Azure Native Qumulo Administrator Guide

Table of Contents

Snapshots

Encryption and Data Security

Data Replication

File System Changes

NFS

NFSv4.1 with Kerberos

SMB

S3 API

Monitoring and Metrics

Getting Started

How Azure Native Qumulo Works

This section explains the main functionality of Azure Native Qumulo (ANQ) and the differences between ANQ v2 and ANQ v1, provides a feature comparison between ANQ and Qumulo on other platforms and ANQ's known limitations and compliance posture, gives an overview of deploying the service in Azure, and lists the supported Azure Regions for the service.

For detailed instructions, see Deploying and Viewing Information about Your Azure Native Qumulo Instance (page 13).

What is Azure Native Qumulo?

ANQ is a fully managed service that provisions a Qumulo file system and creates a resource (for managing the file system) under your Azure subscription. ANQ provides the same multi-protocol support, interfaces, and functionality as Qumulo on premises.

ANQ makes it possible to configure file protocols, quotas, replication, and other features regardless of underlying infrastructure or storage and without tracking resource quotas or costs. The service receives the latest updates and features continuously and, if any issues occur, replaces compute and storage resources automatically.

Names and Versions

In this guide, we refer to the features and functionality of Qumulo Core as *Azure Native Qumulo (ANQ)* or *the service.*

Following ANQ's initial launch, we configured the Qumulo file system in Azure to have significant flexibility and performance improvements. This configuration appears in the Azure Portal as **ANQ v2**. For more information, see Feature Comparison with Qumulo on Other Platforms (page 4).

> **Note**
>
> - For a limited time, you can select the original **ANQ v1** configuration in the Azure Portal (after this time, **ANQ v2** remains the only available configuration).
> - For help with expanding ANQ v1 capacity, email Azure Native Qumulo Support.

Feature Comparison with Qumulo on Other Platforms

The following table compares the features of ANQ with those of Qumulo on other platforms.

Note

Because ANQ is a fully managed service, direct access to hosts with SSH is unavailable. To configure the service, you can use:

- `qq`CLI—from a remote machine
- Qumulo Core Web UI—by using any of the service's IP addresses

Feature	ANQ v2	ANQ v1	Qumulo on AWS as an AMI	Qumulo on Premises
Automatic deployment	✓	✓		
Automatic infrastructure replacement	✓	✓	✓	
Automatic updates	✓	✓		
Availability in Cloud Marketplace	✓	✓	✓	
Customer support	✓	✓	✓	✓
Integration with Azure Portal	✓			
Payment for pre-provisioned file system capacity		✓	✓	✓
Payment for used storage space only	✓			
Performance scales elastically at any capacity	✓			
Performance scales with provisioned capacity		✓	✓	✓
Qumulo Core features	✓	✓	✓	✓
Simple and fast deployment under 15 Minutes	✓			

Known Limitations

- **IPv6 Addresses:** Currently, Azure Networking features don’t support IPv6 addresses.

- **Initial Authentication over SMB:** When you deploy the service initially, all users can use the SMB protocol. However, the `admin` user can authenticate over all protocols except over SMB.

  To allow the `admin` user to authenticate over the SMB protocol, change the `admin` user's password.

- **File Systems Larger than 1 PB:** This limitation applies only to ANQ v1.

  To deploy ANQ v1 instances larger than 1 PB by using the Azure Portal, email Azure Native Qumulo Support.

Qumulo Compliance Posture

For information about Qumulo's third-party attestations, including FIPS 140-2 Level 1, GDPR, HIPAA, and SOC 2 Type II, see Qumulo Trust Center.

Deploying Azure Native Qumulo

This section outlines the process of configuring and deploying ANQ. For detailed instructions, see Deploying and Viewing Information about Your Azure Native Qumulo Instance (page 13).

1. You specify the following configuration.

   - **Regional Settings:** The availability zone and region. For more information, see Supported Azure Regions (page 7)
   - **Networking Settings:** The virtual network in the same region. For more information, see Virtual Networking Prerequisites (page 10)
   - **Usable Capacity:** For ANQ v1 instances, the available file system capacity (in TB).

     > **Note**
     > Because ANQ v2 instances use the Azure Blob Store capacity limit (in EB), it isn't necessary to configure usable capacity in advance.

2. When Qumulo creates your ANQ instance, it deploys and configures the following Azure resources:

   - **Managed Resource Group:** This group contains the networking resources that the service deploys.

