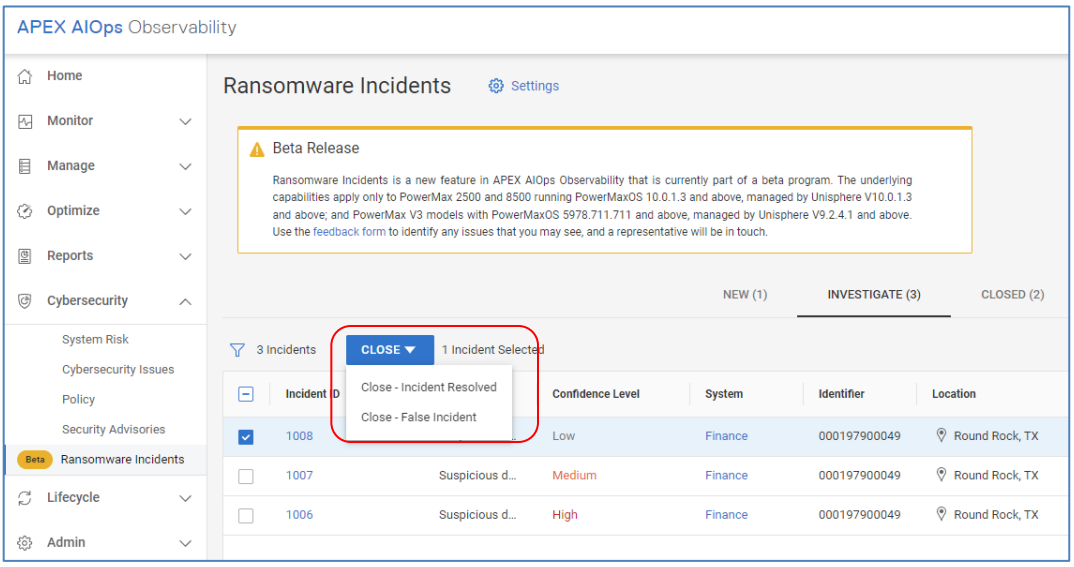
Users can select up to three storage groups at a time to see charts of the reducible data, the historical seasonality, and the anomalies.



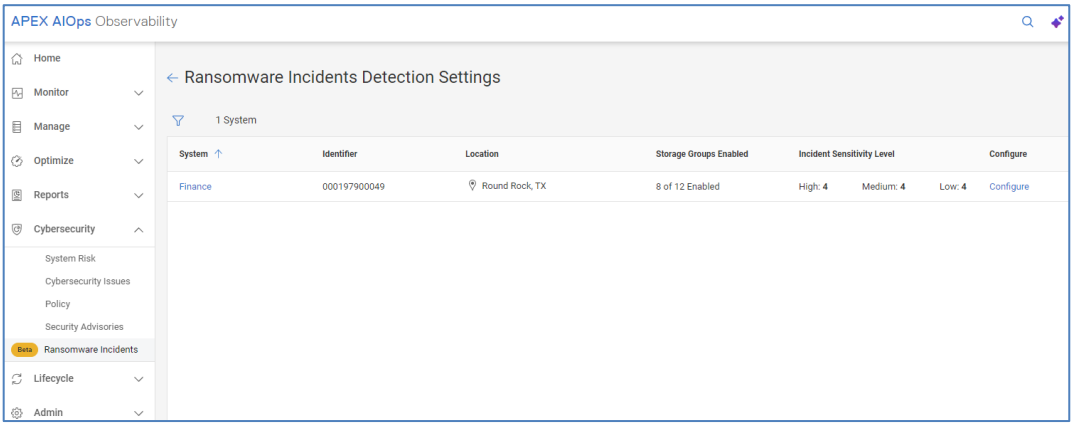
The **Anomalies** tab provides a list of anomalies, also called logs, with their timestamps.



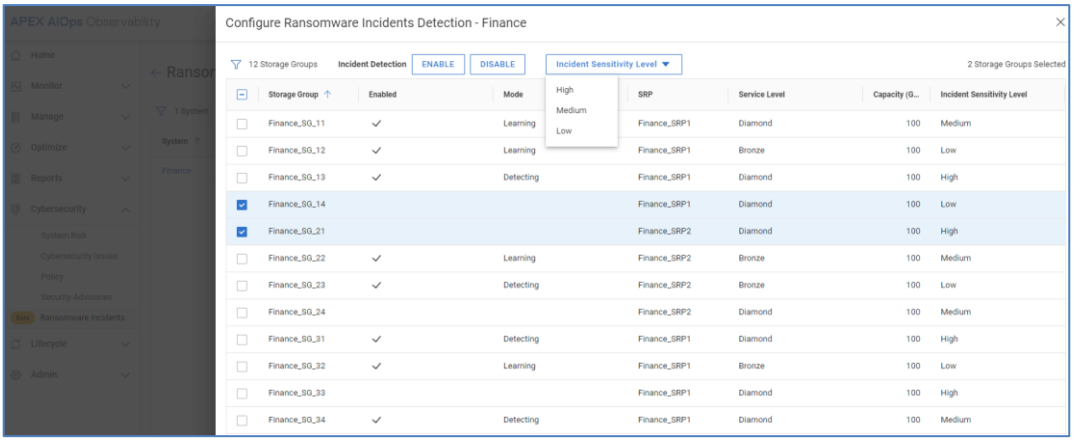
Once the investigation is complete, the user determines if the incident was a valid ransomware attack that was resolved or a false incident. Selecting an incident and then clicking Close gives the user the option to close it with either of these two options.



Ransomware incident monitoring is enabled from the **Settings** link on the **Cybersecurity Incidents** page. The Cybersecurity Incidents Settings page lists the supported systems for ransomware incident monitoring.



Clicking **Configure** on one of the systems opens the **Configure Cybersecurity Incidents** window. In this window, the user can choose to enable or disable any of the storage groups and can set an Incident Sensitivity Level. Users can also see the detection mode, either Learning or Detecting. Learning occurs when the storage group is first enabled or after an incident is closed as a valid incident. During this mode, Observability learns the expected range of reducible data to establish normal behavior. Once the expected behavior is established, the mode switches to detecting and Observability starts monitoring the storage group for ransomware incidents. The sensitivity level lets users tune the detection algorithm. A low sensitivity level results in a lower likelihood of triggering an incident. A high sensitivity level results in a higher likelihood of triggering an event. Users may want to set a sensitivity level of low for less critical applications or for applications that have a higher variation of reducible data. Users may set a sensitivity level of high for more critical applications or applications that have a lower variation of reducible data.



Storage system details

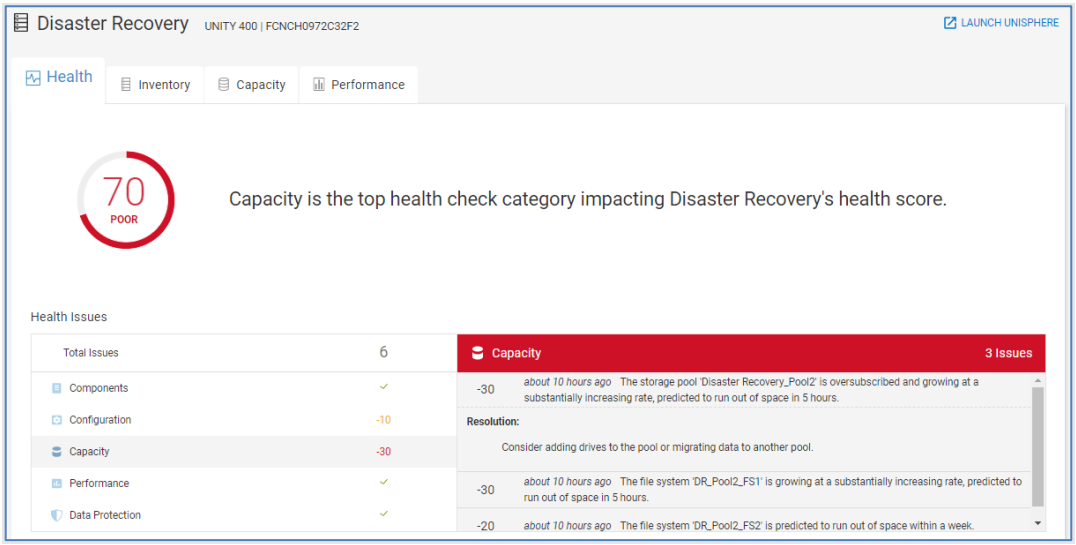
Introduction

Clicking the storage system hyperlink in the Home page or any of the multisystem views opens the System Details page for that system. The following sections discuss each tab of the Storage System Details page in greater depth.

Storage system details – Health

The **Health** tab shows the details for a selected system driving the health score number. The view provides a listing of issues found in each of the following categories:

- Components
- Configuration
- Capacity
- Performance
- Data Protection

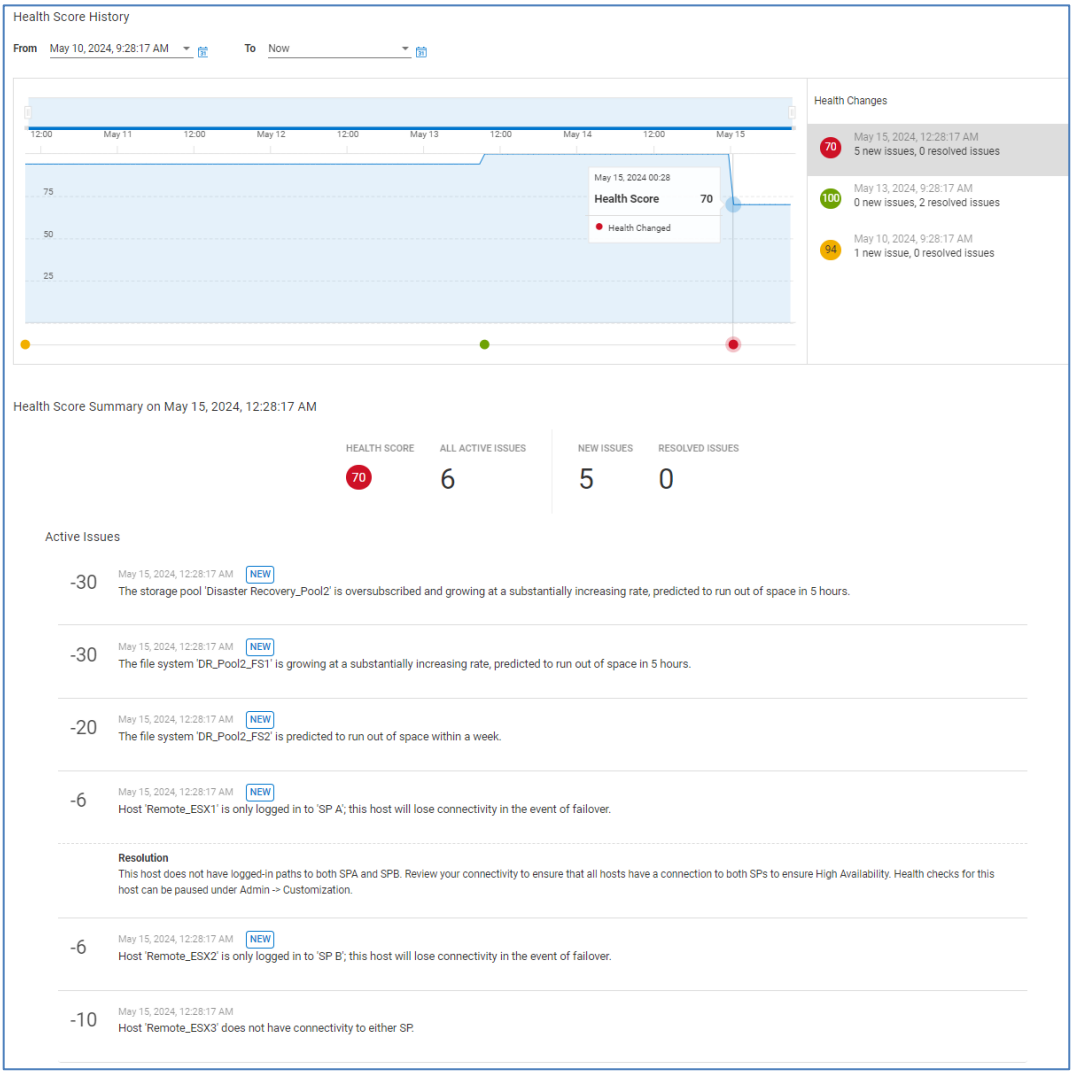


In this example there are six issues, three in the Configuration category and three in the Capacity category. Selecting the category and then selecting one of the issues will display the recommended resolution.

Note:

- The Components and Data Protection categories do not apply for PowerMax/VMAX systems.
- The Performance and Data Protection categories do not apply for PowerVault ME4 systems.
- The Data Protection category does not apply for VxRail systems.
- Only the Components category is used for PowerEdge, Connectrix, and PowerSwitch.
- The health score of VxBlock converged systems based on the health of the associated storage systems.

Scrolling down in this view shows the history of the health score for the system as shown below. This graph displays the historical trend of the health score and details of any issues over the displayed range of time.



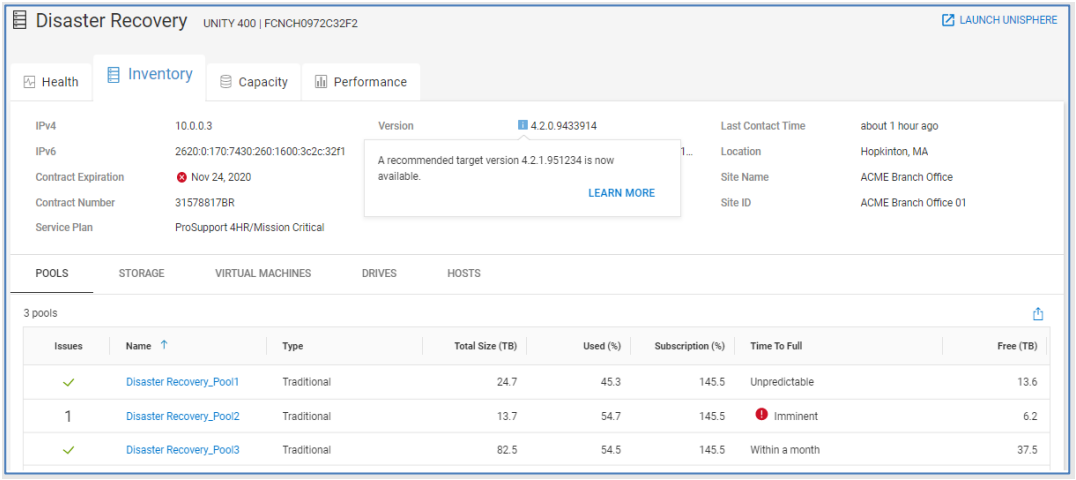
Selecting an issue listed to the right of the graph will mark the change on the timeline and a summary of the active issues will be displayed below the graph. Selecting an individual active issue will open a recommended resolution.

Selecting the calendar will open a drop-down, allowing users to select one of the predefined ranges or enter a custom time range. A custom view is the default. Selecting any of the dates on the right will present the list of issues for that date.

Viewing a history of health issues across a longer-term time range can be helpful in identifying recurring issues in the environment.

Storage system details – Inventory

The **Inventory** tab shows the configuration data and contract information of the selected system as well as the physical and logical components of the system. For traditional storage systems, the upper portion of this view provides the system attributes such as Serial Number/ServiceTag, Model, Location, Code Version, IP Address, and Contract Expiration. Some attributes vary by system type (such as Uptime and Hotfixes for the Unity XT family and Entitlement information for APEX Block Storage for AWS).



As noted earlier, Observability indicates when a storage system has a code update available. In this single system view, there is also an indication if the management software has an available update. Clicking the “Learn More” link opens a dialog with summary information and relevant links to support resources.

The bottom half of the page provides details about the physical and logical components of the system. The tabs differ based on product type but could include:

- Pools (Unity XT family, SC Series, PowerVault, PowerScale/Isilon, APEX File Storage for AWS) / Storage Resource Pools (PowerMax/VMAX)
- Storage (Unity XT family, PowerStore, SC Series, and PowerVault) / Volumes (XtremIO) / Storage Groups (PowerMax/VMAX)
- Virtual Machines (Unity XT family, PowerStore, SC Series, XtremIO, and PowerMax/VMAX)
- Drives (Unity XT family, PowerStore, SC Series, and PowerVault)

- Hosts (PowerStore, PowerMax[13], Unity XT family, and XtremIO) / Servers (SC Series) / Initiators (PowerVault)
- Consistency Groups (XtremIO)
- Service Levels (PowerMax/VMAX)
- File Systems (PowerMax)
- System Health Checks (PowerMax)
- Nodes (PowerScale/Isilon and APEX File Storage for AWS)
- Appliances (PowerStore)
- Storage Containers (PowerStore)
- Quotas (PowerScale/Isilon and APEX File Storage for AWS)
- Block (PowerFlex and APEX Block Storage for AWS)
- Resources (PowerFlex and APEX Block Storage for AWS)
- Gateways (PowerFlex, PowerScale/Isilon, APEX Block Storage for AWS, APEX File Storage for AWS)
- Cloud Infrastructure (APEX Block Storage for AWS and APEX File Storage for AWS)

The **Pools** or **Storage Resource Pools** tab shows various information about the configured storage pools including Total Size, Used %, Subscription %, Time to Full, and Free. This information helps in understanding the pools at risk where the subscription rate is greater than the total free storage and the Time to Full has a defined prediction.

The **Storage** or **Volumes** tab shows all the storage objects in the system. Depending on product type, this tab displays various used and free capacity information for the storage objects.

- PowerStore: Volumes, Volume Groups, and File Systems
- Unity XT family: LUNs, File Systems, VMware vStorage VMFS, and VMware NFS
- SC Series: Volumes
- XtremIO: Volumes
- PowerVault: Base and Snapshot

This view can help to determine which specific object is consuming the greatest amount of storage.

The **Storage Groups** tab lists the storage groups on the system with the capacity, the associated storage resource pool, the service level, and the status of compliance with the service level objective.

The **Virtual Machines** tab lists the VMs on the storage system along with various details including the operating system and associated vCenter, ESXi Server, and ESXi Cluster.

[13] Host information for PowerMax requires Unisphere 9.2 or later.

The **Drives** tab gives the details on the drives for the given storage system and their location in the system. It includes remaining endurance, storage tier, and firmware version. There will also be an indication if there is a firmware update available.

The **Hosts**, **Servers,** or **Initiators** tab gives the details about the hosts attached to this storage system. Host information differs slightly for each storage platform, and may include hostname, IP Address, operating system, initiator protocol, and total accessible storage for each host from the specific storage system. For PowerVault initiators, it lists the initiator name, protocol, and total provisioned storage to each initiator from the storage system. For PowerMax systems, it includes host group name, initiator type, number of initiators, number of masking views, number of PowerPath hosts, and if the Consistent LUN flag is set. For PowerStore, it provides host group name, OS, initiator protocol, number of volumes and number of initiators.

The **Consistency Groups** tab lists the XtremIO consistency groups on the system including their mapped status, number of volumes and total and used capacities.

The **Service Levels** tab lists the configured service levels on PowerMax systems along with the expected response times.

The **File Systems** tab for PowerMax lists the name, used and total capacities, NAS server, and protection and performance policies for each file system.

The **System Health Checks** tab (PowerMax) provides pass or fail information for various system checks.

The **Nodes** tab provides information about each PowerScale/Isilon node such as node type, total, and capacity, used capacity, and associated pool. See the PowerScale Node Details section for additional information.

The **Appliances** tab lists each appliance in the PowerStore cluster along with attributes such as State, Serial Number, CPU, Used, and Provisioned storage.

The **Storage Containers** tab provides capacity information for the storage containers in the PowerStore cluster.

The **Quotas** tab lists each quota path, quota type, threshold size, efficiency, advisory limit, soft limit, and hard limit. See the PowerScale Quotas Details section for additional information.

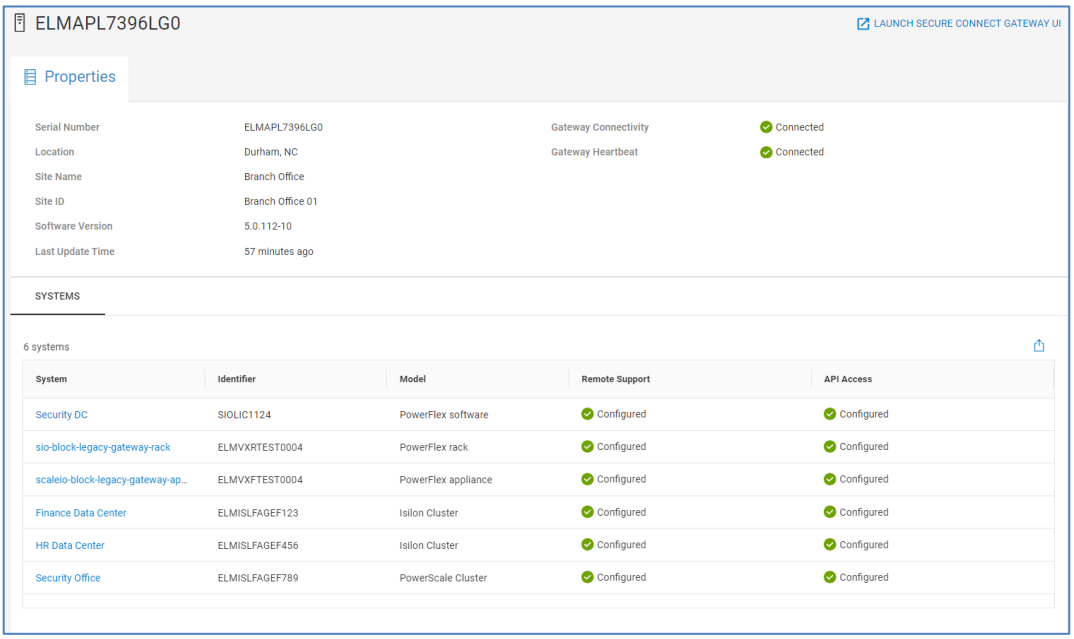
The **Block** tab is a pull-down that displays the following components for PowerFlex systems:

- **Hosts** – Host WWN, Operating System, IP address, Protocol, and Version
- **Protection Domains** – Total, Used, and Free Capacity and Protection Domain State
- **Fault Sets** – Protection Domain Name and Fault Set State
- **SDS** – IP address, Version, State, Total Capacity, Protection Domain, and Fault Set
- **Storage Pools** – Layout, Protection Domain, Total, Used, Spare, and Provisioned Capacity
- **Devices** – Type, Total and Used Capacity, and Storage Pool

- **Volumes** – Type, Size, Mapped status, number of SDCs, Creation Time, Read Only status, Secured state.

The **Resources** tab lists the PowerFlex Metadata Managers (MDMs) and whether they are running in primary, secondary, tiebreaker, or standby mode. Management IP address, version, and count information are also provided.

The **Gateways** tab lists the Secure Connect Gateways in use by the PowerFlex or PowerScale system. Clicking the serial number opens the Secure Connect Gateway Details page shown in the following figure. The Gateway Details page provides information about the Secure Connect Gateway including serial number, version, site and location information, and connectivity status. It also shows which systems it manages.

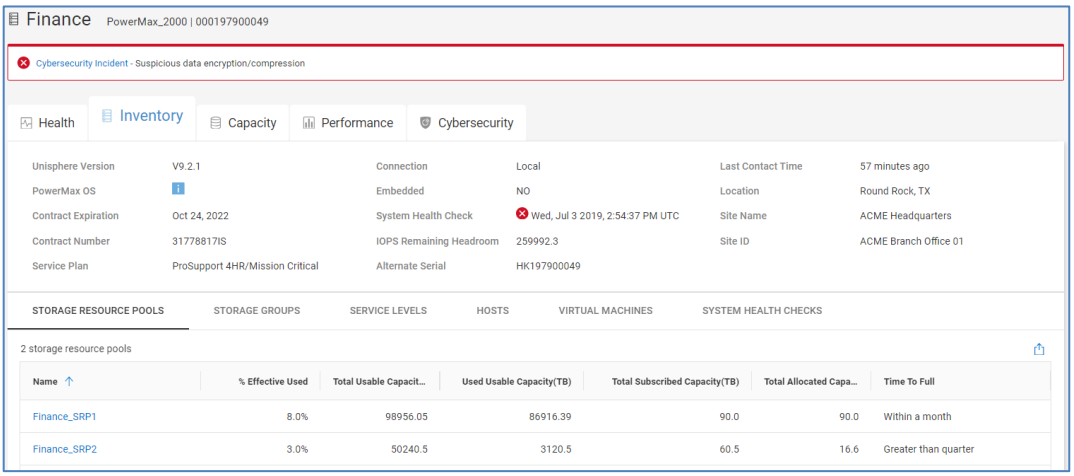


The **Cloud Infrastructure** tab lists information about the cloud environment such as AWS instance information, IP addresses, instance state, availability zone, product version, and protection domain.

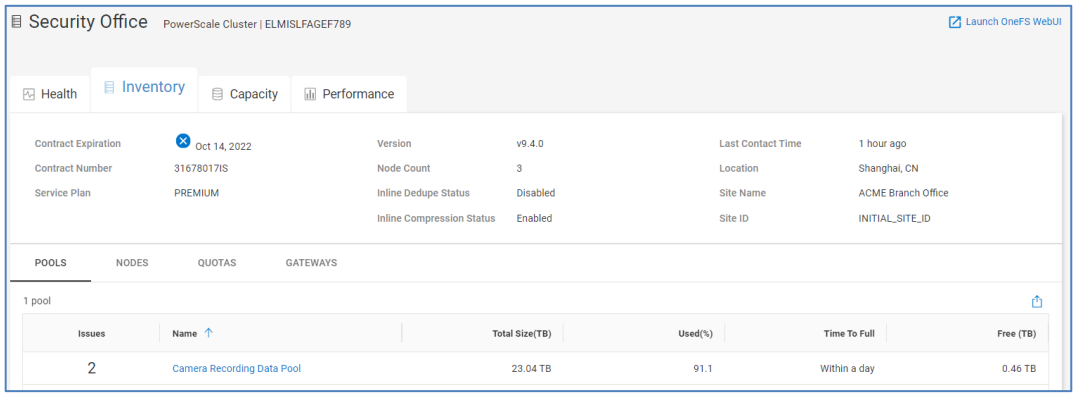
The following series of screenshots shows examples of the Inventory tab for various storage types.

PowerMax:

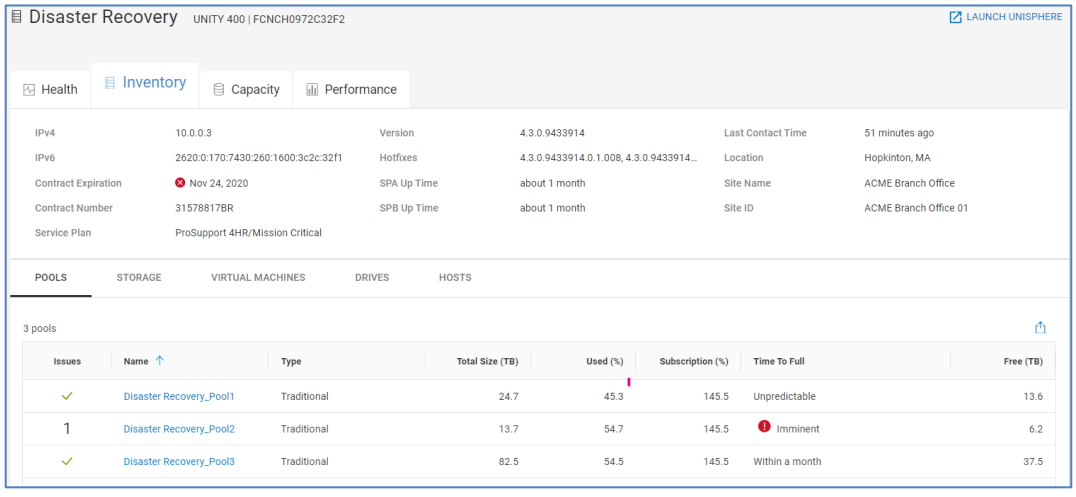
Storage system details



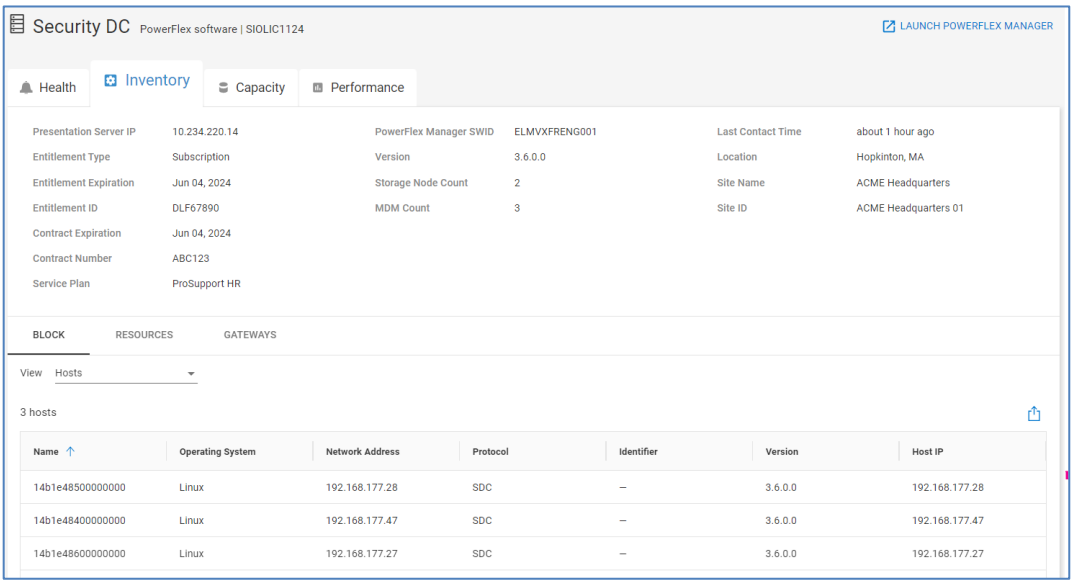
PowerScale:



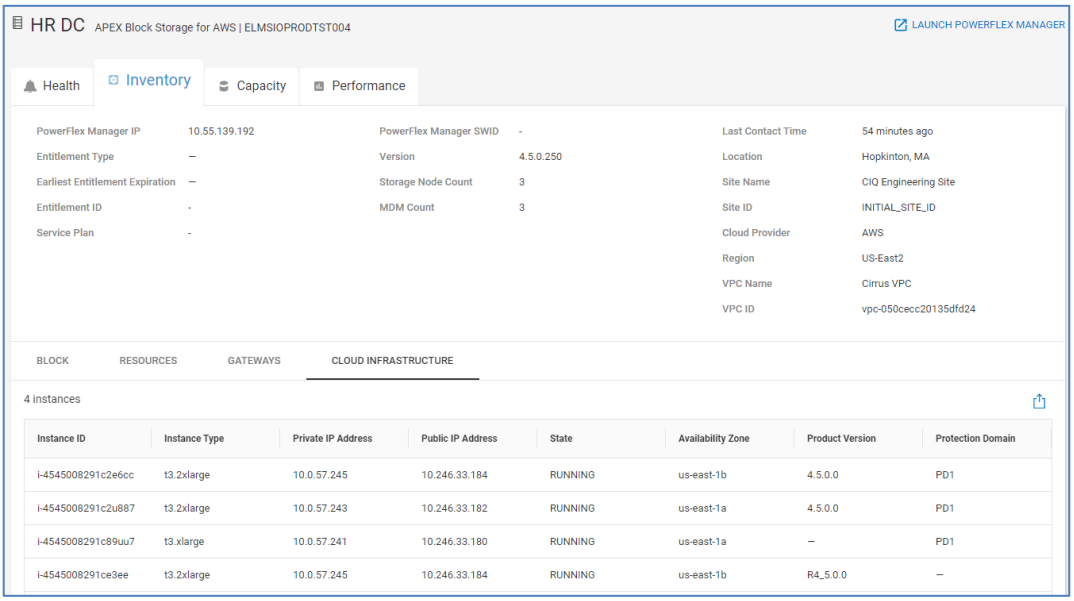
Dell Unity XT:



PowerFlex:



APEX Block Storage for AWS:



Storage system details – Capacity

The **Capacity** tab shows slightly different information depending on the product type. The storage capacity details for PowerStore, Unity XT family, SC Series, PowerVault, PowerFlex, and PowerScale/Isilon include:

- Total Capacity
- Storage Usage
- Drive Type Usage (not available for PowerStore, PowerScale/Isilon, PowerFlex, APEX Block Storage for AWS, or APEX File Storage for AWS)
- Pools (not applicable for PowerStore or PowerFlex)

The **Total Capacity** graph provides a breakdown of raw storage to Used, Free, and Unconfigured Drives (Unprovisioned Capacity for PowerScale or Isilon).

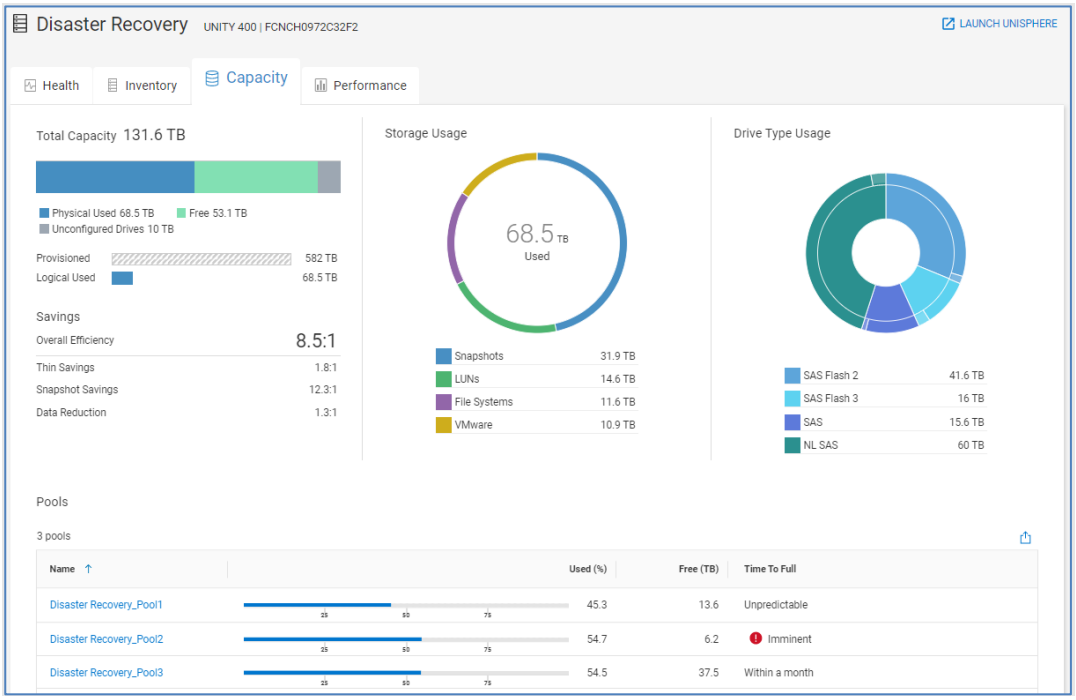
Savings includes a breakdown of the Logical and Used capacity of the total storage visible to the hosts, and the Efficiency Savings explained previously.

Storage Usage shows the consumed capacity of these categories of storage objects:

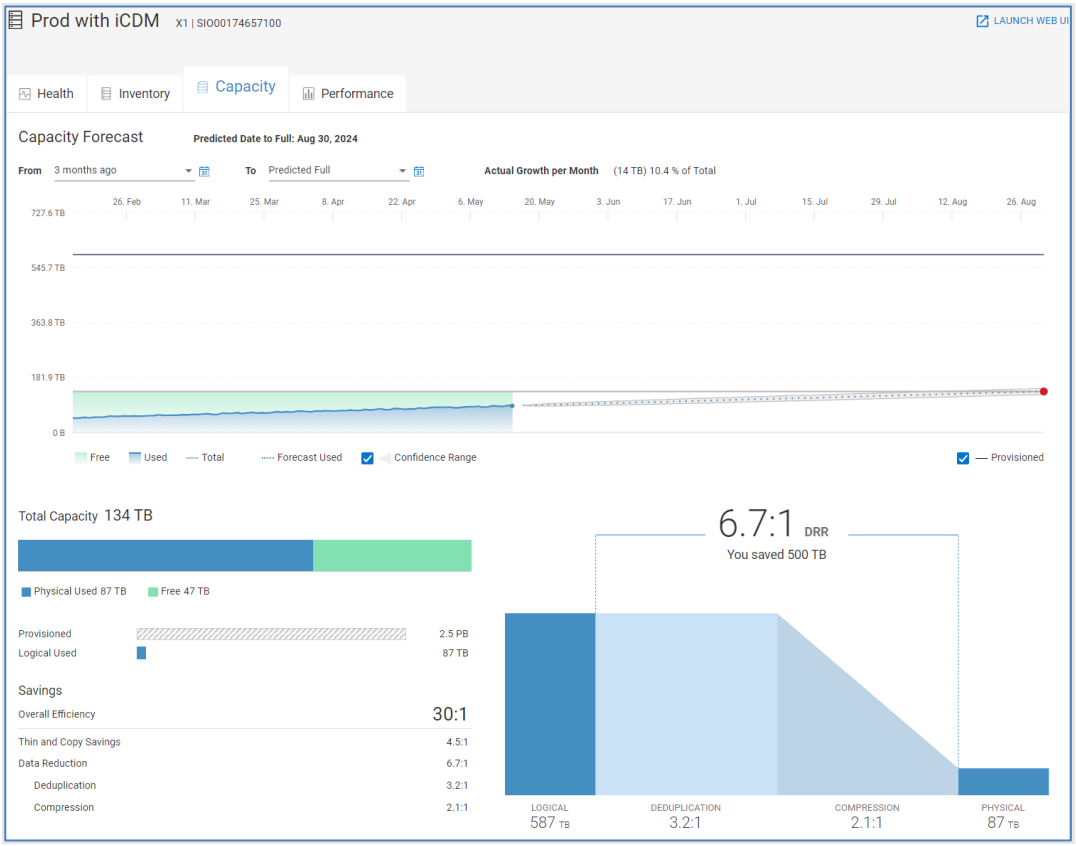
- LUNs (Unity XT family)
- Volumes (PowerStore, SC Series, and PowerVault)
- Thick Volumes (PowerFlex)
- Thin Volumes (PowerFlex)
- File Systems (Unity XT family and PowerStore)
- Virtual Hot Spares (PowerScale/Isilon and APEX File Storage for AWS)
- User data (PowerScale/Isilon and APEX File Storage for AWS)
- VMware (VMware datastores for Unity XT family and PowerStore)
- Snapshots

Drive Type Usage shows the drive types installed in the system, with configured and unconfigured capacity. Hovering over the rings will show the details related to that configuration.

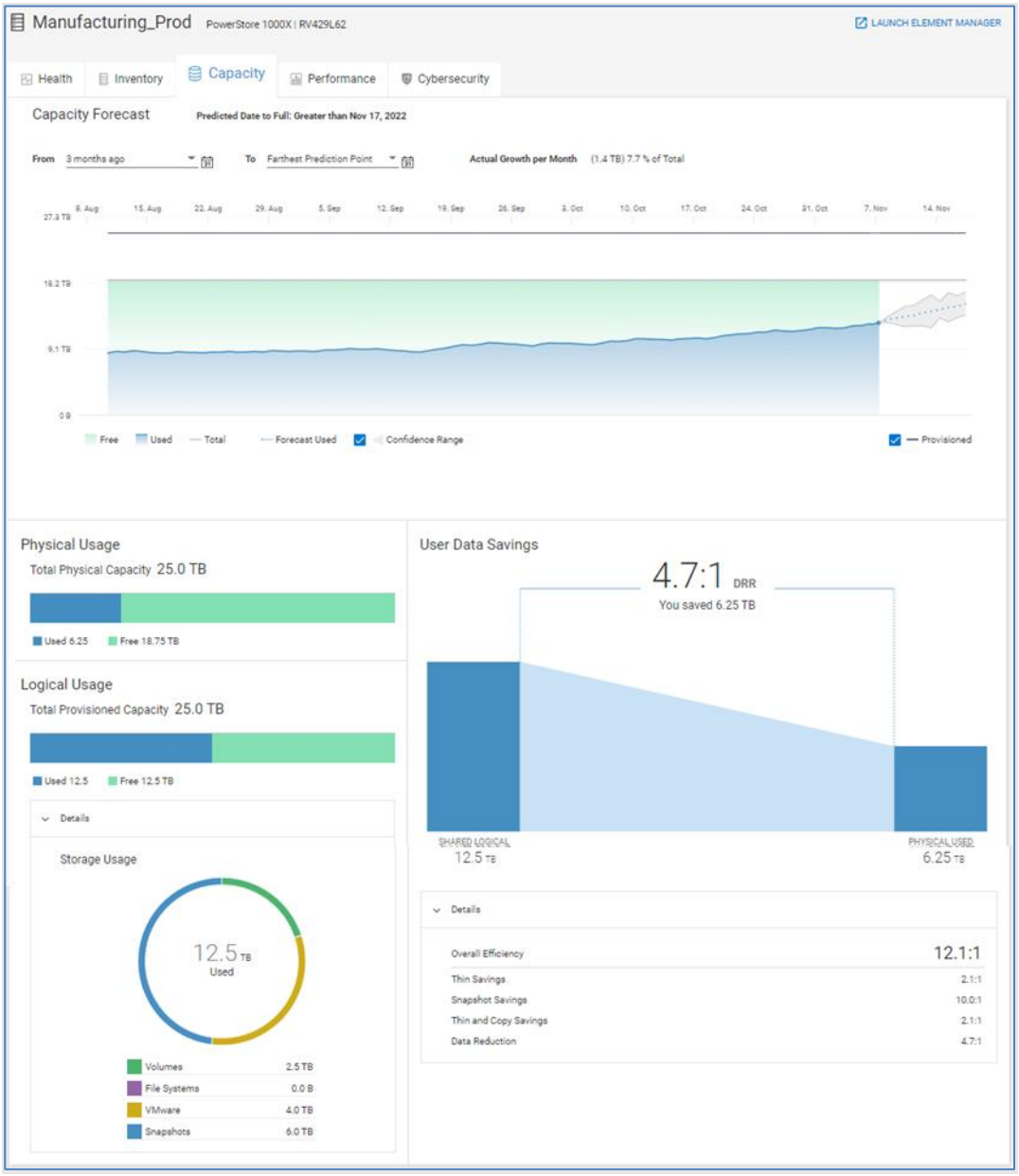
The **Pools** table lists the configured storage pools on the system. It includes the Free, Used, and Time to Full details for each pool. Selecting a pool name navigates the user to the Pool Details page.



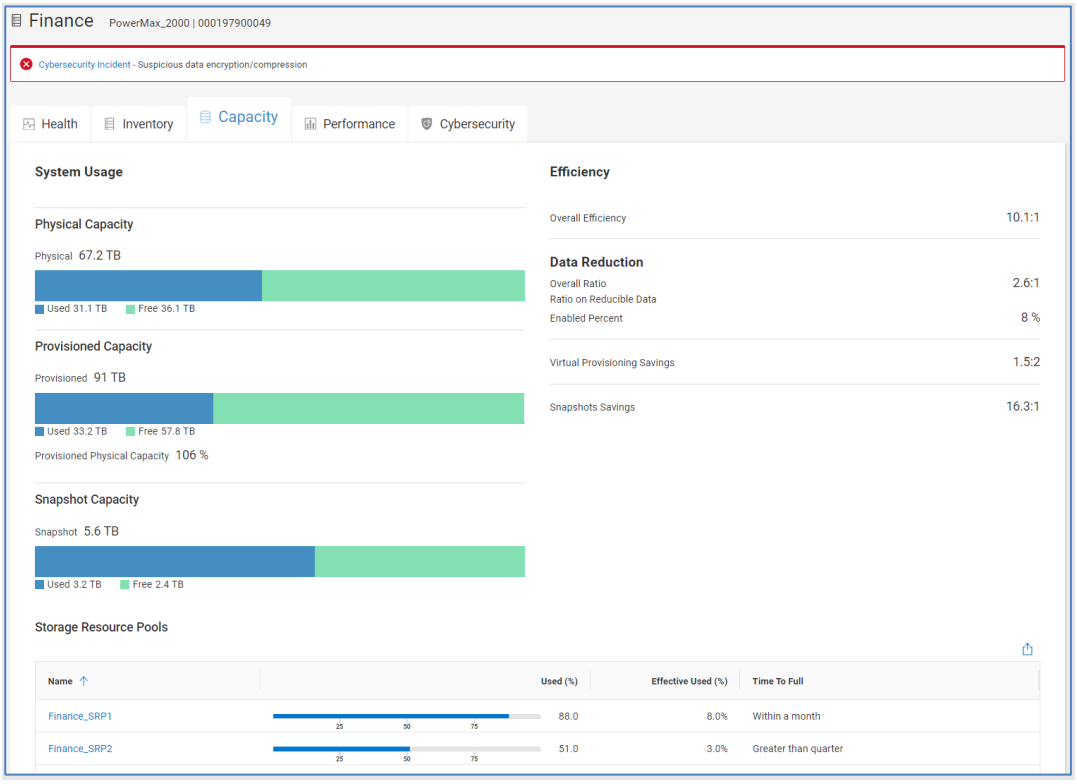
XtremIO systems show the Capacity Forecast chart on the top of the page. The bottom of the page shows the total capacity broken down by used and free along with a detailed data reduction chart.



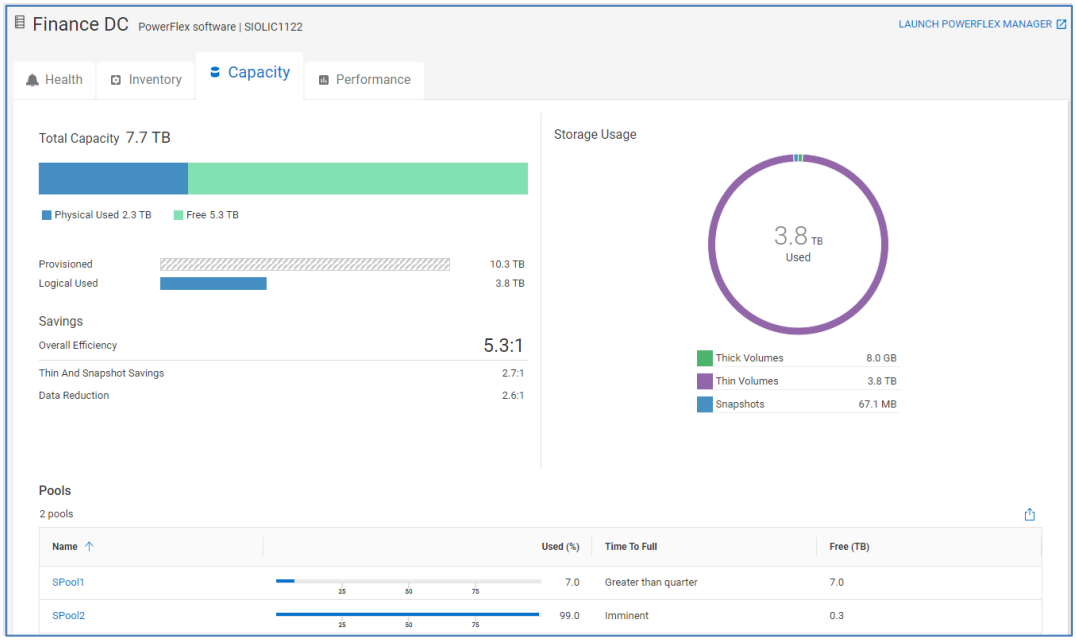
PowerStore systems provide the Capacity Forecast chart at the top of the page. The bottom of the page includes charts for physical and logical usage and the space savings due to data reduction.



PowerMax or VMAX systems display Used and Free capacities for Subscribed, Snapshot, and Usable storage as well as the storage efficiency ratios and the percent used per storage resource pool. PowerMax 2500 and 8500 displays effective capacity.

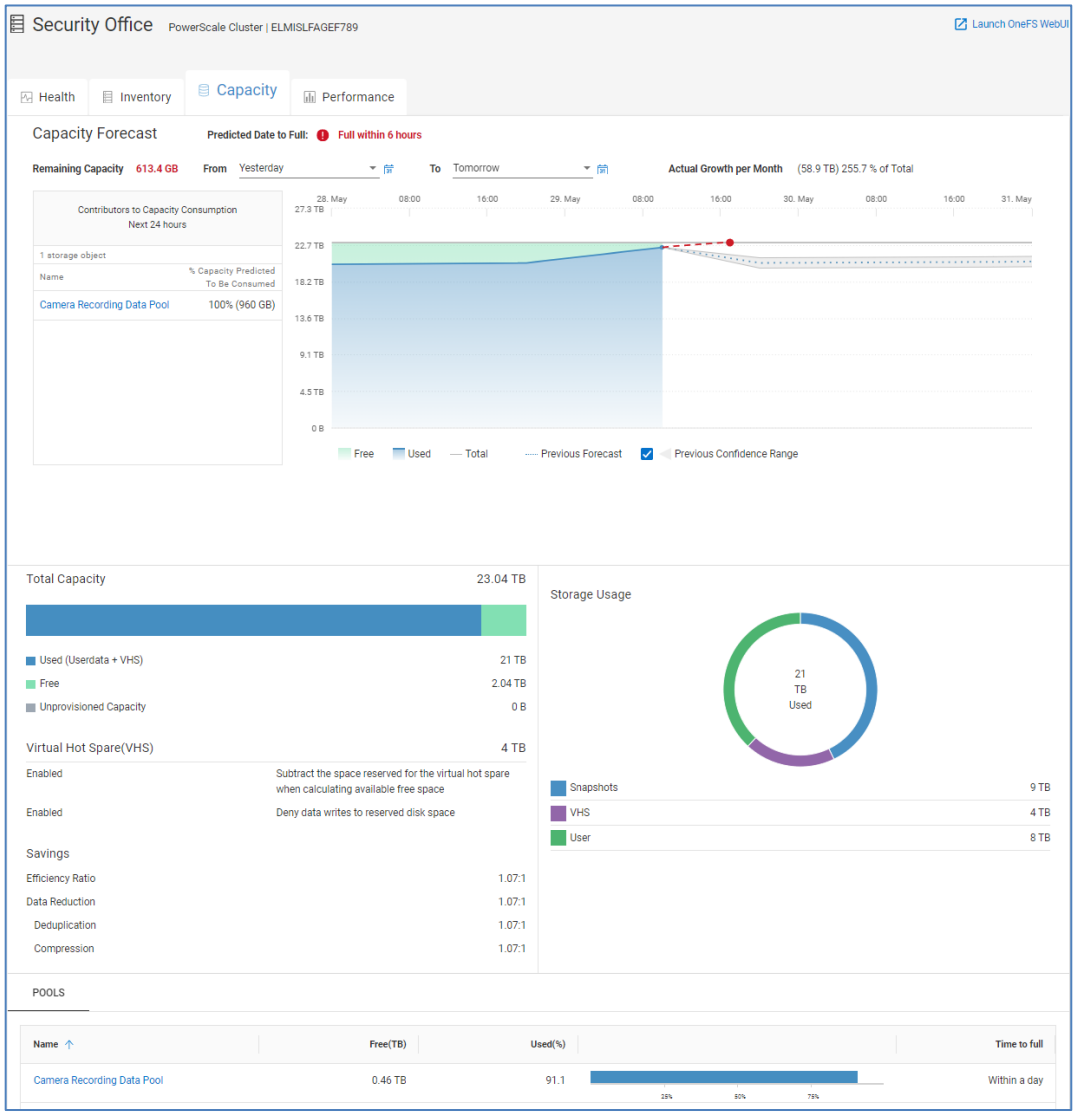


PowerFlex provides a breakdown of Total Capacity based on physical used and free. It also provides total provisioned and logical used charts and overall efficiency based on thin and snapshot savings and data reduction. The bottom of the page provides a listing of pools with used percentage, time to full, and free capacity.



PowerScale and APEX File Storage for AWS provides a capacity forecast chart at the top of the page. The bottom of the page breaks down total capacity by used, free, and

unprovisioned. Virtual hot spare (VHS), efficiency, and data reduction information is also provided. Used storage is broken down by snapshots, VHS, and user data.



Storage system details – Performance

The **Performance** tab is supported for all storage systems and APEX storage for AWS. It is similar to the Performance tab for Pools discussed earlier in this paper. The top portion of this tab is the Object Activity and it shows key performance metrics for storage objects sorted by their 24-hour averages. The result is that the user immediately sees the top contenders for resources on the system.

The following metrics are displayed with a 24-hour trend line and the 24-hour average. It is sorted to show objects with the highest averages over the last 24 hours allowing the user to immediately see the top contenders for resources on the system.

- Latency (PowerStore, PowerMax/VMAX, Unity XT family, XtremIO), Volume Latency (SC Series)
- IOPS (all platforms)

- Bandwidth (all platforms)

Note:

- For PowerMax or VMAX systems, Infrastructure Observability displays these performance metrics at the Storage Group level.
- For PowerStore, the Object Activity charts show data for File Systems and either Individual Volumes or Volume Groups.
- Top Object Activity is not displayed for PowerScale or Isilon, PowerFlex, or APEX Storage for AWS.

The remaining charts show a 24-hour history of key system level performance metrics with an overlay of historic seasonality. The metrics vary slightly by product type:

- Latency (all platforms except PowerVault)
- IOPS (all platforms)
- Backend IOPS (for Unity XT family - if multiple storage tiers exist, each tier has a separate chart)
- Bandwidth (all platforms)
- Storage Processor Utilization (Unity XT family) / Controller Utilization (SC Series) / CPU Utilization (XtremIO, PowerScale or Isilon, and APEX File Storage for AWS)
- Client (PowerScale or Isilon and APEX File Storage for AWS)
- Protocol: Latency (PowerScale or Isilon and APEX File Storage for AWS)
- Protocol: IOPS (PowerScale or Isilon and APEX File Storage for AWS)
- Protocol: Bandwidth (PowerScale or Isilon and APEX File Storage for AWS)

Note: For the Unity XT family, the system performance page has both a Past 24 Hours view and a Forecast view. Performance forecasting is only supported for the Unity XT family and is discussed below.

For additional performance metrics, the user can select the **Create Report** button in the upper right corner of the Object Activity window to access the Report Browser.

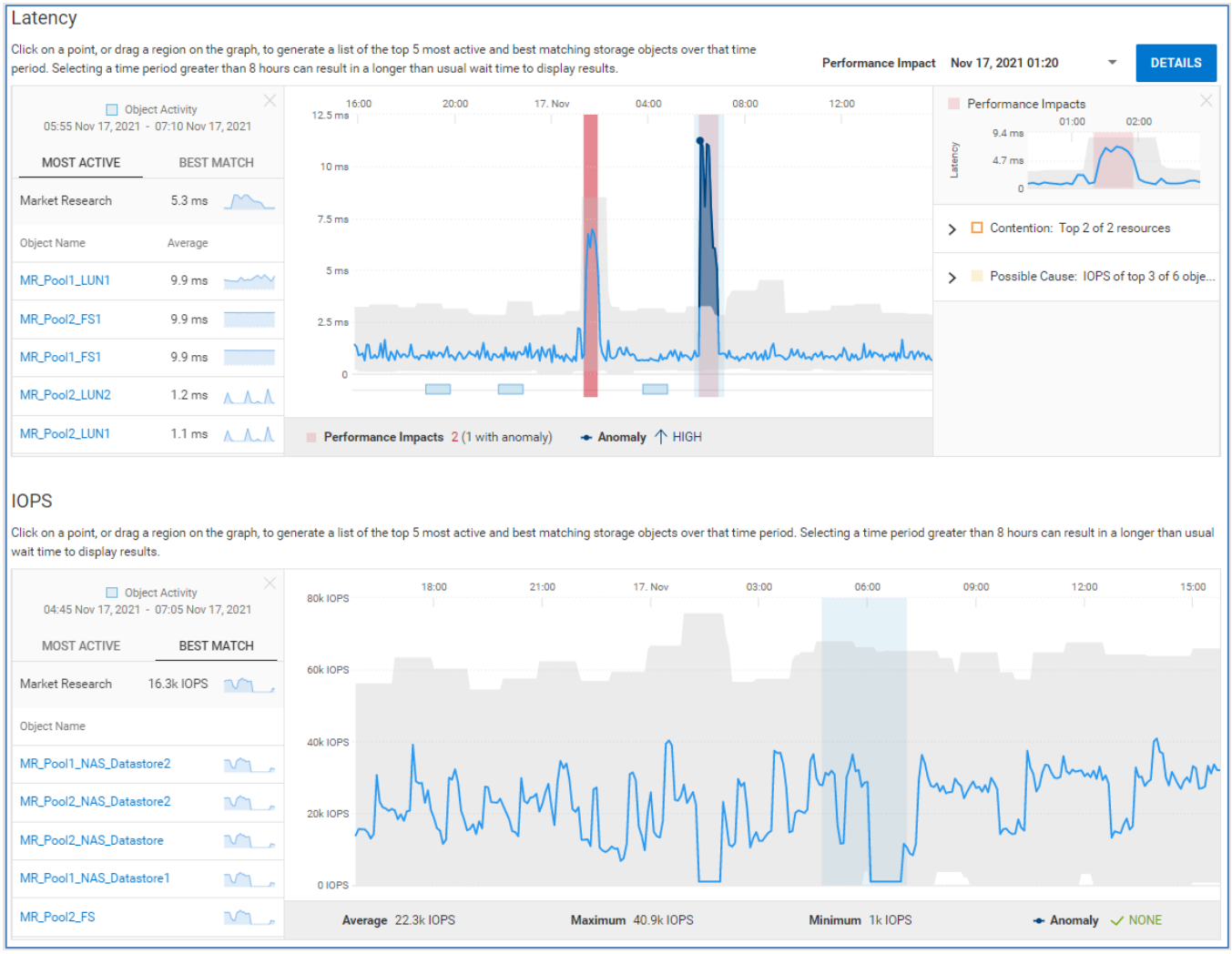
Observability identifies performance anomalies on all system level performance charts for all system types. A shaded blue area identifies performance anomalies. For Unity XT family, PowerStore, PowerMax, PowerScale, and PowerFlex systems, Observability identifies areas of performance impact on the Latency chart. A pink shaded area identifies performance impacts. Similar to the latency chart for Unity XT storage pools, the user can select the DETAILS button to see the most likely competing workloads causing the impact.

For APEX File Storage for AWS, Unity XT family, PowerStore, PowerScale, and PowerVault systems, configuration changes are identified as rectangles along the X-axis of the charts. Selecting the configuration change rectangle opens the Storage Configuration Changes window which contains details of the changes. By identifying when configuration changes occur, Observability helps the user potentially correlate configuration changes in the environment to performance impacts.

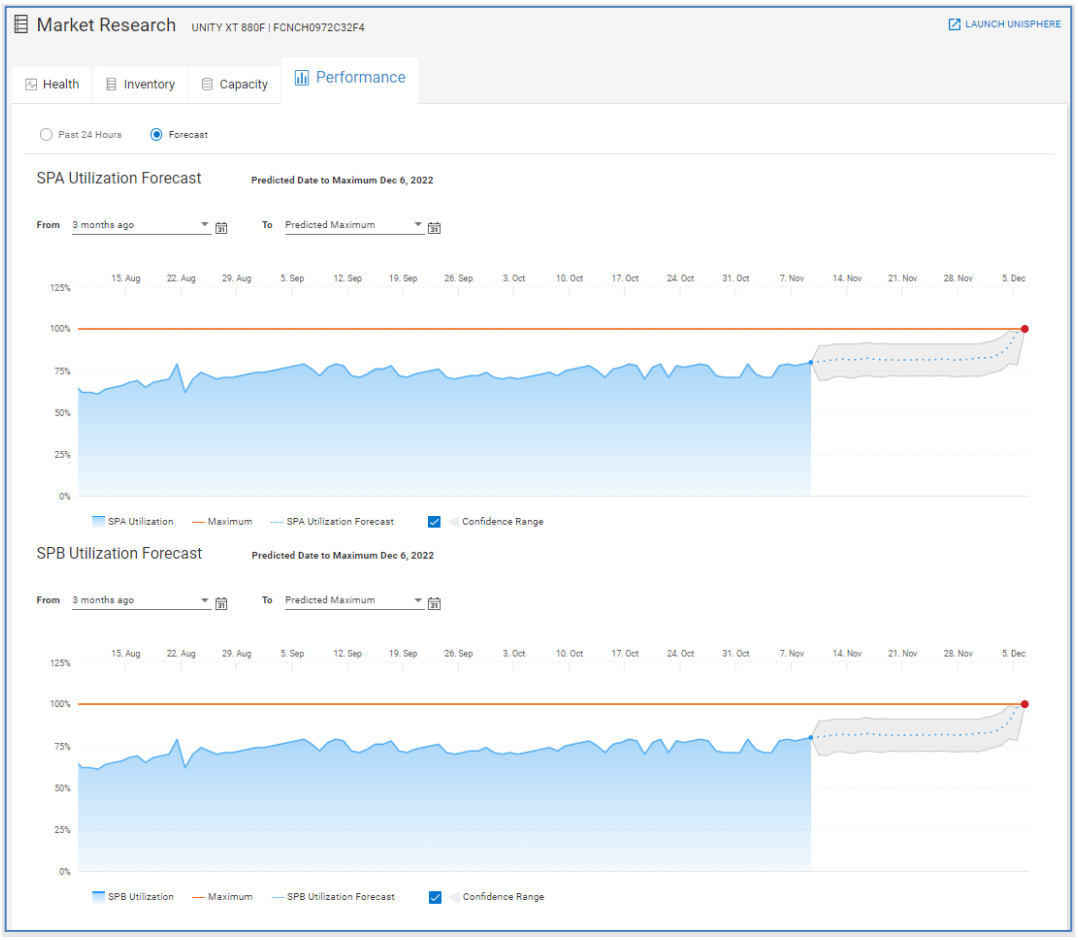
Selecting any area in the Latency, IOPS, and Bandwidth charts for any system type (except APEX Block Storage for AWS and PowerFlex) displays the top five most active storage objects during that time period in the left side of the chart. Objects would be LUNs or file systems for Unity XT family, volumes or file systems for PowerStore, volumes for SC Series, PowerVault and XtremIO, storage groups for PowerMax or VMAX, and nodes for PowerScale and APEX File Storage for AWS. In the example below, the area around the second impact with the performance anomaly is highlighted and it shows the most active objects in the left side of the screen. For PowerStore, Unity XT family, and PowerVault, Observability also provides the Best Match tab identifying objects whose performance characteristics most closely correlate to the selected range in the performance chart. The Best Match tab is shown in the IOPS chart below.

As with Pools performance, the user can select the Details button and see possible causes and resource contention for performance impact.

Note: Resource contention is supported for Unity XT family systems only.



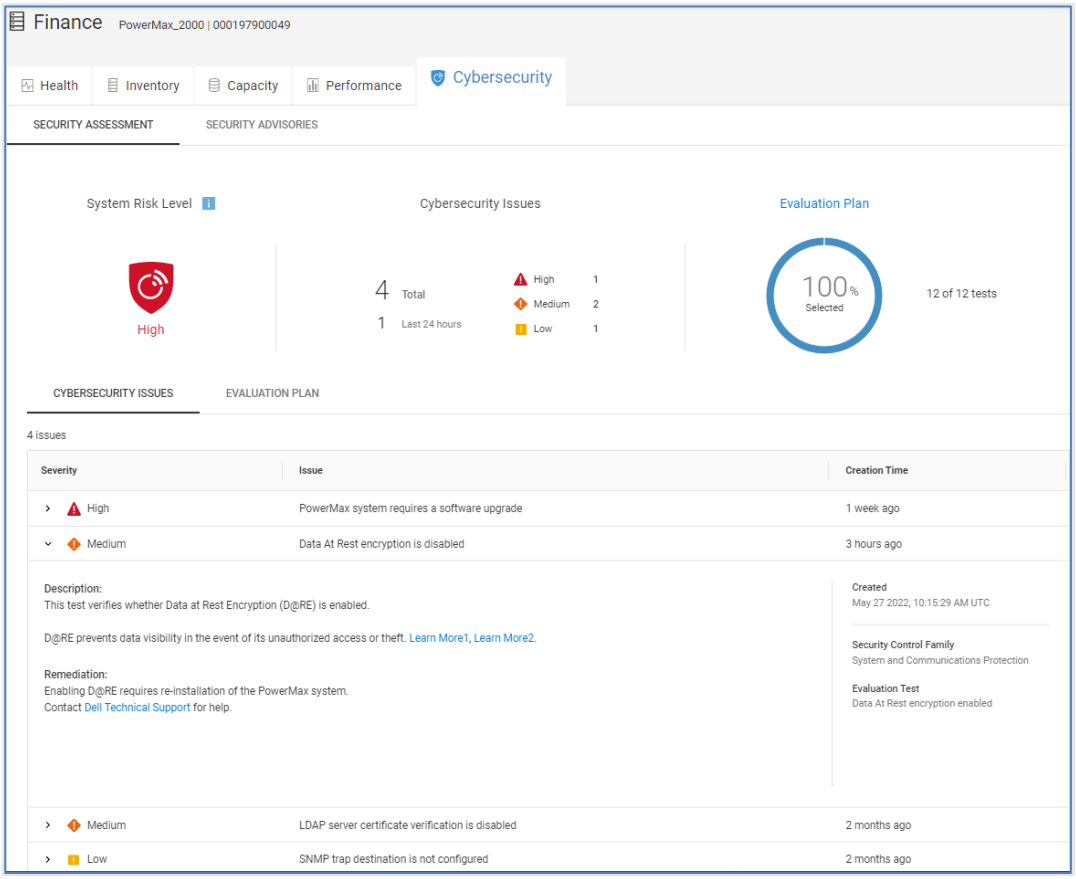
The Unity XT family supports performance forecasting charts. By selecting the **Forecast** radio button, users can see SP Utilization historical trends and forecasting along with predicted date to reach maximum. This allows users to properly balance and plan future workload requirements.



Storage system details – Cybersecurity

The **Cybersecurity** tab is available for systems that have Cybersecurity enabled. Cybersecurity is supported for PowerMax, PowerStore, PowerEdge, and PowerProtect DD systems, and will continue to expand coverage to other Dell assets. The top of the page shows information provided in the multisystem view: The System Risk Level, the summary of active issues, and the percentage of enabled tests in the Evaluation Plan. The bottom of the page has two tabs: Cybersecurity Issues and Evaluation Plan.

The **Cybersecurity Issues** tab lists all active issues identified on this system. Expanding each issue provides a detailed issue description and the recommended remediation. Users can also see the time the issue was created, the security control family (defined by NIST 800-53 R5), and the name of the evaluation test.

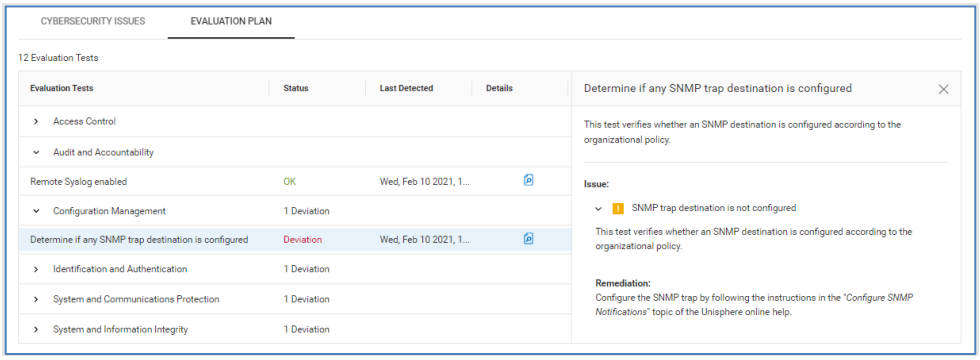


The **Evaluation Plan** tab lists all possible tests for this system type. The evaluation tests are grouped into Security Control Families. Each family can be expanded to show the individual tests that make up the group and one of the following statuses for each test:

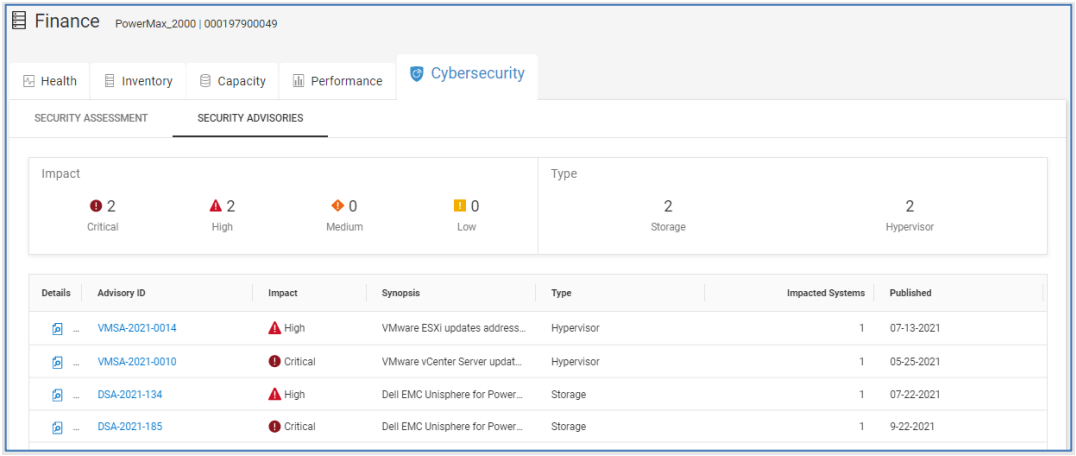
- OK – Test is enabled and no issues identified.
- Deviation – Test is enabled and an active issue exists.
- Not In Plan – Test is not enabled.
- Not Applicable – Test is for a capability that depends on another capability that is disabled.
- Not Supported – Test is not supported for the system version.
- Not Evaluated – Test is for a system where the Evaluation Plan is disabled, or the test has not yet been run.

When an active issue exists, the Last Detected Column shows the first time the issue was detected. When an issue does not exist, it shows the last time this data was changed (as reported by the system).

There is a details icon which shows the details of each test. In instances where there is a deviation, it will also show the recommended remediation.



The **Security Advisories** tab provides information about the applicable Dell Security Advisories that impact this system.



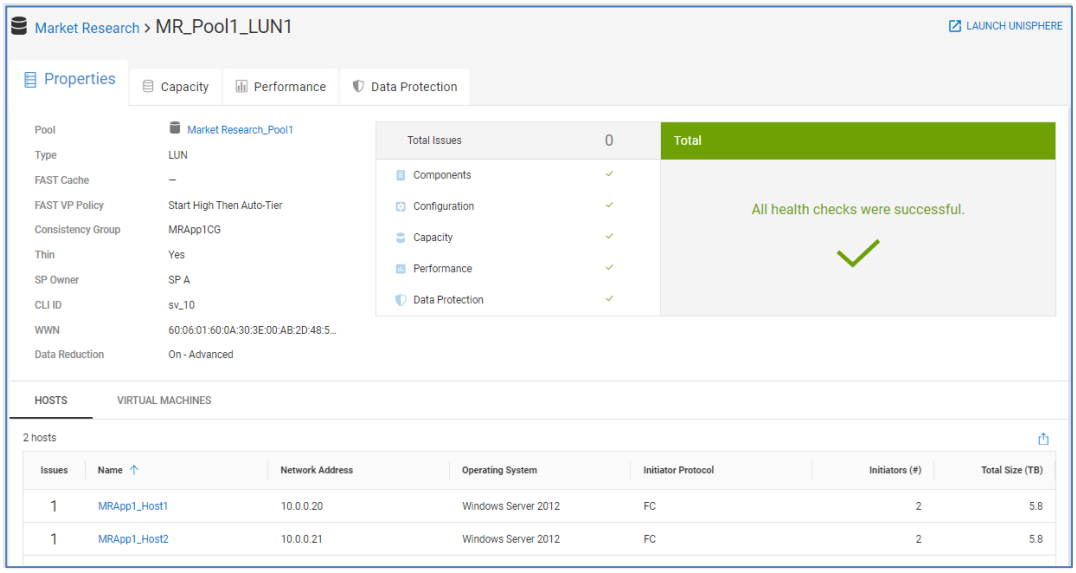
Block object details

Introduction

Block objects include LUNs for Unity XT family systems and volumes for PowerStore, SC Series, XtremIO, PowerFlex, and PowerVault. They can be accessed from the Storage listing for individual systems and pools and can also be found using global search. PowerFlex and APEX Block Storage for AWS volumes are accessed from the Volumes view under the Block tab.

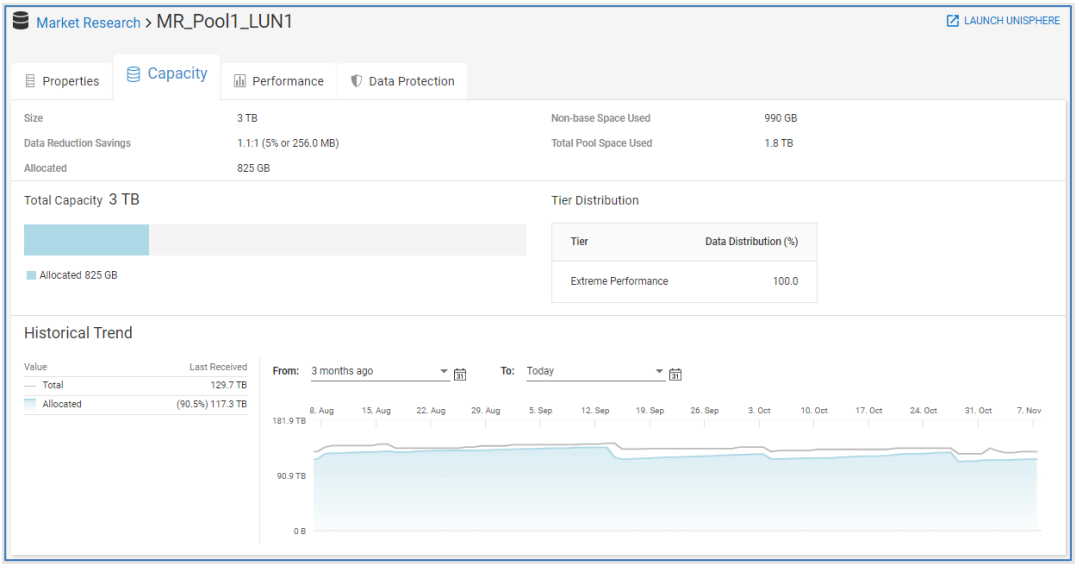
Block object details – Properties

The **Properties** tab for a block object displays attributes for the object and any health issues associated with this object. The bottom of the page varies slightly depending on storage type. It displays the Hosts (for Unity XT family, PowerStore, PowerFlex, and XtremIO systems), Servers (for SC Series), or Initiators (for PowerVault) associated to the object. The Virtual Machines tab lists information for VMs residing on the object and is available for Unity XT family, SC Series, and XtremIO objects. The Consistency Groups tab is available for XtremIO volumes listing consistency group information to which the volume belongs. The VTree tab lists the volume trees for PowerFlex along with the type, provisioned and used space, and creation time. PowerFlex block objects also have a Snapshots tab that lists each snapshot, size, creation time, parent ID, and VTree ID.

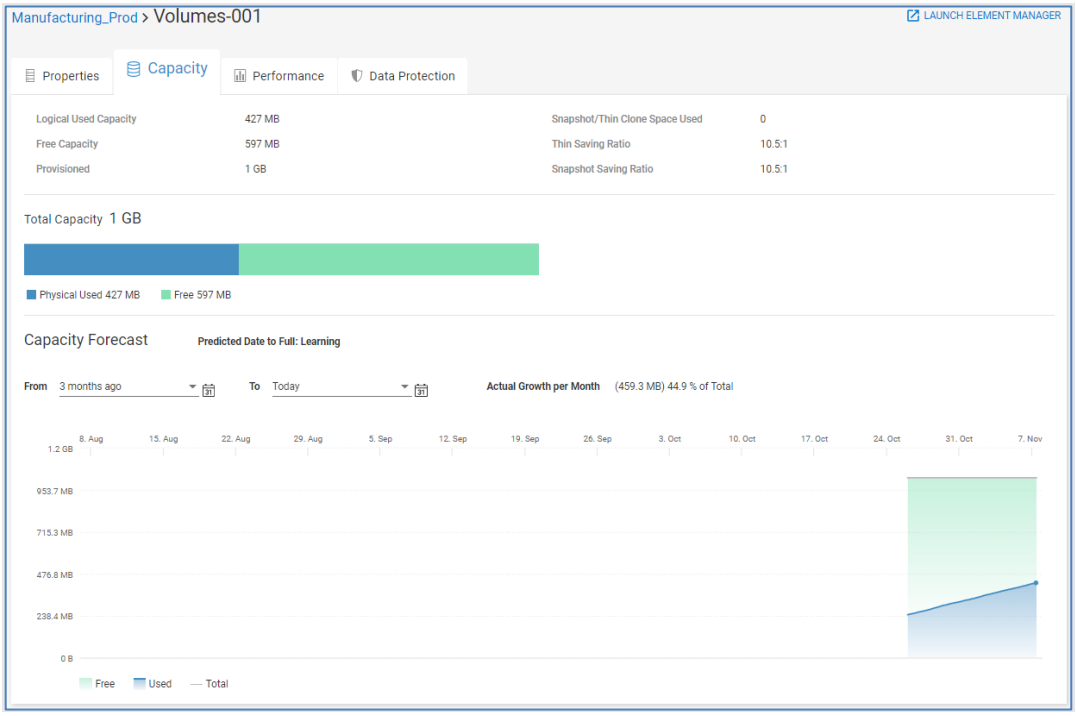


Block object details – Capacity

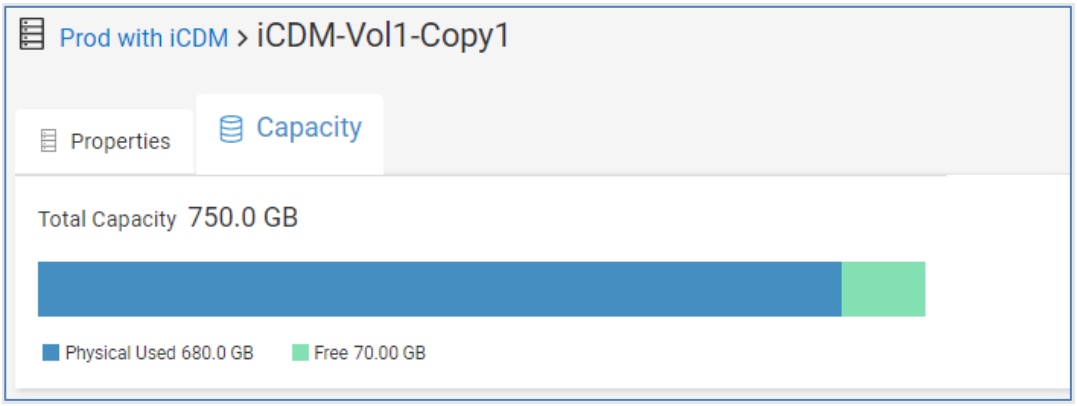
The **Capacity** tab for Unity XT family, SC Series, and PowerVault block objects provides details for the capacity being used including Data Reduction savings and capacity utilization by Snapshots. The Historical Trend shows the capacity changes over time helping users identify increasing trends to anticipate future capacity usage.



The Capacity tab for a PowerStore volume provides provisioned, logical used, physical used, and free capacities along with a capacity trend and forecast.



The Capacity tab for an XtremIO volume does not support the historical trend. Volume Size, Physical Used, and Free metrics are graphed as shown below.

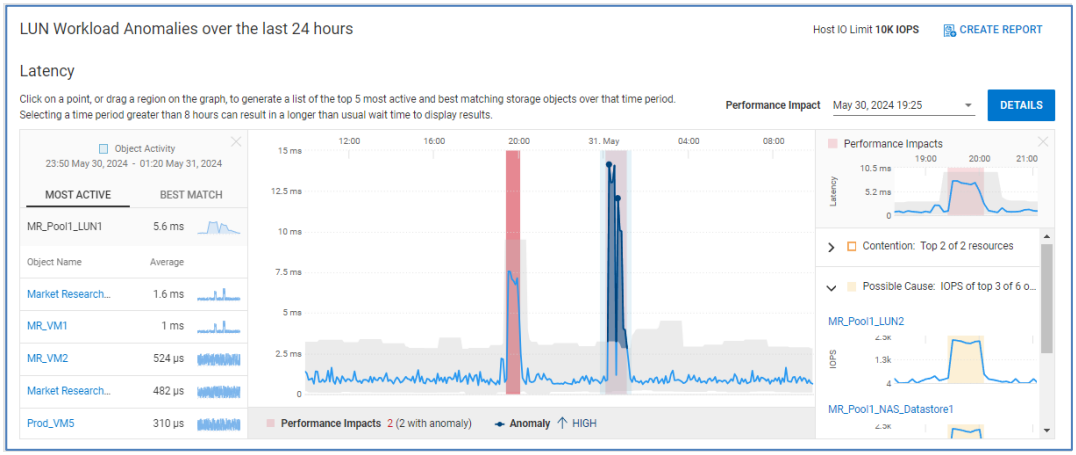


Block object details – Performance

The **Performance** tab for block objects (PowerStore, Unity XT family, SC Series, and PowerVault) provides performance details for the block object activity. Similar to the system and pool level performance charts, Observability identifies performance anomalies for each performance metric. For Unity XT family systems and PowerStore, Observability also identifies performance impacts at the object level.

Highlighting an area in the performance charts for a block object identifies up to the five most active virtual machines contributing to the metric during that time period. Unity XT family systems and PowerStore have the additional feature of providing the virtual machines that most closely correlate to the behavior in the selected time range. This correlation is shown under the Best Match tab.

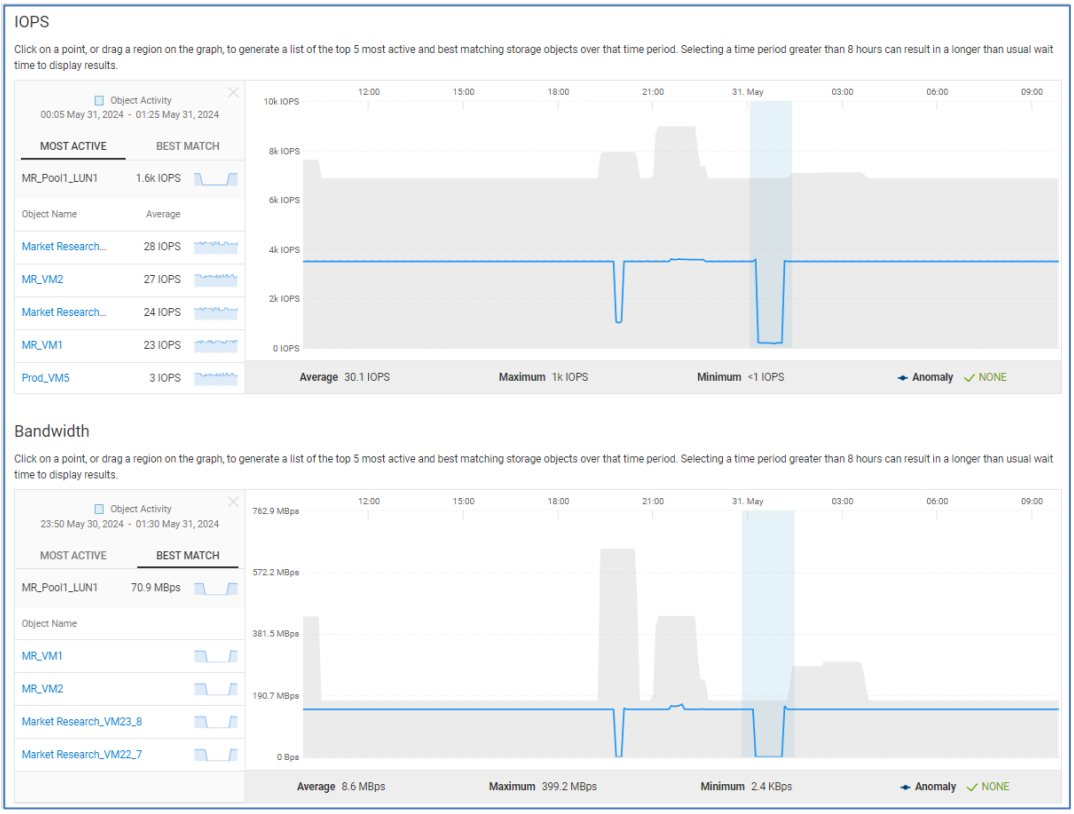
The following shows two performance impacts on a Unity XT block latency chart. The first is an impact only, the second is an impact with a performance anomaly. Selecting the Details button opens a window in the right side of the chart identifying storage objects whose IOPS are correlated with the rise in latency for the impacted LUN. These objects are the most likely candidates causing workload contention and the performance impact. Observability also identifies if there is possible resource contention for Unity XT LUNs experiencing a performance impact.



The bottom of the page displays LUN or Volume performance charts for the following metrics:

- Latency (Unity XT family and SC Series)
- IOPS (all)
- Bandwidth (all)
- % Read (Unity XT family and PowerVault)
- IO Size (Unity XT family, PowerStore, and PowerVault)
- Queue Length (Unity XT family)
- Queue Depth (PowerStore)

In the following screenshot, a region of the IOPS chart is highlighted. The left side of the chart displays the **Most Active** tab which displays the most active virtual machines contributing to the metric during that time period. In the Bandwidth chart, the **Best Match** tab is selected which identifies the VM whose bandwidth most closely correlates to the metric during the selected time period.

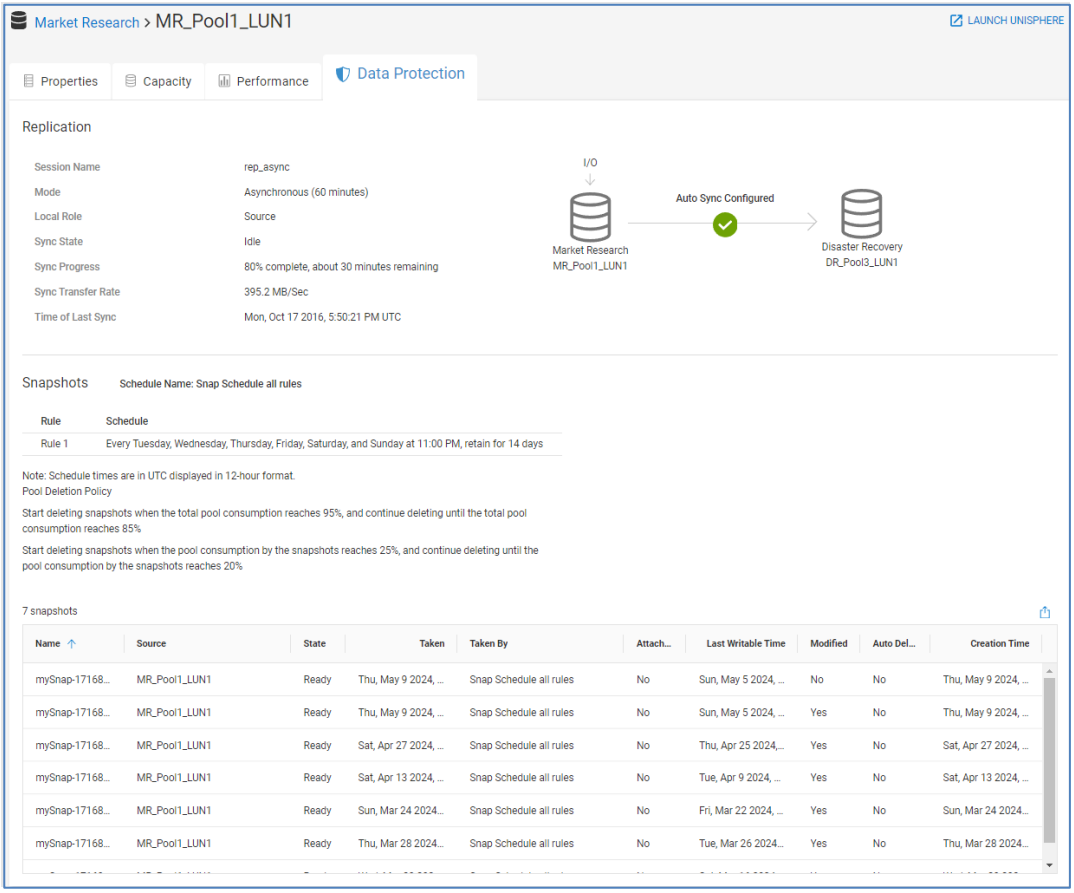


Block object details – Data Protection

The **Data Protection** tab for PowerStore, Unity XT family, and SC Series block objects displays how data protection has been configured for the selected object. There are two levels of data protection available:

- Replication – remote protection from system to system
- Snapshots – local protection within the system

The Replication section on the top of the page shows replication details and status of the replication session. The Snapshots section at the bottom half of the page shows how data is backed up within the system using snapshot technology. Snapshot schedules and deletion policies are displayed. The snapshot list can be exported to a CSV file.



File object details

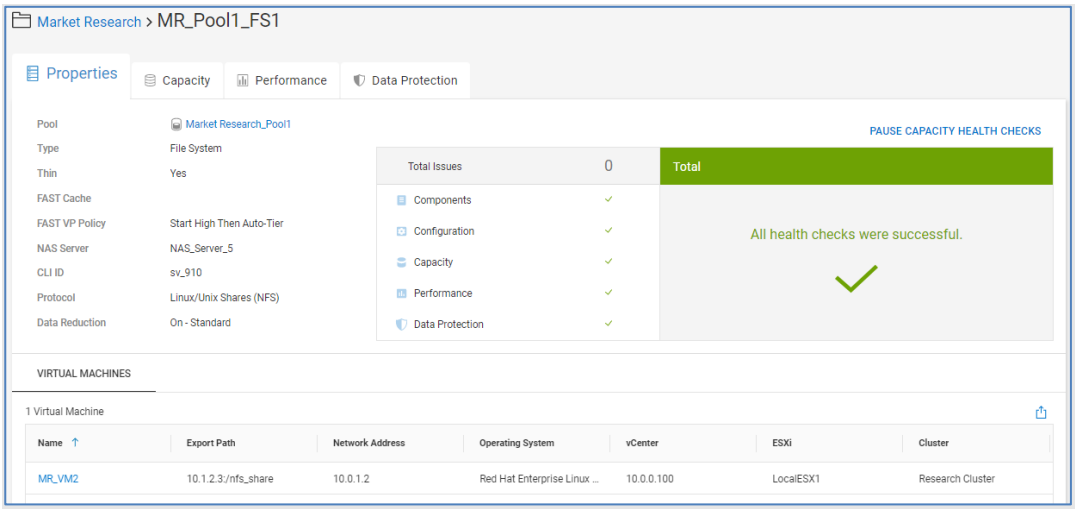
Introduction

File Objects (PowerStore and Unity XT family systems) are accessible in the Storage listing for individual Systems and Pools. File objects can also be accessed using global search.

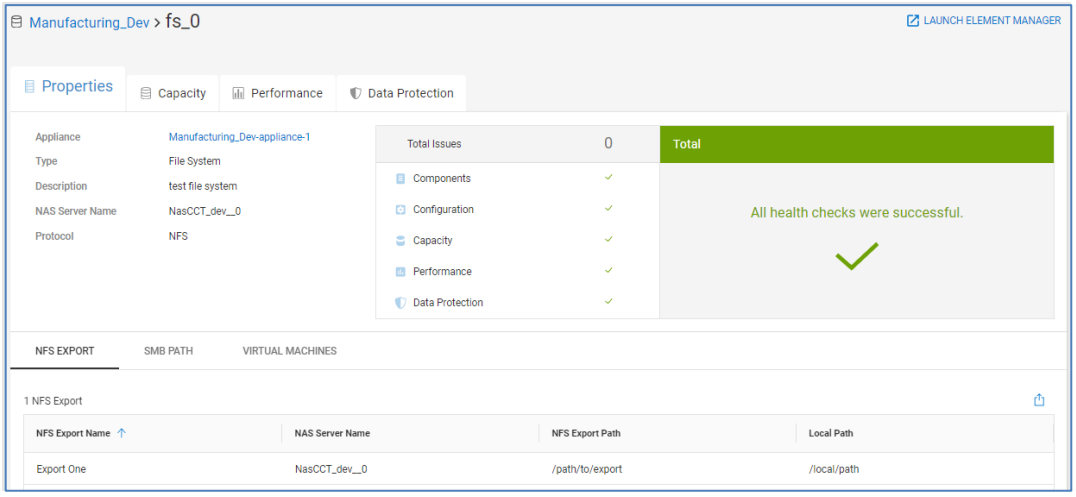
File object details – Properties

The **Properties** tab displays various attributes for the file object and any health issues found for the object. Attributes for Unity XT file objects include the Pool, FAST VP Policy, NAS Server, Protocol, and Data Reduction status. It also allows users to pause the capacity health check for the file system. This can also be accomplished from the Customization menu under Admin. See Infrastructure Observability administration for more details.

The bottom half of the view shows any virtual machines that reside on the file object.



Attributes for PowerStore file objects include description, NAS server, and protocol. The bottom half of the page provides information for NFS export or the SMB path.

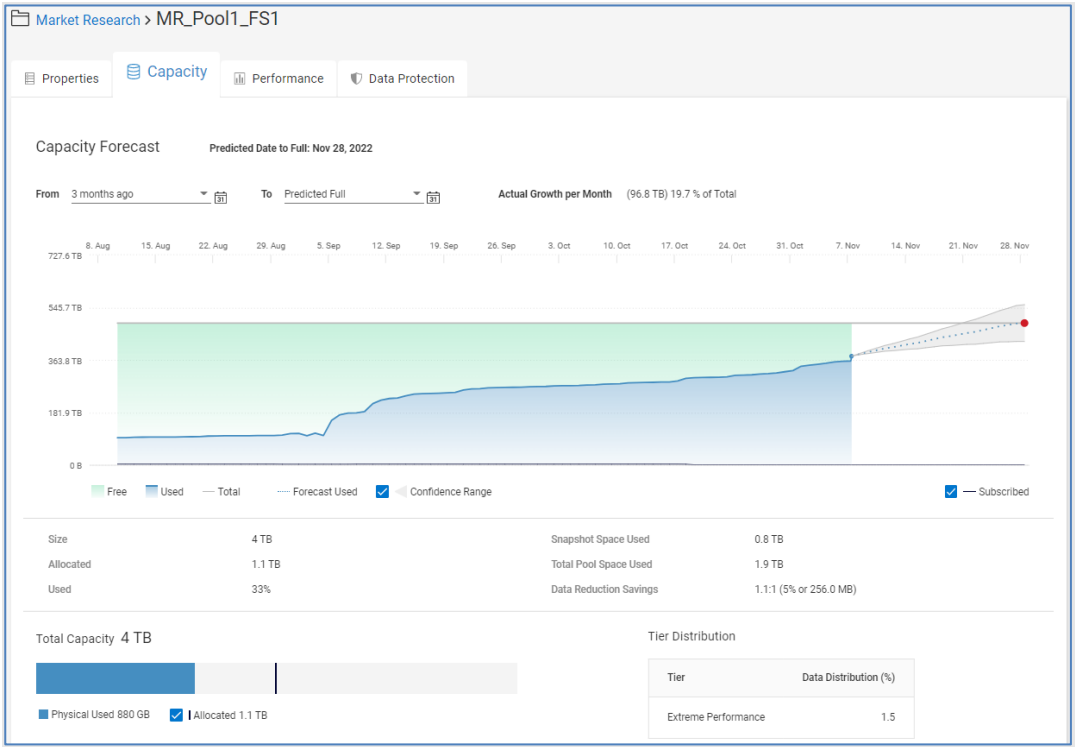


File object details – Capacity

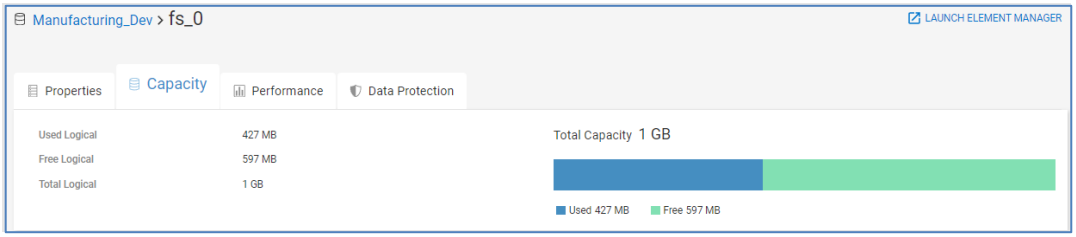
The **Capacity** tab for a Unity XT file object provides details for how the file capacity is being used, including capacity utilization for snapshots and Data Reduction Savings. The percentage used is based on the actual data written to the file system.

The Capacity Forecast shows a historical trend and capacity changes since the object was created. Observability's predictive analytics algorithms are applied to provide ongoing predictions as to when the file system will become full.

Hovering across the trend line displays the total, used, and free values for that selected point in time.



The Capacity tab for a PowerStore file object provides total, used, and free logical capacity metrics.



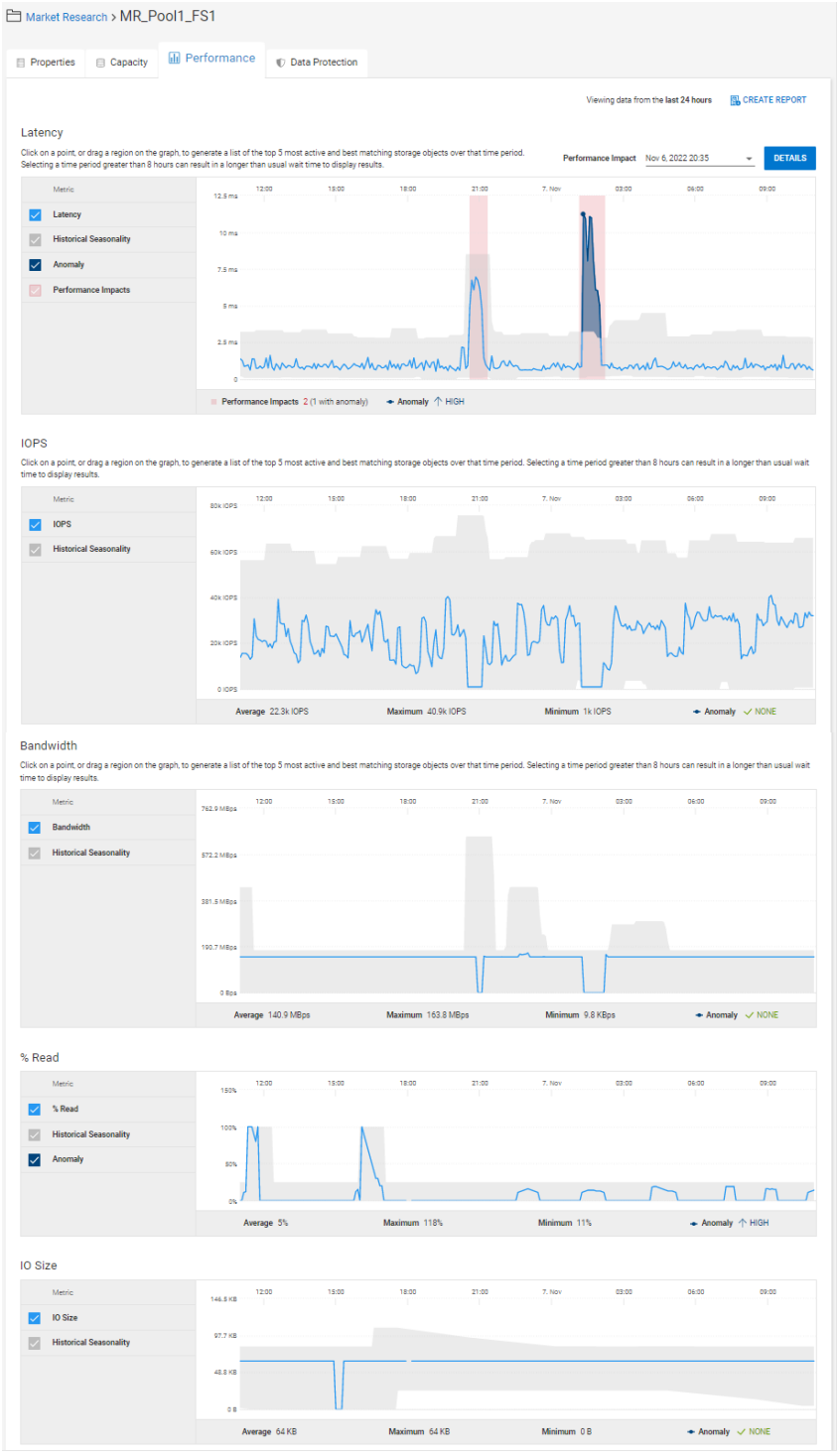
File object details – Performance

The Performance tab provides 24-hour performance charts for the following metrics for both Unity XT and PowerStore with the noted exceptions:

- Latency
- IOPS
- Bandwidth
- %Read (Unity XT only)
- IO Size
- Queue Length (Unity XT only)

Performance impact analysis is supported and identified as pink shaded areas on the Latency chart. Performance anomalies are supported for each of these metrics.

Note: Latency and Queue Length metrics are available for Unity XT v5.0 and higher.

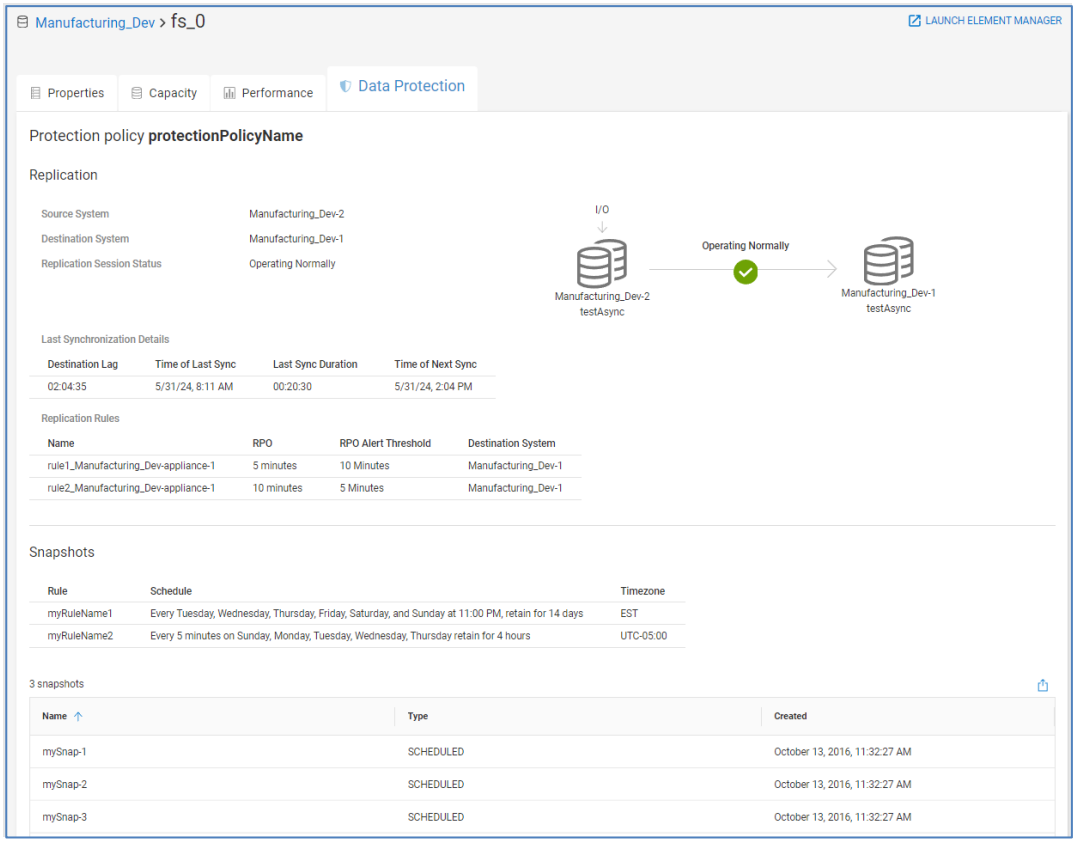


File object details – Data Protection

The **Data Protection** tab displays how data protection has been configured for that object. There are two levels of data protection available:

- Replication – remote protection from system to system
- Snapshots – local protection within the system

The Replication section on the top of the page shows remote replication details and status of the replication session. The Snapshots section at the bottom half of the page shows how data is backed up within the system using snapshot technology. Snapshot schedules are also displayed. The snapshot list can be exported to a CSV file.



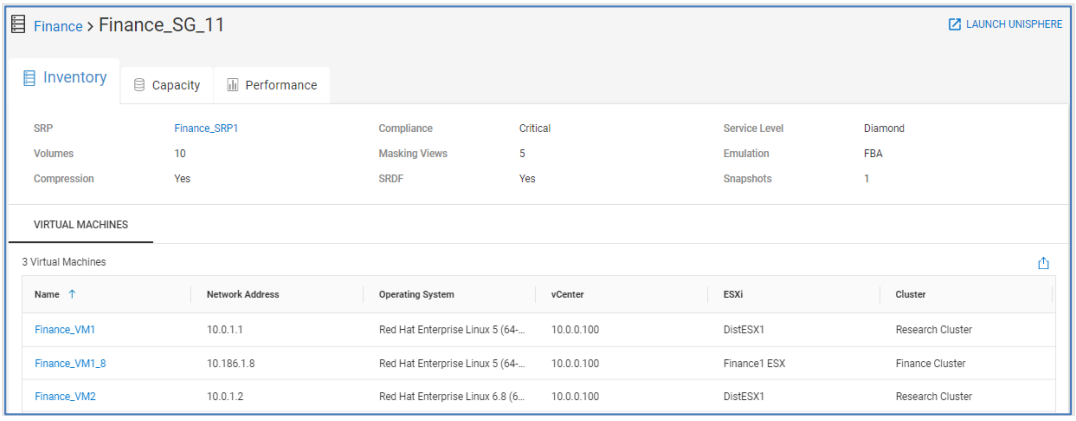
Storage Group Details (PowerMax/VMAX systems)

Introduction

Each PowerMax/VMAX system lists the storage groups with key information including the associated Storage Resource Pool, the assigned Service Level and whether the Storage Group is in compliance. The storage group name is hyperlinked to enable easy navigation to the details pages for a given storage group. The Storage Group Details Page is also accessible using global search of the storage group name.