     When you create your service instance, you can specify an existing resource group or create a new one.

   - **Delegated Subnet:** The delegated subnet that the service uses to provision endpoints for your virtual network.

     When you create your service instance, you can specify an existing delegated subnet or create a new one..

- **Qumulo Service Resource:** The Azure resource that represents one instance of the service.

  You can use this resource to manage and view the service configuration.

- **Marketplace SaaS Resource:** The Qumulo Marketplace SaaS resource that you select.

  Azure uses this resource for billing purposes.

> ☑ Tip
> To automate the creation of ANQ instances for long-term use cases and for short-term components of automated storage workflows, use Azure Resource Manager.

Supported Azure Regions

The following table lists regions in US, Canada, Europe, and the UK that ANQ supports.

Geographical Location	Azure Region	ANQ v2	ANQ v1
US (Arizona)	West US 3	✓	✓
US (California)	West US		✓
US (Illinois)	North Central US		✓
US (Iowa)	Central US	✓	✓
US (Texas)	South Central US	✓	✓
US (Virginia)	East US	✓	✓
US (Virginia)	East US 2	✓	✓
US (Washington)	West US 2	✓	✓
Canada (Toronto)	Canada Central	✓	✓
Europe (Frankfurt)	Germany West Central	✓	✓
Europe (Gavle)	Sweden Central	✓	✓
Europe (Ireland)	North Europe	✓	✓
Europe (Netherlands)	West Europe	✓	✓

Geographical Location	Azure Region	ANQ v2	ANQ v1
Europe (Oslo)	Norway East	✓	✓
Europe (Paris)	France Central	✓	✓
Europe (Zurich)	Switzerland North	✓	✓
UK (London)	UK South	✓	✓
Australia (New South Wales)	Australia East	✓	
Brazil (São Paulo State)	Brazil South	✓	
India (Pune)	Central India	✓	
Japan (Tokyo, Saitama)	Japan East	✓	
Korea (Seoul)	Korea Central	✓	
UAE (Dubai)	UAE North	✓	

Usage Metering and Billing for Azure Native Qumulo

Once an hour, ANQ reports a metering event to Azure Marketplace for each deployed instance.

> **Note**
> ANQ v1 and ANQ v2 use different dimensions for metering.

ANQ v1 Metering for Total Available Capacity

Qumulo provisions ANQ v1 instances with a total available capacity (to increase this capacity, you can contact the Qumulo Care team).

Qumulo performs metering on a single dimension—the total available capacity that your instance reports.

ANQ v2 Metering for Used Capacity and Throughput

Qumulo doesn't provision ANQ v2 instances with a total available capacity. Instead, it performs metering on two dimensions:

- Used capacity
- Used throughput

Note

Because the throughput for an instance can vary significantly within a given hour, Qumulo samples the used throughput *each minute*. It rounds the computed throughput value to 1 GBps and then multiplies it by the used capacity during the given minute. For more information about pay-as-you-go price estimates, see the Pricing and Performance Calculator.

Virtual Networking Prerequisites for Azure Native Qumulo

This section lists the prerequisites for Azure Native Qumulo (ANQ), describes the components of virtual networking for the service, explains how to configure them, and provides virtual networking best practices.

How Qumulo Manages Virtual Networking for Azure Native Qumulo

When you create an ANQ instance, Qumulo manages the underlying storage and compute resources for the service. These resources reside within Qumulo's Azure tenant.

The ANQ instance connects to your Azure subscription by using *VNet injection*, an Azure-specific networking technology that establishes an automatic, direct connection between your resources and service resources without complicated manual configuration or VNet peering.

VNet injection lets you:

- Apply routing and security policies to your ANQ service endpoints by using the Azure Portal, CLI, and API.
- Create endpoints that allow access to ANQ by inserting special network interfaces into your subnet. This process binds these network interfaces directly to the compute resources of your ANQ instance.

When you create your ANQ instance, the Azure Portal guides you to create an appropriate subnet configuration in your virtual network. Then, VNet injection delegates privileges to Qumulo by communicating with the subnet.

Prerequisites for Configuring Virtual Networking

This section explains the prerequisites for configuring virtual networking for ANQ, such as creating roles, configuring dedicated subnets, and load-balancing endpoints.

Creating Owner and Contributor Roles

The service requires an owner or contributor role with access to your Azure subscription.

> ⚠ Important
> A custom role must have write permissions to the resource groups in which you create your delegated subnet and service.