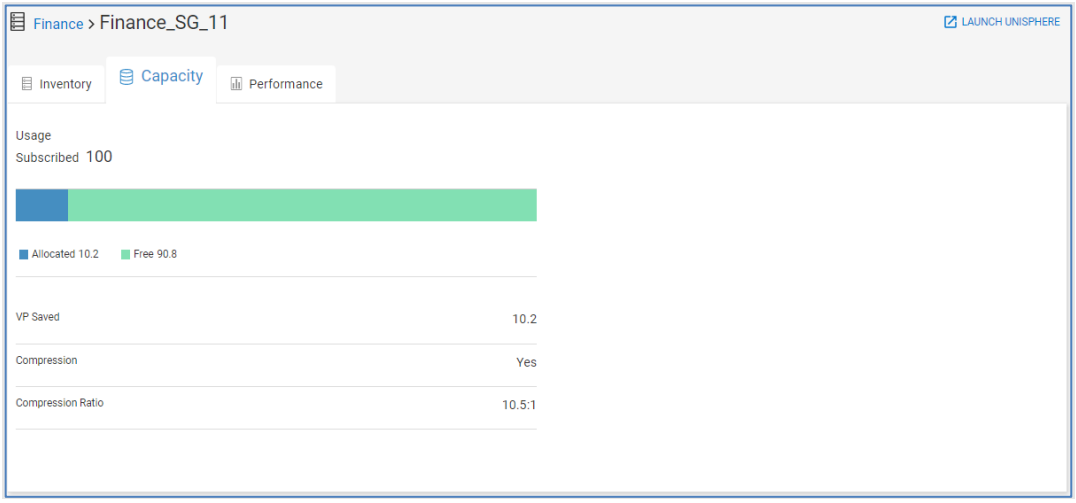
Storage group details – Inventory

The **Inventory** tab for a storage group displays the attributes of the storage group. In the upper right is a link to “Launch Unisphere.” Selecting this link opens the Unisphere element manager for the system hosting this storage group.



Storage group details – Capacity

The **Capacity** tab for a Storage Group provides details for the Storage Group capacity, showing Used and Free Allocation. Also, Storage Efficiency information is provided, including virtual provisioning (VP) savings and the compression ratio.



Storage group details – Performance

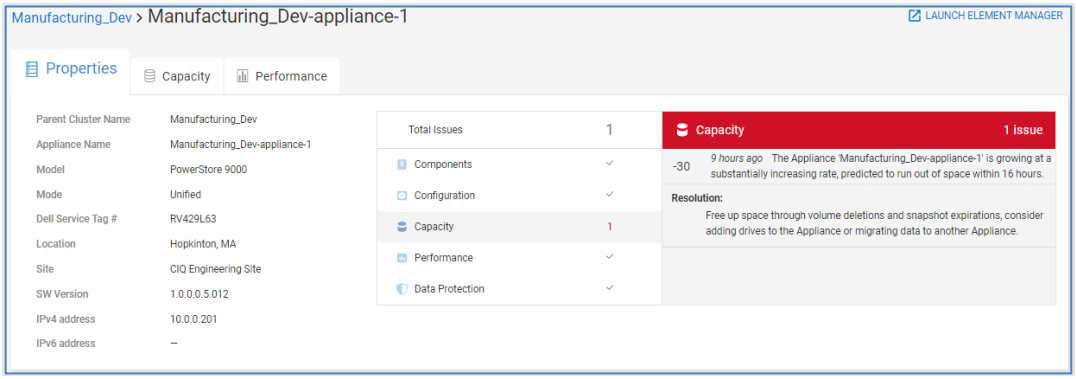
The **Performance** tab for a Storage Group provides performance details over a 24-hour period. Performance charts include Latency, IOPS, Bandwidth, %Read, IO Size, and Queue Length. Observability identifies performance impacts on the Latency chart as pink-shaded areas. Observability identifies performance anomalies on all storage group performance charts as blue-shaded areas. A sample of charts is shown below.

PowerStore appliance details

PowerStore appliance details are accessible by selecting the appliance name hyperlink from the Appliances tab on the PowerStore cluster system details page.

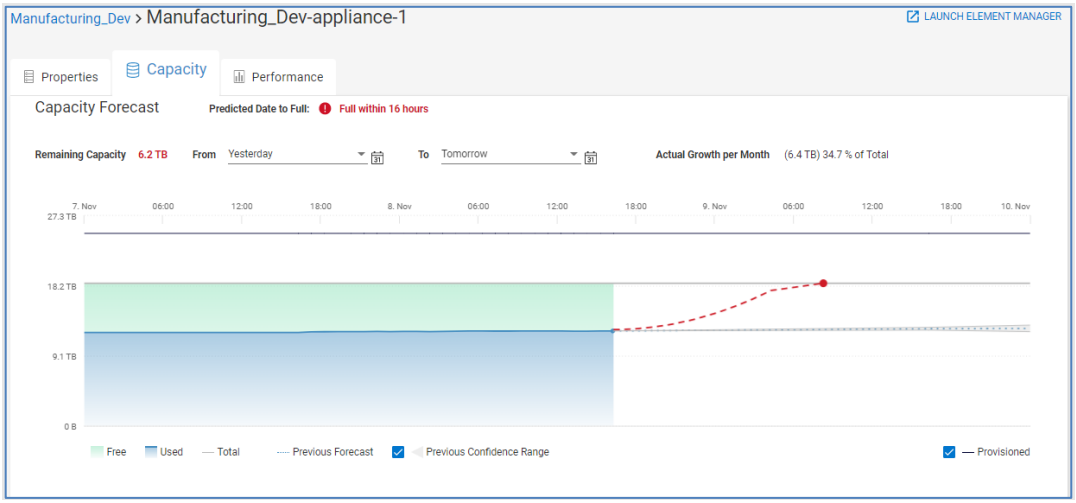
Appliance details - Properties

The **Properties** tab provides general attributes for the PowerStore appliance and any health issues and corresponding remediation. Attributes include the parent cluster name, model, mode, service tag, site and location, version, and IP address.

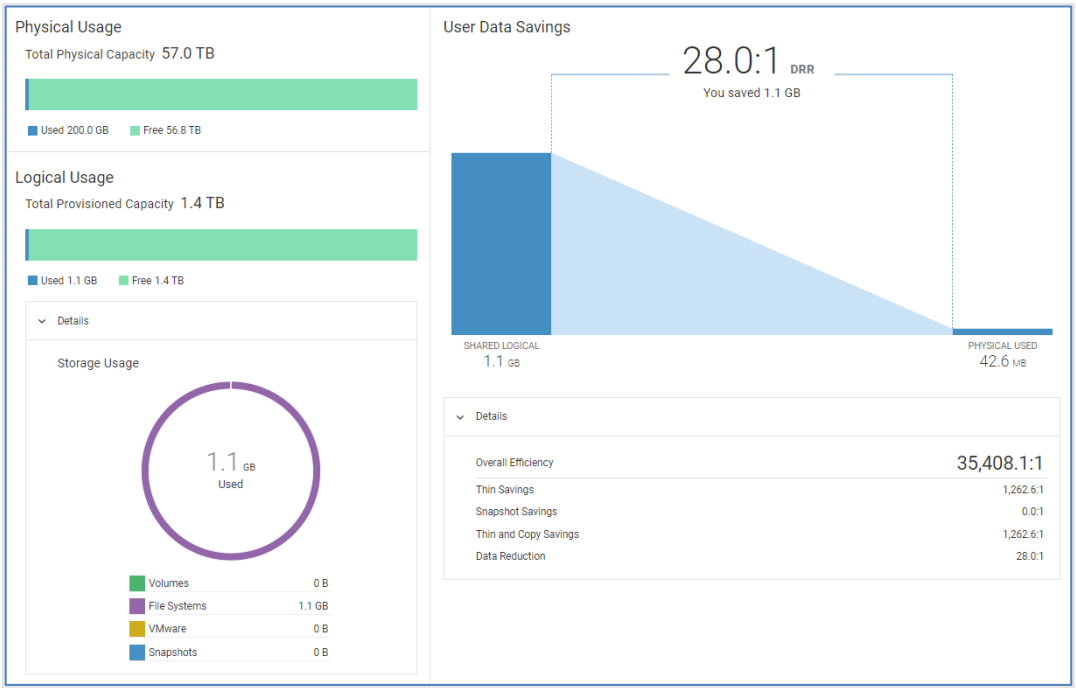


Appliance details - Capacity

The **Capacity** tab displays similar information as to what is provided in the PowerStore cluster capacity tab. The top of the page provides the capacity trend and forecast.

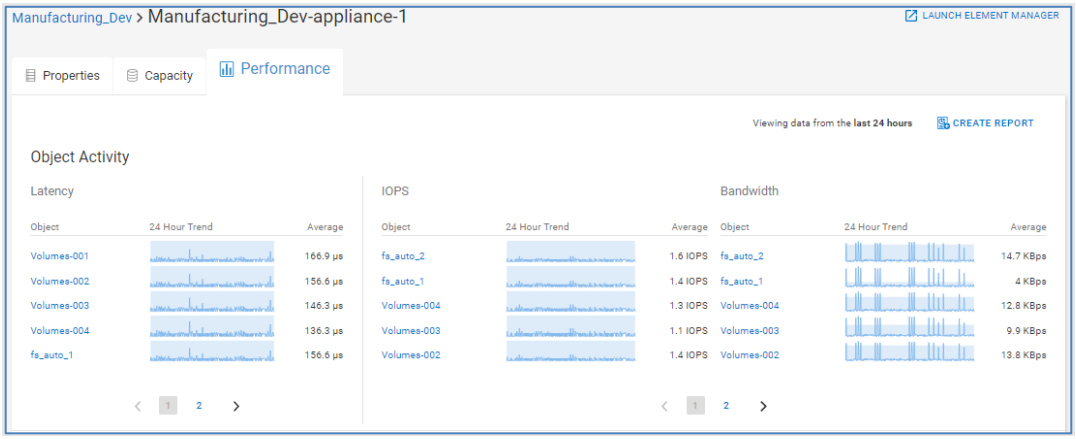


The bottom of the page provides summaries of physical and logical capacity utilization, the Storage Usage chart, and storage efficiencies and savings due to data reduction.

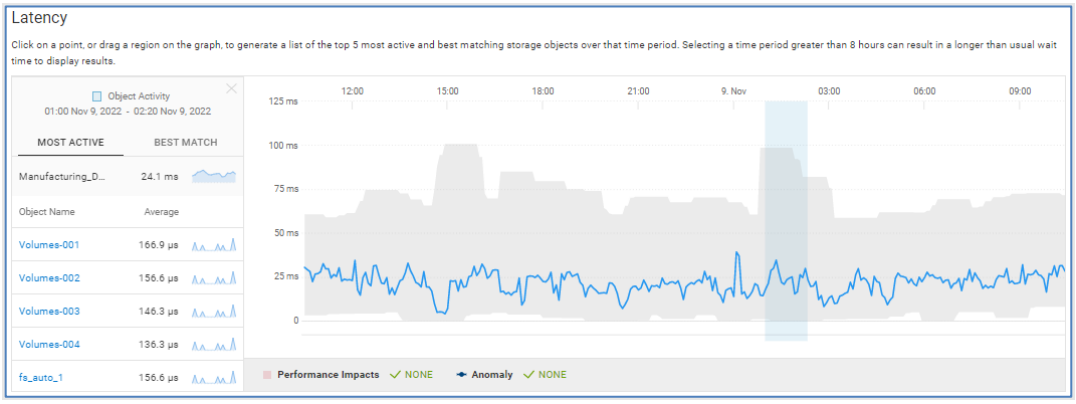


Appliance details – Performance

The **Performance** tab is similar to the performance tab for PowerStore clusters. The top of the page lists the top object activity charts for Latency, IOPS, and Bandwidth.



The remaining page displays 24-hour charts for these metrics and supports both performance anomalies and performance impacts. These charts are selectable to provide the top objects during the selected time range. The Best Match identification identifying the objects with the most closely matching performance shape is also supported. An example of the Latency chart is shown below.

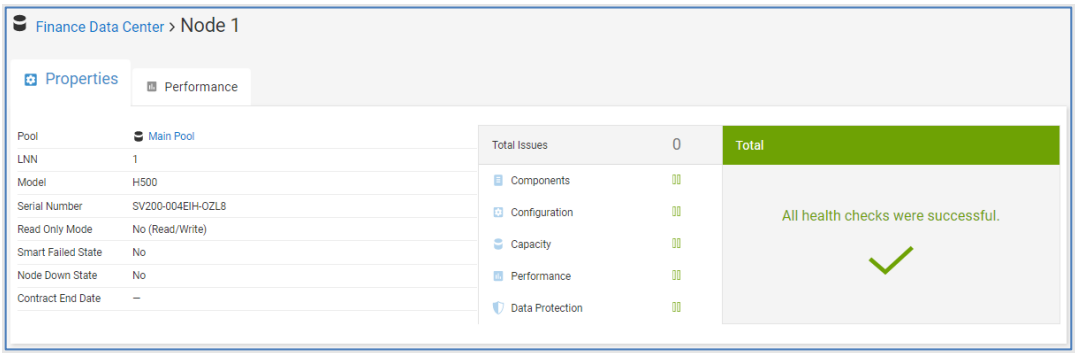


Node details

For PowerScale, Isilon, and APEX File Storage for AWS, Infrastructure Observability provides node details. To begin, select a node hyperlink from the Nodes tab on the system details page.

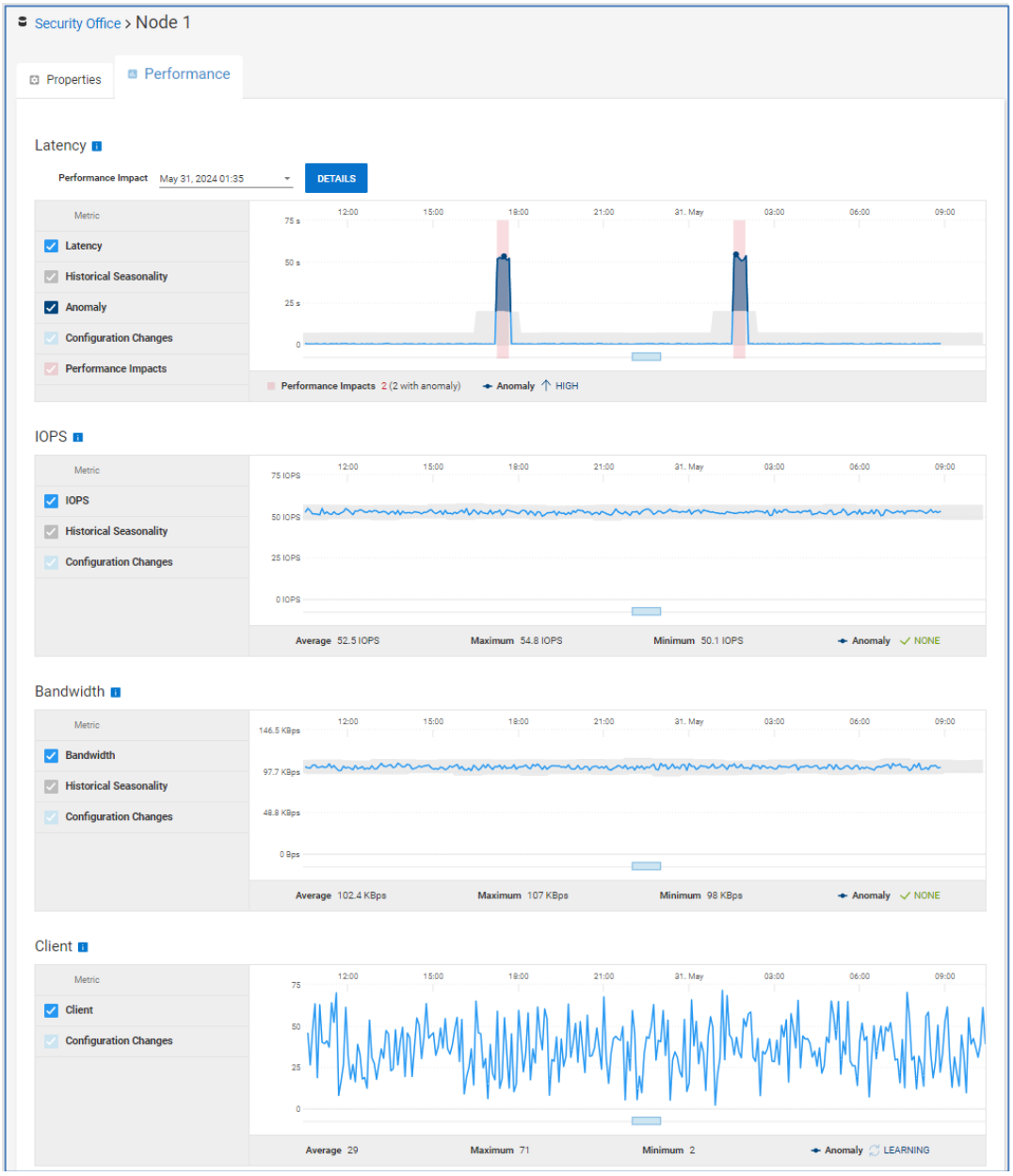
Node details - Properties

The **Properties** tab for a node provides various information associated to the node including the pool, logical node number, model, smart failed state, node state, and contract end date.



Node details - Performance

The **Performance** tab displays 24-hour metrics for several key performance metrics including latency, IOPS, bandwidth, clients, CPU utilization, latency per protocol, IOPS per protocol, and bandwidth per protocol.

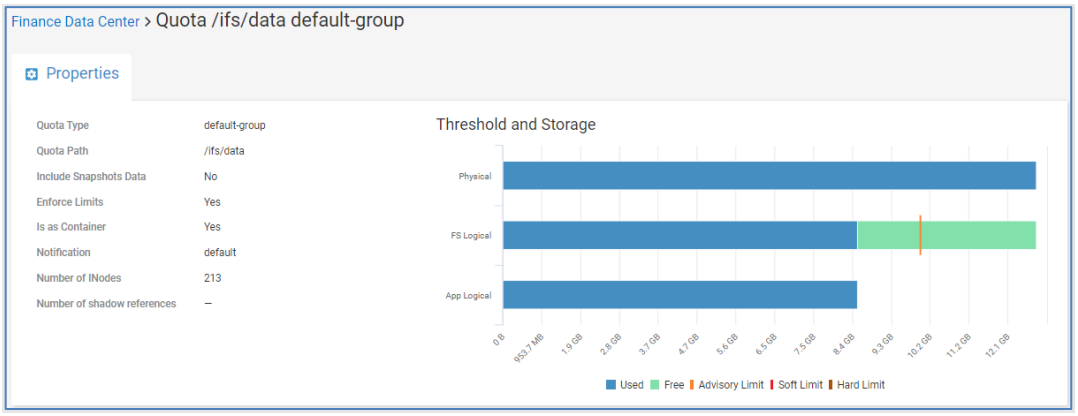

Security Office > Node 1
Properties
Performance
Latency
Performance Impact
May 31, 2024 01:35
DETAILS
Metric
Latency
Historical Seasonality
Anomaly
Configuration Changes
Performance Impacts
Performance Impacts 2 (2 with anomaly)
Anomaly HIGH
IOPS
IOPS
Average 52.5 IOPS
Maximum 54.8 IOPS
Minimum 50.1 IOPS
Anomaly NONE
Bandwidth
Bandwidth
Average 102.4 KBps
Maximum 107 KBps
Minimum 98 KBps
Anomaly NONE
Client
Client
Average 29
Maximum 71
Minimum 2
Anomaly LEARNING

Quota details

Quota details for PowerScale and APEX File Storage for AWS are available by selecting the quota hyperlink from the **Quotas** tab on the system details page.

Quota details - Properties

For each quota, the **Properties** tab provides the quota type, path, if the quota includes snapshots, if the limits are enforced, notification status for enforced quotas, number of inodes, and number of shadow references. Bar charts provide visual representations of physical, file system logical, and app logical capacity utilization along with limits.

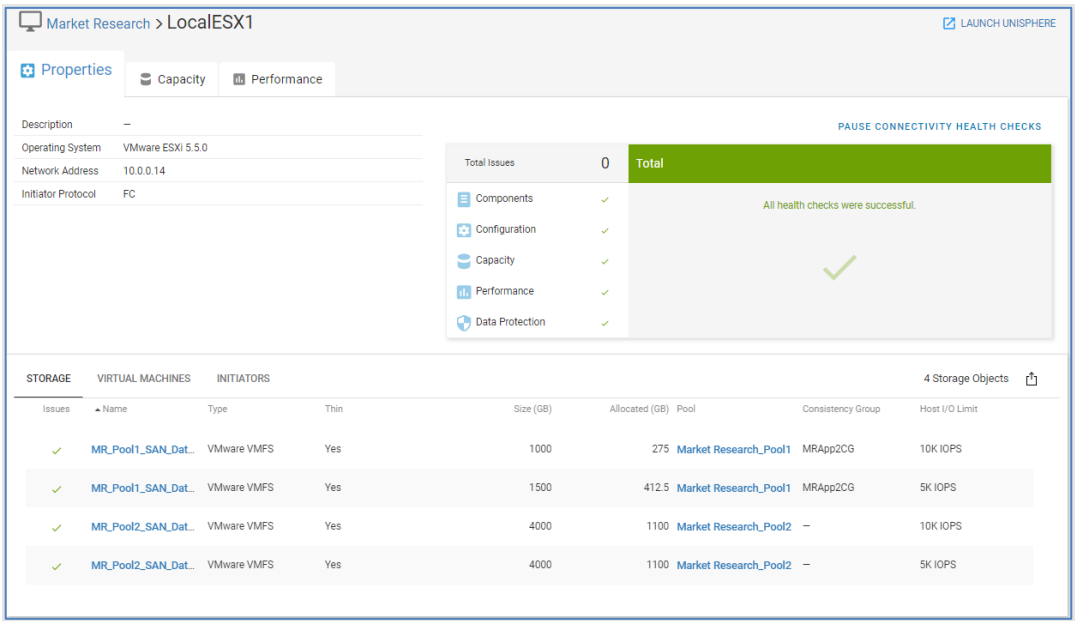


Host details

Host detail drill downs are available for Unity XT family, PowerStore, PowerMax, XtremIO, SC Series (Servers), and PowerVault (Initiators).

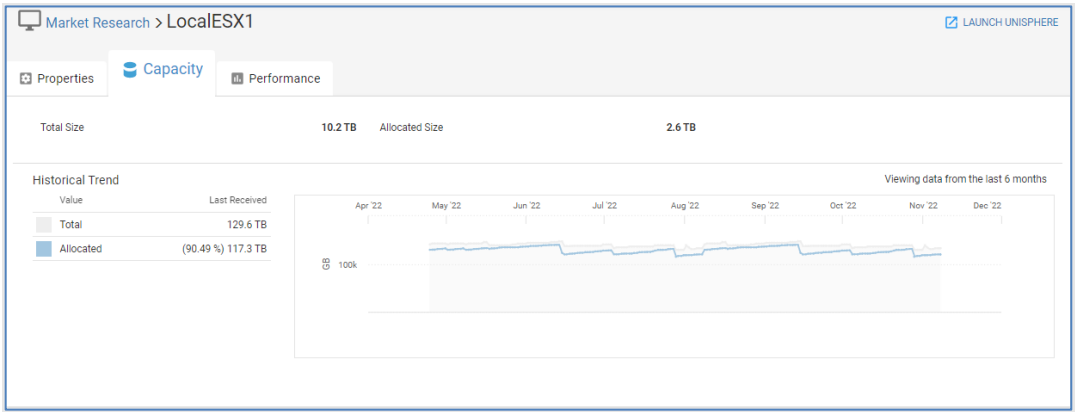
Host details - Properties

The **Properties** tab displays configuration data for a host including the operating system, IP Address, and initiator protocol. It also displays any health issues associated to the host with suggested remediation. Details about the storage objects attached to the host, virtual machines residing on the host, and initiators are provided in the tabs at the bottom of the page.



Host details - Capacity

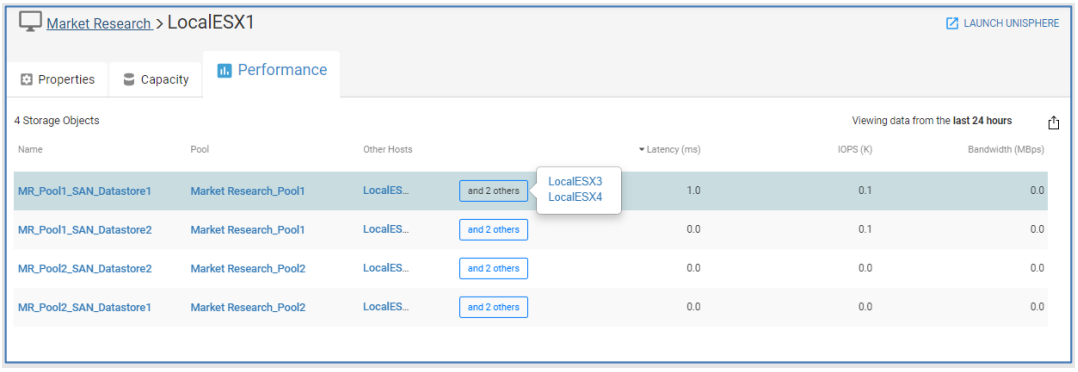
The **Capacity** tab for a host provides details for the current capacity from the associated storage system. These details include provisioned and allocated size, and historical capacity trends, of all the block objects provisioned to that host. The capacity tab is not supported for PowerStore.



Host details – Performance

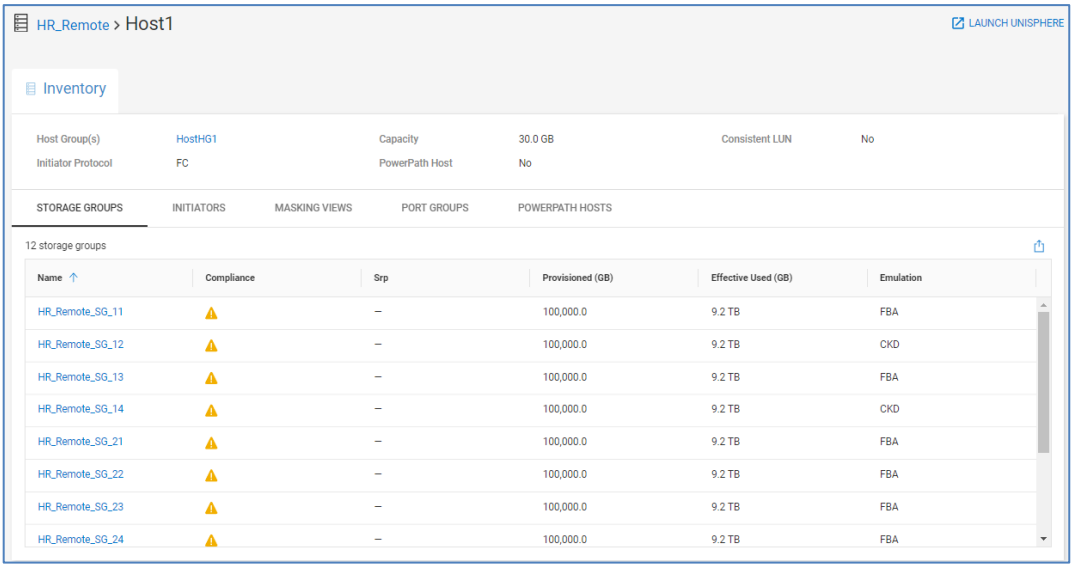
The **Performance** tab for a host provides the 24-hour average values of key performance indicators (Latency, IOPS, and Bandwidth) of each block object provisioned on the host. It also displays the names of other hosts to which the block objects are also provisioned.

The Performance tab is not supported for PowerStore. Latency is not supported for PowerVault initiators.



Host details – Inventory

The host details page for PowerMax systems only has an **Inventory** tab. This tab provides information about the associated storage groups, initiators, port groups, masking views, and PowerPath hosts.



Connectrix and PowerSwitch details

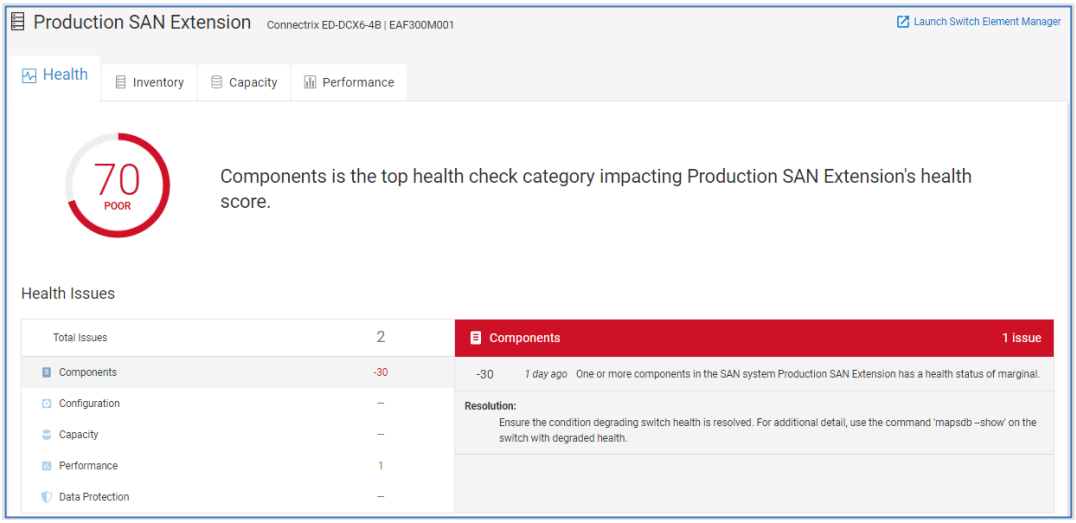
Introduction

Infrastructure Observability can monitor both Connectrix and PowerSwitch networking devices. For both Connectrix and PowerSwitch devices, Observability uses a local collector that communicates to the switches using a read-only privilege. The collector sends the data back to Observability through the Secure Connect Gateway.

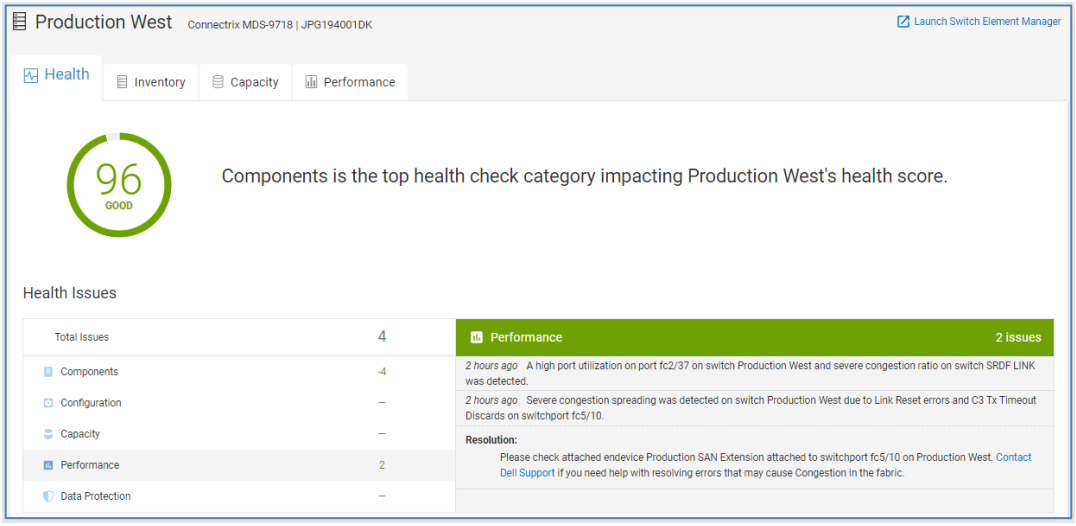
Selecting the switch hyperlink in the home page or any of the multisystem views opens the System Details page for that switch. The following sections discuss each tab of the Switch System Details page in greater depth.

Switch system details – Health

The **Health** tab shows the details for a selected switch driving the health score number. Only the Components category is used in calculating the switch health score, although Observability does detect and report on congestion spreading events under the Performance category for Connectrix. This is discussed in more detail below. Selecting any issue provides a corresponding recommendation for obtaining additional information and resolution. The bottom of the page shows the Health Score History chart for both Connectrix and PowerSwitch devices.

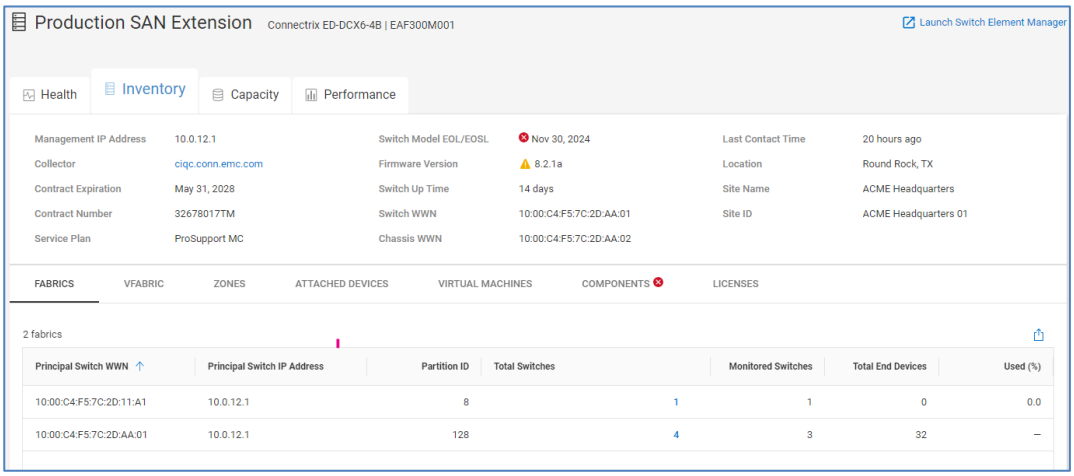


Observability can detect congestion spreading on Connectrix switches. The detection evaluates various conditions including congested ports, port errors, and port utilization on the local switch or connected switches. Health score deductions for these scenarios are under investigation, and this condition does not yet affect the health score of the switch. Instead of displaying a health score deduction, Observability displays the number of congestion spreading events.

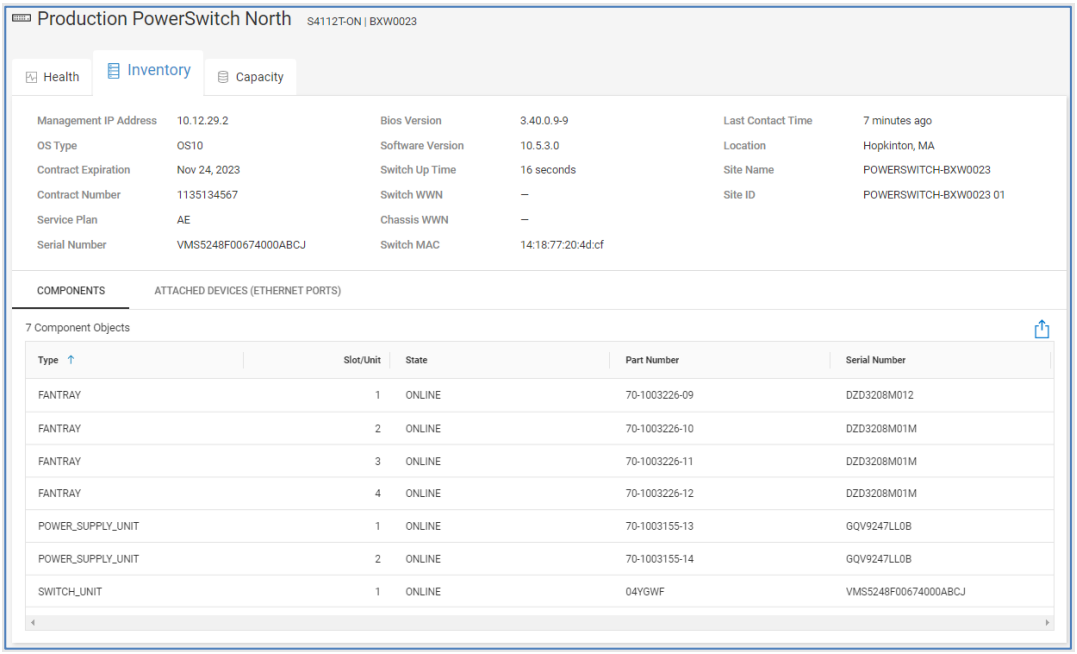


Switch system details – Inventory

The **Inventory** tab differs slightly between Connectrix and PowerSwitch. For Connectrix, it contains various switch attributes at the top half of the screen, including the serial number, model, location, site, firmware, management IP address, and contract information. It also highlights if a model had reached End of Life (EOL) or End of Service Life (EOSL) and identifies if recommended firmware updates are available. The bottom half of the window contains the following tabs: Fabrics, Partitions, Zones, Attached Devices, Virtual Machines, Components, and Licenses.



The top half of the Inventory tab for PowerSwitch includes the service tag, serial number, model, operating-system type, location, site, BIOS or software versions, management IP address, and contract information. The bottom half of the page has the Components and Attached Devices (Ethernet Ports) tabs.

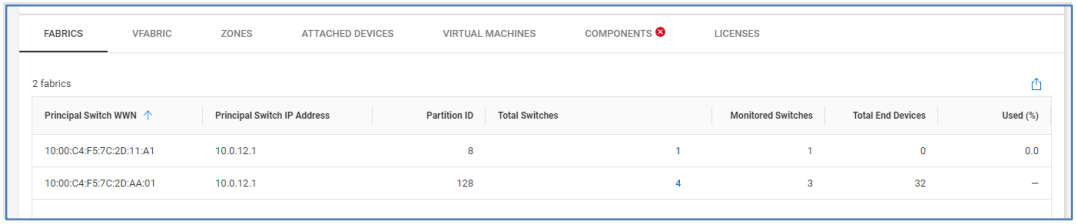


Fabrics

The **Fabrics** tab (Connectrix only) provides the following information about the fabrics in which the switch participates:

- Principal Switch WWN – Worldwide name of the principal switch in the fabric.
- Principal Switch IP – The IP address of the principal switch in the fabric.
- Partition ID
  - B-Series: If Virtual Fabrics (VF) are enabled, this field displays the VF ID for each VF defined on the switch. If not enabled, this field is set to 128.
  - MDS: This field shows the VSAN ID.

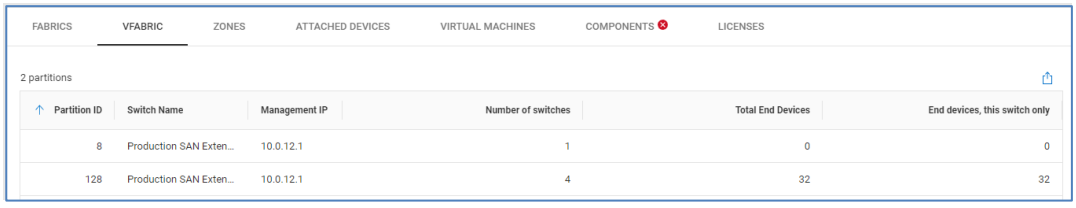
- Total Switches – Total number of switches participating in the fabric that this VF or VSAN or switch is a member of. This number is a hyperlink which, when selected, displays a window listing all switches in the fabric.
- Total End Devices – Total number of N_Ports participating in the fabric that this VF or VSAN or switch is a member of.
- Monitored Switches – Total number of switches participating in the fabric that are also monitored by Observability.
- Used % – Percentage of ports in this fabric that are in use.



VSAN/VFabric

The **VSAN** tab (Connectrix MDS) and **VFabric** tab (Connectrix B-Series) provides information about VSANs and Virtual Fabrics.

- Partition ID
  - B-Series: If Virtual Fabrics (VF) is enabled, this field displays the VF ID for each VF defined on the switch. If not enabled, this field is set to 128.
  - MDS: This field shows the VSAN ID.
- Switch Name – Switch name as defined by the end user. If no switch name is set, this field displays the switch serial number.
- Management IP – IP address of the switch.
- Number of switches – Total number of switches participating in the fabric that this VF or VSAN or switch is a member of.
- Total end devices – Total number of N_Ports participating in the fabric that this VF or VSAN or switch is a member of.
- End devices, this switch only – Total number of N_Ports that are members of this VF or VSAN and are also directly attached to this switch.

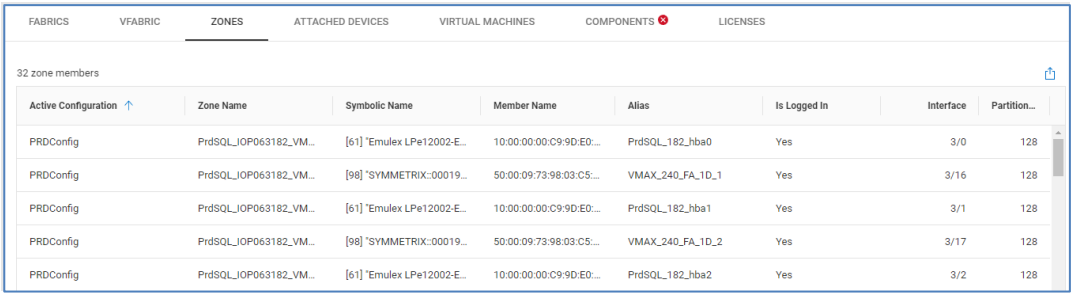


Zones

The **Zones** tab (Connectrix only) lists out zoning information for the zones in the active configuration.

- Active Configuration – Name of the enabled zoning configuration.

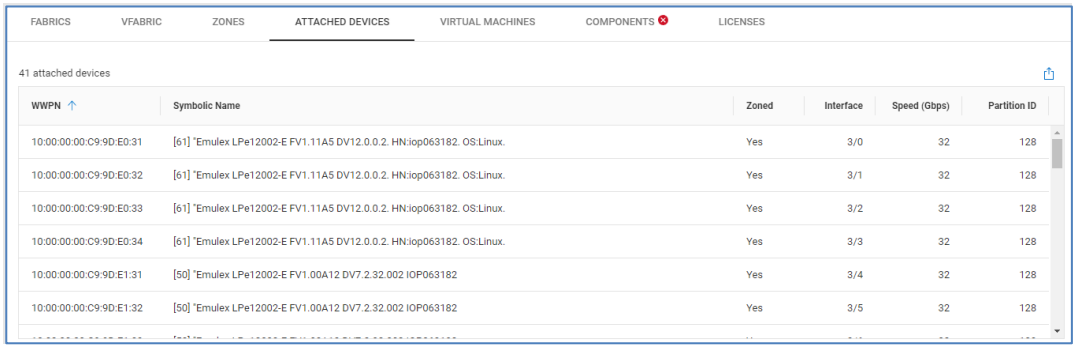
- Zone Name – Name of the zone.
- Symbolic Name – Symbolic name of a zone member (only shown if zone member is logged into the switch).
- Member Name – Name of the zone member. This is typically the WWPN of the attached device but could also be the WWPN of the switch port or the WWNN of the attached device. It could also be in the “Domain, Port” format or “switch wwn, port” format.
- Alias – User-defined alias associated with the zone member.
- Is Logged In – Identifies if the end device is a member of a zone and logged into the fabric.
- Interface – Identifies the interface on the switch where the end device is logged in.
- Partition ID
  - B-series: If Virtual Fabrics (VF) are enabled, this field displays the VF ID for each VF defined on the switch. If not enabled, this field is set to 128.
  - MDS: This field shows the VSAN ID.



Attached Devices (Connectrix)

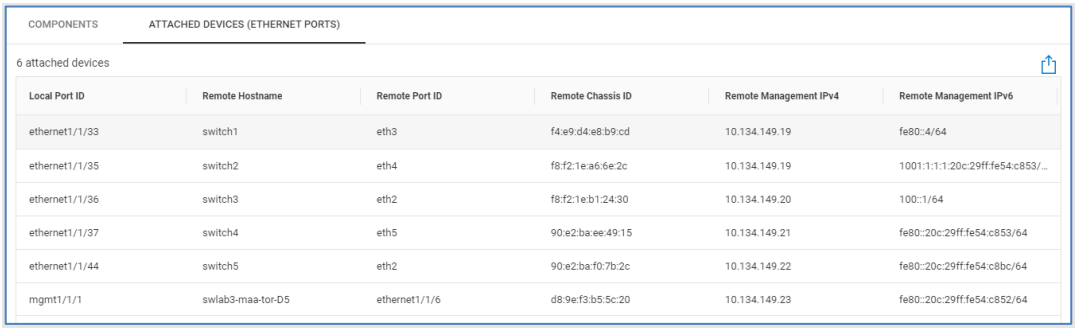
The **Attached Devices** tab lists out various information for devices that are physically attached to the switch.

- WWPN – Worldwide Port Name of the attached device
- Symbolic Name – Symbolic name of the attached device (only shown if the zone member is logged into the switch).
- Zoned – Identifies if the attached device is a member of the zone that is present in the active configuration.
- Interface – Identifies the interface on the switch where the end device is logged in.
- Speed (Gbps) – Speed that the attached device negotiated with the switch during the login process.
- Partition ID
  - B-series: If Virtual Fabrics (VF) is enabled, this field displays the VF ID for each VF defined on the switch. If not enabled, this field is set to 128.
  - MDS: This field shows the VSAN ID.



Attached Devices (Ethernet Ports) (PowerSwitch)

The **Attached Devices** tab for PowerSwitch lists each of the devices attached to the Ethernet ports of the switch.

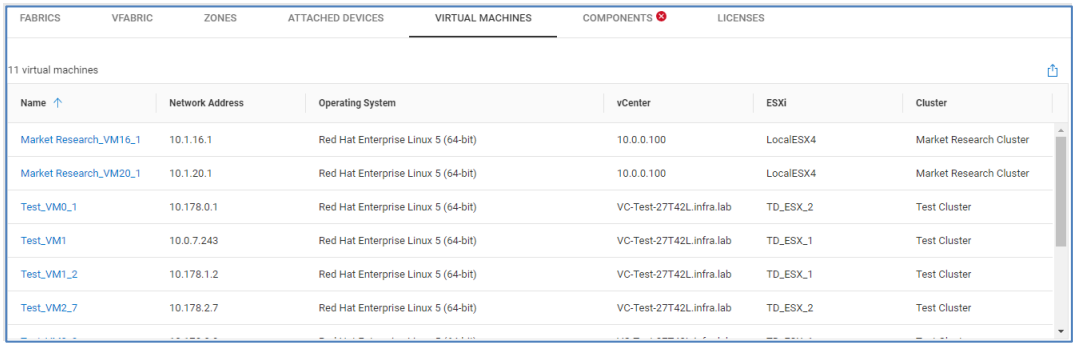


- Local Port ID – The Port ID of the switch.
- Remote Hostname – Hostname of the attached device.
- Remote Port ID – Port ID of the attached device.
- Remote Chassis ID – Chassis ID of the attached device.
- Remote Management IPv4 – Management IPv4 address of the attached device.
- Remote Management IPv6 – Management IPv6 address of the attached device.

Virtual Machines

The **Virtual Machines** tab (Connectrix only) shows virtual machines residing on ESXi servers that are connected to the switch.

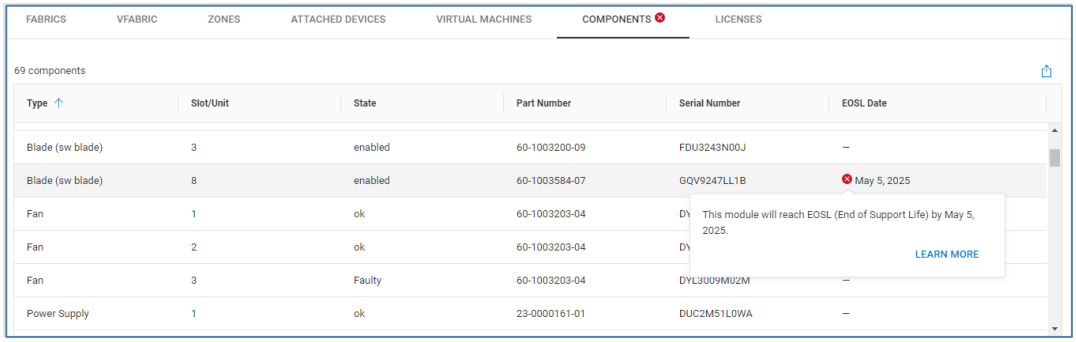
- Name – Name of the virtual machine.
- Network Address – IP address of the virtual machine.
- Operating System – Operating system installed on the virtual machine.
- vCenter – Hostname of vCenter managing the virtual machine.
- ESXi – Hostname of ESXi server hosting the virtual machine.
- Cluster – Name of ESXi Cluster hosting the virtual machine.



Components

The **Components** tab lists out the system hardware for both Connectrix and PowerSwitch.

- Type – The type of component installed in the chassis.
- Slot/Unit – Location of the component in the chassis.
- State – For optics, this field provides the strength of the optical signal being received. For other hardware components, this field provides the operational state of the component.
- Part Number – Part number of the component.
- Serial Number – Serial number of the component.
- EOSL Date (Connectrix only) – Identifies components with upcoming End of Life (EOL) and End of Support Life (EOSL) dates.

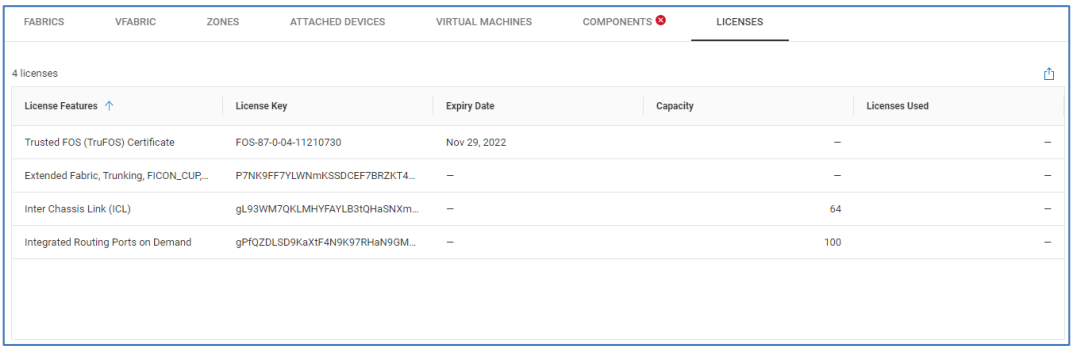


Licenses

The **Licenses** tab (Connectrix) provides information about the licenses on each switch.

- License features – List of features for each license for B-Series and name of the license feature for MDS.
- License key (B-Series) – Key used to install the license.
- Expiration date – Expiration date of the license.
- Capacity (B-Series) – Count of the additional ports that are allowed.
- Count (MDS) – Sum of base license ports and additional assigned ports if smart license is disabled. The additional ports that are assigned to the switch if smart license is enabled.

- Licenses used – applicable for Ports on Demand switch port licenses for B-Series. Applicable only for PORT_ACTIV* or FC_PORT_ACTIV* switch ports for MDS.

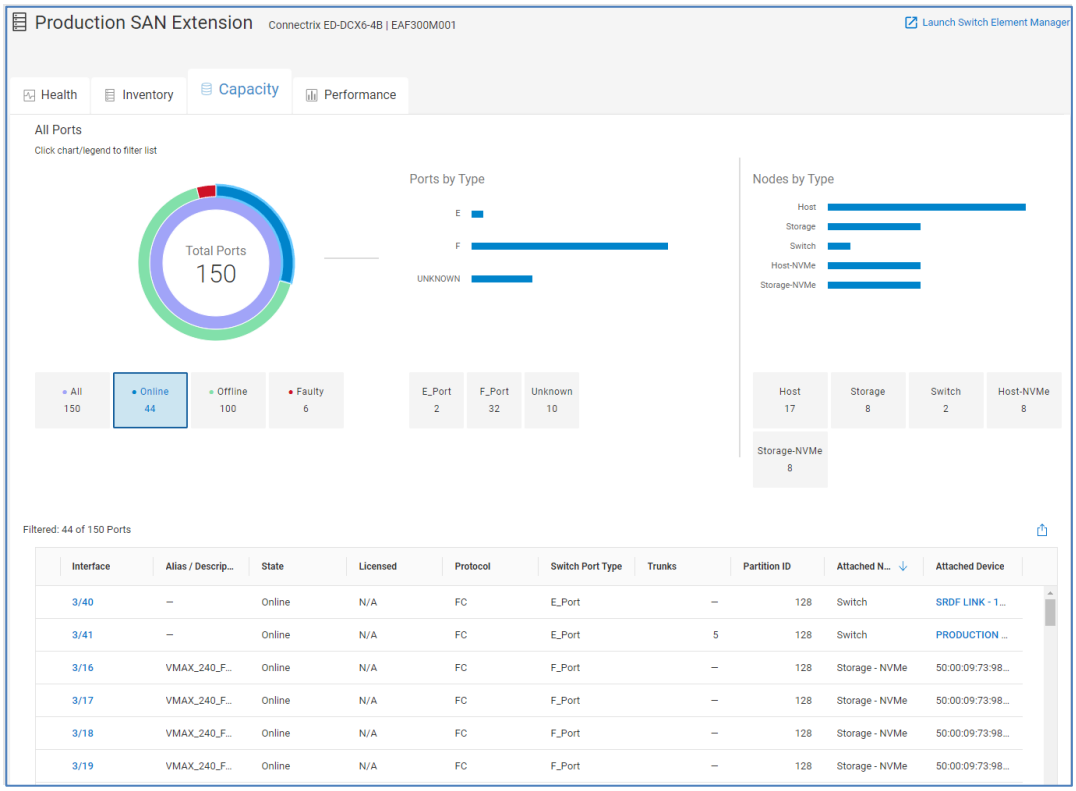


Switch system details – Capacity

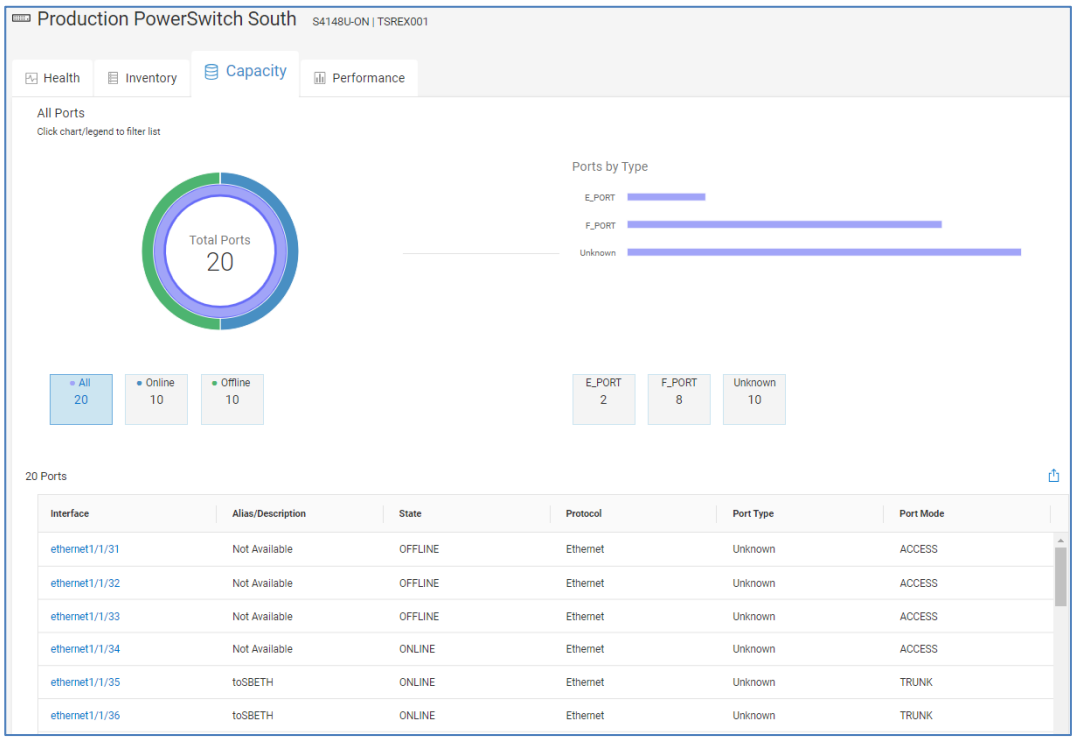
The **Capacity** tab for a switch provides port usage details for both Connectrix and PowerSwitch. The upper left portion of the view shows a breakdown of the ports on the switch broken down by Online, Offline, and Error status. The Ports by Type bar charts show a filtered list of ports broken down by port type. For Connectrix, the Nodes Attached bar charts show a breakdown of attached nodes by Host Ports, Storage Ports, and Switch ports. The bottom of the page displays a filtered list of ports based on the filters selected in the top half of the page. The following columns are displayed at the bottom of the page:

- Interface – Location of the port, shown as slot/port number. For Connectrix, it is also a hyperlink which directs user to port performance charts.
- Alias/Description – Switch port alias, if defined.
- State – Status of the switch port.
- Licensed – Shows whether the port is licensed, not licensed, or N/A for directors.
- Protocol – Protocol configured for the switch port.
- Switch Port Type – Logical configuration of the switch port. Possible values include F_PORT, N_PORT, E_PORT, Unknown, or Disabled for FC ports. Set to Unknown for Ethernet ports.
- Port Mode (PowerSwitch only) – Logical configuration of the interface, such as Access or Trunk.
- Trunks (B-Series)/Simple Channel (MDS) – Value of trunk or port channel if the physical port is being aggregated.
- Partition ID (Connectrix only)
  - Brocade: If Virtual Fabrics (VF) are enabled, this field displays the VF ID for each VF defined on the switch. If not enabled, this field is set to 128.
  - Cisco: This field shows the VSAN ID.
- Attached Node Type (Connectrix only) – Describes the device attached to the switch port.
- Attached Device (Connectrix only) – Worldwide name of the attached device.

Capacity tab for Connectrix:



Capacity tab for PowerSwitch:

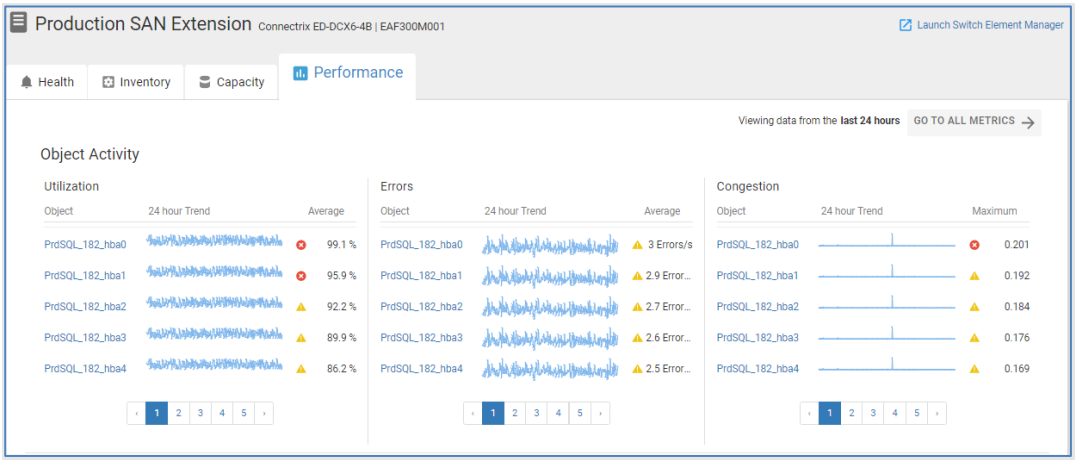


Switch system details – Performance

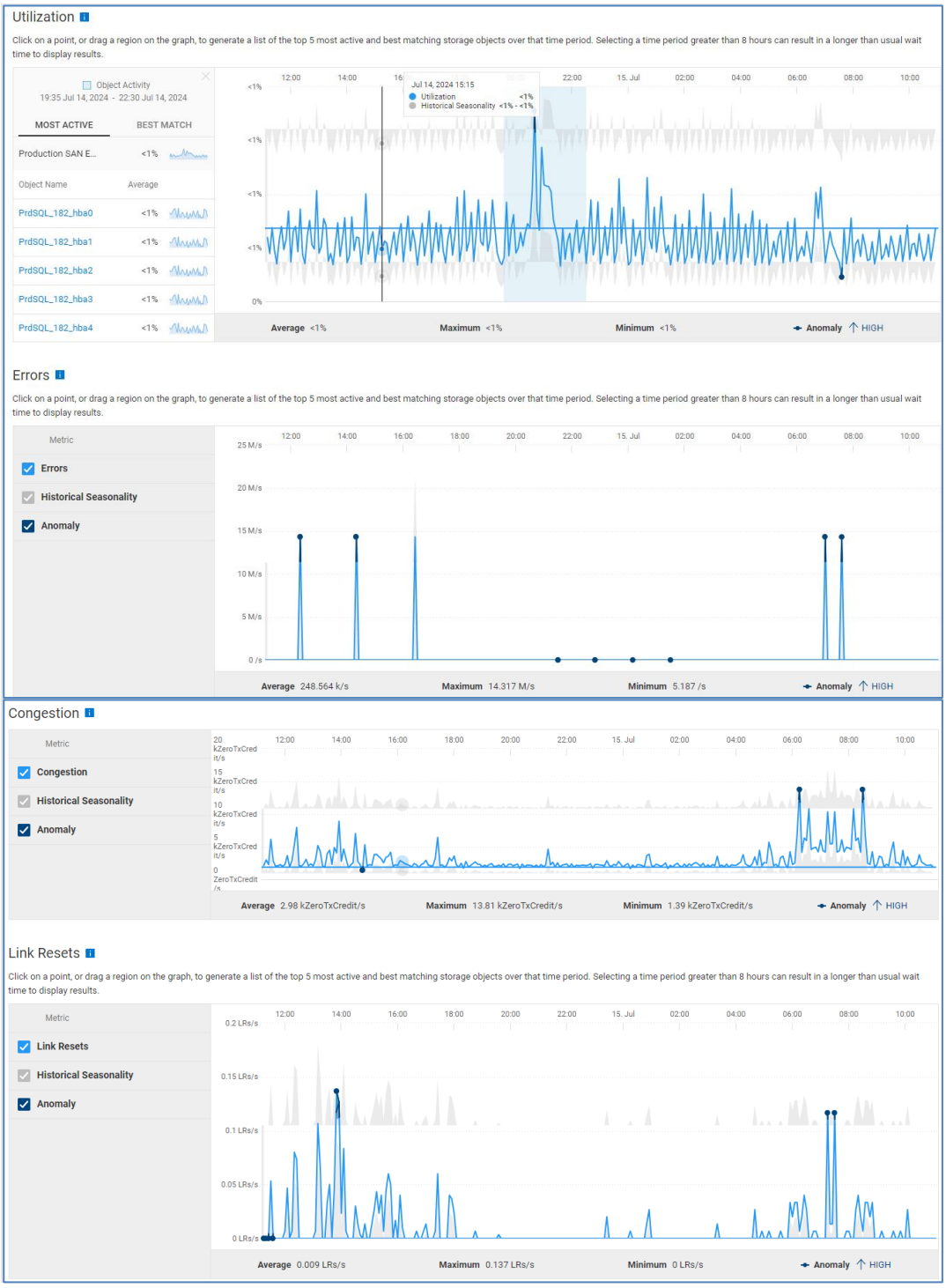
The top section of the **Performance** tab for Connectrix switches is Object Activity, and it displays the top ports contributing to Utilization, Errors, and Congestion sorted by their 24-hour average. Showing the top objects first allows the user to quickly identify ports using the most resources and experiencing the most errors in the last 24 hours.

The user can scroll down to see 24-hour charts for the following Connectrix switch performance metrics:

- Utilization – The percentage of system bandwidth in use. This value represents the percentage of transmit bandwidth being used across all switch interfaces.
- Congestion – The sum of all “time spent at zero transmit” counters across all switch interfaces.
- Errors – The sum of all bit error counters across all switch interfaces.
- Link Resets – The sum of all Link Reset primitives that have been either transmitted or received across all switch interfaces.



Highlighting an area in any of these performance charts shows the top five port contributors to that performance metric during that time period in the Most Active tab on the left side of the chart. The Best Match tab lists the ports with the most closely matched shape during the selected period. The ports listed in the left side of each chart are hyperlinks that direct the user to port-level performance charts. Performance anomaly detection is supported in each of these performance charts.

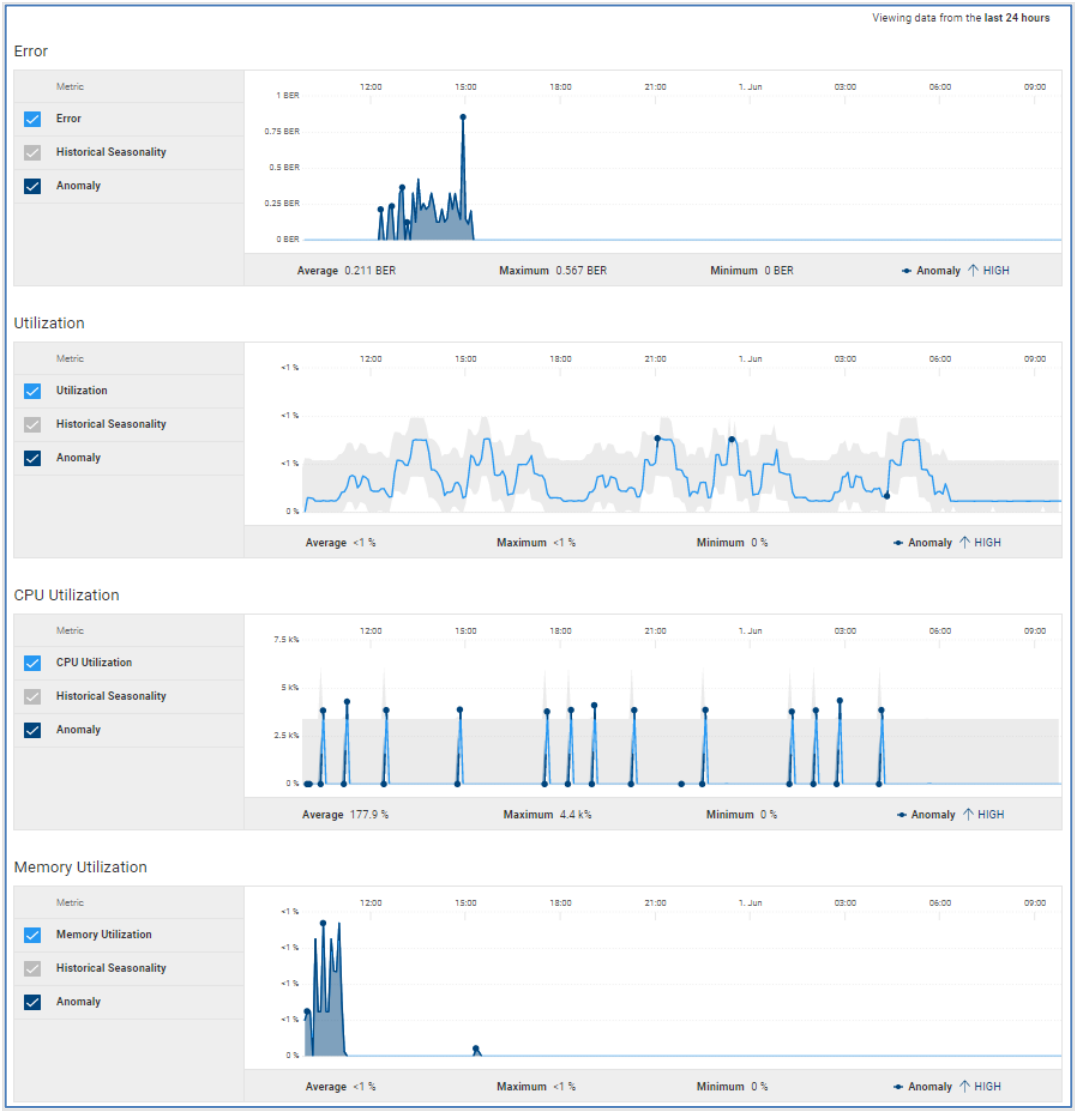


PowerSwitch devices show 24-hour charts and performance anomalies for the following performance metrics:

- Error – The Bit Error Rate across all switch interfaces.
- Utilization – The percentage of transmit bandwidth being used across all switch interfaces.
- CPU Utilization – The percentage of CPU usage over the selected time period.

- Memory Utilization – The percentage of memory usage used by various processes running on the switch.

Note: Performance metrics required minimum of OS10 version 10.5.3.2. Memory utilization requires a minimum of OS10 version 10.5.4.

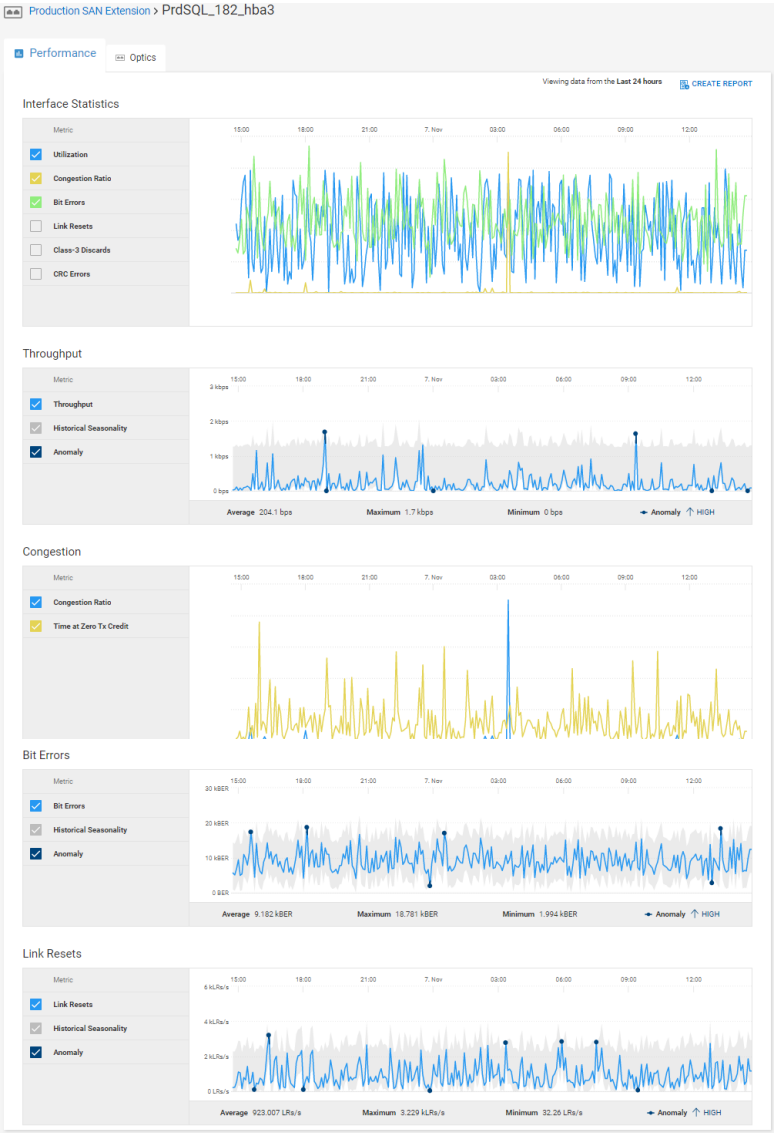


Switch port details – Performance

Users can access port-level performance metrics for Connectrix switches. Select the port from the Interface column in the Switch Capacity page or select the port hyperlink in the top object activity shown in the previous section. Port-level performance metrics are shown in the following charts:

- Interface Statistics
  - Utilization
  - Congestion Ratio
  - Bit Errors
  - Link Resets

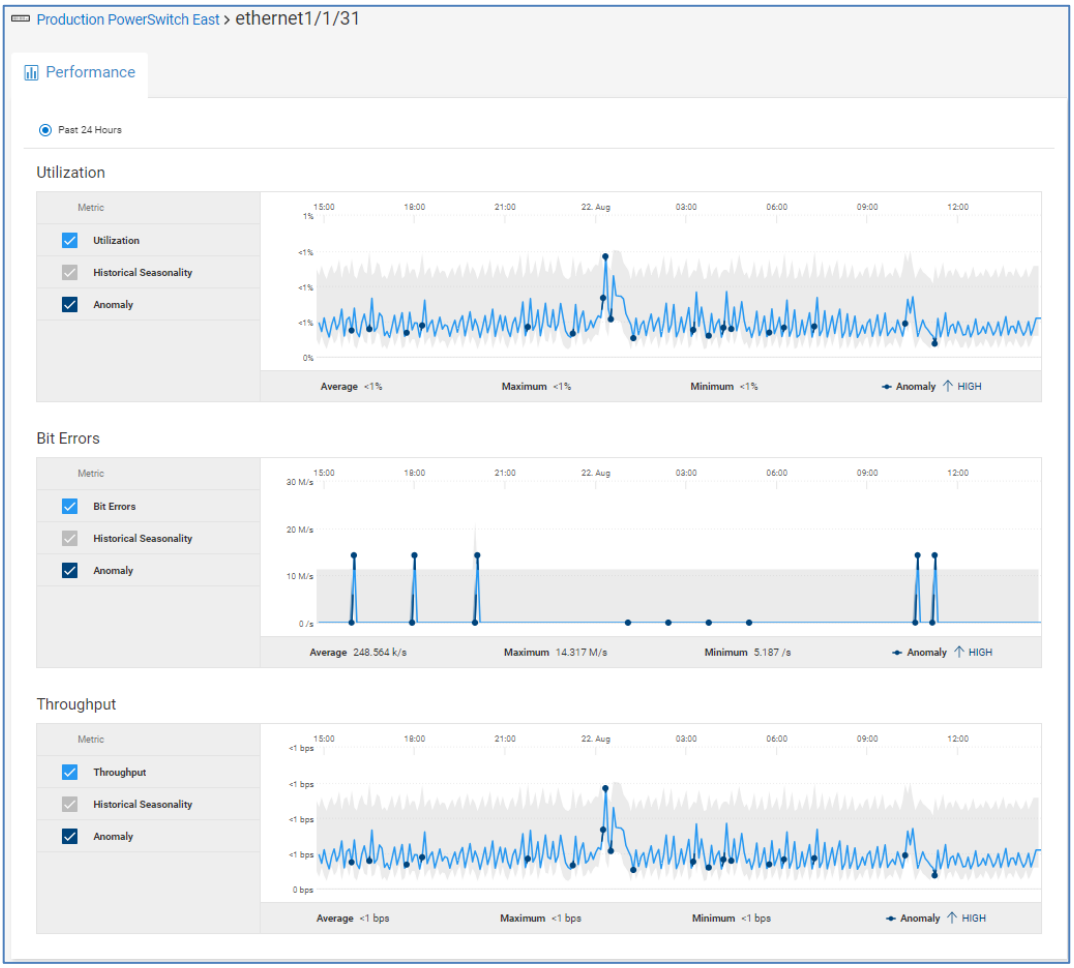
  - Class-3 Discards
  - CRC Errors
- Throughput
- Congestion
  - Congestion Ratio
  - Time at Zero Tx Credit
- Bit Errors
- Link Resets



Users can access PowerSwitch port performance by selecting the port name hyperlink in Interface column of the Switch Capacity tab. PowerSwitch port performance charts include 24-hour charts for the following:

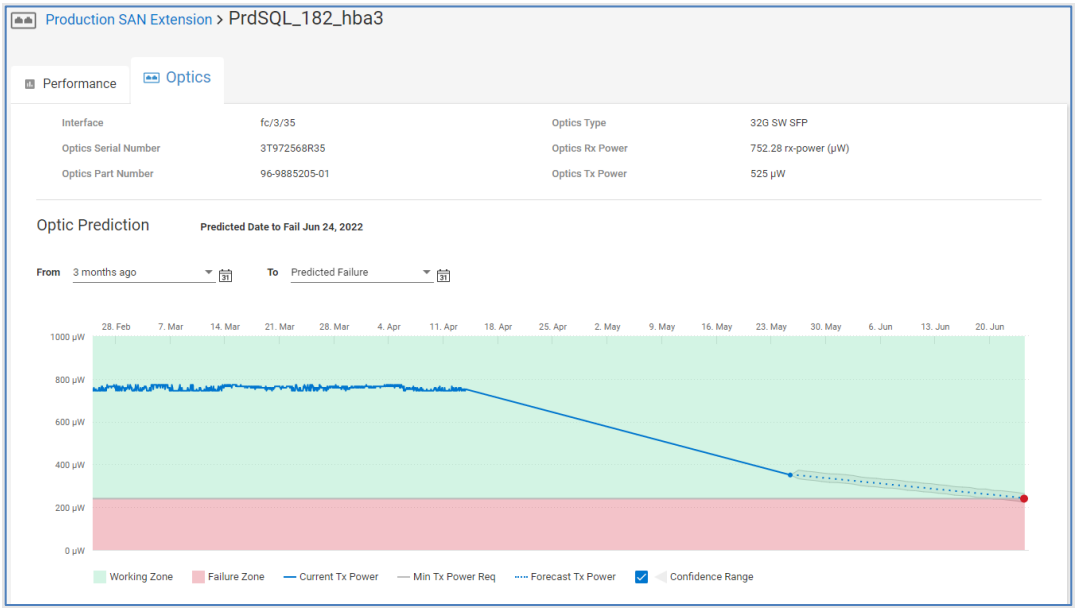
- Utilization

- Bit Errors
- Throughput



Switch port details – Optics

The **Optics** tab for Connectrix switches provides various property information about the optic on the top of the page and graphs the historical and predicted Tx power at the bottom of the page. The chart provides the working and failure zones and the predicted time until failure, giving users the ability to plan ahead and take mitigating measures to address expected failures.



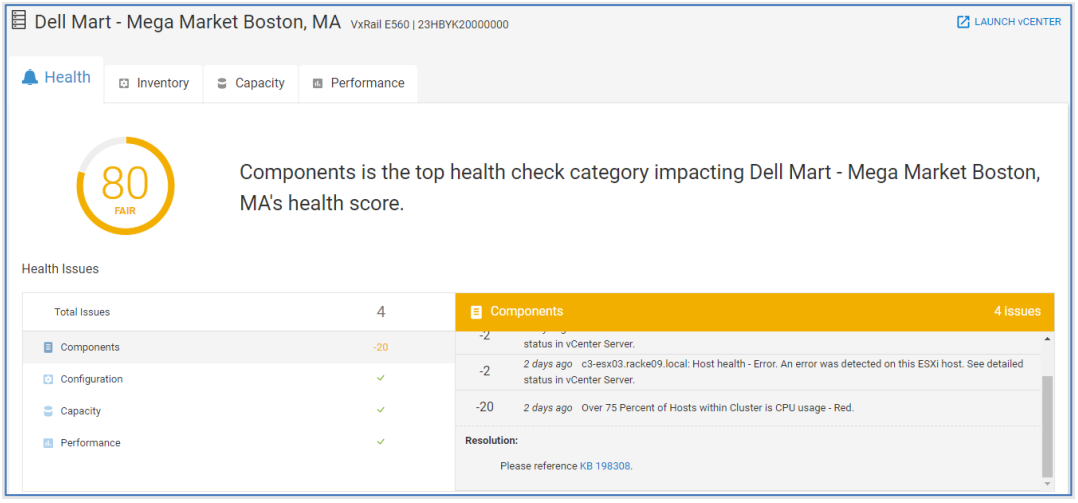
Hyperconverged infrastructure systems details

Introduction

Infrastructure Observability supports VxRail HCI systems, APEX Private Cloud Services, and APEX Hybrid Cloud Services. The HCI tab in the various multisystem views has been discussed earlier in this paper. This section describes the information provided in the system details view for an HCI cluster. Each cluster has the Health, Inventory, Capacity, and Performance tabs. Each tab provides the Launch vCenter hyperlink to easily go to vCenter for more detailed information or to make configuration changes. The details of each tab are presented below.

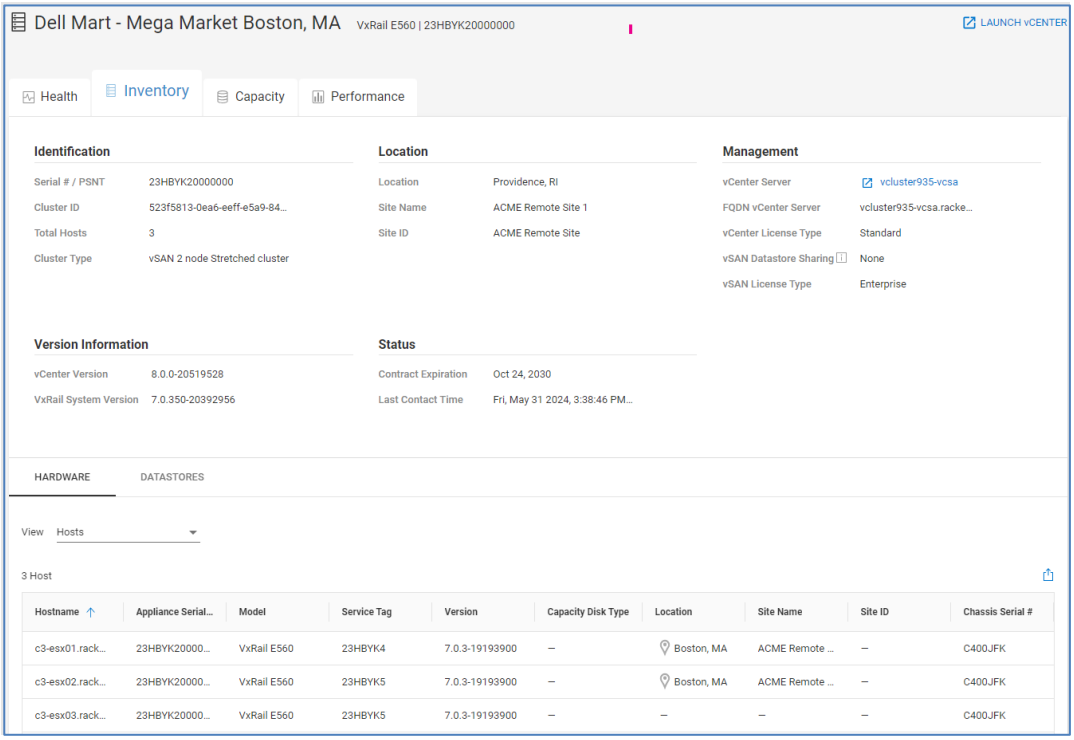
HCI system details – Health

The **Health** tab for HCI clusters is similar to other systems. The Health Score is determined by monitoring issues in the following categories: Components, Configuration, Capacity, and Performance. Each issue provides a recommended remediation or link to an applicable knowledge base article. Health Score history is also supported for HCI clusters.



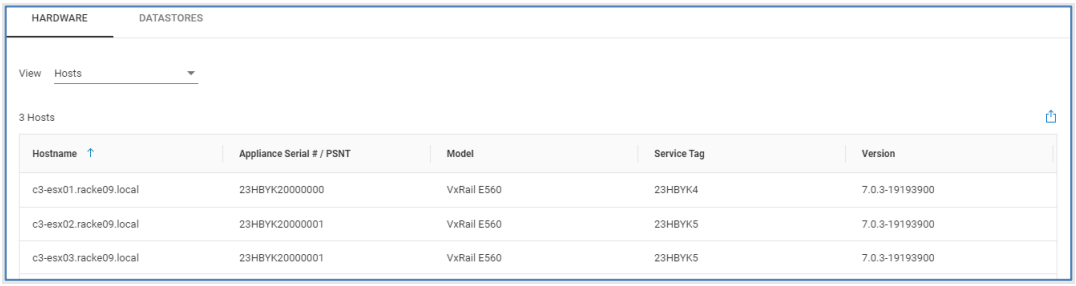
HCI system details – Inventory

The **Inventory** tab provides various cluster attributes at the top half of the screen, including the serial number, cluster ID, location, site, version, various vCenter information, and contract information. The bottom half of the window contains the following tabs: Hardware and Datastores. The Hardware tab provides views for Hosts, Disks, Power Supplies, and Version Information.



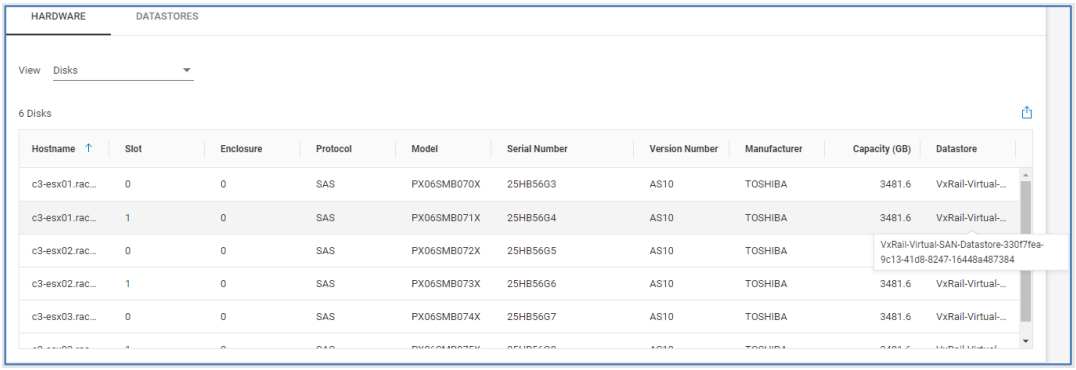
Hardware – Hosts

The **Hosts** view lists the appliances that make up the cluster and their model, service tag, and version.



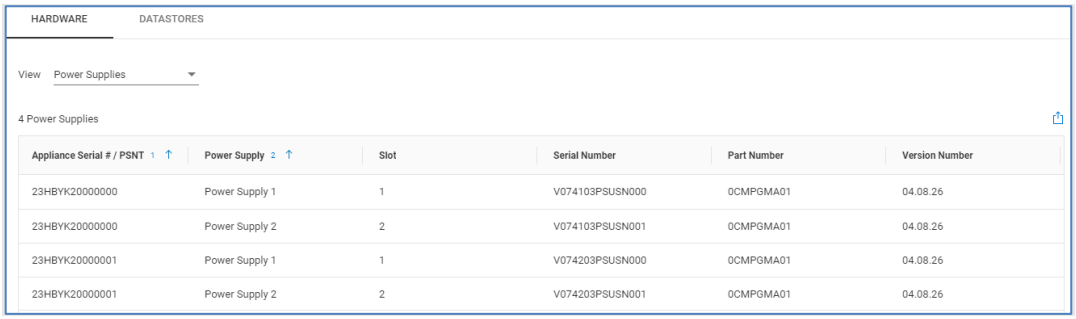
Hardware - Disks

The **Disks** view provides a listing of the hard drives in the cluster. This tab includes the ESXi host, slot and enclosure, serial number, and firmware. The capacity and datastore are also listed.



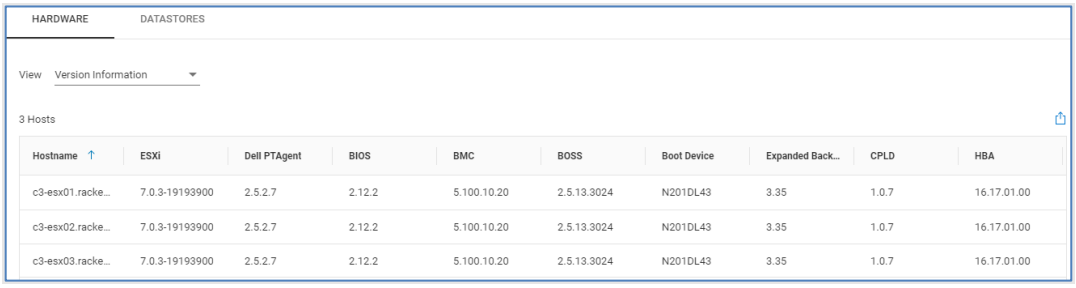
Hardware - Power Supplies

The **Power Supplies** view displays each power supply along with its location, serial number, part number, and version.



Hardware - Version Information

The **Version Information** view provides the version information for the different objects on the system.

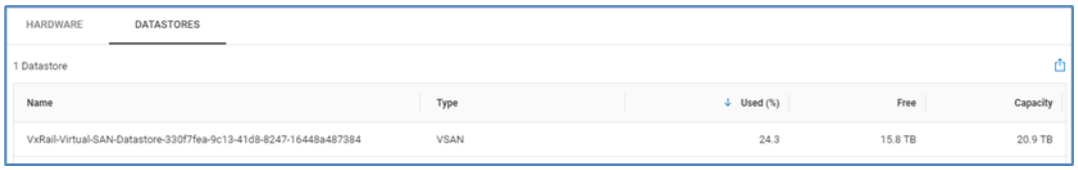


Hardware – Data Processing Unit

The **Data Processing Unit** view displays the DPU details of each node in the system.

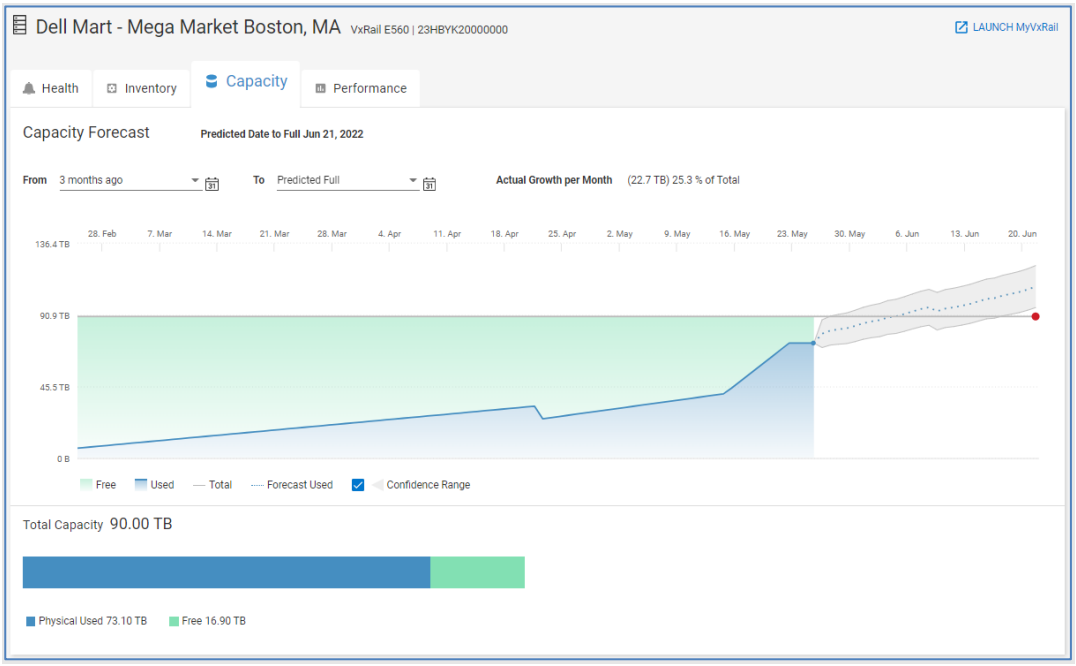
Datastores

The **Datastores** tab provides capacity utilization information for each of the datastores on the cluster.



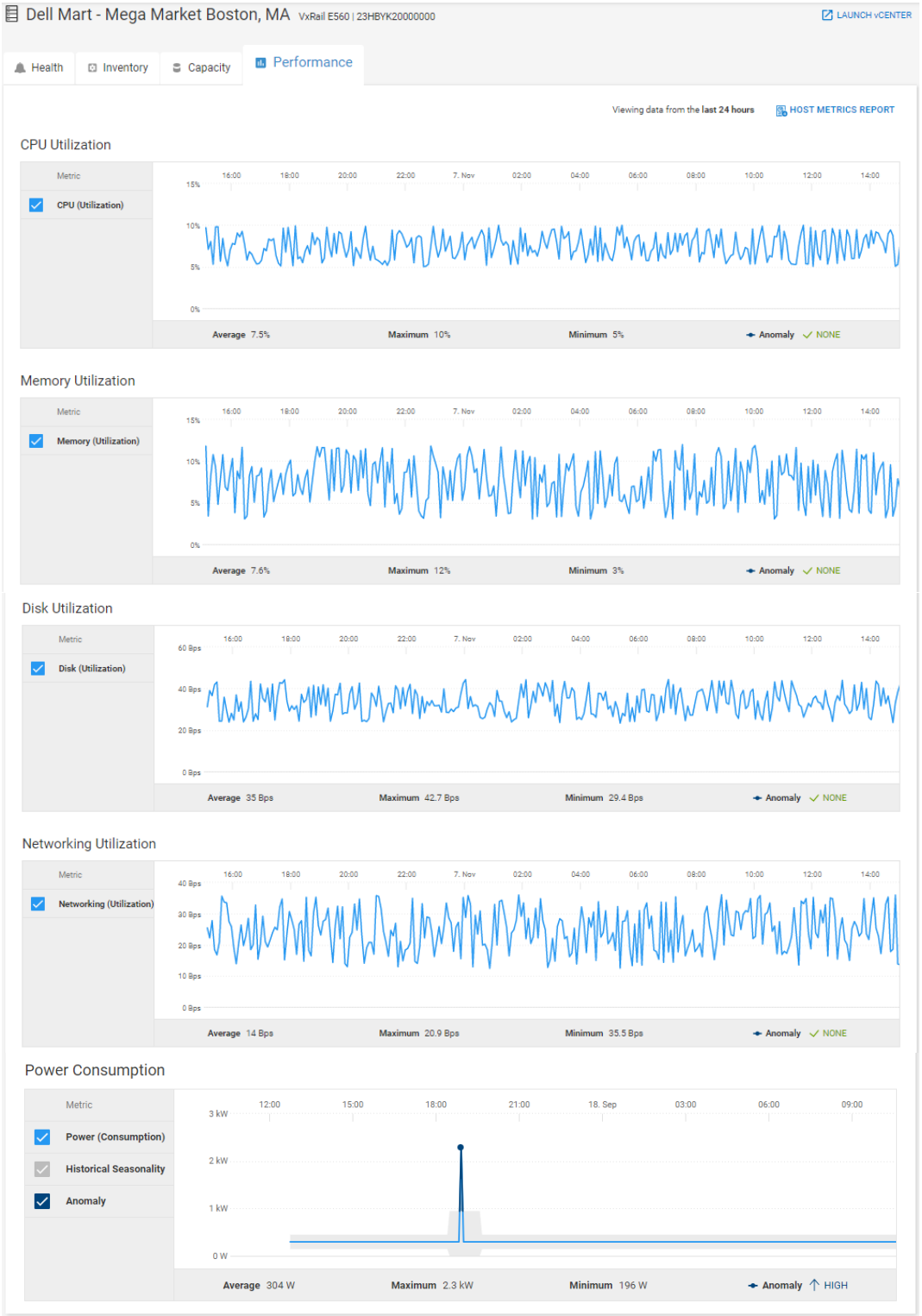
HCI system details – Capacity

The **Capacity** tab provides a capacity forecast chart on the top of the page. As with other systems, the chart displays the predicted full date along with a confidence range. The time range of the chart can be changed using the “From” and “To” drop-down menus. The bottom of the page displays a simple horizontal bar chart showing the breakdown of Total, Used, and Free capacity on the cluster.



HCI system details – Performance

The **Performance** tab provides 24-hour charts of CPU, Memory, Disk, Networking utilization, and Power consumption on the system. Clicking the Host Metrics Report link creates a custom report on CPU, memory, disk, and networking utilization for each host in the VxRail cluster.



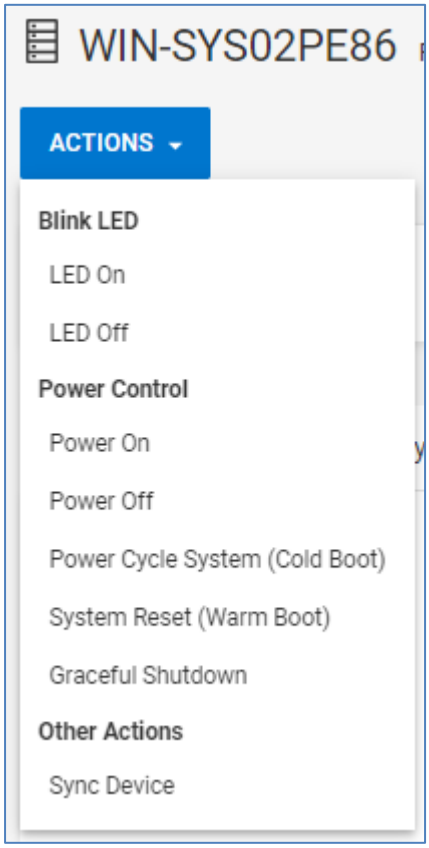
Server details

Introduction

Infrastructure Observability supports the monitoring of PowerEdge servers and modular chassis through a plug-in to OpenManage Enterprise. The multisystem views for servers

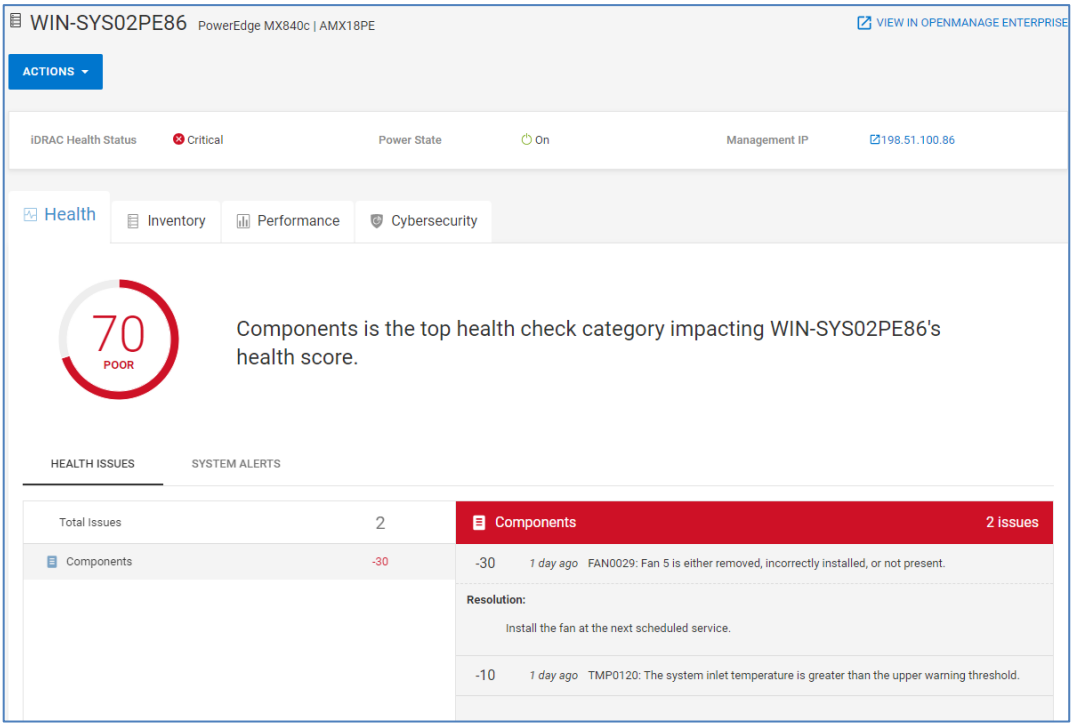
have been discussed earlier in this paper. This section documents the available information in the system details page for a PowerEdge server. Each server has the Health, Inventory, and Performance tab, and will have a Cybersecurity tab if that feature is enabled. Each tab provides a link to view the server in OpenManage Enterprise. The details of each tab are described in the following sections.

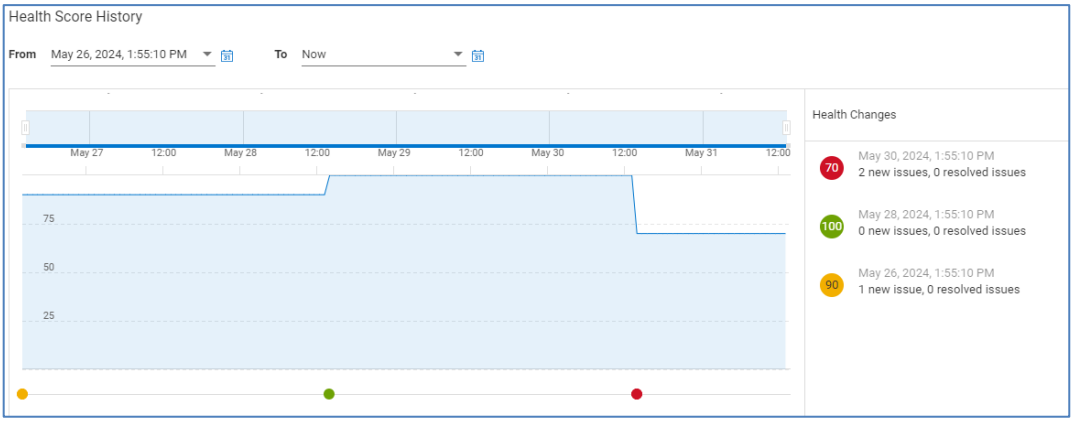
Each tab also provides an **Actions** menu. If remote operations are enabled in OpenManage Enterprise, and the Observability user has a role of Server Admin, then that user can perform maintenance actions on the PowerEdge system. These actions include blinking the LED to help locate the server in the data center. Users can also perform power control operations such as power on, power off, and shutdown. The sync device option refreshes the server to retrieve the latest data for inventory, health, alerts, and cybersecurity.



PowerEdge system details – Health

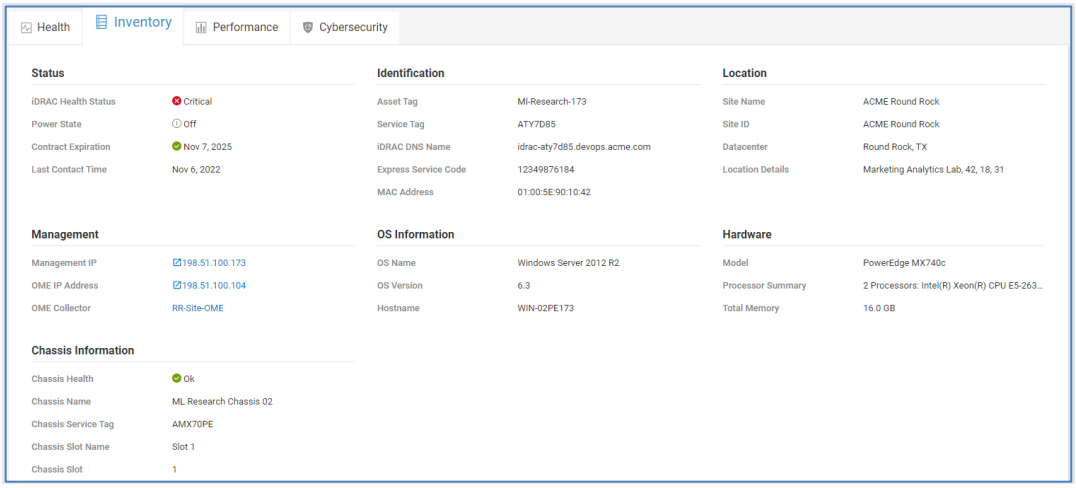
Observability provides the Proactive Health Score for each server monitored by Observability. Only the Components category is used to calculate the health score for servers. As with other systems, each health issue identified in Observability has a corresponding recommended remediation. Servers also have a System Alerts tab to allow the user to quickly see any alerts that are potentially impacting the system health. The Health Score History is tracked at the bottom of the page to help identify recurring issues.





PowerEdge system details – Inventory

The **Inventory** page provides configuration, firmware, contract, and license information for the server. The top half of Inventory provides various attributes about the server including operating system name and version, memory and CPU information, and Chassis information.

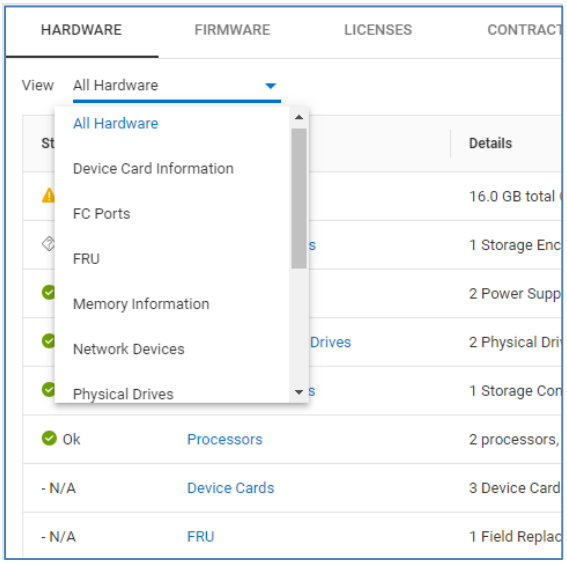


The bottom of the page has the following tabs: Hardware, Firmware, Licenses, Contract, and Management Info. A Virtual Machines tab is available and populated for servers running ESXi. Virtual machine information requires discovery of vCenter using the Observability Collector. See Appendix A: Enabling Infrastructure Observability at the system for additional details.