Creating A Dedicated Subnet

The service requires a dedicated subnet.

> **Note**
>
> - Your subnet address range should be at least `/24` (it should contain at least 256 IP addresses, including 251 free IP addresses and 5 IP addresses reserved for Azure.)
> - Your subnet must be in the same region as the ANQ file system.

To Create a Dedicated Subnet Automatically

We recommend using the Azure Portal's automatic subnet creation and configuration functionality.

1. Create your ANQ instance. For detailed instructions, see Deploying and Viewing Information about Your Azure Native Qumulo Instance (page 13).
2. In the Azure Portal, click **Manage Subnet Configuration**.
3. When prompted, enter an IP address range for your subnet.

The Azure Portal configures your subnet and the required delegation for VNet injection automatically.

To Create a Dedicated Subnet Manually

To apply a specific subnet configuration, you can first create a subnet and then select it when you create your ANQ instance.

1. Identify the region in which you want to subscribe to ANQ.
2. In the region, create a new virtual network or select an existing virtual network.
3. In your virtual network, create a new subnet.

   Use the default configuration or update the subnet network configuration based on your network policy.
4. Delegate the newly created subnet to `Qumulo.Storage/fileSystems`.

Load-Balancing ANQ Endpoints

Qumulo provisions multiple endpoints to allow access to ANQ. Every endpoint appears in the Azure Portal as a network interface with an IP address. Qumulo creates a managed resource group under your subscription for these endpoints.

> **Tip**
> To view links to your managed resource groups and network interfaces, use the **Portal** view of your `Qumulo.Storage/fileSystems` resource.

To avoid the bandwidth limits of individual endpoints, use round-robin DNS to distribute your workload traffic across your endpoints.

Configuring Virtual Networking

This section provides an overview of configuring virtual networking for ANQ, including configuration of network security groups, route tables, and back- and front-end networking.

> ⚠ Important
> To enforce network policies for traffic to and from the service, you can apply network security groups and route tables to a delegated subnet.

Configuring Network Security Groups

Network security groups let administrators enforce networking traffic rules. You can assign network security groups to individual network interfaces or to entire subnets.

> ☑ Tip
> Because it is possible to create or remove network interfaces from an ANQ instance, we recommend assigning security groups to a delegated subnet.

To ensure that your configuration doesn't block a specific protocol, follow the guidance in Required Networking Ports for Qumulo Core.

Configuring Route Tables

To configure explicit traffic routing to and from the service, you must attach an Azure route table to a delegated subnet, and then configure your route table.

Common configuration scenarios include routing service traffic:

- Through a firewall
- Through a gateway appliance
- Across multiple virtual network peering configurations

Configuring Back-End and Front-End Networking

The ANQ service uses a *split-networking configuration* in which different network interfaces handle back-end and front-end traffic.

Because it isn't possible to access the back-end network configuration or affect back-end traffic within your ANQ instance, you can configure firewalls and security groups within your virtual network without having to consider back-end connectivity requirements.

Deploying and Viewing Information about Your Azure Native Qumulo Instance

This section explains how to deploy Azure Native Qumulo (ANQ), view information about your service, and connect to the Qumulo Web UI.

For an introduction, see How Azure Native Qumulo Works (page 4).

To Deploy

This section explains how to deploy the ANQ service in Azure.

1. Log in to the Azure Portal and search for `Azure Native Qumulo`.
2. On the **Create a Qumulo resource in Azure** page, on the **Basics** tab, in the **Project details** section:
    a. Select a **Subscription** that you can access as an owner or contributor.
    b. Select a **Resource group** or click **Create new**.

    > **Note**
    > A *resource group* is a container that holds related Azure resources. We recommend creating a resource group exclusive to your Qumulo infrastructure.

3. In the **Azure resource details** section:
    a. Enter a **Resource name**.

    This is the name of your service.

    b. Select a **Region**.

    For more information, see Supported Azure Regions (page 7).

    c. Select an **Availability zone**.

    Azure pins the service resources in a region to this availability zone.

    > **Note**
    > By creating all your Qumulo resources within the same availability zone, Azure can reduce latency.

4. In the **Administrator account** section, enter a **Password** and then re-enter it.

5. In the **Qumulo file system details** section:
    a. Select the **Standard** or **Performance** storage type.
    b. Specify the size of the service to create in TB.
6. In the **Pricing plan** section, select a pricing plan.