Hardware

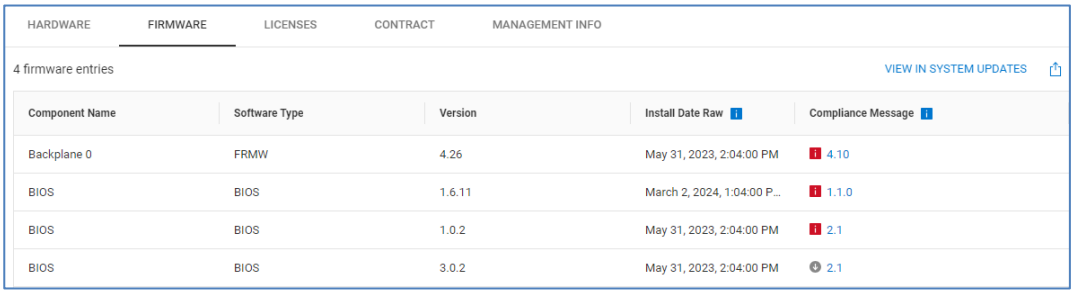
The **Hardware** tab has an additional drop-down menu to view information for the following components:

- All Hardware
- Device Card Information
- FC Ports
- FRU
- Memory Information
- Network Devices
- Physical Drives
- Power Supplies
- Processors
- Storage Controllers
- Storage Enclosures
- Virtual Flash



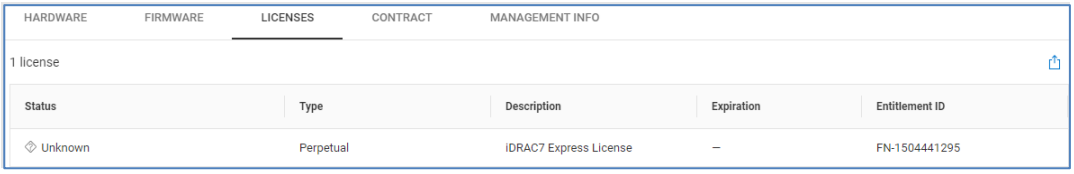
Firmware

The **Firmware** tab lists out BIOS and Firmware versions, installation dates, and latest available versions.



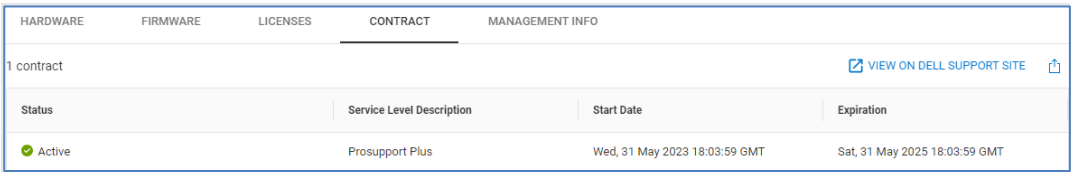
Licenses

The **Licenses** tab shows various information about the license including the status, the license type (perpetual or evaluation), a description, license expiration (for evaluation licenses), and the Entitlement ID.



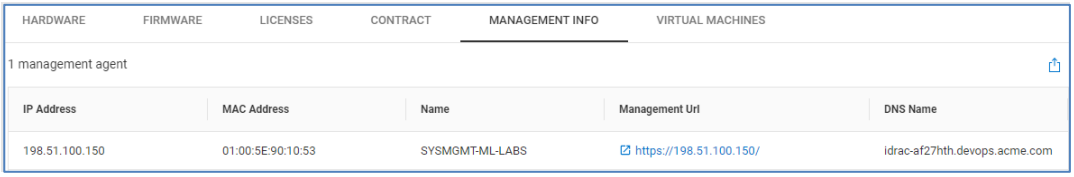
Contract

The **Contract** tab shows support contract information. This includes Status, a description, the contract type, and start and end dates.



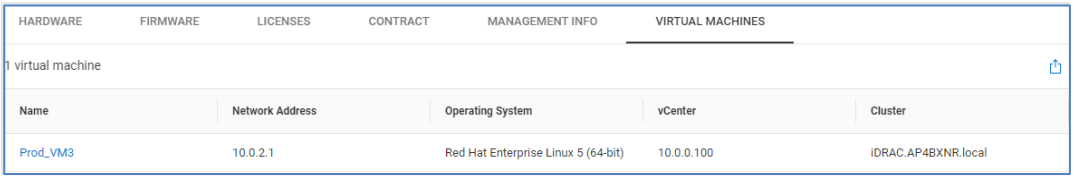
Management Info

The **Management Info** tab provides the IP Address, MAC Address, Name, and DNS Name of the iDRAC. There is also a hyperlink to launch the iDRAC management URL so that users can quickly go to the iDRAC and perform any necessary remote management tasks.



Virtual Machines

The **Virtual Machines** tab is visible for servers running ESXi and lists out various information about each VM including name, IP address, operating system, vCenter name, and ESXi Cluster.

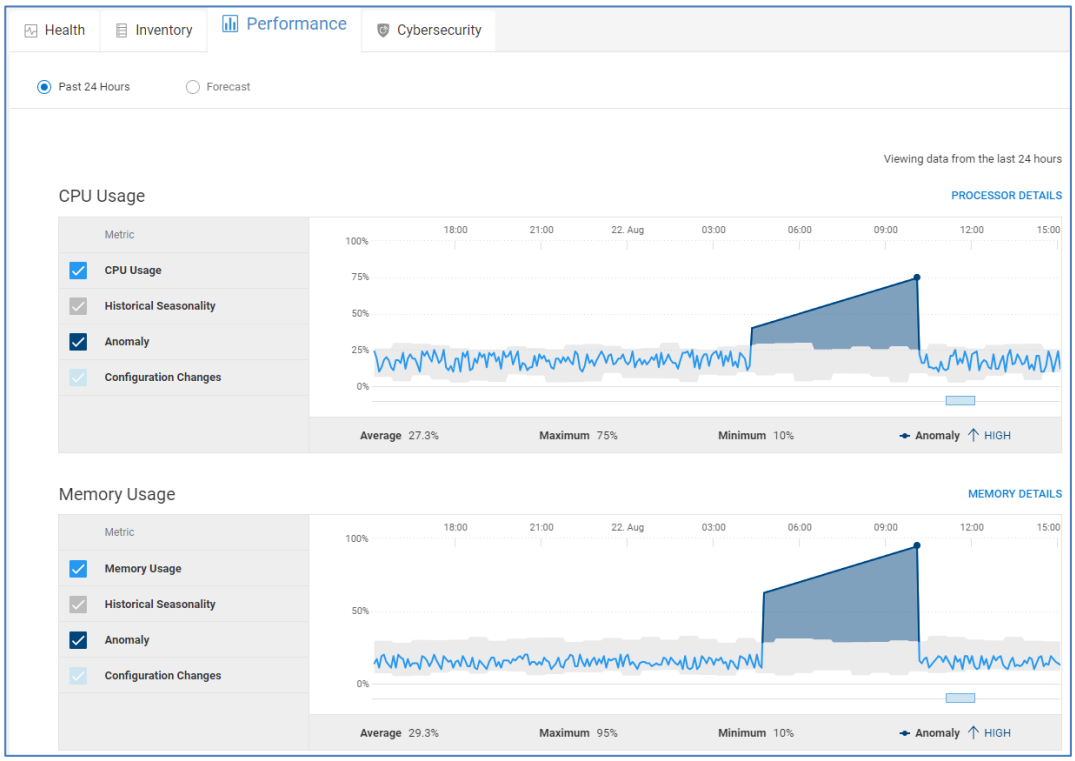


PowerEdge system details – Performance

The **Performance** tab provides 24-hour charts for key performance metrics including:

- CPU Usage
- Memory Usage
- SYS Usage
- System Board IO Usage
- CPU Temperature
- System Inlet Temperature
- System Net Airflow
- Power Consumption

Each chart provides the average, minimum and maximum values of the metric during the time period. Performance anomalies are highlighted in the charts as dark blue shaded areas. Configuration changes are identified with blue rectangles along the X-axis. Clicking the rectangle opens a window that provides details about the configuration change. The following is an example of the CPU and Memory Usage chart.

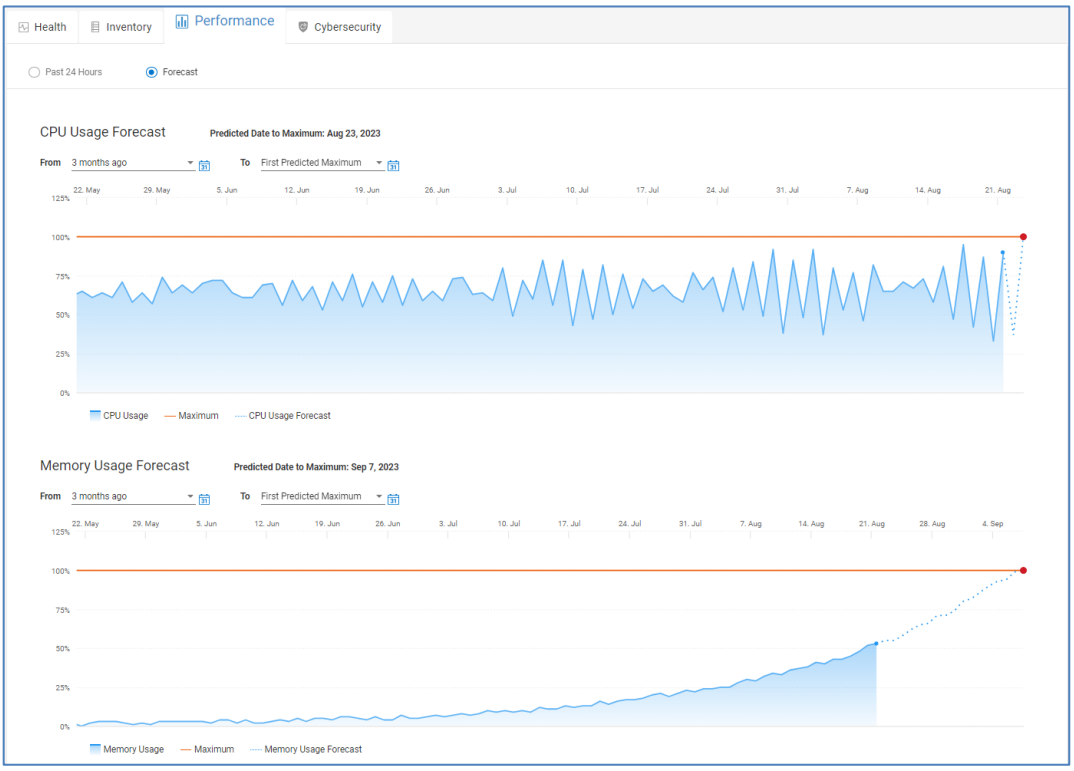


Note: Available metrics vary based on license type, hardware, and firmware levels. See the CloudIQ for PowerEdge section of the OpenManage Portfolio Software Licensing Guide for additional details.

Observability also provides performance forecasting charts for PowerEdge. The forecasting charts are available for:

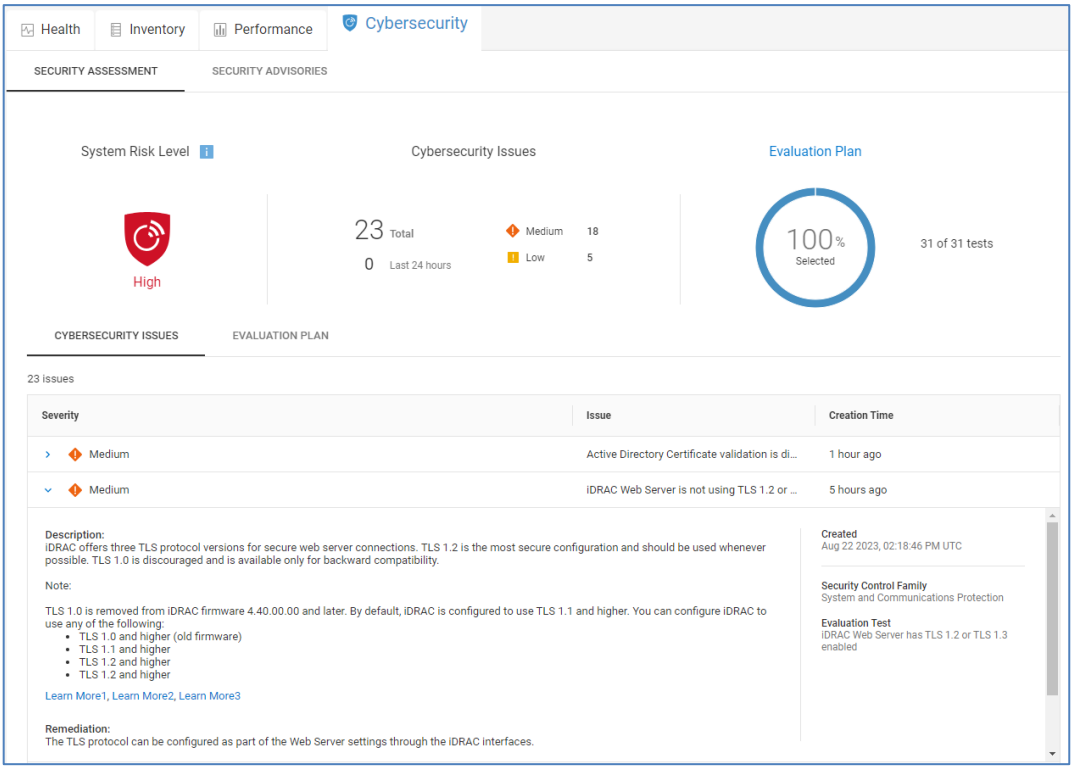
- CPU Usage
- Memory Usage
- System Usage
- IO Usage

Observability uses predictive analytics to understand the historical trends and usage and determine when these resources will reach their maximum value. By identifying when a resource will be fully used, Observability helps with workload planning, allowing users to plan to add additional resources to a server or migrate certain workloads to lesser used systems.



PowerEdge system details - Cybersecurity

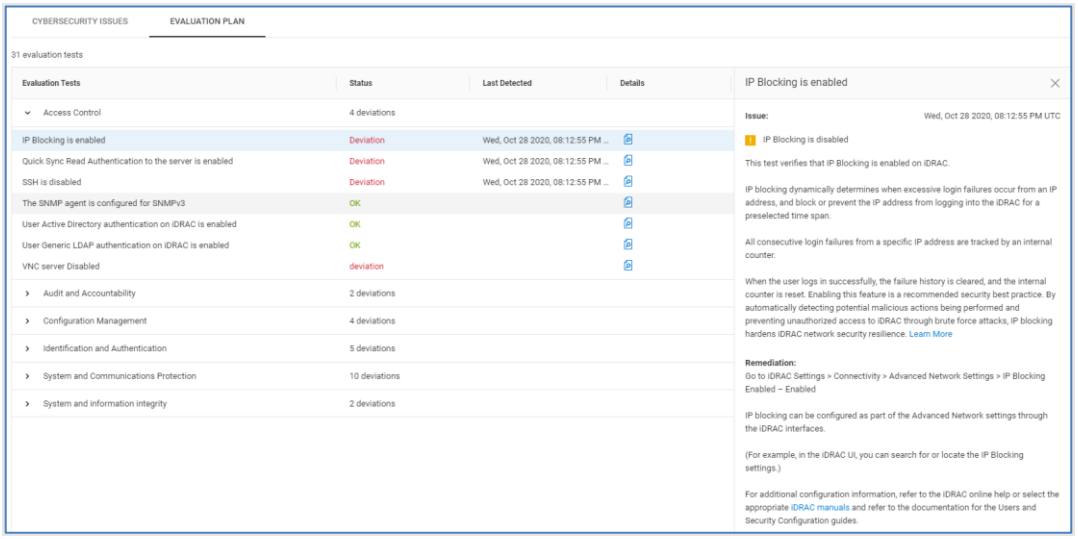
The **Cybersecurity** tab is available for PowerEdge servers and chassis that have cybersecurity collections enabled in OpenManage Enterprise. The Security Assessment tab provides the risk level of the system, a summary of the cybersecurity issues and severities, and a chart showing the percentage of enabled tests in the evaluation plan. There are two tabs at the bottom of the screen: Cybersecurity Issues and Evaluation Plan. The Cybersecurity Issues tab lists the active issues along with the recommended remediation and the time the issue was identified.



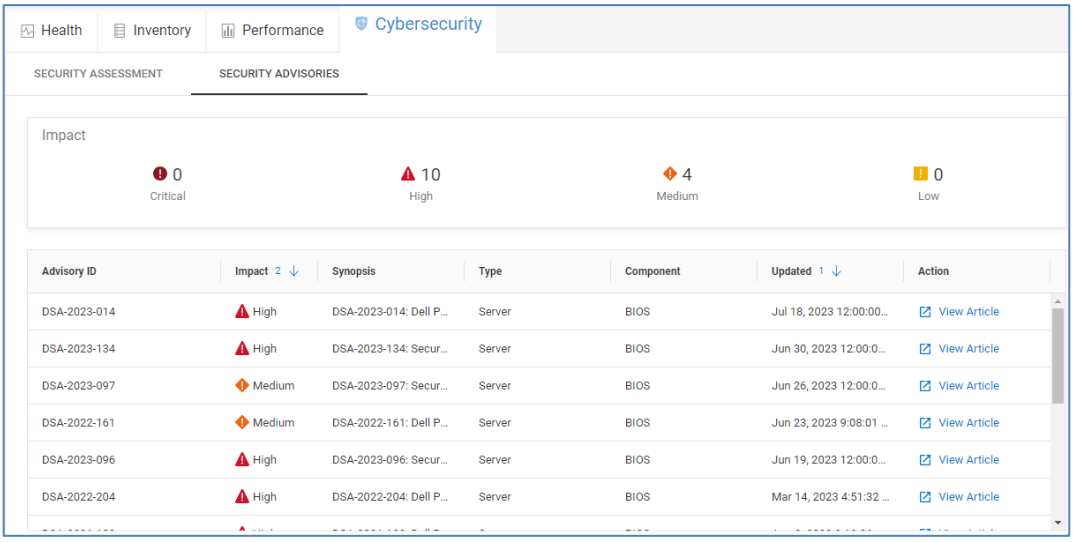
The Evaluation Plan tab lists the possible tests and the status of each test:

- Not in Plan: The test is not part of the evaluation plan.
- Deviation: The test is enabled, and there is an active issue.
- OK: The test is enabled, and there are no active issues.
- Not Supported: The test is not supported.
- Not Applicable: The test is for a capability that depends on another capability that is disabled.
- Not Evaluated: The test is for a system with a disabled evaluation plan or for a system with an enabled evaluation plan, but the test has not yet been run.

The Details icon shows the test description and in instances where there is an active deviation, it shows the recommended remediation.



The Security Advisories tab lists any Dell Security Advisories that are applicable to the server or chassis. Selecting the View Article link directs the user to the corresponding knowledge base article for the DSA.



Data protection details

Introduction

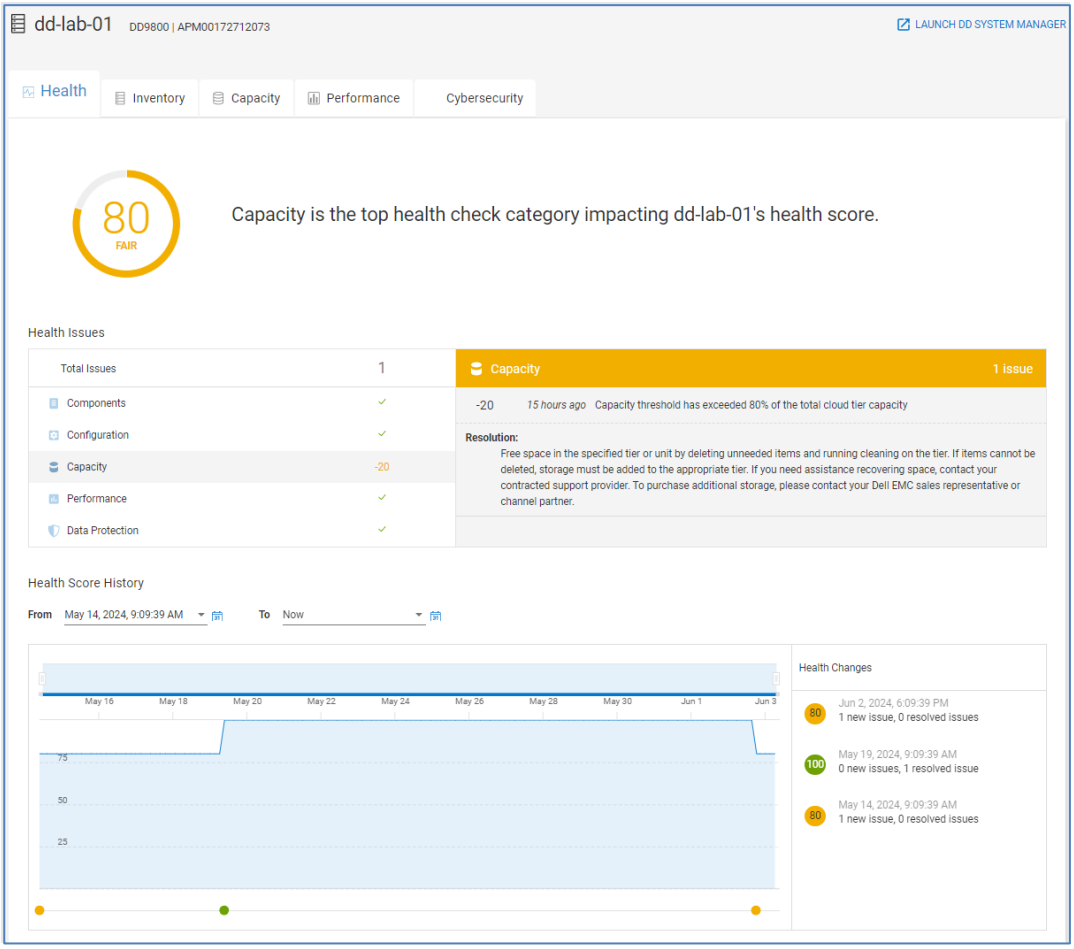
Infrastructure Observability includes the ability to monitor PowerProtect DD series backup storage systems and PowerProtect Data Manager. This section describes the current use cases for each.

PowerProtect DD

There are at least four tabs available on the system details page for PowerProtect DD: Health, Inventory, Capacity, and Performance. The Cybersecurity tab is available for those PPDD systems that have cybersecurity collections enabled in DD System Manager. The “Launch DD System Manager” hyperlink is available on each tab to allow users to quickly go to the element manager in circumstances where additional detailed information is needed. The details available in each tab are presented below.

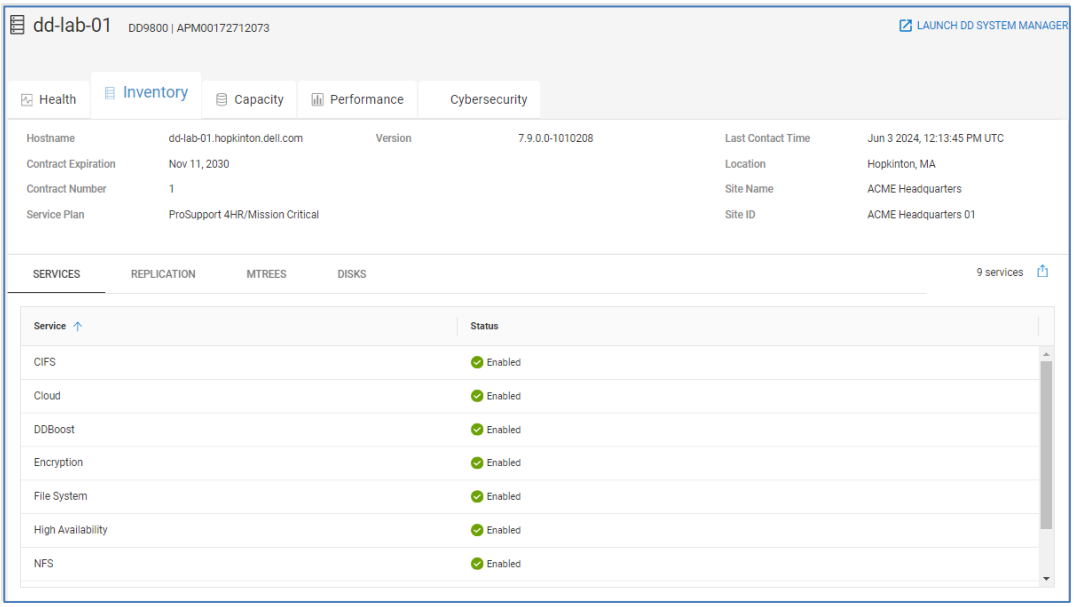
PowerProtect DD system details – Health

All five categories are supported for determining the health score of each DD system. As with all other systems, each issue has a recommended resolution and the health score history is available at the bottom of the page.



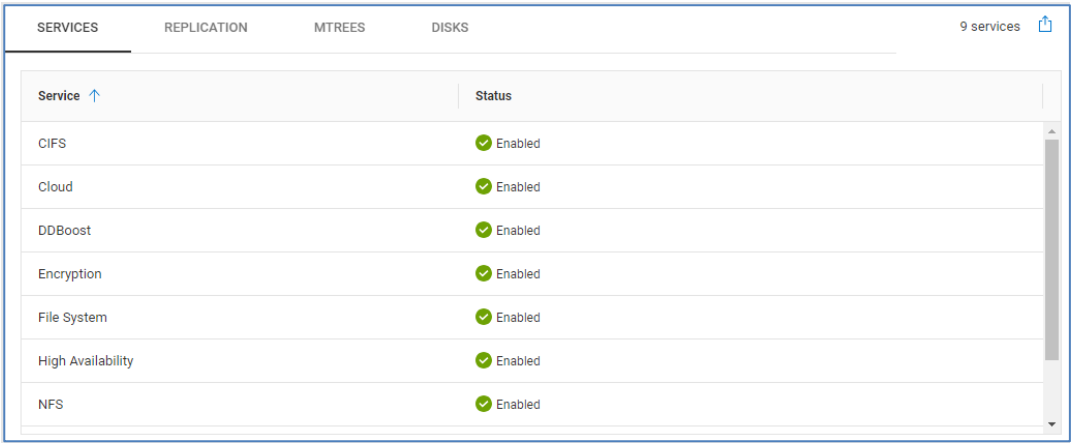
PowerProtect DD system details – Inventory

The top portion of the **Inventory** tab provides various attributes including the serial number, model, site, location, version, and contract information. The bottom of the page contains the following tabs: Services, Replication, MTrees, and Disks. Each tab is discussed below.



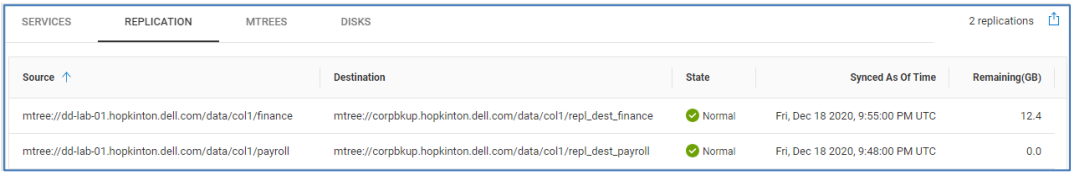
Services

The **Services** tab provides a listing of the various services running on the system along with their status.



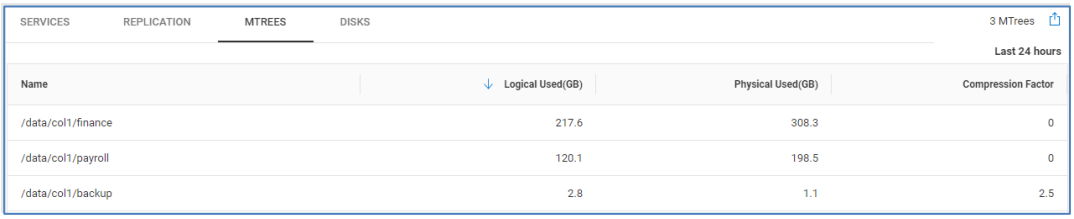
Replication

The **Replication** tab provides a listing and status of the replication sessions on the system. This information includes the source and destination, the state, the time of the last sync, and amount of remaining data to replicate from the source to the destination.



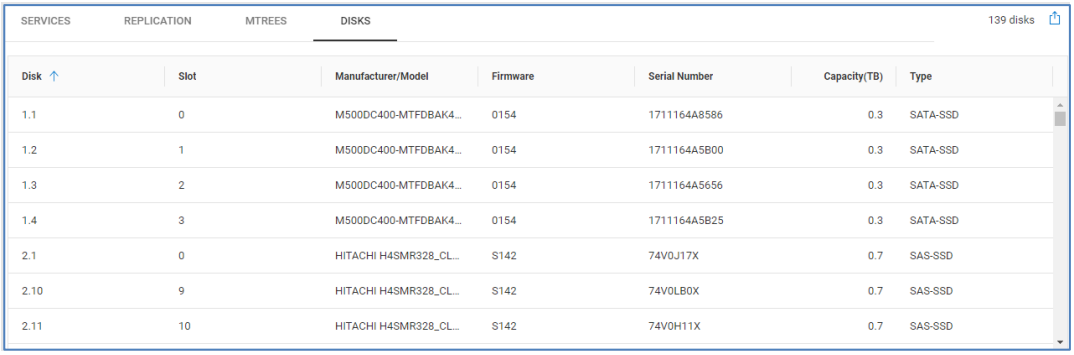
MTrees

The **MTrees** tab lists each of the configured MTrees, Storage Units, Virtual Tape Library (VTL) Pools, and so on, with the logical used, physical used, and compression factor for the last 24 hours.



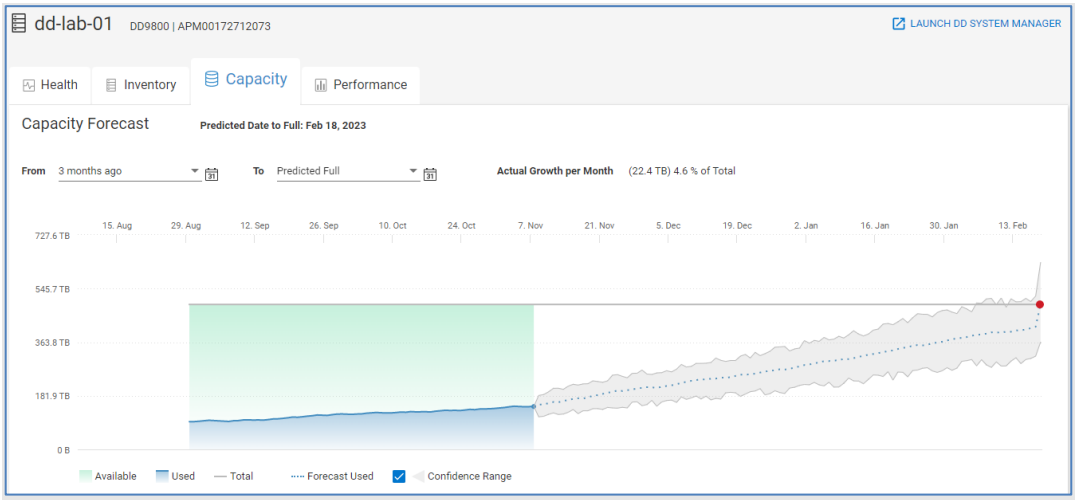
Disks

The final tab is the **Disks** tab. Each disk is listed with its slot, model, firmware, serial number, capacity, and type.



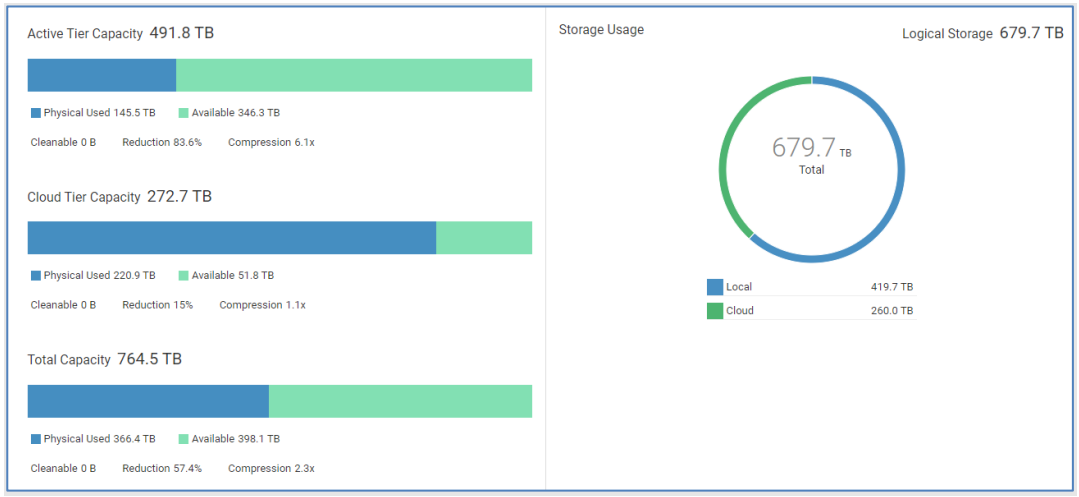
PowerProtect DD system details – Capacity

The top of the **Capacity** tab displays the Capacity Forecast chart with the historical available and used capacity and the predicted used capacity with the confidence range.



The bottom of the page breaks down the physical and logical capacity on the DD system. The left side of this view displays horizontal bar charts for Active Tier and Cloud Tier Capacity. A third chart shows the total of active and cloud tier capacity. Each chart provides the total, used and free capacity. The amount of cleanable storage is also displayed as well as the reduction percentage and compression factor.

The right half of this view provides a doughnut chart of total logical storage broken down between local and cloud. This page allows users to gain insight into the capacity utilization on the system and savings due to reduction and compression.

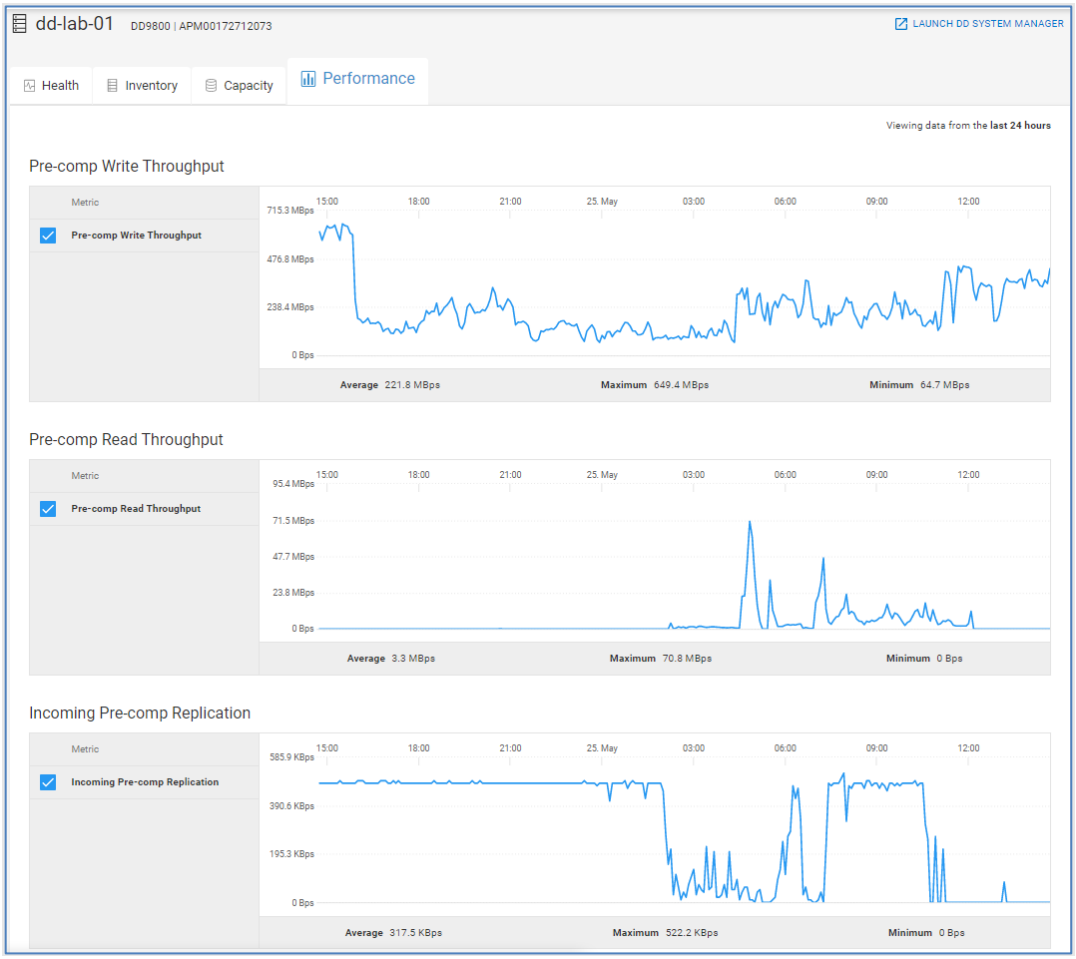


PowerProtect DD system details – Performance

The **Performance** tab provides 24-hour performance charts for the following metrics:

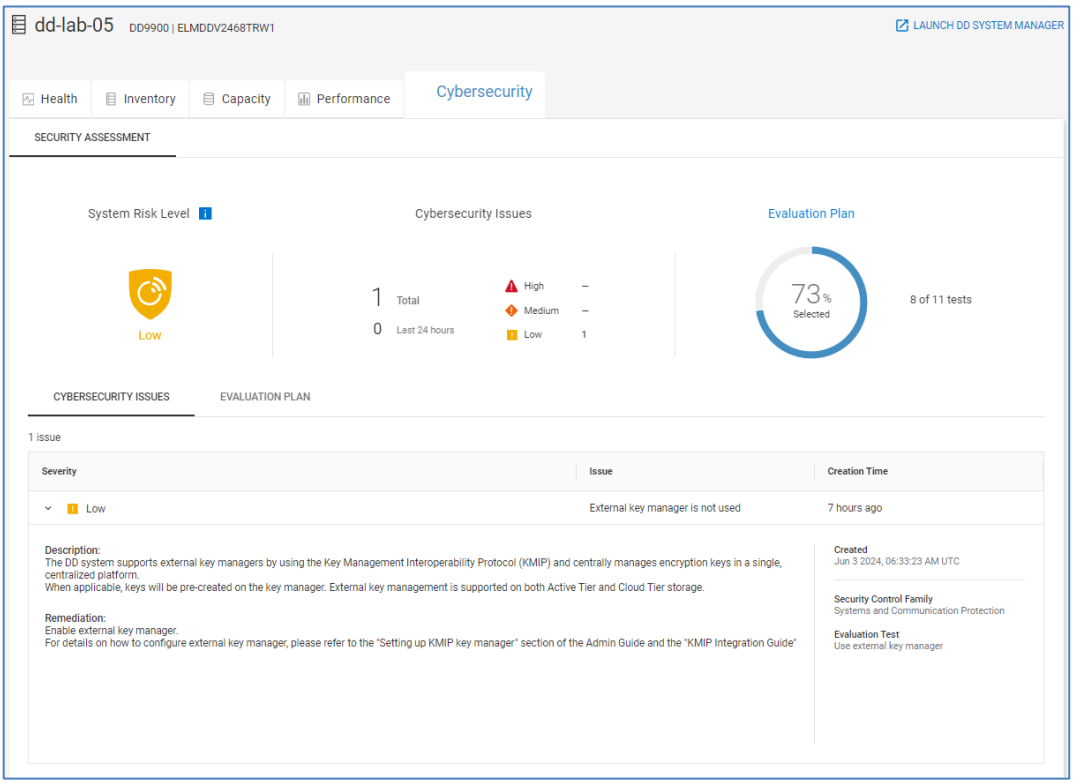
- Pre-compressed Write Throughput
- Pre-compressed Read Throughput
- Incoming Pre-compressed Replication
- Outgoing Pre-compressed Replication
- CPU Usage
- Replication Streams Count (incoming and outgoing)
- Streams Count (reads and writes)

An example of the first few charts is shown below.



PowerProtect DD system details – Cybersecurity

The **Cybersecurity** tab provides the cybersecurity risk level for the PPDD system. When a cybersecurity issue is identified, the recommended remediation is provided for each issue. The **Evaluation Plan** tab lists out the status of each of the possible configuration tests.

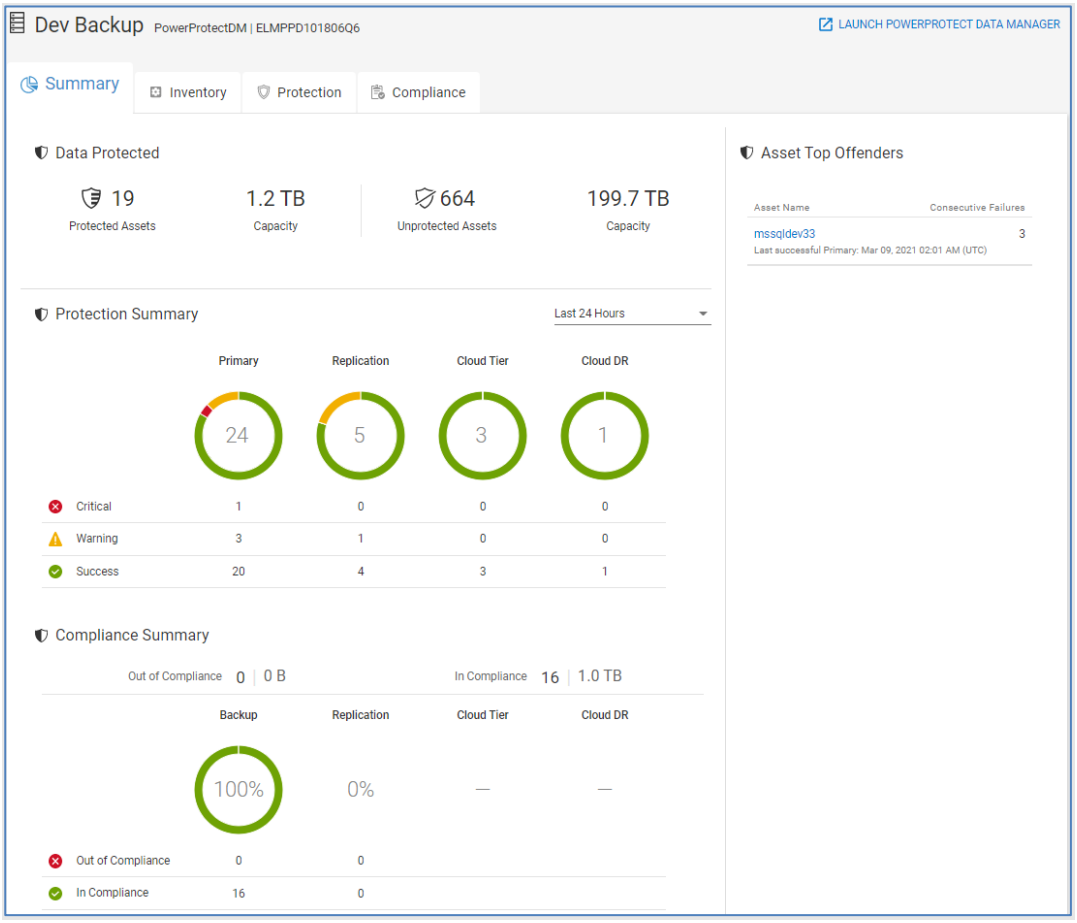


PowerProtect Data Manager

In addition to PowerProtect DD, Observability can monitor instances of PowerProtect Data Manager. This allows users to see reports from Data Manager directly in the Observability UI. We saw earlier that instances of PowerProtect Data Manager are displayed in Data Protection tab in the multisystem view for Inventory. Selecting an individual instance of Data Manager directs the user to the details page which has four tabs: Summary, Inventory, Protection, and Compliance. Each tab is discussed below.

PowerProtect Data Manager details – Summary

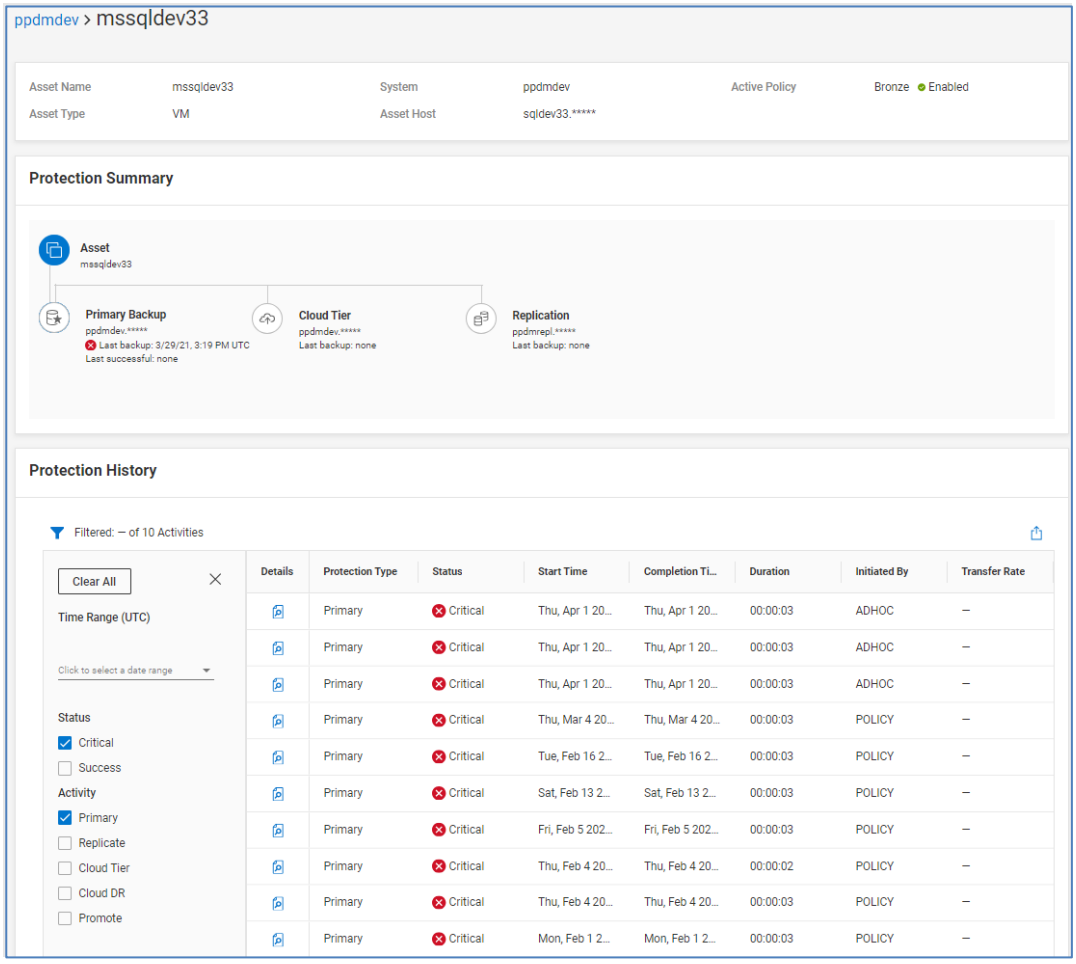
The **Summary** tab allows the user to quickly see status and resource information for the protection environment. The Data Protected section provides total amount of protected and unprotected assets with their capacity.



The **Protection Summary** section summarizes the number of assets that are protected within a specified time range. The last 24 hours is the default time range, but this can be changed to either last 3 days or last 7 days. The status is critical if all protection activities failed during the selected time range. Warning means that the asset has both failed and successful protection activities. Success means all protection activities completed successfully. The assets are grouped into one of the following four backup categories: Primary, Replication, Cloud Tier, and Cloud DR.

The **Compliance Summary** section displays the number and percentage of assets in each of the four backup categories that are in and out of compliance with their protection policy.

The **Asset Top Offenders** section lists those assets with the most consecutive failures. For those assets, a link to the asset details page is available. The asset details page shows the status of the last backup and the protection history of the asset. Users can filter the Protection History table by time range, status, or activity.

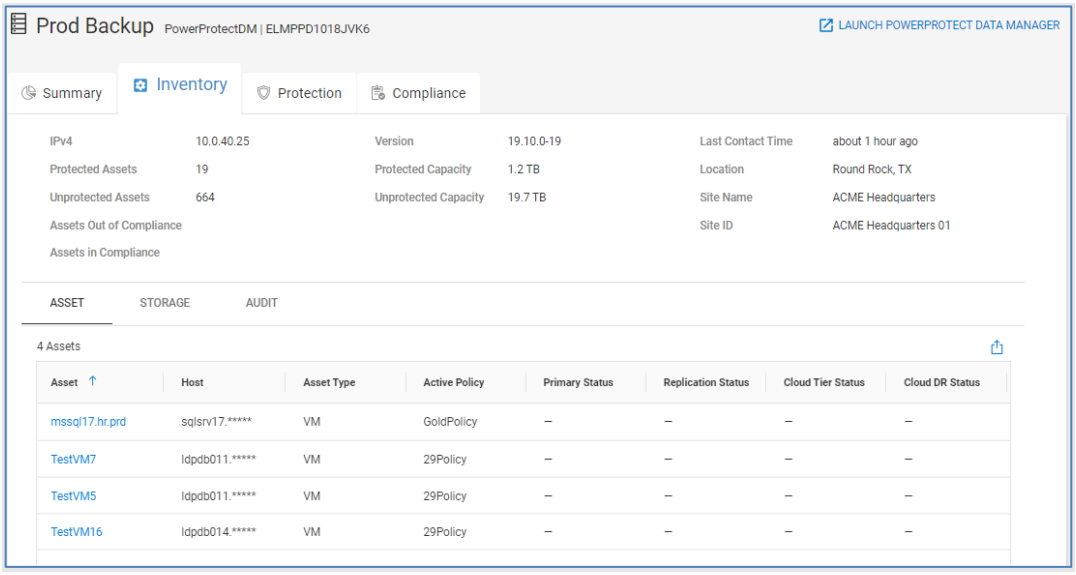


PowerProtect Data Manager details – Inventory

The **Inventory** tab shows various configuration information at the top of the page. The bottom of the page has three tabs: Asset, Storage, and Audit.

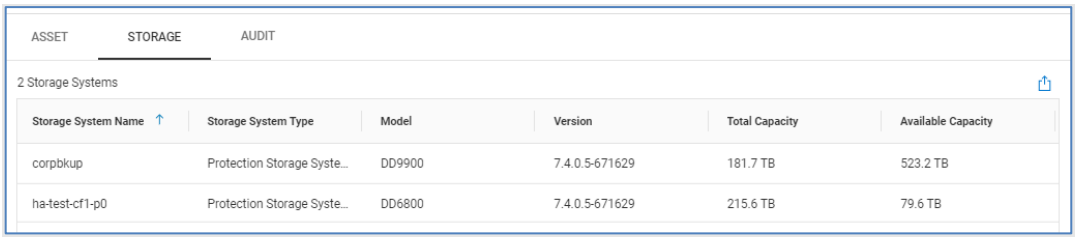
Asset

The **Asset** tab shows the assets discovered by PowerProtect Data Manager along with the host, asset type, active policy, and status of the most recent backup.



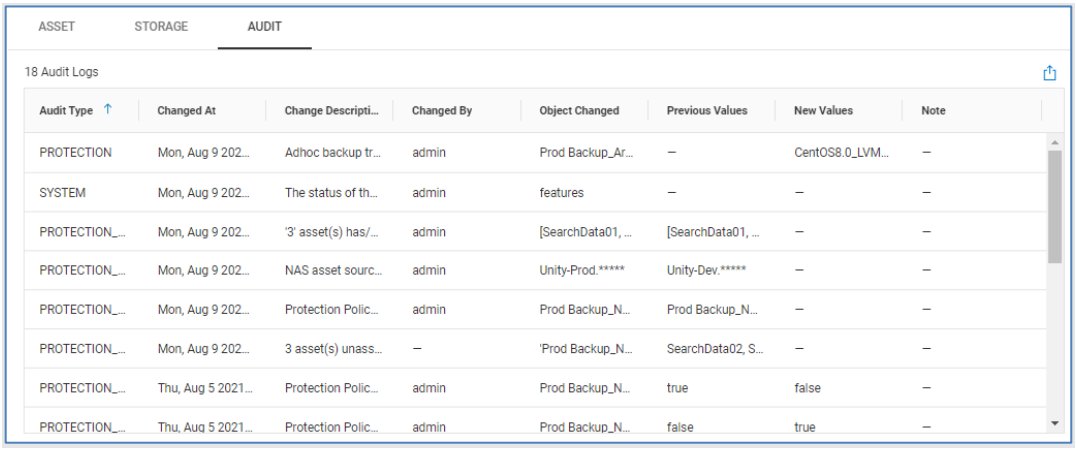
Storage

The **Storage** tab shows the storage systems available to PowerProtect Data Manager systems. The model and total and available capacity are listed for each system.



Audit

The **Audit** tab aggregates the audit information from each of the PowerProtect Data Manager systems. It provides a list of changes on the system, time of the change, the user that made the change, the changed object, and the old and new values.



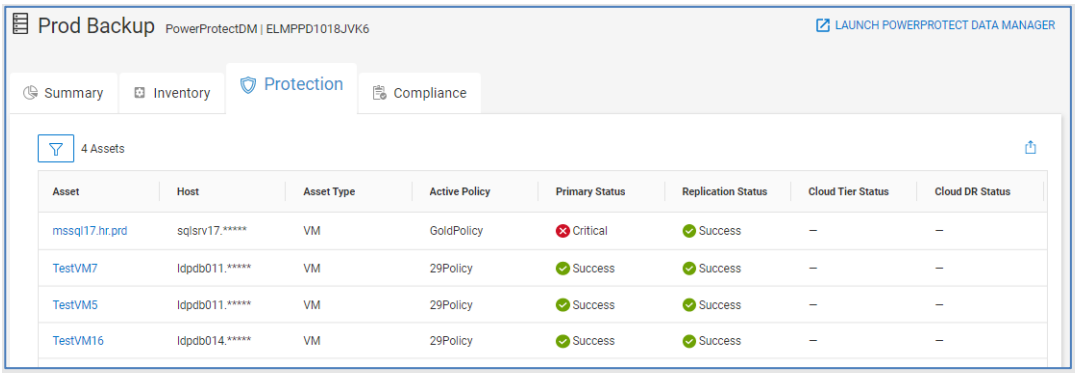
PowerProtect Data Manager details – Protection

The **Protection** tab provides additional details of the protection status for each asset. This tab includes the following:

- Asset name and the host on which it is running

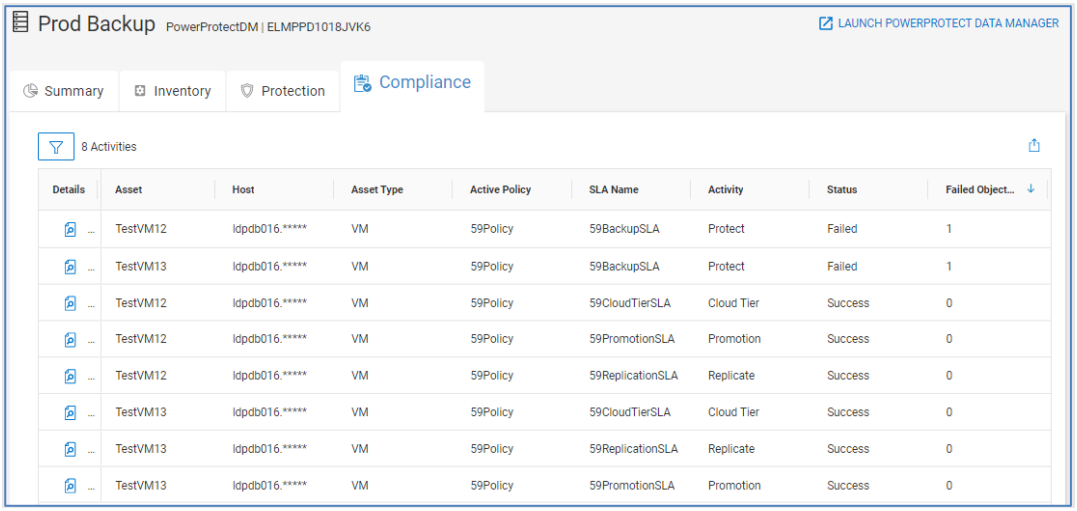
- Asset type (VM, Database, File System, VMAX Storage Group, or Kubernetes)
- Name of the active protection policy
- Status of each protection activity for the asset

A dash indicates that protection activity is not configured for the asset.

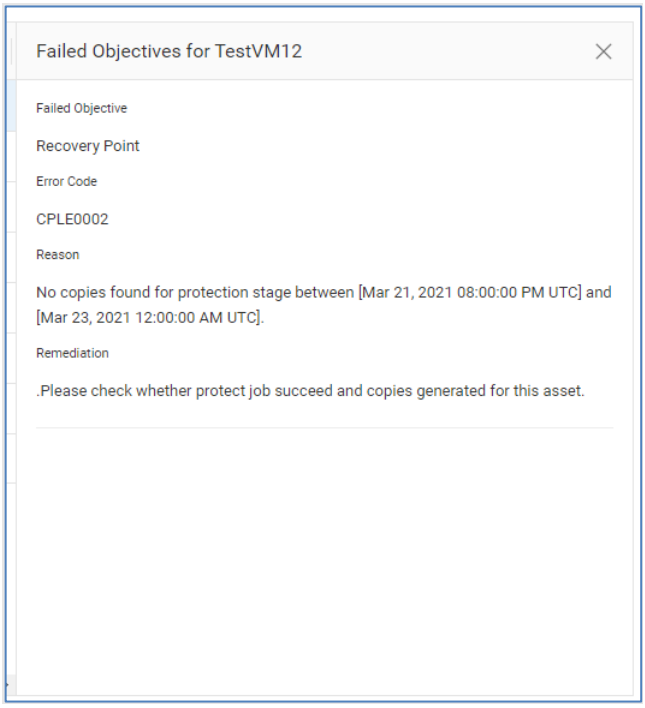


PowerProtect Data Manager Details – Compliance

The **Compliance** tab displays details of each asset's compliance for each configured activity to the defined service level agreements in the protection policy. This tab includes the asset name and the host on which it is running, the asset type, the active policy, SLA name, activity type, status, and the number of failed objectives.



For instances where there is a compliance failure, the Details button provides additional information. This information includes the failed objective, the error code, the reason, and remediation.



Converged Systems details

Introduction

Infrastructure Observability can monitor VBlock and VxBlock Converged Systems. Converged Systems component information is displayed in the Health and Inventory views under the CONVERGED tab. The Health category is available for the storage components of the system and only if the storage component is registered in Observability.

The **Lifecycle** menu provides the various milestone dates for each of the components in the Converged System. It also has a **Service Contracts** page and a **CI Code Compare** page. Each of these areas is described in the following sections. Selecting the Converged System hyperlink from either the Health or Inventory multisystem view opens the system details page.

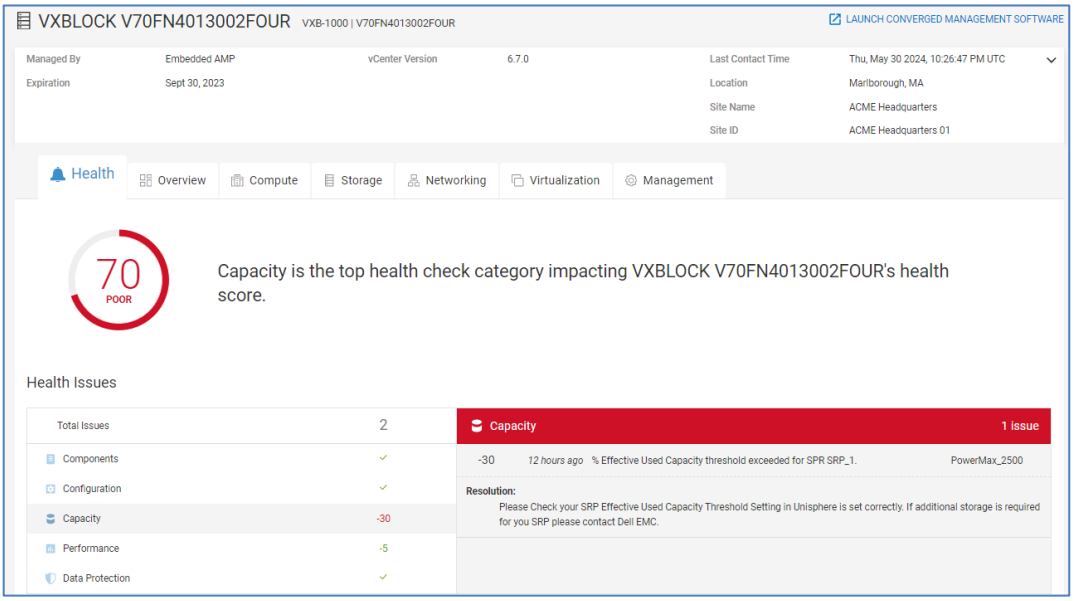
Selecting the system name hyperlink for the Converged System from the Inventory menu opens the system details page. The top of the system details page provides information similar to what is displayed in the multisystem view. The bottom of the page has up to seven tabs: Health, Overview, Compute, Storage, Networking, Virtualization, and Management for more detailed information.

Note: Users can onboard VMware, Connectrix, and Storage components of a VxBlock individually to use other Observability features described in this document.

Converged System - Health

The **Health** tab provides a proactive health score for the system. The health score is determined by the storage in the system. The health score is based on the lowest health score of all the storage systems associated to the converged system. The storage systems must be configured to send data back to Observability independently from the

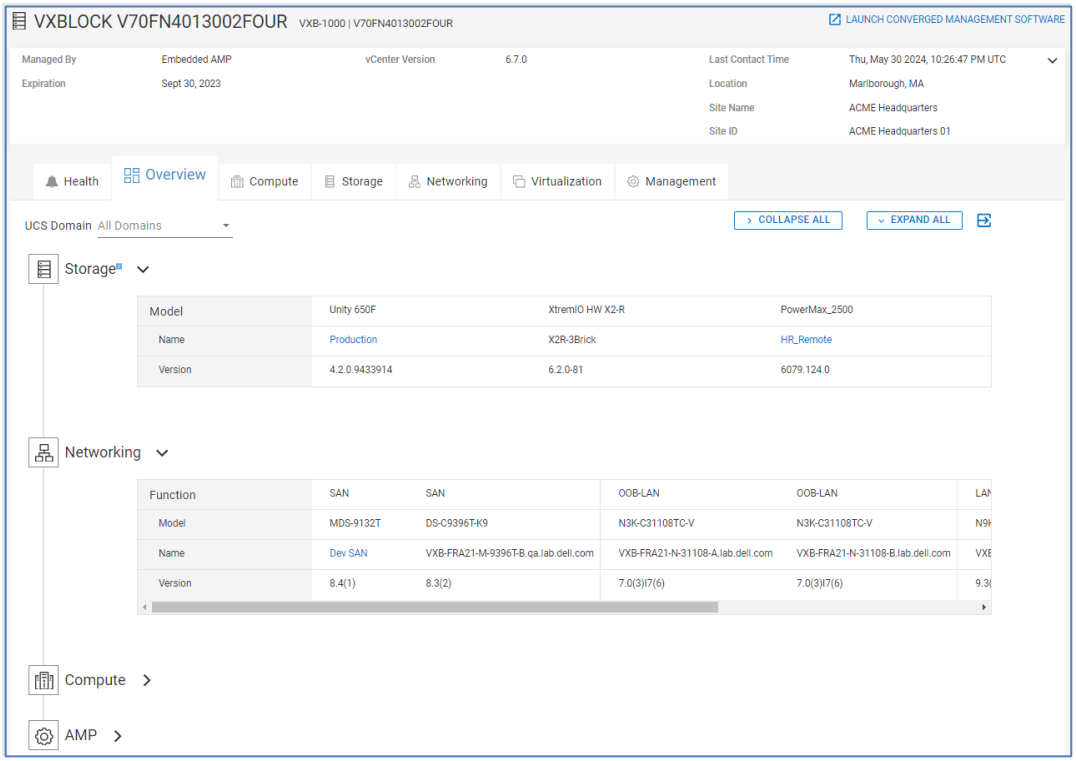
Converged System. As with other systems, recommended remediations and health score history are available.



Converged Systems – Overview

The **Overview** tab provides a high-level view of the components, software, and firmware versions that make up the converged system. The components include storage, networking, compute, and AMP (management).

- **Storage** – Listing of the types of storage arrays in the Converged System along with the names and firmware versions of the arrays.
- **Networking** – Listing of the LAN and SAN switches in the Converged System along with switch model, name, and firmware version.
- **Compute** – Listing of compute resources including the fabric interconnects per domain, chassis information, FEX information, and server profiles.
- **AMP** - Details of the storage array, managed applications, and server profiles for the Advanced Management Pod (AMP).



Converged Systems - Compute

The **Compute** tab provides information about the UCS servers in the Converged System and their resources. There can be up to four tabs under computer including server profiles, fabric interconnects, chassis, and fabric extenders (FEX).

Server Profiles – Provides number of Cisco UCS servers aggregated by server type and the number of UCS blade and rackmount servers. Also displays server profile information including profile name, number of servers in each profile, type of UCS server, and software version running on the server. The details of each profile can be opened and displays information in the following tabs: Summary and Servers.

- **Summary** – Displays hardware and software information about the profile including the operating system, storage, and MLOMs and mezzanines.
- **Servers** – Displays the location, serial number, hostname, and CPU information for each server in the server profile.

Fabric Interconnects – Provides the number of each type of fabric interconnect switch and the number and type of each of UCS server. Also displays a list of FI switches including the switch name, model number, fabric connected to the FI, UCS manager version of the FI and the FI serial number. The details of each FI switch can be opened and displays information in the following tabs: Summary, Configuration, Ports, and Hardware.

- **Summary** – Displays versions of Cisco switch operating system and UCS software running on the FI switch.
- **Configuration** – Displays number of ports for each role, including server, LAN, and SAN uplink ports. Also displays LAN and FC aggregate bandwidth for LAN and SAN ports, respectively.

- **Ports** – Displays port information including connections, port speed, and port role. The user can filter the port list.
- **Hardware** – Displays hardware information about FI switch including number of fan bays, number of fans and number of power supplies.

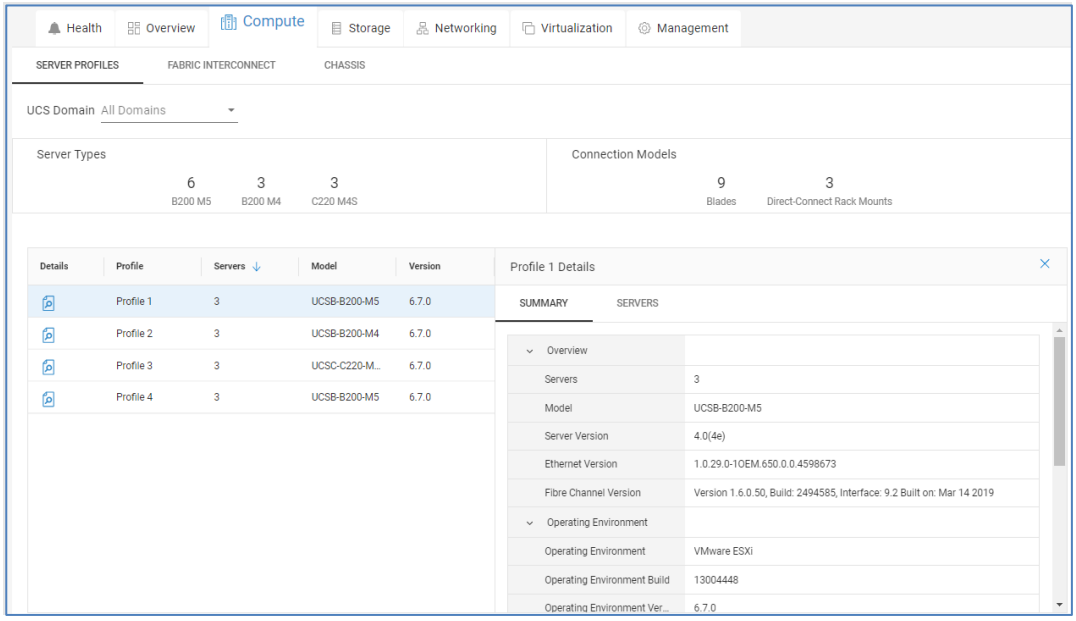
Chassis – Displays information about the UCS Chassis including the number of each type of UCS Blade servers and the number of used and available slots in the chassis. Also displays high-level chassis information including the UCS domain, chassis name, and serial number. The details of the chassis can be opened and displays information in the following tabs: IOMs and Hardware.

- **IOMs** - Displays the chassis model, serial number, number of active links, aggregated bandwidth, and firmware version for each IOM.
- **Hardware** – Displays number of fans, fan bays, and power supplies for the chassis.

Fabric Extenders – Displays the number of each type of UCS server connected to the FEX. Also displays high-level information about the FEX switches including UCS domain name, FEX name, model number, the fabric interconnect to which the FEX is connected and the FEX serial number. The details of each FEX can be opened and displays information in the following tabs: Configuration, Ports, and Hardware.

- **Configuration** – Displays number of ports connected to UCS servers and uplinks as well as the uplink bandwidth and aggregate bandwidth for each fabric.
- **Ports** – Displays port information including connections, port speed, and port role. The user can filter by port role to see only those ports connected to servers or FI uplinks.
- **Hardware** – Displays hardware information for each FEX including name, product ID, serial number, and software version running on the FEX. Hardware Summary provides number of fans and power supplies for the FEX.

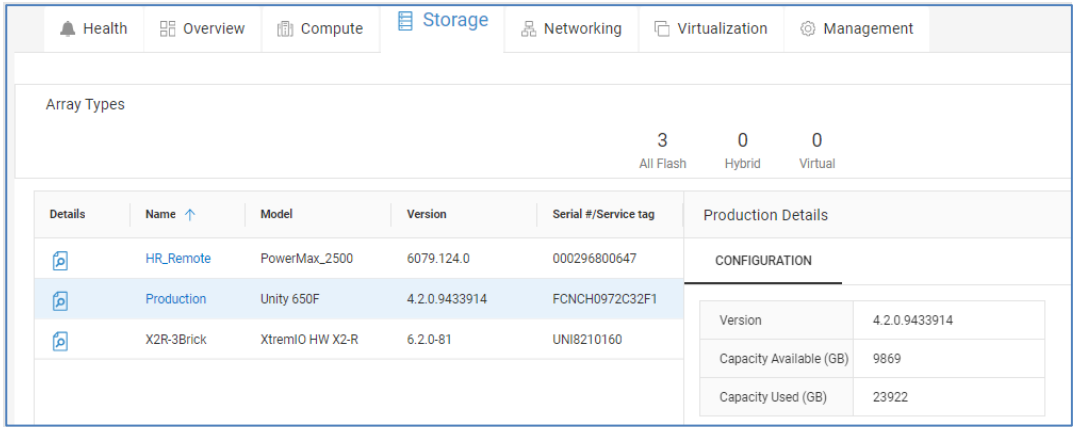
The following shows an example of the Server Profiles tab under Compute.



Storage

The **Storage** tab provides information about each storage array. Configuration and hardware information is provided for each storage array; additional information will differ depending on the array type.

- **Configuration** – Listing of software versions, firmware versions, and capacity information.
- **Hardware** – Listing of drive enclosures and disks.

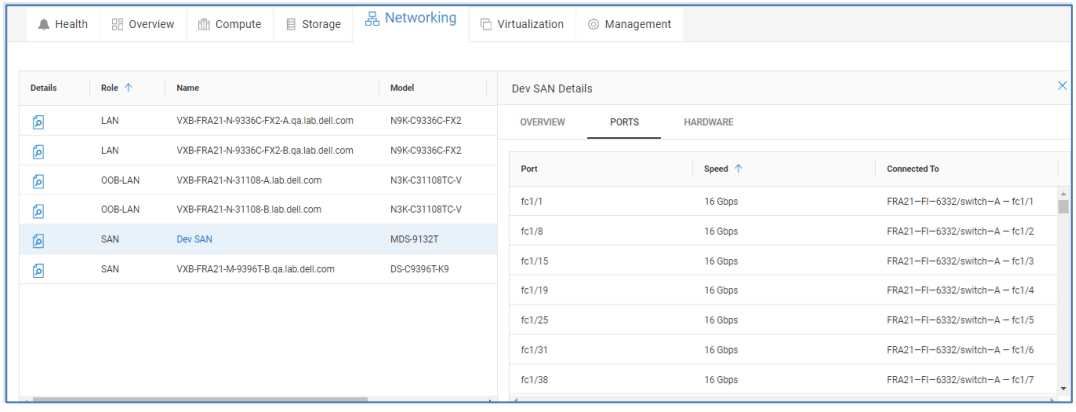


Networking

The **Networking** tab provides information about the network switches in the system including role, name, model, software version, and serial number.

Opening the details about each switch provides the following tabs: Overview, Ports, and Hardware.

- **Overview** – shows port breakout utilization and port usage
- **Ports** – shows port, port speed and connected to device
- **Hardware** – summary of fans, fan bays, power supplies, and power supply bays



Virtualization

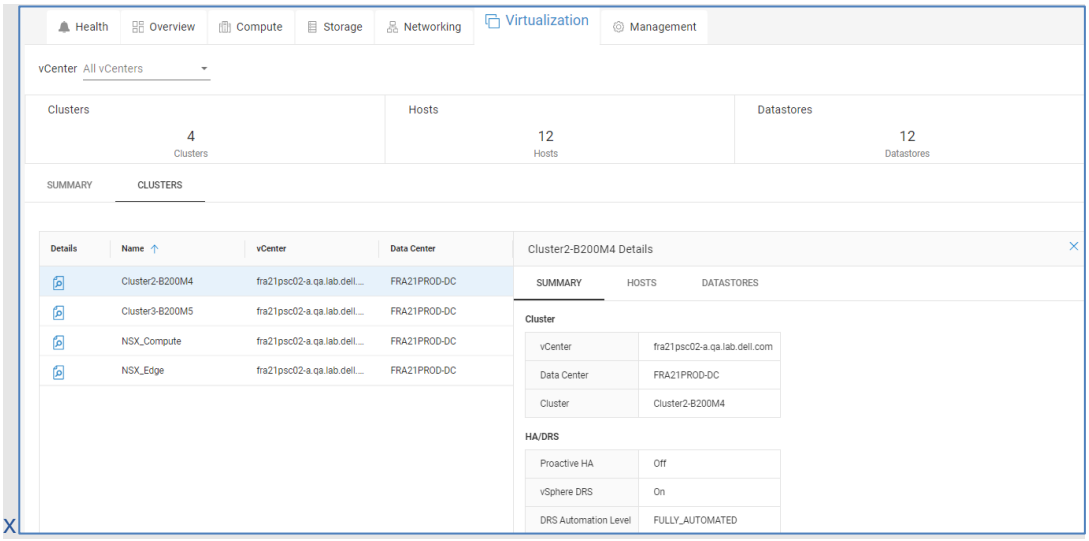
The **Virtualization** tab provides information about each VMware vCenter in the Converged System. Summary level information at the top of this view includes number of

clusters, hosts, and datastores associated with the vCenter server. There are two tabs under Virtualization: Summary and Clusters.

Summary – vCenter Configuration information including name of the vCenter server, hostname, vCenter version, and workload type (AMP or Production).

Clusters – Name of the cluster, name of the vCenter managing the cluster and the data center name. The details of each cluster can be opened and displays information in the following three tabs: Summary, Hosts, and Datastores.

- **Summary** – Summary level information for the cluster and the HA or DRS configuration.
- **Hosts** – Listing of ESXi hosts that make up the cluster including ESXi version, Ethernet version, Fibre Channel version, and server type.
- **Datastores** – Listing of associated datastores for the cluster including datastore name, total capacity, and free capacity.



Management

The **Management** tab provides information about the AMP and is divided into the following tabs: Server Profiles, Storage, Virtualization Summary, and Workload.

Server Profiles – Includes name of the server profile, number of UCS servers in the server profile, model of UCS servers and firmware version of each UCS Blade server. The details of each profile can be opened and displays information in the following tabs: Summary and Servers.

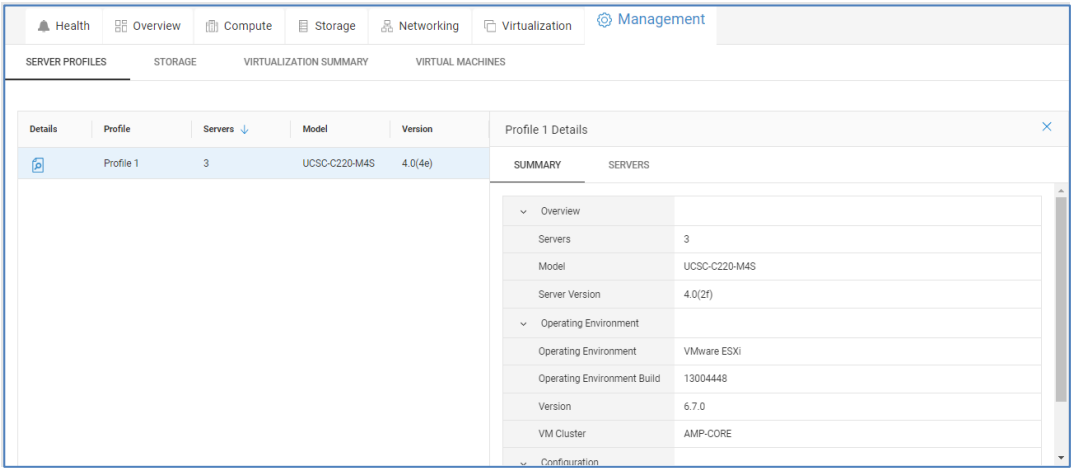
- Summary – Hardware and software information about the server profile including the operating environment, storage, and MLOMs and mezzanines.
- Servers – Displays the serial number, hostname, and memory for each server in the server profile.

Storage – Information about the storage for the AMP including the name, model, and operating system. The details of each storage system can be opened and displays information in the following tabs: Configuration and Hardware.

- Configuration – Displays firmware and total and free capacity.
- Hardware – Displays number of drive enclosures and disks.

Virtualization Summary – Virtualization information about the AMP including vCenter configuration and virtual resources.

Workload – Provides virtual machine information about the AMP including VM name, ESXi host, VM operating system, and the running state of the VM.



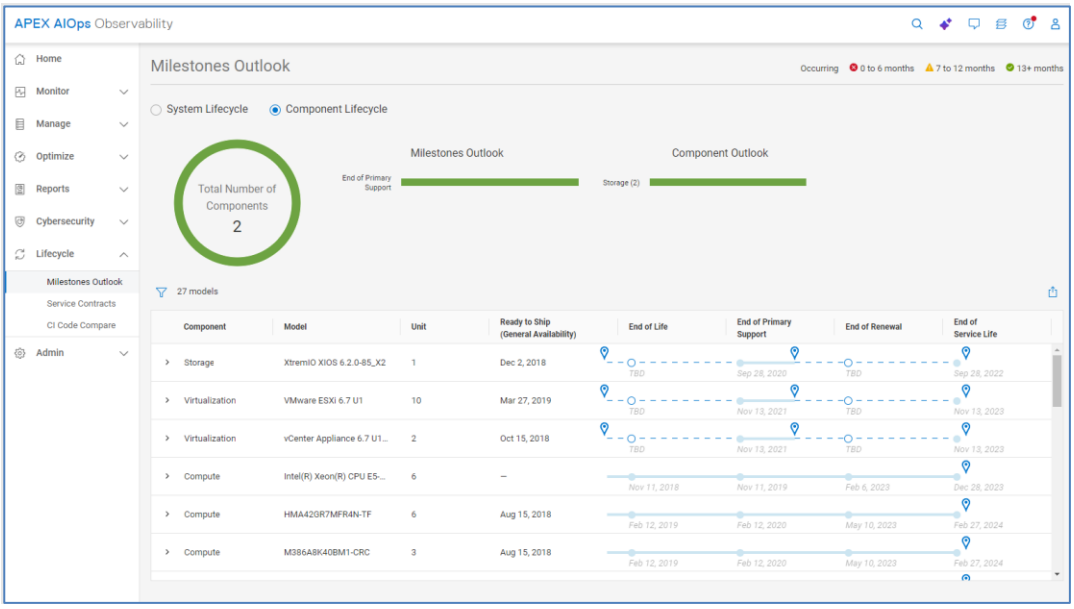
Converged Systems – Milestones Outlook

Observability helps provide life-cycle support for the various components of a Converged System. The Milestones Outlook page lists out the various components that make up the Converged System and provides timelines with the following dates: General Availability, End of Life, End of Support Life, End of Renewal and End of Service Life.

The information provided in the timeline helps users to:

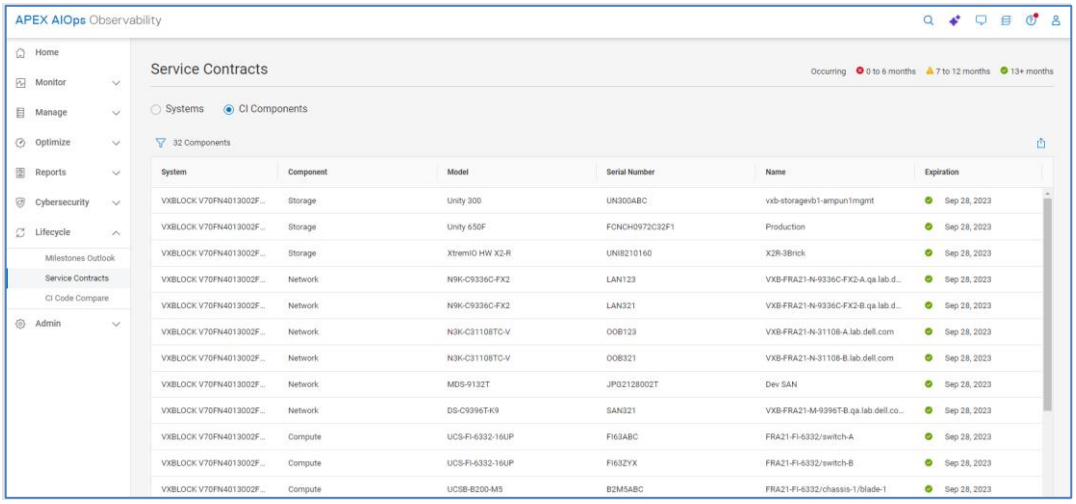
- Develop plans to order next generation of components to replace existing components reaching their end of service life date.
- Determine financial needs and budget for components that require replacement in the next 0-6, 7-12, or 12+ months.
- Schedule upgrades and hardware replacements during off peak hours that do not impact operations.

The top of the page provides a graphical representation of the total number of components and highlights in red the number of components reaching a milestone date within six months. The bottom of the page provides the timelines for each component. The Refine button allows the user to filter the information based on System Name or Component Type. It also allows the user to select from a predefined set of life-cycle dates or enter a custom date range. For example, to see all components with a milestone date during 2022, enter a date range of 01/2022-12/2022 as shown below.



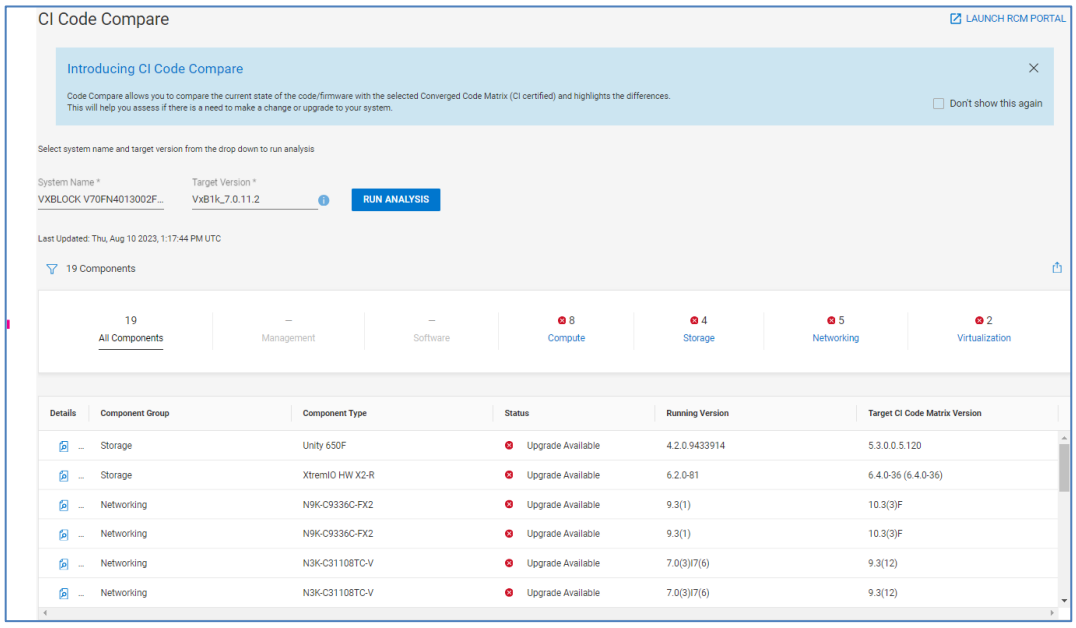
Converged Systems – Service Contracts

The **Service Contracts** page lists service contract information for both the VxBlock system and the components of the system. Users can select between the Systems and CI Components view using the radio button on the top of the page. The following screenshot shows contract information for the components. The filter allows users to refine the view based on system ID, component type, expiration date, or a custom date range.



Converged Systems – CI Code Compare

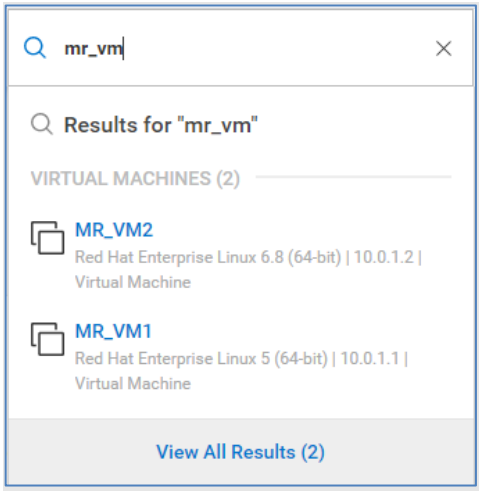
The **CI Code Compare** page allows users to compare the current state of the code and firmware with the selected target Converged Code Matrix (CI certified) and highlights the differences. This helps users identify which components of the system need to be upgraded.



VMware details

Infrastructure Observability supports integration with VMware environments. It uses a local collector that communicates to vCenter using a read-only privilege. The collector sends the data back to Observability through the Secure Connect Gateway.

Besides viewing VMs in the Virtual Machines tabs detailed earlier in this document, users can search to find a VM and access the Virtual Machines Details page.



The search results immediately provide some initial information about the VM including name, operating system, and IP address. Selecting “View All Results” provides additional details including vCenter, ESXi, Datacenter, and ESXi Cluster.

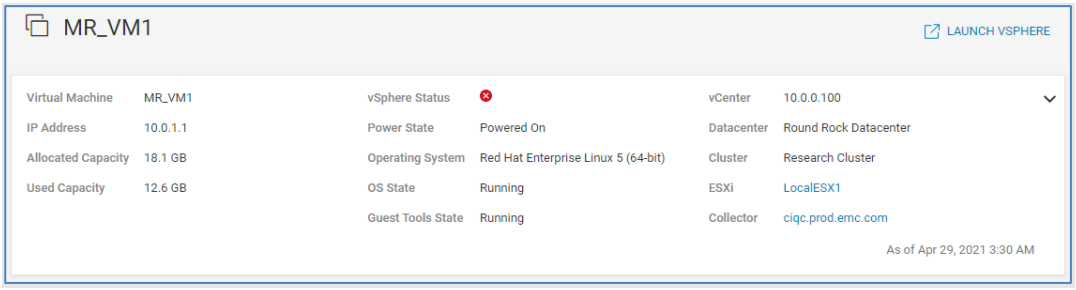
The search feature will find the following VM-related properties:

- VM name

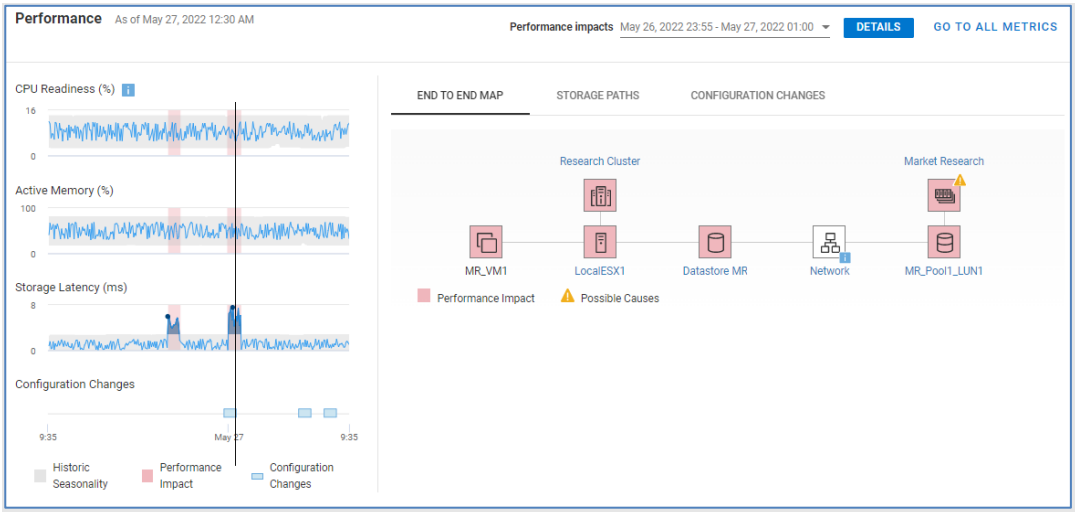
- vCenter
- ESXi Server
- ESXi Cluster
- Datacenter

Selecting the VM name hyperlink directs the user to the Virtual Machine Details page.

The top of the VMware Details page contains various properties and attributes for the VM. It includes capacity information to understand the amount of storage allocated and used by the VM as well as vCenter and ESXi cluster information to understand where the VM resides. The downward pointing carat in the upper right of the window will minimize this section of the UI.



The bottom half of the page is dedicated to performance and storage path information. The left side of the window displays three 24-hour charts for the following key performance metrics: CPU Readiness (%), Active Memory (%), and Storage Latency (ms). Performance anomalies are identified in any of the charts as shaded blue areas. Observability identifies performance impacts on the storage latency chart with pink shading. There is also a 24-hour chart that identifies configuration changes. Selecting a box along the horizontal axis opens a window with details of the configuration change. Selecting a point in the performance charts displays a window showing the values of the historic seasonality and actual value at the selected time.



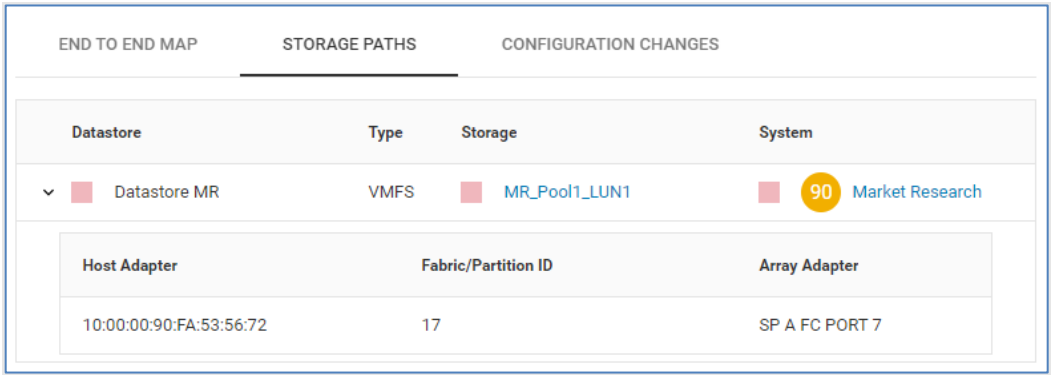
The right side of the window has three tabs: End to End Map, Storage Paths, and Configuration Changes.

End to End Map (shown above) – This tab is an interactive end-to-end map of the following items:

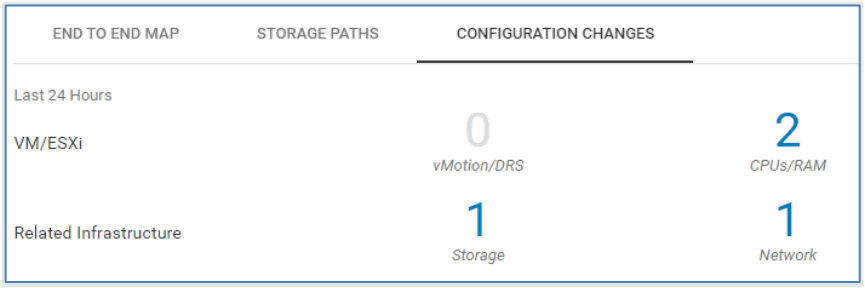
- Virtual machine
- ESXi Server
- ESXi Cluster
- Datastore
- Network
- Storage Object (LUN, volume, or storage group)
- Storage System

Key performance metrics are displayed for the selected items in the map. By default, the latest value is displayed for each metric. However, if the user selects a point in time in the VM performance charts on the left, this view is updated to show the corresponding values at the selected time. Users can select a time of interest in the VM performance charts and then select various objects in the data path to view their corresponding performance metrics.

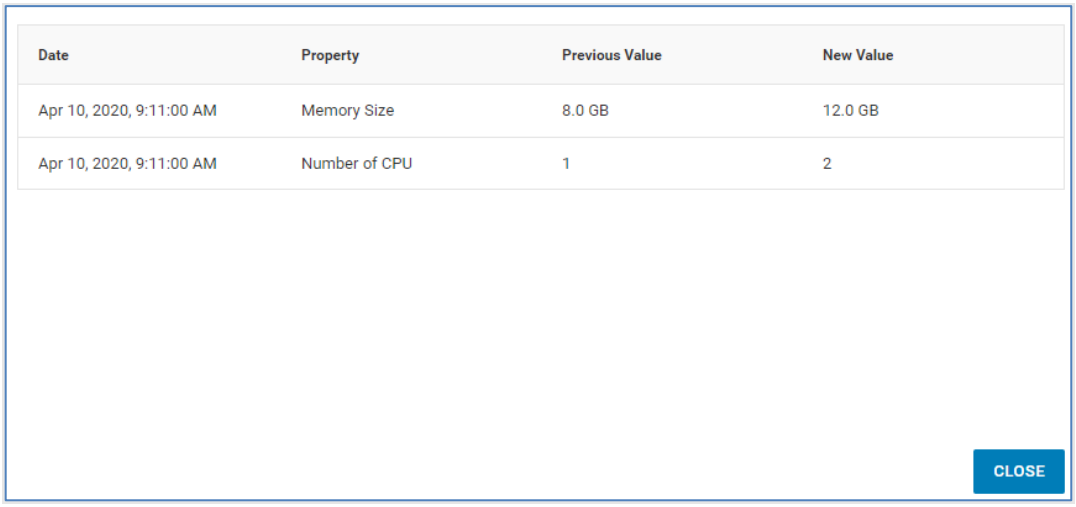
Storage Paths – This tab maps each datastore to the storage object (LUN, volume, or storage group) on each system. This information allows users to map different datastores to different storage objects. If a performance impact is selected in the performance charts, the impacted components are highlighted with a pink square.



Configuration Changes – This tab provides a summary of VM-related and infrastructure-related configuration changes over that last 24-hour time period.



Selecting the number in the Configuration Changes view opens a window that displays details about the configuration change or changes. This allows the user to correlate configuration changes in the environment with potential performance impacts.



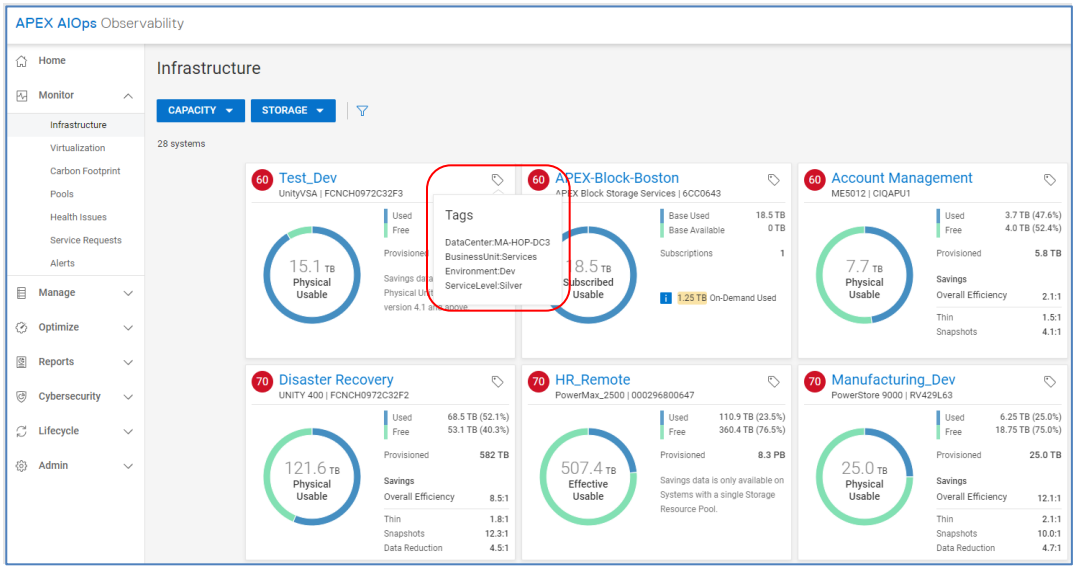
Custom Tags

Introduction

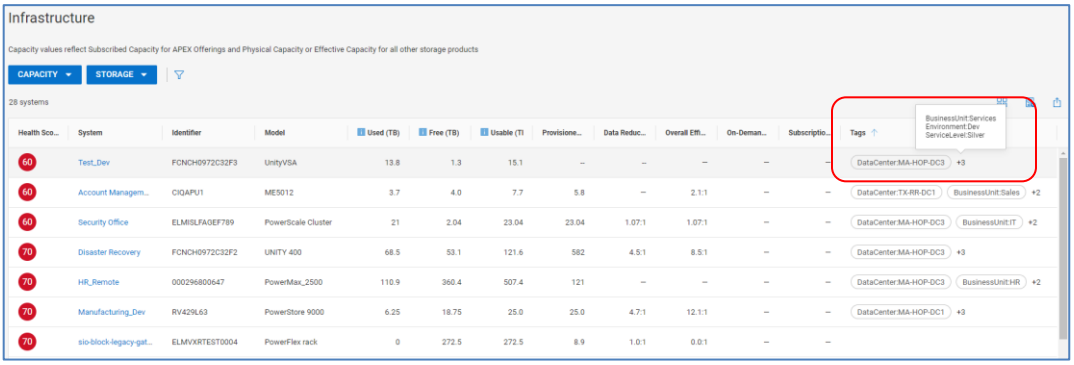
Users can enhance the collected data in Infrastructure Observability with customer-specific metadata called tags. Tags can be used to tag systems and components with business-specific data. Tags are entered as a Key:Value pair. For example, BusinessUnit:Engineering is a tag where BusinessUnit is the tag key and Engineering is the tag value. A second tag may be BusinessUnit:Finance. This example allows users to assign different business units to various assets.

Accessing tags

System level tags can be seen in any of the multisystem views. Once systems are tagged, views can be filtered based on one or more tags. The following figure shows the multisystem view for capacity for storage. By hovering over the tag icon in the upper right corner of each card, the user can see the defined tags for the system.

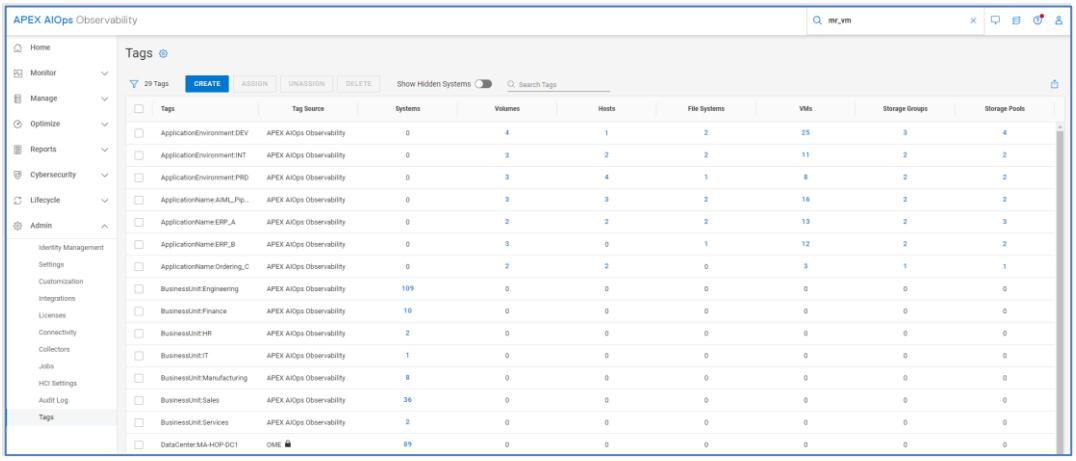


Users can also switch to the list view and see them under the **Tags** column. When the text in the Tags field exceeds the column width, a +X is shown where X is the additional number of tags defined for that system. To view the additional tags, hover over the +X.

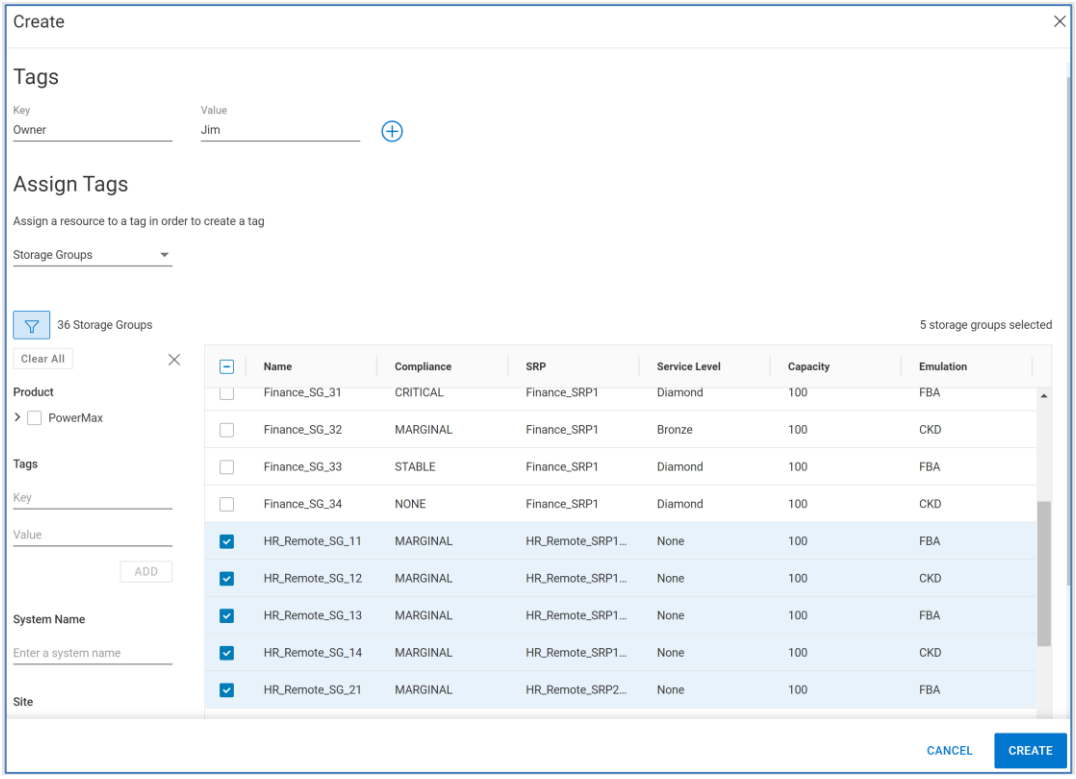


Editing tags

Custom tags are created and modified in the Tags page from the **Admin > Tags** menu selection. The Tags page lists all configured tags and allows users to create tags, delete existing tags, and perform the assigning and unassigning of tags to various assets.



Clicking **Create** displays the create tag window. The tag key and value are entered and then the user assigns the tags to one or more components. The following example shows an Owner tag with a value of Jim being assigned to various storage groups on the HR_REMOTE system.

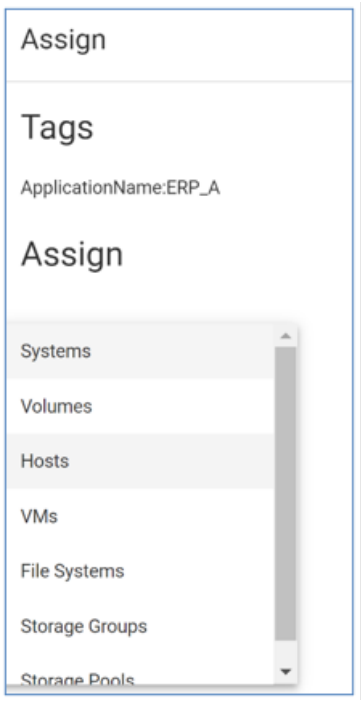


Tags can be assigned to any of the following assets:

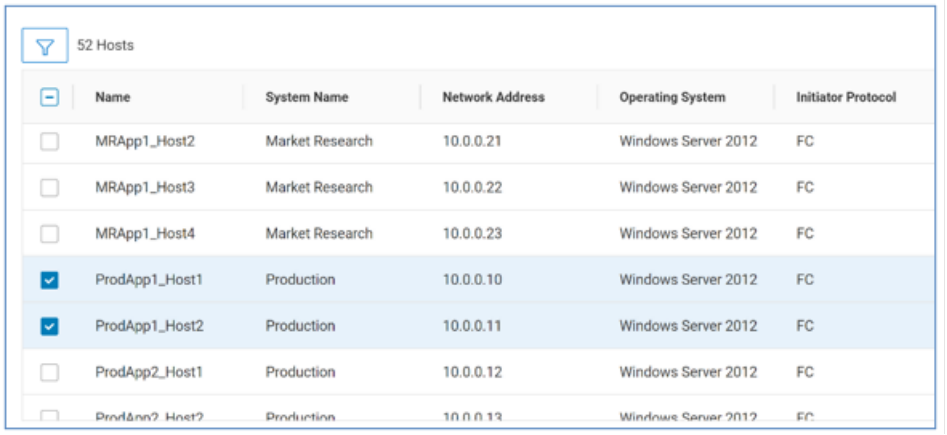
- Systems
- Volumes
- Host
- VMs File Systems
- Storage Groups
- Storage Pools

Tags are fully supported in custom reporting. By providing the ability to tag assets at component levels, users can create custom reports that display the tags and filter the reports on those tags. This allows customer-specific reports to be created and delivered to appropriate individuals. Reports can be created for various business units or applications to provide storage utilization and show back information.

Existing tags can be assigned or unassigned to objects by selecting the tag in the Tags view and selecting the appropriate button. The following shows the Assign window for the ApplicationName:ERP_A tag.



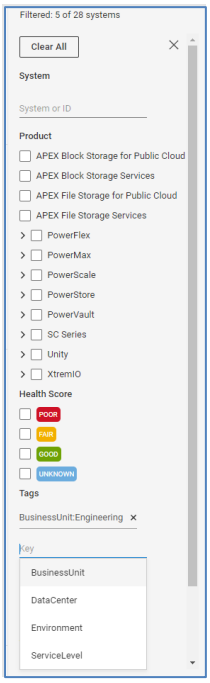
Users first select the category of asset, in this case Hosts. Then they select the objects from that category, in this example ProdApp1_Host1 and ProdApp1_Host2.



The **Show Hidden Systems** toggle allows users to see systems that are filtered out from their view based on the settings in Admin > Settings > Sites and Systems. See the Infrastructure Observability administration section for details.

Filtering tags

In addition to using tags in custom reports, users can filter on custom tags in any of the filter views in Observability. For example, the multisystem views can be filtered using the tags.



Select in the “Key” field and begin typing the tag key or select the key tag from the list of defined keys. When the key is chosen, select in the “Value” field and begin typing the tag value or select it from the list of defined values.

Select ADD to add the tag filter.

Multiple tags can be added.

Infrastructure Observability administration

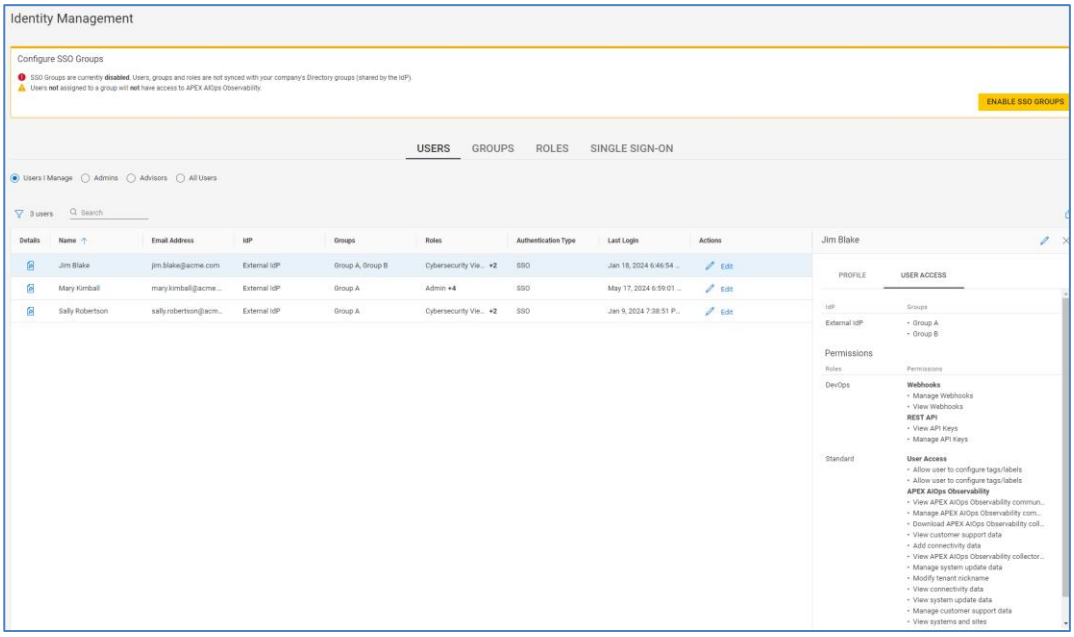
Identity Management

The Identity Management section allows Observability administrators to set up access controls by assigning users to predefined roles. Administrators can also initiate an invitation to their Identity Provider (IdP) experts to become Dell Identity Admins and federate with their IdP to enable single sign-on. When single sign-on is enabled, users can also use SSO groups that map Observability roles to customers’ active directory groups. This gives customers control over all Observability roles including the Standard and Admin roles.

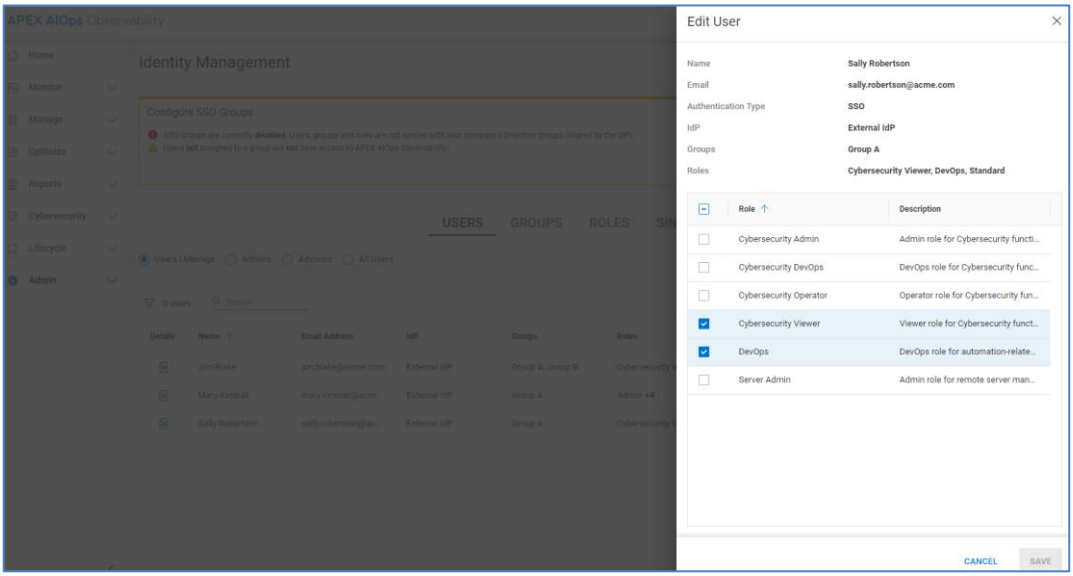
The administrator of an organization uses MyService360 to define the organization profile. See KB#000183704 for details about using MyService360 for company administration. See KB#000191817 for details about determining Admins for a company in the Dell Support portal.

Note: When SSO groups are not enabled, MyService360 users with a company admin role are automatically mapped to the Observability Admin role. Other users are mapped to the Observability Standard role.

Administrators will see four tabs in the Identity Management page: The USERS tab provides several views of users. The Users | Manage view lists users who have logged into Observability at least once and can be managed by the current admin user. This view shows the username, email address, IdP, Groups, assigned roles, authentication type, and last login. Selecting the Details icon for an individual user provides details about the user profile and assigned roles and permissions.



When SSO groups are not enabled, Administrators can select the Edit button to assign roles to a user. In this case, the Admin and Standard user roles are not managed through the Observability UI but are determined by their status in MyService360.

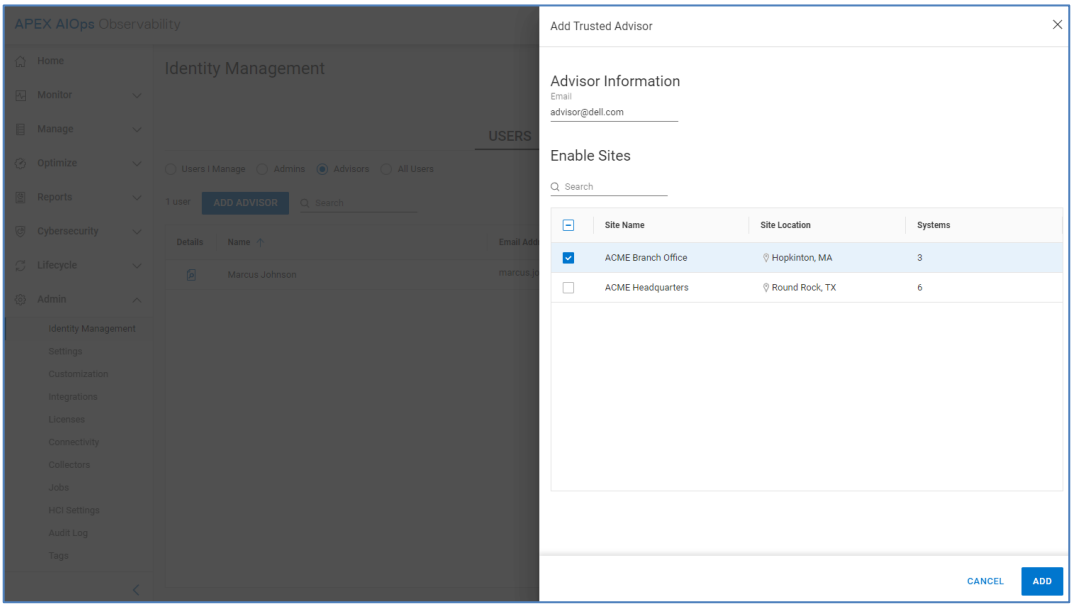


The Admins view provides a list of users with the Admin role. This allows users to see who they may need to contact in order to request different levels of access to Observability.

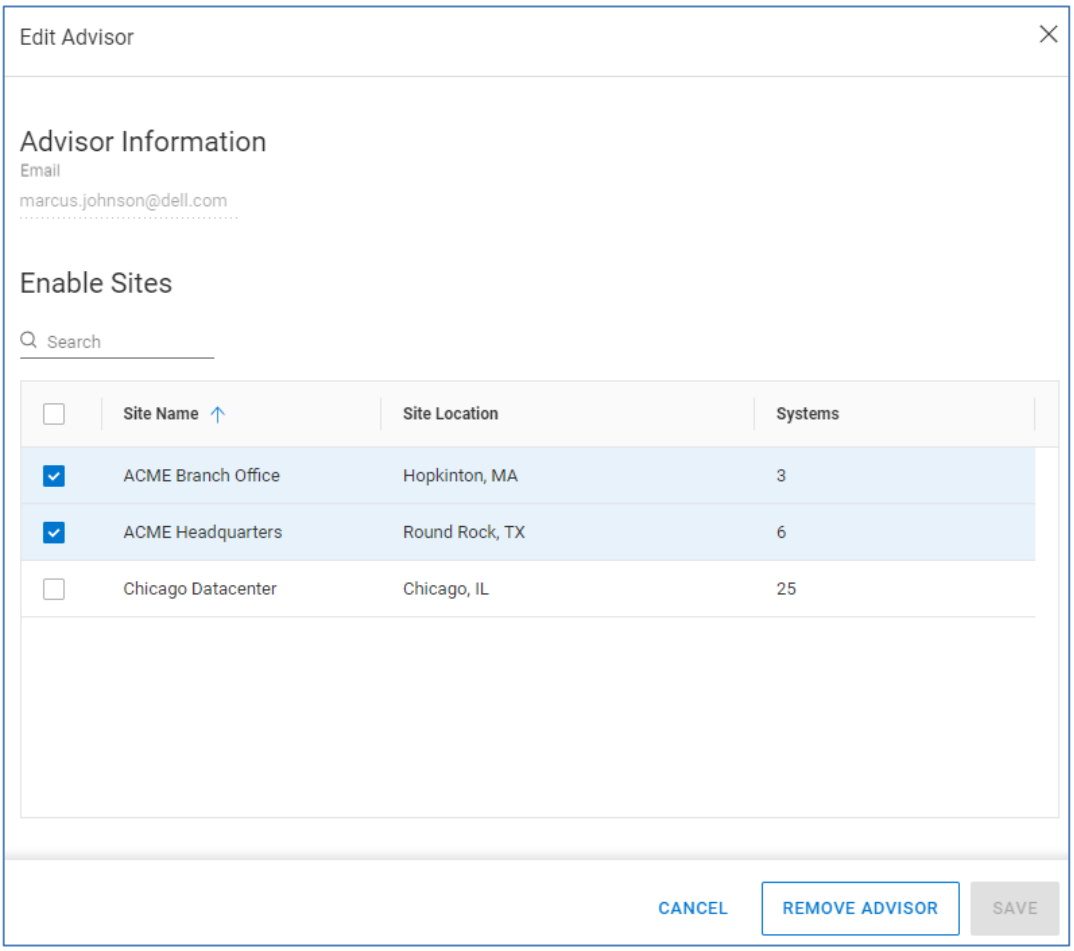
The Advisors view shows a list of all Advisors who have been given access to Observability. Both Admins and Standard Users can view, add, and remove advisor access to Infrastructure Observability. Dell Advisors are members of the account team or other Dell employees or partners whom customers want to proactively and routinely view their systems in Observability. The purpose of this role is to assist and make recommendations to customers to help them optimize their storage usage. Dell employees and Partners must explicitly be provided access to Observability from the customer. See the following KB article for details:

https://www.dell.com/support/kbdoc/000020659

To add an advisor, users click the **Add Advisor** button. In the Add Trusted Advisor window, enter the advisor email address and select which site or sites to give the advisor access, and click Add.

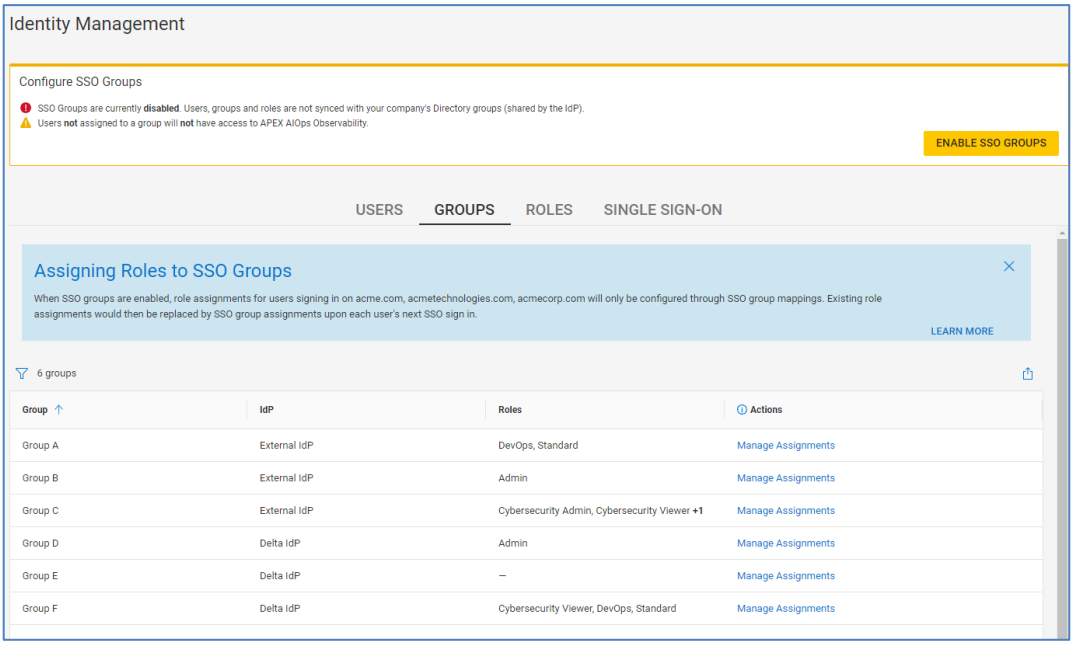


To remove access to an existing advisor, the user clicks the Edit link under the Actions column for the advisor they want to remove and clicks Remove Advisor.

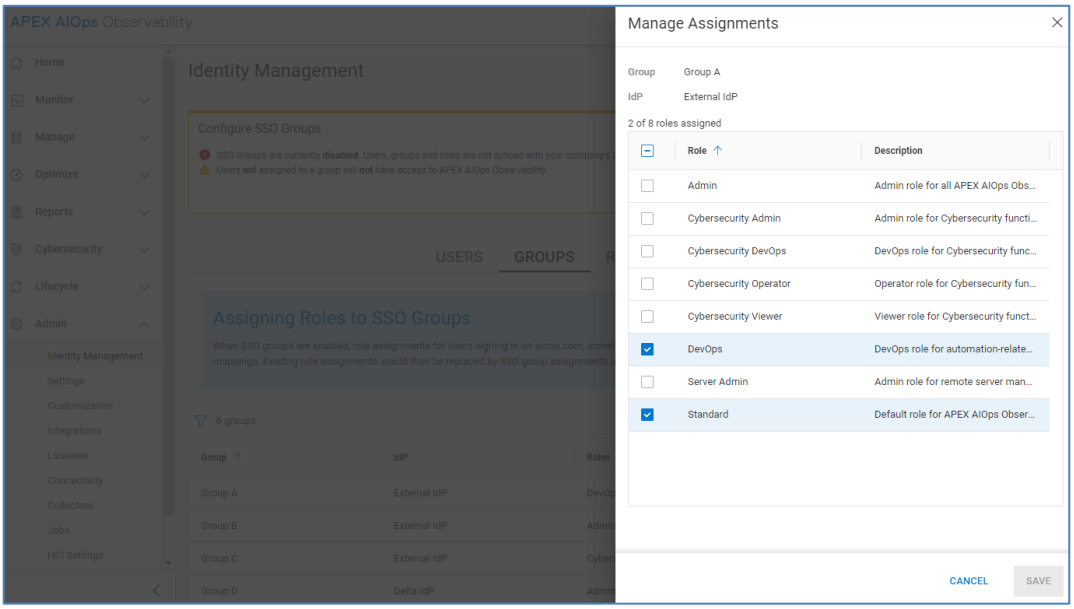


The All Users view lists all users with access to Observability, including those users who are not managed by the existing user logged in to the UI.

The GROUPS tab is visible to Admin users and allows the admin to assign Observability roles to SSO groups after SSO has been enabled. The listed SSO groups are imported from the Dell Identity Portal and were shared by the company's identity expert when performing the federated IdP configuration.



Clicking the Manage Assignments link for each group allows the Observability Admin to assign one or more roles to the group.



Note that the Enable SSO Groups button is not active until the Admin role is assigned to at least one group. Group role assignments are aggregated so if a user is a member of more than one group, that user receives the roles from all groups.

The ROLES tab lists out the available roles with their description and the number of assigned users. There are nine roles in Observability: Admin, Advisor, Cybersecurity Admin, Cybersecurity DevOps, Cybersecurity Operator, Cybersecurity Viewer, DevOps, Server Admin, and Standard. If SSO Groups are not enabled, users with a Company Administrator role in an organization are automatically assigned the Admin role. Users who are not Company Administrators are automatically assigned the Standard role. These

roles are automatically assigned based on the user's role in their organization. This behavior changes when single sign-on is configured and SSO Groups are enabled. When SSO Groups are enabled, the user has full control over these roles and can assign them to a group just like all other roles. It is important to mention that a user must have either the Admin or the Standard role to access Observability.

The Advisor role is another role that is not managed within Observability. It is assigned to any user that has been invited and accepted the invitation to be an advisor for the company.

The Cybersecurity Admin role gives users access to cybersecurity related features in Observability. These include viewing and editing policies, viewing and editing security incident email preferences, viewing and editing ransomware incidents, viewing Security Advisories, and viewing security status data.

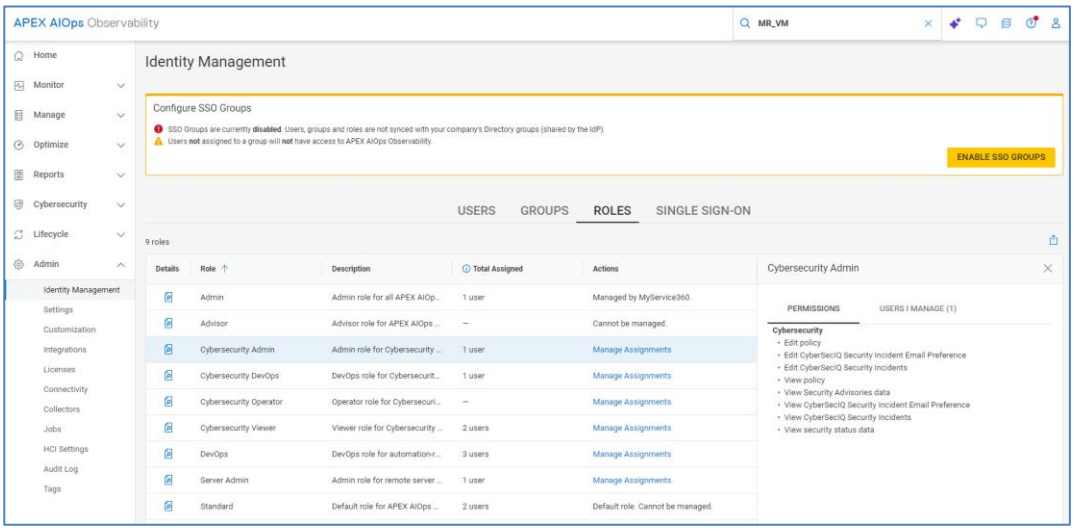
The Cybersecurity DevOps role gives users access to the Integrations menu to view and configure cybersecurity-related Webhooks, including the Cybersecurity Ransomware Incident, Cybersecurity Misconfigurations, and Cybersecurity Configuration Webhooks.

The Cybersecurity Operator role is designed to give a user access to edit and view cybersecurity ransomware incidents. The permissions include viewing and editing security incident email preferences, viewing and editing ransomware incidents, viewing policies, viewing Security Advisories, and viewing security status data.

The Cybersecurity Viewer role is a view-only role for cybersecurity features with the additional permission of editing their security incident email preferences. Permissions include viewing policies, viewing Security Advisories, viewing ransomware incidents, and viewing security status data.

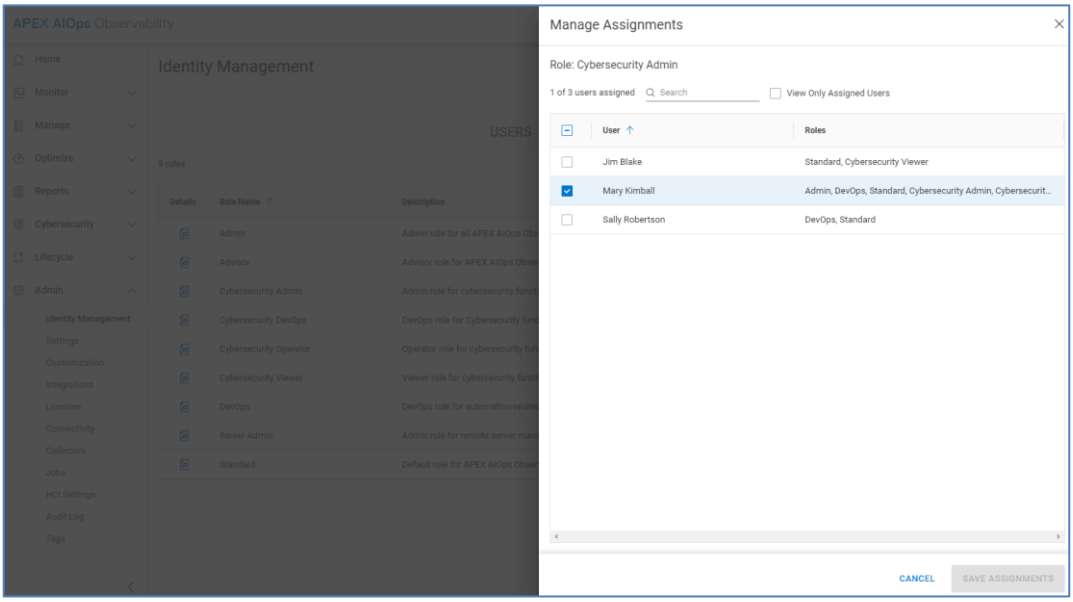
The DevOps role allows users access to the Integrations menu to view and configure Webhooks and REST API credentials. A user with DevOps role can view and configure Health Issue Change webhooks.

The Server role is required for users who want to initiate remote management functions on PowerEdge servers. Note that additional remote management permissions need to be enabled in the CloudIQ plugin in OpenManage Enterprise.

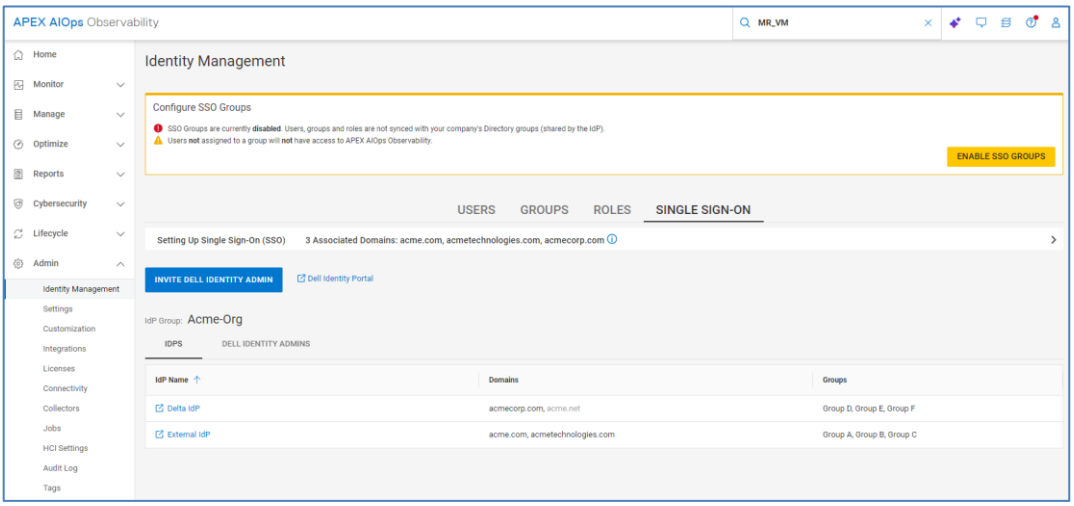


Note that Admins must assign themselves any of the additional roles to gain those privileges.

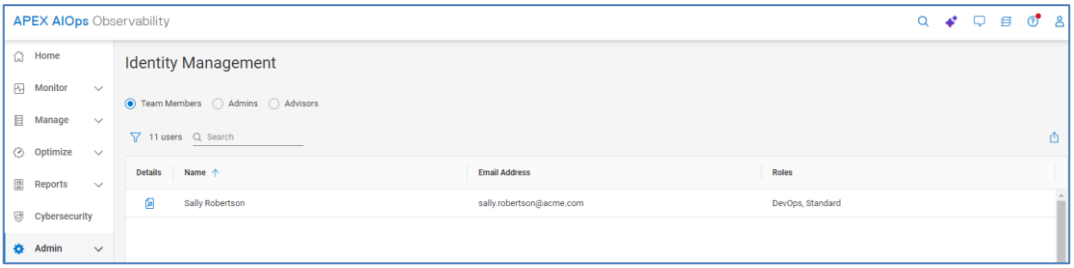
The Manage Assignments link is used to assign roles to either users (when SSO Groups are not enabled) or to groups (when SSO Groups are enabled).



The Single Sign-On tab allows Observability Admins to send an invitation to their Identity Provider Administrators to become Dell Identity Admins. The Dell Identity Admin can then configure single sign-on on the Dell Identity Portal and federate with their IdP. This allows organizations to manage users' Observability authorization using their IdP. After the Identity Admin federates their IdP, the IdP is listed under the IdPs tab. Clicking the IdP hyperlink opens the Dell Identity Portal. Users can also see a list of Dell Identity Admins who can manage the IdP group. For additional information, see KB#000212047.



The Identity Management page for Standard users displays a subset of the Users tab. Standard users can see Team Members, Admins, and Advisors. The Admins button allows users to identify their Admins from the Observability UI to contact them if they need additional roles and permissions. The Advisors tab allows users to add and remove advisors.

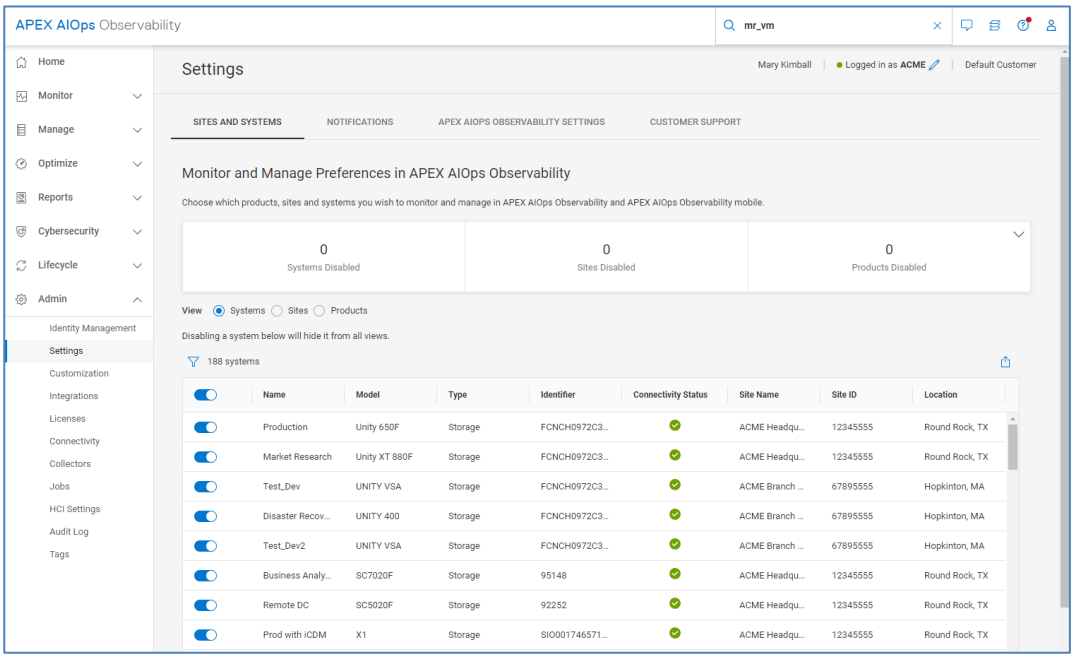


Settings

The **Settings** section allows users to control asset visibility, set up email notifications, and enable access to Dell Customer Support. Users can also set their preferred language. Supported languages include English, German, Spanish, French, Italian, Korean, and Japanese.

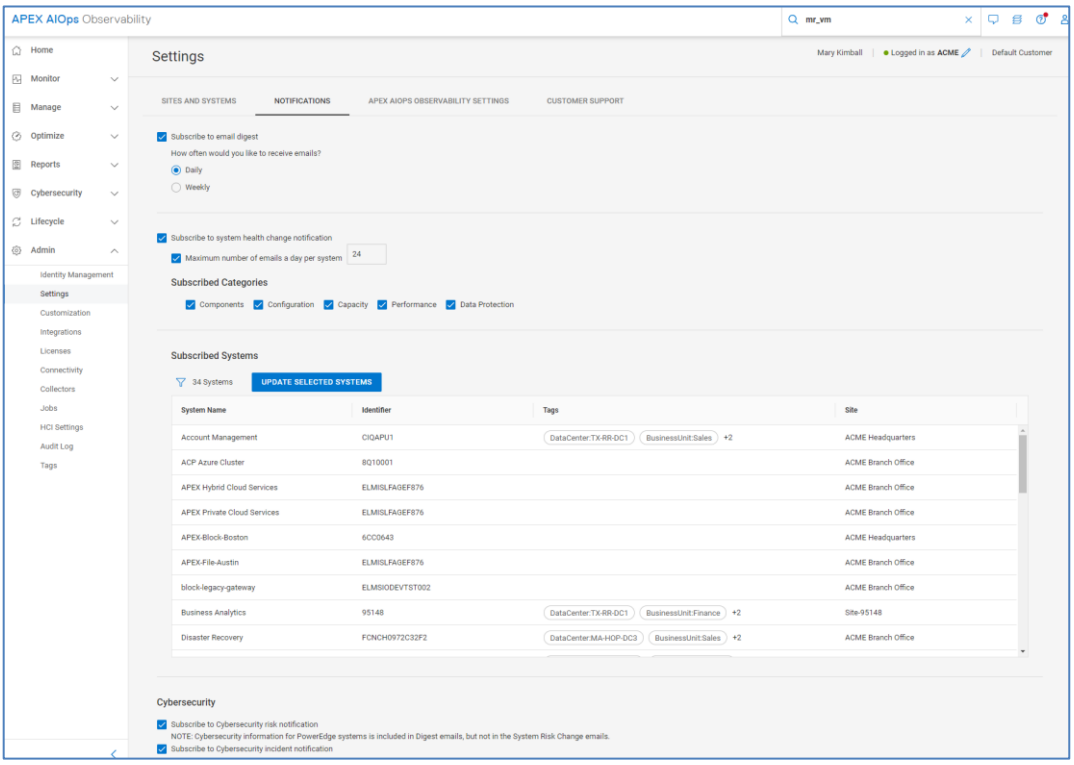
Sites and Systems

Users can set filters on which systems are available to view and receive notifications for in the Observability UI and the Observability mobile app. This also filters the systems from Webhook configuration. For example, an administrator can set their view to see systems from certain sites or see systems of one or more storage types such as Unity XT family and PowerStore. The filtering is set on a per-user basis and can be configured based on systems, sites, and products. This feature is accessible under the Sites and Systems tab under the Admin > Settings > Sites and Systems.



Notifications

The **Notifications** tab allows users to subscribe to email notifications for various events such health change notifications, job status change notifications, cybersecurity risk notifications, and ransomware incident notifications. Users can also subscribe to a daily or weekly email digest or a daily or weekly Data Protection email digest.

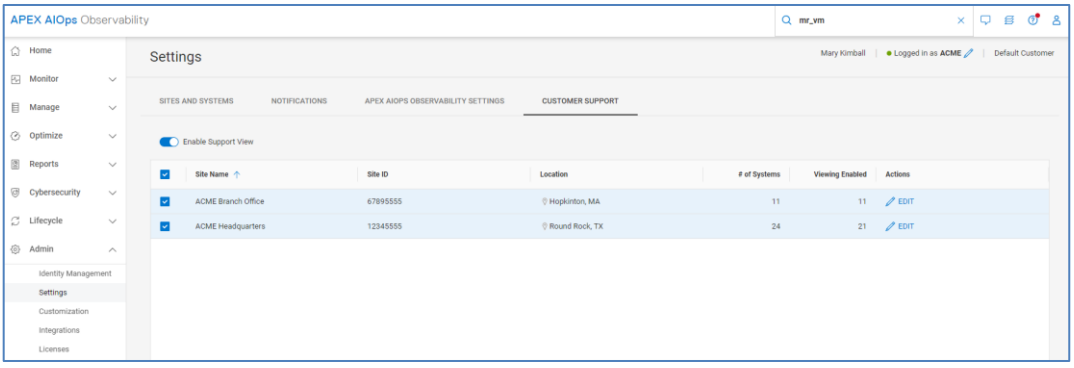


APEX AIOps Observability Settings

Users can set their language preference under the APEX AIOps Observability Settings tab.

Customer Support

Users can enable and disable Observability access for Dell Customer Support. They can enable specific sites or, by selecting the Edit link for a specific site, enable specific systems within a site. This is useful for sharing the view of the system with Dell Support when troubleshooting an issue in Observability or for using the information in the Observability UI to help troubleshoot other issues.



Customization

Infrastructure Observability allows users to temporarily pause host connectivity health checks and file system capacity checks from being included in the system health score. Users may want to do this for nonprocessing hosts or during times of maintenance when

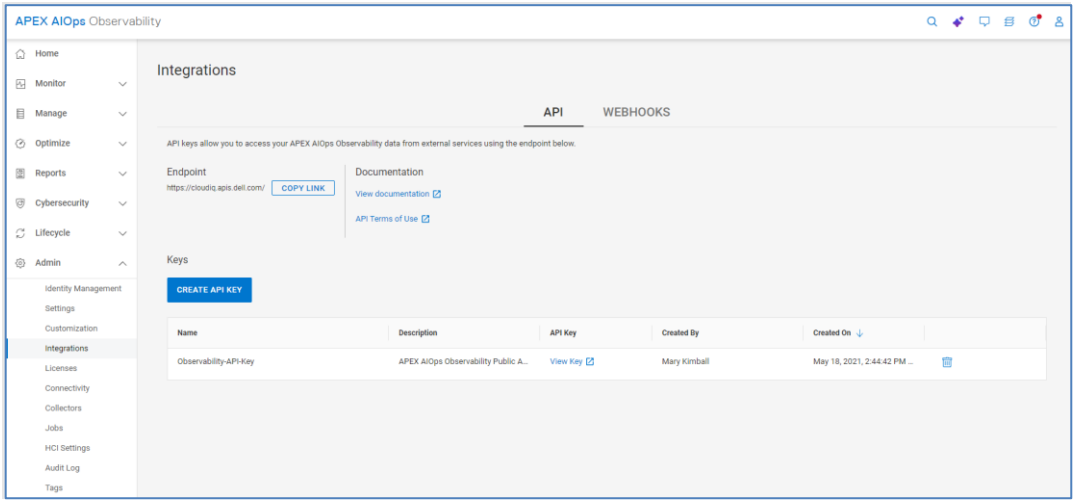
single-pathed hosts may be expected. Host connectivity checks are supported for both Unity XT family and SC Series systems. File system capacity checks are supported for Unity XT and PowerMax systems.

Integrations

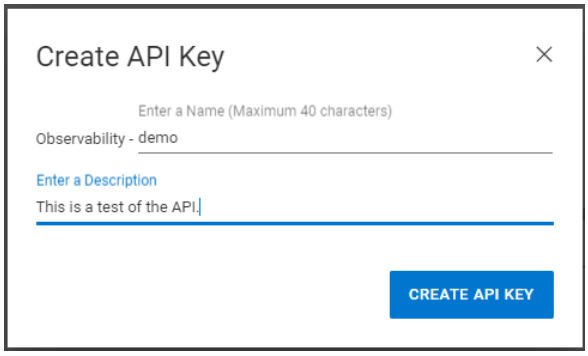
The **Integrations** section allows users with the DevOps or Cybersecurity DevOps role to configure Webhooks. Users with the DevOps role can configure REST API credentials. Users must have the role of DevOps or Cybersecurity DevOps to access the Integrations menu. This is described in the Identity Management section.

REST API

The public REST API allows users to pull data from Observability to integrate with collaboration and automation tools used in day to day IT operations. It is a read-only API allowing users to access inventory, configuration, performance, and capacity metrics available in Observability. It uses the OAuth2 protocol for authentication and authorization. The API client credentials are obtained by selecting the Create API Key button under the API tab.



Enter an API key name and description and select Create API Key.



When the API key is created, the user selects the View Key link to obtain the Client ID and Client Secret. The user then uses these credentials to authenticate to a specific API endpoint to obtain an Access Token. When the user obtains the Access Token, the user can make the chosen REST API calls. The access token is active for one hour, and the client credentials are valid for one year.

Documentation for syntax and available API calls is available at https://developer.dell.com/apis/products/analytics/cloudiq. Use these links to developer blogs access examples for Postman and Python and Jupyter.

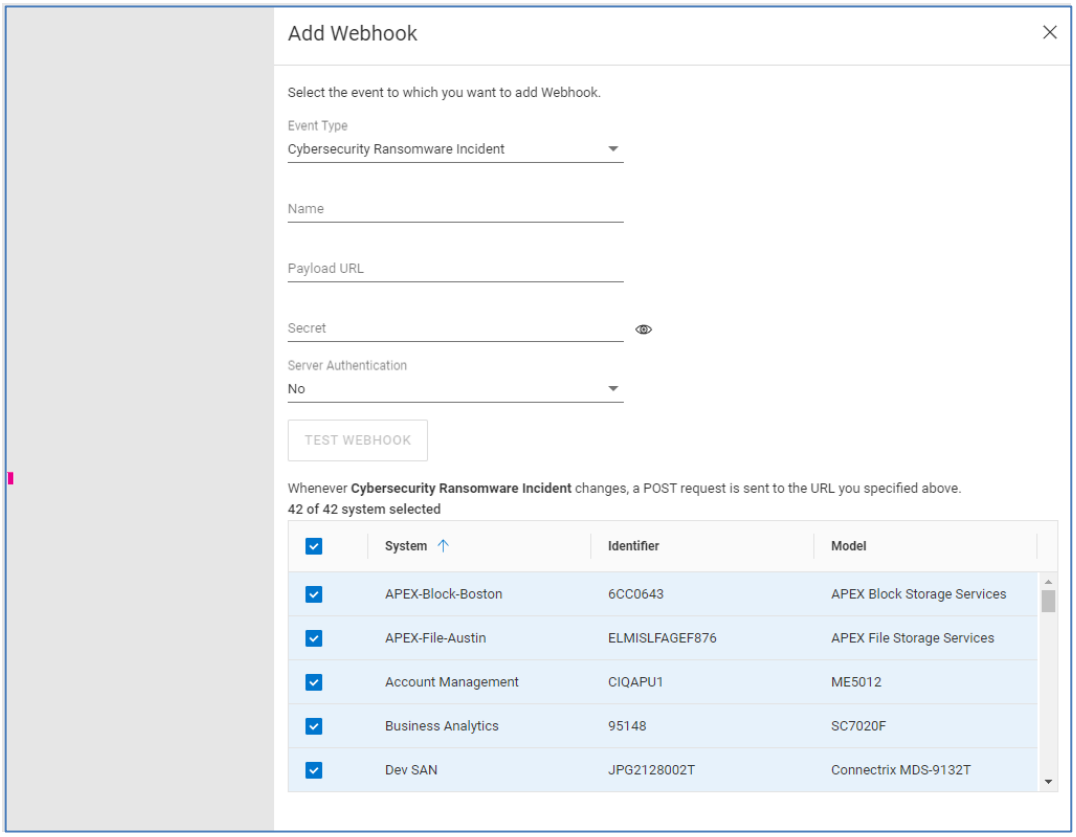
Webhooks

Webhooks is a push mechanism to integrate with third-party applications such as ServiceNow and Slack. The following Webhook notifications are supported:

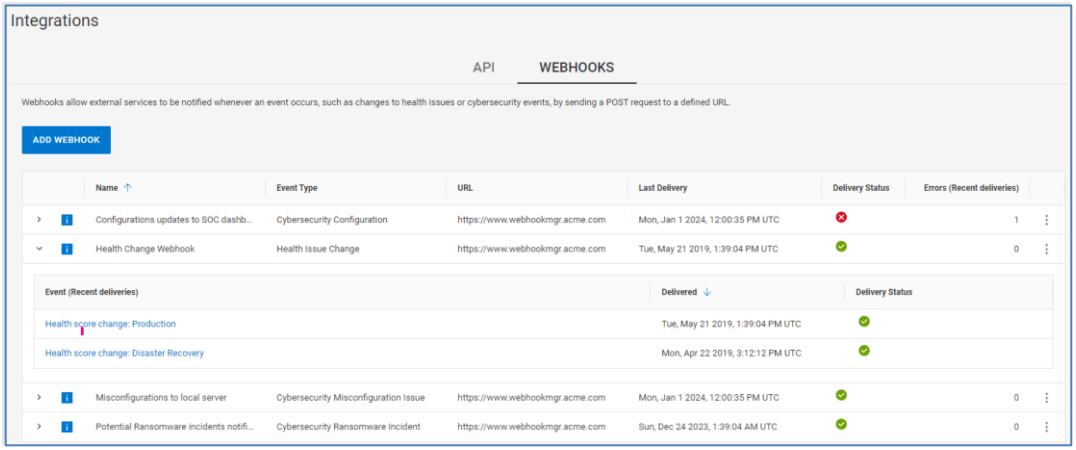
- Cybersecurity Ransomware Incident – Delivered when Observability identifies a potential ransomware incident.
- Cybersecurity Misconfiguration Issue – Delivered when Observability identifies a security configuration deviation.
- Cybersecurity Configuration – Delivered when a change is made to an evaluation plan.
- Health Issue Change – Delivered when Observability identifies a health issue change.

A brief tutorial for ServiceNow and Slack integration can be found here. Other examples can be found by searching for CloudIQ at the Dell Developer Community.

Configuration of Webhooks requires the user to enter an Event Type, a Name, the Payload URL (destination to send the Webhook), a Secret, and Server Authentication. The secret is a user-supplied string sent along with the payload and is used to create a signature that is passed as a header during the POST request. The URL server can create its own matching signature using its stored secret and the POST payload to verify that the signature in the header matches its own generated signature. Users can then select which systems to monitor. The Test Webhook button sends a test notification to the server with a NULL payload. This is used to quickly test connectivity to the Webhook destination.



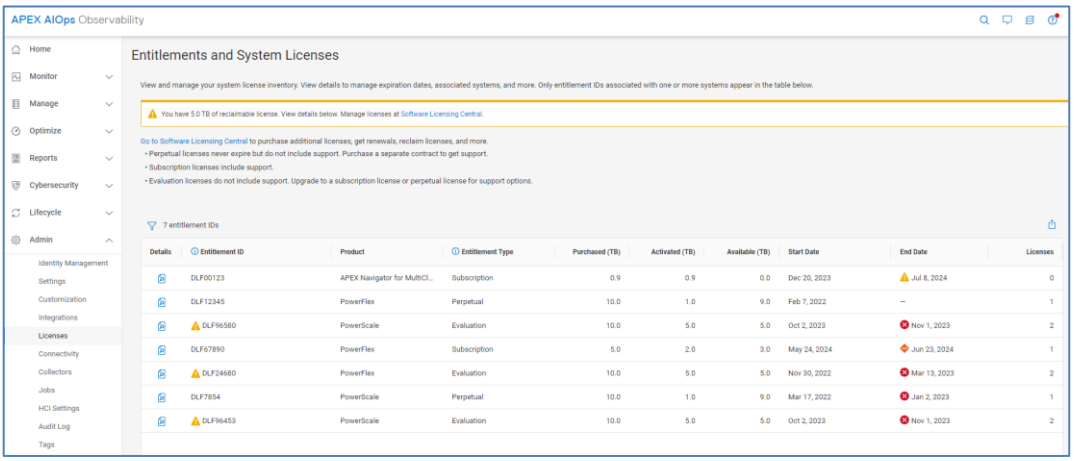
After a Webhook is configured and triggered, those events are captured on the Integrations page showing the time and status of the delivery.



The user can select an event to see the Headers and Payload of the request and the response. A Redeliver button allows users to resend the event which is helpful for testing Webhook integration. Due to the potential sensitivity of cybersecurity information in the payload, users will only see header information in the Observability UI.

Licenses

The **Licenses** page shows license and entitlement details. Supported for PowerFlex, PowerScale, and APEX Navigator for Multi-Cloud, this page allows users to see purchased, activated, and available capacity for each entitlement. The table also displays the entitlement type, start date, and expiration date. Users can use the link to Dell Software Licensing Central to manage their licenses.

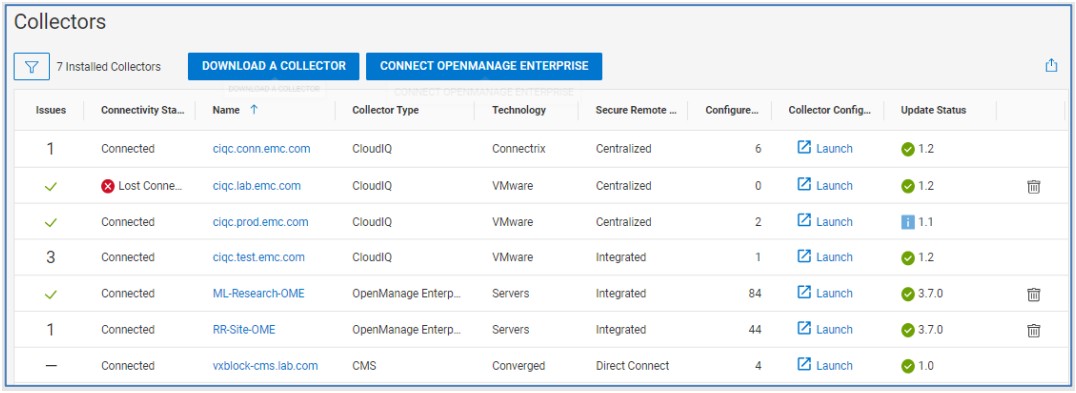


Connectivity

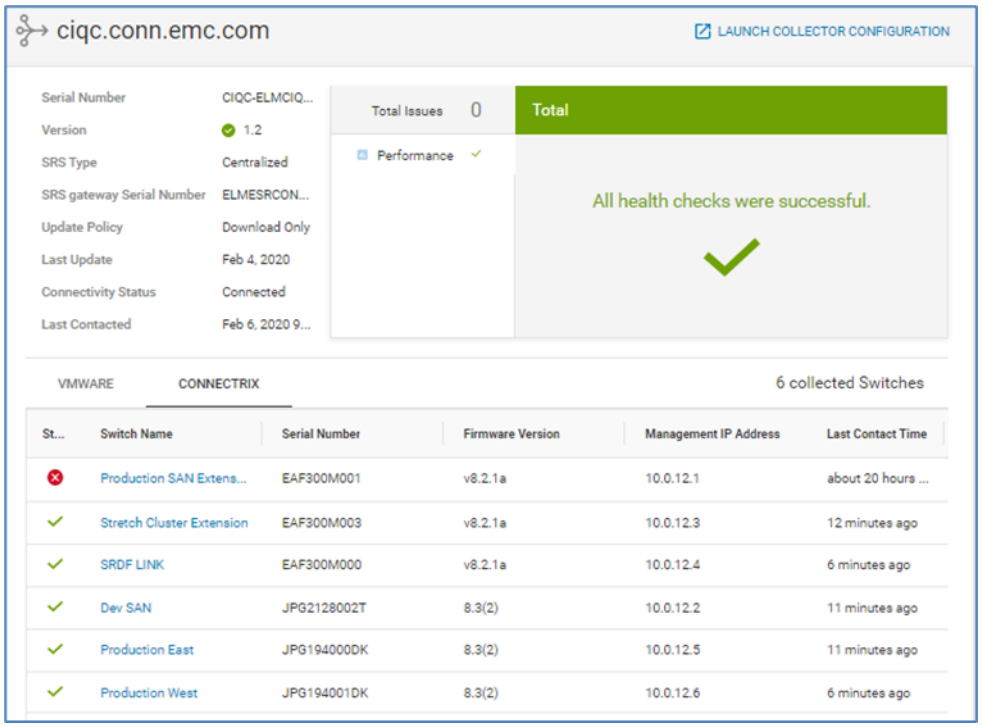
The **Connectivity** page shows customers all systems that are connected, have lost connection, or need additional configuration work before Infrastructure Observability can display data for them. The filter allows users to filter based on Connectivity Status, System ID, Product, Product Type, Site, Location, or Contract Status. It also provides links to onboard SC Series, PowerVault, and VxBlock systems. These systems require the user to enter information into Observability to complete the onboarding process.

Collectors

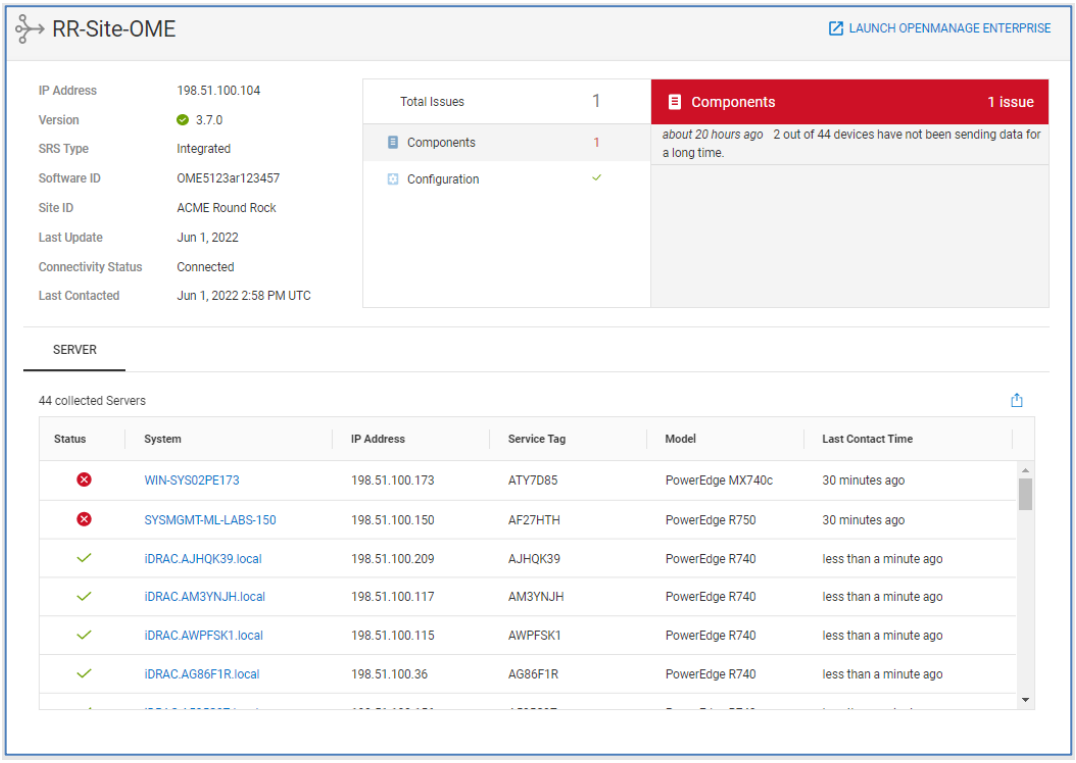
The **Collectors** page lists each Observability Collector, OpenManage Enterprise installation, and Converged Management Software system associated to Infrastructure Observability. The Observability Collector is used to collect VMware, Connectrix, and PowerSwitch data and sends that data back to Observability using Secure Connect Gateway. OpenManage Enterprise is required for PowerEdge collections. CMS is used for VxBlock collections. This page shows the connectivity status and versions of installed collectors. It also provides a download link to obtain the collector and instructions about how to configure OpenManage Enterprise. Offline collectors can be removed from Observability using the delete icon on the right side of the page.



The user can select the hyperlink in the Name column to open the Collector Details page. This page provides health-related information for the selected collector. It also provides as an inventory of devices for which it is configured.



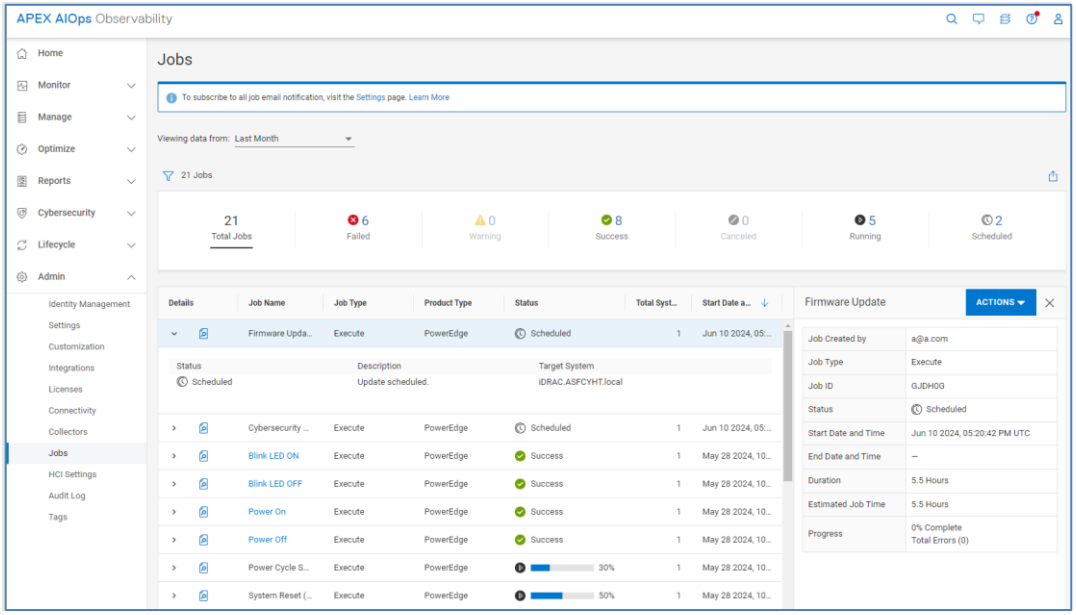
For OpenManage Enterprise instances, it shows the health and the list of monitored PowerEdge servers and their collection status.



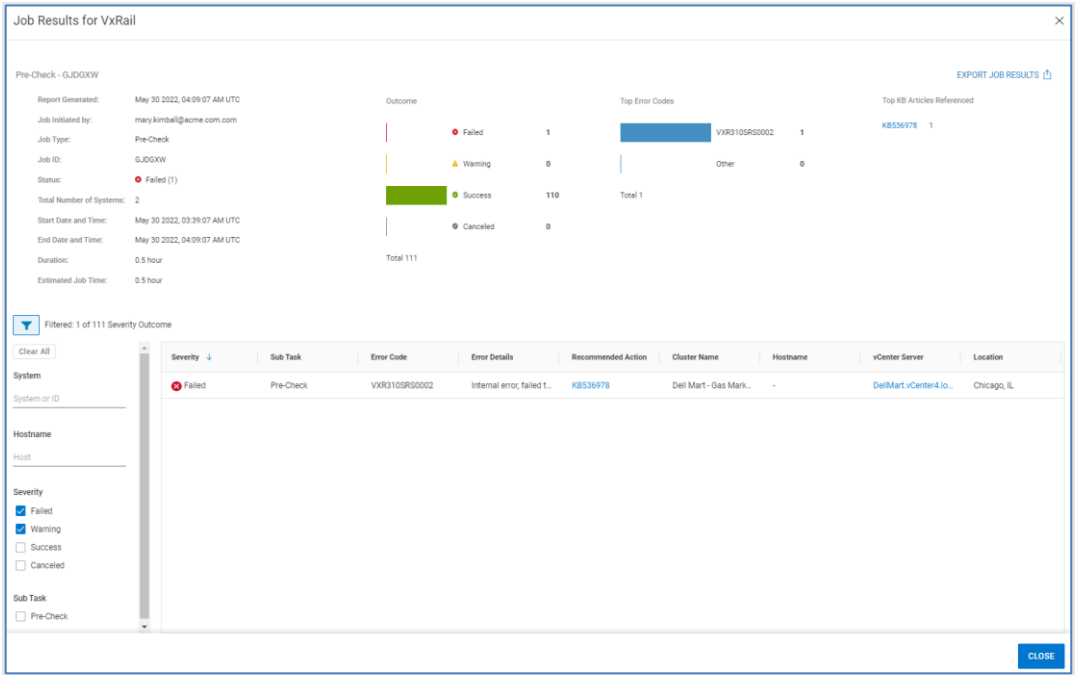
Jobs

The **Jobs** page lists the existing update tasks and their status. The top of the page provides a summary banner of the total number jobs and their status. It also acts as a filter allowing users to view jobs with a specific status. The bottom of the page lists each

job with details about the job. Selecting the Details icon on the left opens the details window on the right which shows start and end times, duration of the job, and total number of errors if any were encountered. From the job details window, the user can choose to cancel a running task, view job results, retry a failed job, or edit the job name.



When a user selects View Job Results, the Job Results window is displayed showing details of the job and each action. The top of the page summarizes each outcome by status and lists the top error codes and KB articles if a failure occurred. The bottom of the page lists the actions with a failed or warning status by default along with the recommended action. The filter allows users to filter on additional status and system name, hostname, or sub task type.



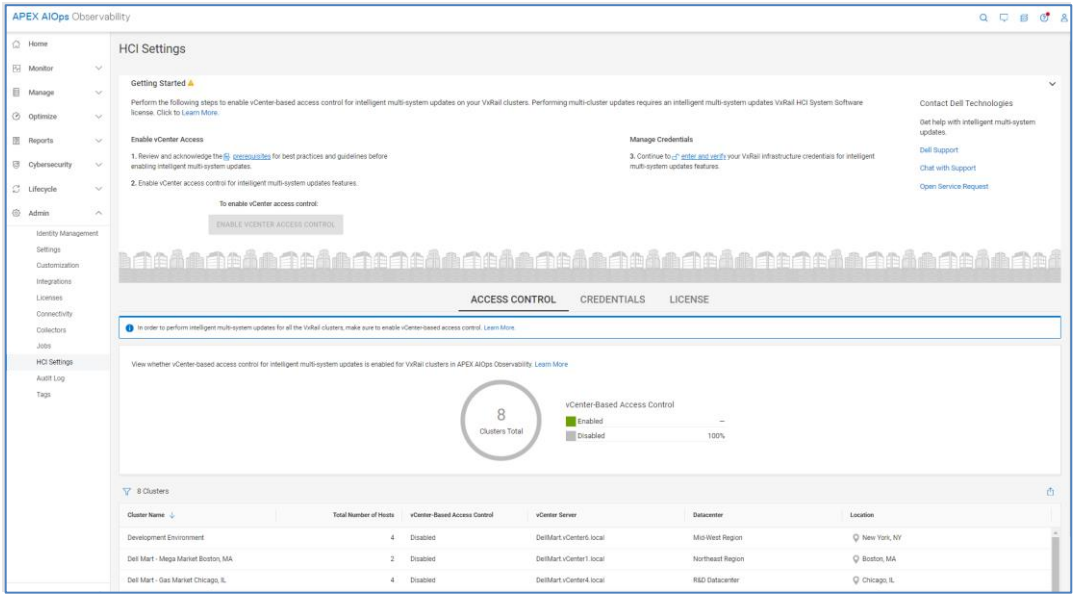
HCI Settings

The **HCI Settings** page has three tabs that allow users to set up vCenter access controls, enter user credentials, and verify VxRail HCI System Software licenses. Each tab is described below.

Access Control

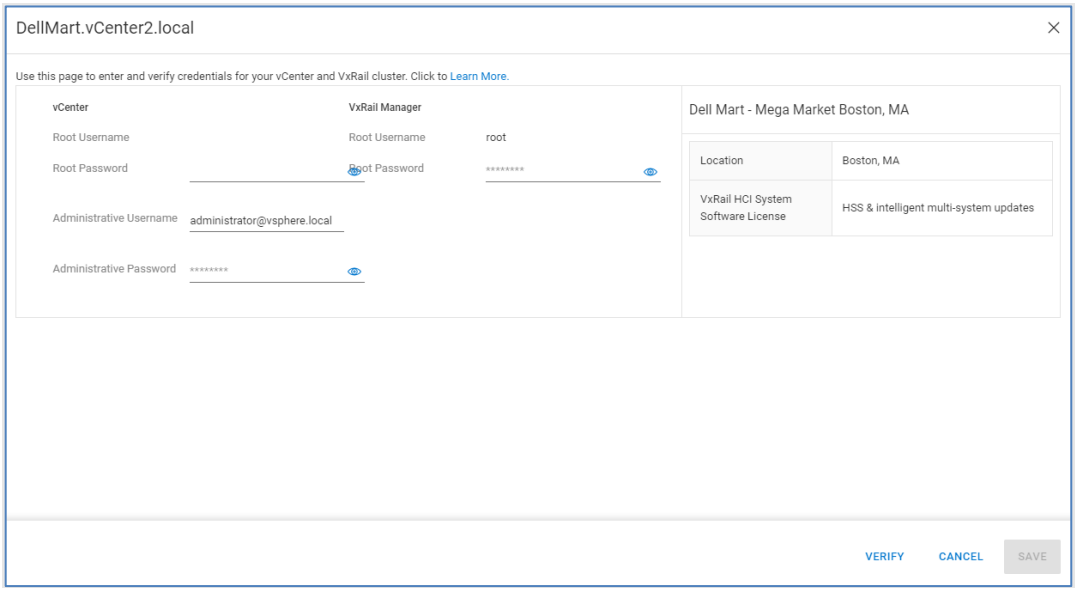
The **Access Control** tab allows users to enable vCenter-based role-based access controls for intelligent multisystem updates. Users enter the vCenter Administrator account to build out the following privileges on vCenter which can then be assigned to the appropriate roles to which user accounts can be associated:

- Download software bundle: Downloads and stages the VxRail software bundle to the cluster
- Run health check: Performs an on-demand pre-update health check on the cluster
- Run cluster update: Initiates the cluster update operation on the cluster
- Manage update credentials: Modifies the VxRail infrastructure credentials used for active management



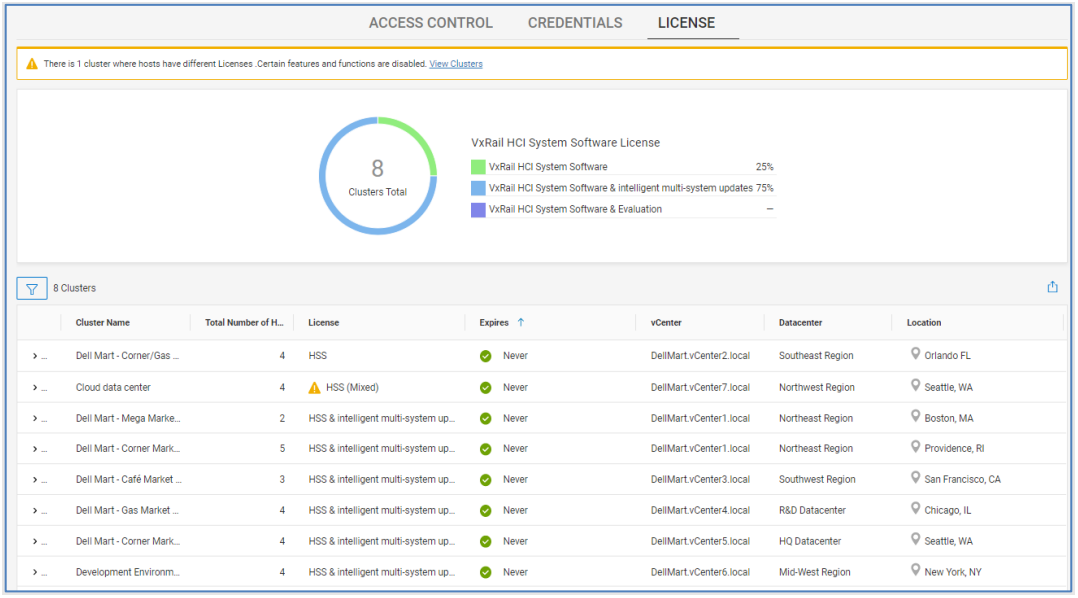
Credentials

The **Credentials** tab is used to manage and verify the user credentials used to perform cluster updates. Typically, when performing a cluster update, users need to enter root account credentials for vCenter server, Platform Services Controller, and VxRail Manager. This becomes cumbersome when performing updates on multiple clusters. This allows administrators to enter the credentials once while setting up active management and then provide the appropriate update permissions to users without sharing the credentials. Credentials entered are stored in an encrypted RSA lockbox on each VxRail Manager. Infrastructure Observability does not store passwords and credentials.



License

The **License** tab provides a summary of license information for VxRail clusters. The doughnut chart breaks down the number of clusters with the HCI System Software (HSS) license, the HSS and Intelligent multisystem update license, and the HSS and Evaluation license. The HCI System Software license is the standard license for all VxRail nodes. The Intelligent multisystem update license is an add-on license that enables the cluster update capability from Observability. The Evaluation license is a time-based license that your sales team can request from the VxRail product management team.



Audit Log

The **Audit Log** tracks activities performed in the Observability UI. It includes the time of the activity, the type of action, the user who initiated the action, the status, and a status message. The Audit Log is only visible to users with the Admin role.

Tags

For information about tags, see the Custom Tags section in this document.

Mobile application

Introduction

Infrastructure Observability also has a mobile application available for both iOS and Android phones. The mobile app has an Overview screen that shows similar information to the Overview Page in the browser version of the UI. It also includes support for Health, Capacity, and Performance details for the supported Dell storage platforms. The user can also configure push notifications to be updated in the app for any health change notifications.

Users can see additional details of the health for any given system and can even text or email the recommended remediation to a colleague for help with performing the resolution.

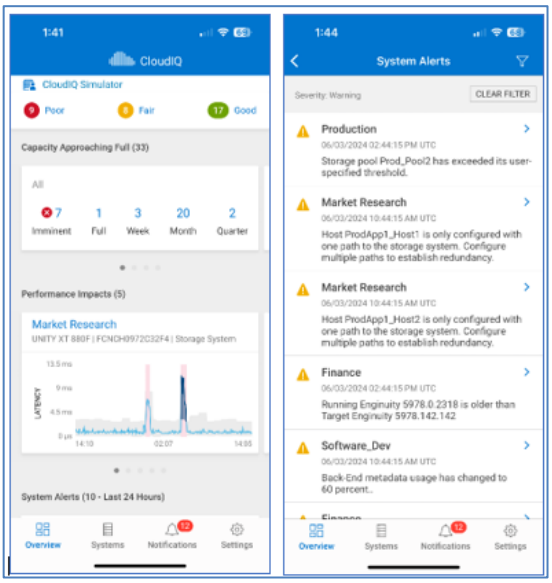
Users can also see if there are any connectivity issues in the environment.

Finally, users can manage push notifications by turning them on or off and can also submit feedback to the Observability team.

All storage platforms are supported except PowerFlex. HCI systems and Connectrix switches are also supported. Data Protection, Converged, Servers, and PowerSwitch devices are not supported at the time of this publication.

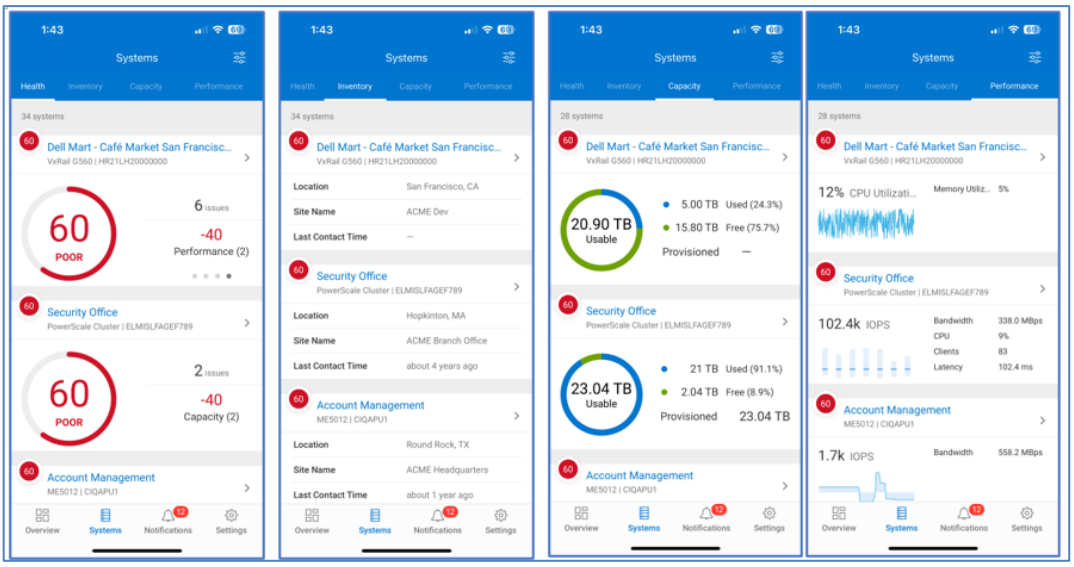
Overview

The **Overview** screen of the mobile app summarizes the health scores, alerts, system connectivity, and capacity approaching full. These views are similar to the tiles on the Overview page of browser version of Observability. Selecting items in the Overview screen will show additional details. The following images show the Overview screen and the details for System Alerts.



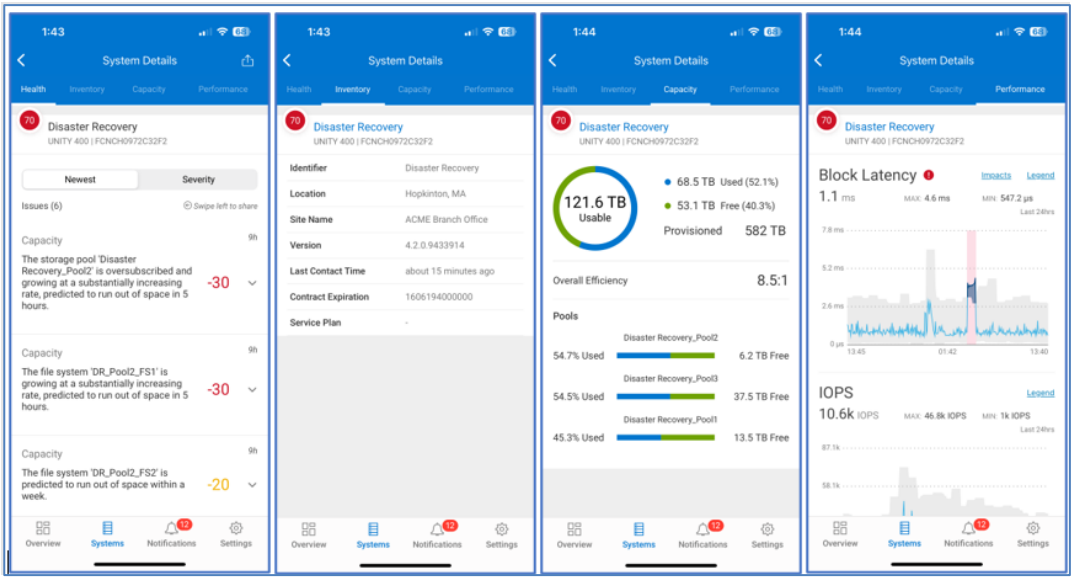
System views

The user can select Systems at the bottom of the screen to see System level views for Health, Inventory, Capacity, and Performance.



System details

The user can analyze single system details for Health, Inventory, Capacity, and Performance. These details include the identification and remediation recommendations for health issues, capacity summaries including efficiencies and pool details, and 24-hour performance charts for key system level performance metrics. The health issue and remediation can be emailed or texted using controls in the app.



Appendix A: Enabling Infrastructure Observability at the system

Unity XT family, XtremIO, PowerMax/VMAX, PowerScale/Isilon, and PowerFlex systems

The Unity XT family, XtremIO, PowerMax/VMAX and PowerScale/Isilon systems use Secure Connect Gateway for Infrastructure Observability data collection. This configuration must be enabled successfully on each individual Dell storage system before users can send data to Infrastructure Observability. Once the secure connection has been configured within the Element Manger interface, Observability must be enabled.

- Unity XT family
  - For Unity XT 4.2 and later, go to **Settings** > **Support Configuration** > **CloudIQ**, and then select Send data to CloudIQ.
  - For Unity XT 4.1, go to **Settings** > **Management** > **Centralized Management**. For the CloudIQ tab in Centralized Management, ensure the checkmark to **Send data to CloudIQ** is checked, and then click **Apply**.
- XtremIO
  - For XMS 6.2 and higher, access the Top Menu Bar and click the System Settings Icon to display cluster-level and XMS-level setting options. Next, select **XMS** > **Notifications** > **CloudIQ Reporting**, and ensure that **CloudIQ Reporting** is set to **YES**.
- PowerMax/VMAX
  - For Unisphere 9.0.1 or higher, go to **Settings** > **Management** > **CloudIQ** and select **I agree to send data to CloudIQ for local systems**, and then click **Apply**.
  - For Cybersecurity, in Unisphere 9.2.1 or higher, go to **Settings** > **Management** > **CloudIQ Cybersecurity** and select **I agree to send data to CyberSecIQ**.
- PowerScale/Isilon
  - For PowerScale/Isilon systems, connectivity to Secure Connect Gateway and Observability is established with the following CLI command:

```
isi esrs modify --enabled=true --primary-esrs-
gateway=<gateway-server>
--gateway-access-pool=subnetx:poolx --username=<username>
[--password=<password>]
```

- PowerFlex software and Ready Node with PowerFlex Gateway
  - Log in to PowerFlex Installer and go to **Maintain** tab
  - Enter MDM admin username and password, LIA authentication type, and LIA password
  - Select **Retrieve system topology**
  - On **Maintain** tab, select **System Logs & Analysis**
  - Enter Secure Connect Gateway information

  - Verify **Send data to CloudIQ** box is checked
- PowerFlex Appliance with PowerFlex Manager v3.7
  - Log in to PowerFlex Manager and go to **Settings > Virtual Appliance Management**
  - Click **Add Alert Connector**
  - Under **Device Registration** section, enter Device Type, ELMS Software ID, Solution Serial Number
  - Check **SRS** box
  - Check **Enable CloudIQ** box
  - Under **Connector Settings** section, enter Secure Connect Gateway information
- PowerFlex Appliance with PowerFlex Manager v4.0 or higher
  - Log in to PowerFlex Manager and go to **Settings** > **Events and Alerts**
  - Under Policies, select **Configure Now** for SupportAssist
  - Accept the **License Agreement** and **Telemetry Agreement**
  - Choose either **Connect Directly** or **Connect via Gateway Server**
  - If connecting through the gateway server, enter **Secure Connect Gateway IP**
  - Verify that **Connect to CloudIQ** is selected
  - Enter SupportAssist Access Key and Pin (see KB#000180688), device type, ELMS software unique ID, solution serial number, and site ID
  - Enter Support contact information

The user can then go to https://cloudiq.dell.com and log in with their valid service account credentials to view their systems in Observability. The amount of time it takes for a system to appear in Observability varies, but typically is visible within one hour.

For detailed information about onboarding the Dell storage arrays, see the following documents:

Unity XT family – https://www.dell.com/support/kbdoc/000067484

XtremIO – https://www.dell.com/support/kbdoc/000155454

PowerMax/VMAX – https://www.dell.com/support/kbdoc/000062039

PowerScale/Isilon – https://www.dell.com/support/kbdoc/000157794

PowerFlex – https://www.dell.com/support/kbdoc/000187624

Dell PowerStore

Dell PowerStore systems use SupportAssist for Observability data collection. This must be enabled and configured successfully on each appliance in the PowerStore cluster.

To configure SupportAssist in PowerStore Manager, go to **Settings > Support > SupportAssist**. Click the SupportAssist setting to “Enabled” and configure one of the SupportAssist options. Verify that the **Connect to CloudIQ** box is checked.

For PowerStore 4.0 and above:

Go to **Settings > Support > Support Connectivity**. Click the **Connection Type** tab. Configure the remote connectivity for either Connect Directly or Connect via Secure Connect Gateway. Verify that the **Connect to CloudIQ** box is checked.

For detailed information about onboarding PowerStore systems, see https://www.dell.com/support/kbdoc/000157595.

Dell SC Series

The Dell SC Series Observability solution leverages Dell's SupportAssist for data collection. This must be enabled and configured successfully on each individual Dell SC Series system before users can send data to Observability.

To configure SupportAssist in Unisphere Central for Dell SC Series, open the Data Collector menu and select **Monitoring > SupportAssist > Turn On SupportAssist.**

To configure SupportAssist in the DSM thick Client, click **Storage > Edit Storage Center Settings > SupportAssist** tab**.**

Collect the following information from Unisphere as it will be required to complete the onboarding process in Observability:

- System Serial Number
- Service Tag
- Storage Center Version

Log in to the Observability UI and go to the **Admin > Connectivity** page. Select the **ADD SC SERIES** button and step through the wizard which prompts the user for the Serial Number, Service Tag, and Storage Center Version that was previously collected.

For detailed information about onboarding Dell SC Series arrays, see: https://www.dell.com/support/kbdoc/000155957.

Dell PowerVault

The Dell PowerVault systems use SupportAssist for Observability data collection. This must be enabled in the PowerVault ME Storage Manager.

To configure SupportAssist in ME Storage Manager, go to **System Settings > SupportAssist**, select the SupportAssist box, and verify the system is successfully connected.

Select the **CloudIQ Settings** tab and select the **Enable CloudIQ** box.

Collect the following information from ME Storage Manager as it is required to complete the onboarding process in Observability:

- WWN
- Service Tag
- Firmware Version

Alternatively, login to the system and use the CLI to collect the above information.

Log in to the Observability UI and go to the **Admin > Connectivity** page. Select the **ADD POWERVAULT** button and step through the wizard which prompts the user for the WWN, Service Tag, and Firmware Version that was previously collected.

For detailed information about onboarding Dell PowerVault systems, see: https://www.dell.com/support/kbdoc/000022224.

Dell VxBlock/VBlock

Dell Converged systems use Secure Connect Gateway/Dell Technologies Services configured in Converged Management Software (CMS) for data collection.

To configure Observability data collection, log in to CMS using administrator privileges. Select **Settings > Configure Dell Technologies services**. Enter the Access Key and PIN. If you do not have an access key and PIN, you can request a new one from the link on the screen. Enter the **Software ID** (SWID) and click **Save**.

Collect the following information from CMS as it is required to complete the onboarding process in Observability:

- System Serial Number
- Network Switch Serial Numbers

Log in to the Observability UI and go to the **Admin > Connectivity** page. Select ADD VXBLOCK and step through the wizard which prompts the user for the System Serial Number, Core Network Switch A Serial Number, and Core Network Switch B Serial Number.

For detailed information about onboarding Dell VxBlock/VBlock systems, see: https://www.dell.com/support/kbdoc/0000208967.

Dell VxRail

Starting with v 7.0.350, VxRail Hyper-Converged Infrastructure systems require Secure Connect Gateway for Observability Data Collection. See the appropriate VxRail Administration Guide for the correct procedures.

V7.0.x – VxRail Administration Guide

V8.0.x – VxRail Administration Guide

Alternately, see Solve Online for VxRail.

Telemetry must also be enabled for Observability collections. This is accomplished by enabling Customer Improvement Program. The default and recommended collection level is Medium. This collects samples once per hour.

For detailed information about onboarding VxRail systems, see: https://www.dell.com/support/kbdoc/000184396

PowerEdge

OpenManage Enterprise 3.7 or greater is needed to collect data from PowerEdge servers and sends the data to Observability. For versions below 4.0, the CloudIQ plug-in is required to be installed in OpenManage Enterprise to enable the flow of data to Observability.

1. Install OpenManage Enterprise 3.7 or greater.
2. In OpenManage Enterprise, go to **Application Settings > Console and Plugins.**
3. Select the CloudIQ plug-in, and click **Install Plugin.**
4. Select **Accept** on the licensing agreement.
5. Select **I agree that I have captured a snapshot of the OpenManage Enterprise appliance.**
6. Click **Confirm Install.**

After it is installed, the CloudIQ plug-in must be configured.

1. In OpenManage Enterprise, go to **Plugins > CloudIQ > Overview.**
2. Select **Activate Now.**
3. On the Authentication page, enter the Access Key and PIN to register OpenManage Enterprise with the Dell Connectivity Service. Generate the Access Key and PIN as documented in Dell KB article 000180688.
4. Enter a **Collector Name** on the Collector Name page.
5. Click **Select Groups** on the Device Groups page and select devices for monitoring in Infrastructure Observability.
6. Select **Next** to see the summary of the configuration and click **Finish** to complete the configuration.

Note: Starting with OpenManage Enterprise 4.0, the CloudIQ Plugin is installed by default.

For detailed information about onboarding PowerEdge servers to Observability, see: https://www.dell.com/support/kbdoc/000189403.

Dell PowerProtect DD

PowerProtect DD systems use Secure Connect Gateway for Observability data collection. To configure Secure Connect Gateway in DD System Manager, open the **Configuration** tab under **Maintenance** > **Support**.

Enable Secure Connect Gateway under the **Channel** section.

Select the Enable button under the **CloudIQ** section.

Verify “Share Data with CloudIQ” is set to Enabled.

For detailed information about onboarding PowerProtect DD systems, see: https://www.dell.com/support/kbdoc/000183656

Dell PowerProtect Data Manager

PowerProtect Data Manager uses Secure Remote Services or Secure Connect Gateway for Observability data collection. To configure Secure Remote Services in PowerProtect Data Manager, go to the **Support** menu under the **System Settings** menu.

In the **Secure Remote Services** section, enter the Secure Connect Gateway Hostname, Username, and Password.

In the **Auto Support** section, switch **Enable Auto Support** to Enabled.

Select **Save** to save the configuration.

For detailed information about onboarding PowerProtect Data Manager systems, see: https://www.dell.com/support/kbdoc/000184014

Connectrix Switches

Connectrix switches use the Observability Collector to collect the data from the switches and send the data back to Observability using Secure Connect Gateway. The collector is a vApp that is downloaded from the Admin > Collectors menu in the Observability user-interface or from support.dell.com. Then, it must be installed locally in the data center.

After it is deployed, the collector is configured to communicate to the Secure Connect Gateway and the Connectrix switches by accessing the collector administration UI using a web browser: https://<collector hostname or IP>.

Communication between the Collector and the switches is done using REST API. The following guidelines can be used to verify and enable the REST API interface for both Brocade and Cisco.

Brocade

The following command can be used to verify that the REST API is enabled:

```
mgmtapp --show
  REST Interface State: Enabled
  REST Session Count: 3
  REST Throttling Configurations:
     Sample Requests      : 30
     Sample Time (in sec) : 30
     Idle Time (in sec)   : 3
  KeepAlive : Disabled
  KeepAliveTimeout : 15sec
```

The following command can be used to enable REST API if it is not enabled:

```
mgmtapp --enable rest
```

Cisco

The following commands can be used to ensure that REST API is enabled:

```
switch# config t
switch(config)# feature nxapi
```

For detailed information about onboarding Connectrix switches, see: https://www.dell.com/support/kbdoc/000157620.

PowerSwitch

PowerSwitch devices use the Observability Collector to collect the data from the switches and send the data back to Observability using Secure Connect Gateway. The collector is a vApp that is downloaded from the Admin > Collectors menu in the Observability user-interface or from support.dell.com. Then, it must be installed locally in the data center. The Collector must be running v1.11.0 or later.

After the Collector vApp is deployed, the collector is configured to communicate to the Secure Connect Gateway and PowerSwitch devices by accessing the collector using a web browser: https://<collector hostname or IP>.

Communication between the Collector and the switches is done using REST API. The following guidelines can be used to verify and enable the RESTCONF API service for each PowerSwitch.

To verify mode:

```
OS10# show switch-operating mode
Switch-Operating-Mode : Full Switch Mode
```

Enter Configuration mode:

```
OS10# configure terminal
OS10(config)#
```

Enable RESTCONF API:

```
OS10(config)# rest api restconf
OS10(config)# exit
```

Note: For SONiC, RESTCONF API is enabled by default.

It is recommended to use a user account with netoperator privileges.

For detailed information about onboarding PowerSwitch, see https://www.dell.com/support/kbdoc/000192029.

VMware

VMware uses the Observability Collector to communicate to vCenter and send data back to Observability using Secure Connect Gateway. The collector is a vApp that is downloaded from the Admin > Collectors menu in the Observability user-interface or from https://support.dell.com. It is then installed locally in the data center. The collector requires read-only privileges to access and pull data from vCenter.

Once the Collector vApp is deployed, the collector is configured to communicate to the Secure Connect Gateway and vCenter by accessing the collector using a web browser: https://<collector hostname or IP>.

For detailed information about onboarding VMware, see: https://www.dell.com/support/kbdoc/000021264.

Appendix B: APEX AIOps Infrastructure Observability security

Infrastructure Observability Security summary

Infrastructure Observability takes numerous steps to protect your information in transit and at rest. In addition, Observability has been developed using architectural controls as part of the Dell standard secure development life cycle. This standard defines the security-focused activities that Dell product teams must follow when building and releasing products. It enables Dell Technologies to minimize the risks to our products and customer environments from security vulnerabilities. See the Security white paper for more information.

Infrastructure Observability data in transit to Dell

Infrastructure Observability subscribes to notifications from Dell Secure Remote Services, Secure Connect Gateway, and Dell Phone Home services when storage system metadata arrives over those channels. This metadata can include, for example, system logs, system configuration, system capacity, and performance metrics. No customer data is sent, and only data generated by the customer's systems is sent. Customers control which systems send information over these channels. See the document Secure Connect Gateway Security for more information.

All data arriving through those channels is protected in transit by industry-standard best practices. Both channels use digital certificates and customer-controlled access policies to establish point-to-point encryption and ensure all data is securely transported to the Dell IT-managed infrastructure. In addition, Secure Connect Gateway provides for dedicated VPN and multifactor authentication. Once the data arrives, Infrastructure Observability stores data relating to those systems which have Observability management enabled in its own Dell IT-managed infrastructure.

Infrastructure Observability data at rest

Infrastructure Observability data is stored on Dell infrastructure, which is highly available, fault tolerant, and provides a 4-hour Disaster Recovery SLA. Dell's Global Security Organization (GSO), led by a Chief Information Security Officer, is responsible for security and protection of Dell's information technology infrastructure. This is accomplished using establishment of governing security policies and procedures, and enforcement of Information Security control. This includes measures such as multilayered firewalls, intrusion detection systems, industry-leading anti-virus, and malware protection.

The Dell cybersecurity team is involved in running continuous vulnerability scans on the application and underlying environment. Any required remediation is handled through an ongoing vulnerability remediation program such as software upgrades, patches, or configuration changes.

All data sent to Infrastructure Observability is stored on infrastructure hosted in the Dell data center. The Information Security Policy ensures that all Dell information and resources are properly protected, information owners must ensure all resources are accounted for, and each resource has a designated custodian. All infrastructure is in the core network behind corporate firewalls, and is not exposed to external direct access. No individual direct login to the database server and database is allowed, expect for members of the System Administrator and Database Administrator teams. Database application accounts are managed using standard database password authentication.

Dell has implemented an industry best practice Change Management process to ensure that Dell production line assets are stable, controlled, and protected. Change Management provides the policies, procedures, and tools needed to govern these changes, to ensure that they undergo the appropriate reviews, approvals, and are communicated to users.

Accessing Infrastructure Observability data

Infrastructure Observability access requires that each user has a valid Dell support account. Customers use their existing support account to log in to Observability. Authentication is handled by the Dell Single-Sign-On (SSO) infrastructure, and multifactor authentication is enforced.

Infrastructure Observability leverages information in the user profile stored in Dell Service Center related to company and site mapping for access control. The user profile is created and associated with a valid company profile when the user registers for an account with Dell.

Infrastructure Observability provides each customer with an independent secure view of their systems and ensures that they will only be able to see their own data in Observability. Each user can only see those systems in Observability which are part of that user's site access as per the configuration of that user in Dell Service Center.

Appendix C: Data collection frequencies and samples

The following chart provides the data collection frequency per system type.

	Performance	Capacity	Configuration
PowerMax/VMAX	5 minutes	1 hour	1 hour
PowerStore	5 minutes	5 minutes	1 hour
PowerScale/Isilon	5 minutes[14]	1 hour	1 hour
PowerVault	15 minutes	1 hour	1 hour
PowerFlex	5 minutes	1 hour	1 hour
Unity XT family	5 minutes	1 hour	1 hour
XtremIO	5 minutes	1 hour	1 hour
SC Series	5 minutes	1 hour	1 hour
VxBlock	N/A	N/A	24 hours
PowerEdge	5 minutes	N/A	1 hour
Connectrix	5 minutes	5 minutes	5 minutes
PowerSwitch	5 minutes	1 hour	1 hour
VMware	5 minutes	5 minutes	5 minutes
VxRail[15]	5 minutes	5 minutes	24 hours
PowerProtect DD	5 minutes	1 hour	1 hour

The following charts display the collected metric types for various components of the systems. The P column represents performance metrics, and the C column represents capacity metrics. See the section Report Browser metrics for a full list of individual performance metrics collected for each component type.

[14] Some PowerScale performance charts provide 24-hour interval metrics.

[15] VxRail sends the 5-minute performance and capacity data to Observability at 30-minute, 60-minute, or 24-hour intervals. The telemetry setting in VxRail Manager determines the upload interval.

	System		Node / Appliance		Pool		Volume / LUN		File System		Storage Group		Drives		Host / Initiator	
	P	C	P	C	P	C	P	C	P	C	P	C	P	C	P	C
PowerMax / VMAX	✓	✓			✓	✓					✓	✓				
PowerStore	✓	✓	✓	✓			✓	✓	✓	✓			✓		✓	✓
PowerScale / Isilon	✓	✓	✓	✓		✓										
PowerVault	✓	✓			✓	✓	✓	✓					✓	✓	✓	✓
PowerFlex	✓	✓														
Unity XT family	✓	✓			✓	✓	✓	✓	✓	✓			✓	✓	✓	✓
XtremIO	✓	✓					✓	✓								
SC Series	✓	✓			✓		✓	✓					✓	✓	✓	✓

Connectrix Switches

	Switch		Partition		Zone		Attached Devices		Interface	
	Perf	Cap	Perf	Cap	Perf	Cap	Perf	Cap	Perf	Cap
Connectrix	✓	✓							✓	
PowerSwitch		✓								

VMware

	ESXi Cluster		ESXi Server		Datastore		Virtual Machine	
	Perf	Cap	Perf	Cap	Perf	Cap	Perf	Cap
VMware	✓		✓		✓	✓	✓	✓

Appendix D: Report Browser metrics

The following charts provide the time series metrics available in Report Browser.

Connectrix

Fibre Channel only

Metric	Switchport	System
Buffer Errors	X	
Buffer Errors by All Buffer Errors	X	
Buffer Errors by B2B Credit Zero	X	
Class-3 Discards	X	
Congestion Ratio	X	
CRC Errors	X	
Link Resets	X	X
Link Resets by In/Out	X	X
Physical Layer Errors	X	
Physical Layer Errors by All Physical Layers	X	
Physical Layer Errors by Encoding Errors	X	
Physical Layer Errors by FEC Blocks	X	
Protocol Errors	X	
Protocol Errors by All Protocol Errors	X	
Protocol Errors by Frames Length	X	
Protocol Errors by Non Operational Sequence	X	
Protocol Errors by Offline Sequence	X	
Throughput	X	X
Throughput by Rx/Tx	X	
Time at Zero Tx Credit	X	
Utilization	X	X
Utilization by Rx/Tx	X	
B2B Credit Zero/sec		X
Errors		X
Daily Carbon Footprint		X

Metric	Switchport	System
Daily Energy		X
Power Consumption		X

PowerEdge

Available PowerEdge metrics vary based on model, license, and firmware. See the CloudIQ section of the OpenManage Portfolio Software Licensing Guide for more details.

Chassis
Amount of Energy Consumed (kWh, Avg over last 15 min)
Amount of Energy Consumed (kWh, Max over last 15 min)
Amount of Energy Consumed (kWh, Min over last 15 min)
Inlet Temperature (°C, Avg over last 15 min)
Peak Inlet Temperature (°C, Max over last 15 min)
Peak Inlet Temperature (°C, Min over last 15 min)
Power Consumption (W, Avg over last 15 min)
Power Consumption (W, Max over last 15 min)
Power Consumption (W, Min over last 15 min)
Power Headroom (W, Avg Available power minus peak consumed over last 15 min)
Power Headroom (W, Max Available power minus peak consumed over last 15 min)
Power Headroom (W, Min Available power minus peak consumed over last 15 min)

Drives	
NVMe	Storage Disk
Available Spare Threshold (%)	Command Timeout (Count for last hour)
Composite Temp (°C, Max over last 15 min)	CRC Errors (Count for last hour)
Critical Warnings	Drive Life Remaining (%)
Percentage Used (Max over last 1 hour)	Drive Temperature (°C, Avg over last hour)
	Erase Failures (Count for last hour)
	Exception Mode Status (Count for last hour)
	Media Writes (Count for last hour)
	Power On Hours
	Program Fail (Count for last hour)
	Read Error Rate (Count for last hour)
	Reallocated Block (Count for last hour)
	Uncorrectable Error (Count for last hour)

Drives	
	Uncorrectable LBA (Count for last hour)
	Volatile Memory Backup Source Failures (Count for last hour)

FC Port
Invalid CRCs (Count for last 5 min)
Link Failures (Count for last 5 min)
Received Bytes (Total over last 5 min)
Transmitted Bytes (Total over last 5 min)

Network Port
Discarded Packets (Count for last 5 min)
Excessive Collision Packets (Count for last 5 min)
FCoE Packets Received (Count for last 5 min)
FCoE Packets Transmitted (Count for last 5 min)
FCoE/FIP Link Failures (Count for last 5 min)
FCS Error Packets Received (Count for last 5 min)
Jabber Packets (Count for last 5 min)
Multiple Collision Packets (Count for last 5 min)
RDMA Bytes Transmitted (Total over last 1 min)
RDMA Packets Received (Count for last 5 min)
RDMA Packets Transmitted (Count for last 5 min)
Received Bytes (Total over last 5 min)
Transmitted Bytes (Total over last 5 min)

Processor (CPU/GPU)
CPU Temperature (°C, Avg. over last 5 min)
GPU: Board Temperature (°C, Avg. over last 15 min)
GPU: DBE Retired Pages (Count for last 15 min)
GPU: Power Consumption (W, Avg. over last 15 min)
GPU: Primary Temperature (°C, Avg. over last 15 min)
GPU: SBE Retired Pages (Count for last 15 min)
GPU: Secondary Temperature (°C, Avg. over last 15 min)

Server

Server
Avg. CPU Usage
Avg. IO Usage
Avg. Memory Usage
Avg. System Usage
Daily Carbon Footprint
Daily Energy
Inlet Temperature (°C, Avg. over last 15 min)
Peak Inlet Temperature (°C, Max. over last 15 min)
Power Consumption (W, Avg. over last 15 min)
Power Consumption (W, Max. over last 15 min)
Power Consumption (W, Min. over last 15 min)
System Net Airflow (CFM, Avg. over last 15 min)
Total CPU Power (W, Total over last 15 min)
Total Memory Power (W, Total over last 15 min)

PowerFlex

Metric	Device	Fault Set	Host	Protection Domain	SDS	Storage Pool	System
% Read	X		X	X	X	X	X
% Write	X		X	X	X	X	X
Bandwidth	X		X	X		X	X
Bandwidth by Read/Write	X		X	X		X	X
Capacity in Use	X			X		X	X
IOPS	X		X	X		X	X
IOPS by Read/Write	X		X	X		X	X
Latency	X		X	X	X		X
Latency by Read/Write	X		X	X	X		X
Unused Capacity	X			X			X
Spare Capacity						X	X
Compression Ratio		X		X	X	X	X
Provisioned				X		X	X
Total Capacity				X		X	X
Net Thin Capacity Provisioned							X
Used Thick Capacity							X
Used Thin Capacity							X

PowerMax

Metric	FE Dir	FE Port	Host	RDF Dir	RDF Port	RDFA Group	RDFS Group	Storage Group	Storage Resource Pool	System	File System
% Busy	X	X		X	X						
% Hit							X				
% Write							X				
% Read								X	X	X	
Allocated Size								X			
Used Size									X		
Bandwidth	X	X	X	X	X		X	X	X	X	X
Bandwidth by Read/Write		X	X	X	X			X	X	X	
IO Size		X			X			X	X	X	
IO Size by Read/Write		X			X			X	X	X	
IOPS	X	X	X	X	X		X	X	X	X	X
IOPS by Read/Write		X	X		X		X	X	X	X	
Latency		X	X				X	X	X	X	
Latency by Read/Write		X	X				X	X	X	X	
Queue Length								X	X	X	
Queue Length by Read/Write								X	X	X	
Queue Depth Utilization	X										
Read Latency	X										X
Write Latency	X										X
Reducible Data								X			
Total Size								X			
Unreducible Data								X			
Avg IO Service Time						X					
Compressed Bandwidth						X					
Compressed Bandwidth by Read/Write						X					

Metric	FE Dir	FE Port	Host	RDF Dir	RDF Port	RDFA Group	RDFS Group	Storage Group	Storage Resource Pool	System	File System
RDF R1 to R2 Bandwidth						X					
RDF R1 to R2 IOPS						X					
RDF R2 to R1 Bandwidth						X					
RDF R2 to R1 IOPS						X					
RDF/A WP Count						X					

PowerProtect DD

Metric	Data Protection System	Replication
Average CPU Utilization	X	
Incoming Pre-comp Replication	X	X
Incoming Replication Streams	X	X
Outgoing Pre-comp Replication	X	X
Outgoing Replication Streams	X	X
Pre-comp Read Throughput	X	
Pre-comp Write Throughput	X	
Read Streams	X	
Write Streams	X	

PowerScale

Metric	Node	System	Pool
Active Client Number	X	X	
Bandwidth	X	X	
Configured Size		X	
CPU	X	X	
Daily Carbon Footprint		X	
Daily Energy		X	
Free Size		X	
Free Size on 5 mins interval			X

Metric	Node	System	Pool
Free Size on one day interval			X
IOPS	X	X	
Latency	X	X	
Power Consumption		X	
Used Percent		X	X
Used Size		X	
Used Size on 5 mins interval			X
Used Size on one day interval			X

PowerStore

Metric	Appliance	Ethernet	Fibre Channel	File System	iSCSI	Node	System	Volume	Volume Group
% Read				X					
Bandwidth	X	X	X	X	X	X	X	X	X
Bandwidth by Read/Write	X		X	X	X	X	X	X	X
Bandwidth by Received/Transmitted		X							
CPU Utilization	X					X			
Data Reduction Ratio							X		
Errors		X							
Errors by Type		X							
Free Logical Size							X		
Free Size				X			X	X	X
Invalid Count Errors			X						
Invalid Counts by Type			X						
IO Size	X		X	X	X	X		X	X
IO Size by Read/Write	X		X	X	X	X		X	X
IOPS	X		X	X	X	X	X	X	X
IOPS by Read/Write	X		X	X	X	X	X	X	X

Metric	Appliance	Ethernet	Fibre Channel	File System	iSCSI	Node	System	Volume	Volume Group
Latency	X		X	X	X	X	X	X	X
Latency by Read/Write	X		X	X	X	X	X	X	X
Logical Size							X		
Loss Errors			X						
Loss Errors by Type			X						
Packets		X							
Packets by Received/Transmitted		X							
Queue Depth	X					X		X	
Total Size				X			X	X	X
Total Used Logical Size							X		
Unique Physical Used Size								X	
Used Size				X			X	X	X

PowerVault

Metric	Controller	Drive	Host	Pool	Pool Backend	System	System Backend	Volume
% Read	X	X	X	X	X	X	X	X
% Read Hits								X
% Write Hits								X
Bandwidth	X	X	X	X	X	X	X	X
Bandwidth by Read/Write	X	X	X	X	X	X	X	X
Free Size				X				
IO Size	X	X	X	X	X	X	X	X
IO Size by Read/Write	X	X	X	X	X	X	X	X
IOPS	X	X	X	X	X	X	X	X
IOPS by Read/Write	X	X	X	X	X	X	X	X
Total Size								X
Used Size				X				X

SC Series

Metric	Drive	FC, SAS, iSCSI	Pool	Pool Backend	System	System Backend	Volume
% Read	X	X	X	X	X	X	X
Bandwidth	X	X	X	X	X	X	X
Bandwidth by Read/Write	X	X	X	X	X	X	X
CPU Utilization					X		
Free Size			X				
IO Size		X	X	X	X	X	X
IO Size by Read/Write		X	X	X	X	X	X
IOPS	X	X	X	X	X	X	X
IOPS by Read/Write	X	X	X	X	X	X	X

Metric	Drive	FC, SAS, iSCSI	Pool	Pool Backend	System	System Backend	Volume
Latency	X	X	X	X	X	X	X
Latency by Read/Write	X	X	X	X	X	X	X
Queue Length	X	X	X	X	X	X	X
Total Size							X
Used Size			X				X

Unity XT family

Metric	Block	Drive	Ethernet	Fibre Channel	File	iSCSI	Pool	Pool Backend	System	System Backend	System-Cache
% Read	X	X			X		X	X	X	X	
Allocated Size	X				X						
Bandwidth	X	X	X	X	X	X	X	X	X	X	
Bandwidth by In/Out			X								
Bandwidth by Read/Write	X	X		X	X	X	X	X	X	X	
Bandwidth by SP	X	X			X		X	X	X	X	
Bandwidth by SP and Read/Write	X	X			X		X	X	X	X	
CPU Utilization									X		
Daily Carbon Footprint									X		
Daily Energy									X		
Errors			X								
Errors by In/Out			X								
Free Size							X		X		
IO Size	X				X		X	X	X	X	
IO Size by Read/Write	X				X		X	X	X	X	

Metric	Block	Drive	Ethernet	Fibre Channel	File	iSCSI	Pool	Pool Backend	System	System Backend	System-Cache
IO Size by SP	X				X		X	X	X	X	
IO Size by SP and Read/Write	X				X		X	X	X	X	
IOPS	X	X			X		X	X	X	X	
IOPS by Read/Write	X	X			X		X	X	X	X	
IOPS by SP	X	X			X		X	X	X	X	
IOPS by SP and Read/Write	X	X			X		X	X	X	X	
Latency	X				X		X		X		
Latency by Read/Write	X				X		X		X		
Latency by SP	X				X		X		X		
Latency by SP and Read/Write	X				X		X		X		
Packets			X								
Packets by In/Out			X								
Power Consumption									X		
Queue Length	X				X		X		X		
Requests				X		X					
Requests by Read/Write				X		X					
Total Size	X				X						
Used Size					X		X		X		
vVol Latency							X		X		
Total Link Errors				X							
Total Link Errors by Link Error				X							

Metric	Block	Drive	Ethernet	Fibre Channel	File	iSCSI	Pool	Pool Backend	System	System Backend	System-Cache
% Clean											X
% Dirty											X
% Free											X
Flushed											X

VMware

Metric	ESXi	Virtual Machine	Datastore
Active Memory	X	X	
Bandwidth per Datastore		X	
CPU Readiness		X	
CPU Usage	X	X	
IOPS per Datastore		X	
Latency per Datastore		X	
Storage Latency		X	
Capacity			X
Free Space			X
Uncommitted			X

VxRail

Metric	HCI System	Host
CPU Hertz		X
CPU Ready Summation		X
CPU Utilization (%)		X
Daily Carbon Footprint	X	
Daily Energy	X	
Disk Latency		X
Disk Utilization		X
Memory Consumed Average		X
Memory Overhead Average		X
Memory SwapInRate Average		X
Memory SwapOutRate Average		X
Memory Utilization (%)		X
Memory VM Control Average		X
Networking Utilization		X

Metric	HCI System	Host
Power Consumption (Avg W over last hr)	X	

XtremIO

Metric	Initiator	System	Target	Volume
Bandwidth	X	X	X	X
Bandwidth by Read/Write	X	X	X	X
Block Latency	X	X	X	X
Block Latency by Read/Write	X	X	X	X
CPU Utilization		X		
Free Size		X		
IOPS	X	X	X	X
IOPS by Read/Write	X	X	X	X
Logical Size		X		
Used Size		X		