    The pay-as-you-go plan is the default plan.

    - For more information about pay-as-you-go price estimates, see the Pricing and Performance Calculator.
    - For up-front pricing plans and free trials, email Azure Native Qumulo Support.
7. On the **Networking** tab, in the **Configure virtual network** section:
    a. Select the **Virtual network** for hosting your service. For more information, see Virtual Networking Prerequisites for ANQ (page 10).
    b. Do one of the following:
        - Select an existing delegated subnet to associate with your service.
        - To create a new delegated subnet, click **Manage subnet configuration**.

    > **Note**
    > You can associate only one delegated subnet with one service instance.
8. On the **Tags** tab, enter any custom tags as a name-value pair.
9. To create a service, click **Next: Review + Create >**.

Viewing Service Information and Connecting to the Qumulo Core Web UI

When Azure finishes creating your service, you can view information about the service and start using the Qumulo Core Web UI.

Viewing the IP Addresses of Your Service

To view the IP addresses associated with your service, click **IP Addresses** on the sidebar.

> **Tip**
> We recommend using round-robin DNS to load balance (page 11) traffic across your service IP addresses.

To Log in to the Qumulo Core Web UI

To log in to the Qumulo Core Web UI, you must identify your service endpoint.

1. Click **Overview** and then copy the **Qumulo Core Web UI Login** URL. For example:

```
https://192.0.0.4/login
```

2. Enter the URL into a browser from a machine that runs, or is connected to, the virtual network where you deployed ANQ.

   > **Note**
   >
   > - If you connect from a machine that is in a different virtual network, establish virtual network peering between the two virtual networks.
   > - If you connect from an on-premises machine, ensure that you connect by using Azure VPN Gateway or Azure ExpressRoute.

3. When the page prompts you for a **Username**, enter `admin`.
4. When the page prompts you for a **Password**, enter the administrator password that you configured previously (page 13).

Connecting Azure Native Qumulo to Microsoft Entra Domain Services

This section explains how to connect Azure Native Qumulo (ANQ) to Microsoft Entra Domain Services (DS).

> ⚠ Important
> On October 1, 2023, Microsoft renamed Azure Active Directory Domain Services to Microsoft Entra Domain Services.

Microsoft Entra DS provides managed domain services such as Windows Domain Join, Group Policy, LDAP, and Kerberos authentication. You can connect your ANQ to standard Active Directory (on-premises AD or self-managed AD in the cloud) or to Microsoft Entra DS.

For information about joining ANQ to standard AD, see Join Your Qumulo Cluster to Active Directory on Qumulo Care.

For information about joining Microsoft Entra DS, see the following resources in the Microsoft Entra documentation.

- Tutorial: Configure virtual networking for a Microsoft Entra Domain Services managed domain
- Tutorial: Join a Windows Server virtual machine to a Microsoft Entra Domain Services managed domain

To Configure Microsoft Entra Domain Services (Microsoft Entra DS)

1. Create an instance of Microsoft Entra DS by entering the following details.
    - **Name:** Your domain name.

      We recommend entering `$DOMAIN.onmicrosoft.com` that the system creates for you.

      You can also use your own custom domain name that acts as a routable or non-routable domain suffix.
    - **VNet:** A VNet and a resource group for your Microsoft Entra DS instance.
    - **SKU:** Standard
    - **Forest:** User

    After the system completes deploying your managed domain (this takes 1-2 hours), it creates the VNet that you specified.
2. Configure DNS for your managed domain.

a. Log in to the Azure portal and search for `microsoft entra domain services`.

b. Click your domain.

c. In the **Required configuration steps** section, under **Update DNS server settings for your virtual network**, write down the domain controllers (DNS servers) that the managed domain deployment created for you, and then click **Configure**.

   For more information, see Update DNS settings for the Azure virtual network in the Microsoft Entra Domain Services documentation.

3. (Optional) If the Microsoft Entra DS managed domain VNet is different from the VNet that you used for deploying ANQ, peer the two VNets.

   For more information, see Configure virtual network peering in the Microsoft Entra Domain Services documentation.

4. Configure the ANQ DNS servers to point to the servers that the managed domain provided for you.

   For more information, see Custom DNS Configuration on Qumulo Care.

5. To finish configuring your file system to work with Microsoft Entra DS, join your Qumulo cluster to AD.

   > **Note**
   > We recommend giving an administrative role to the user who joins the domain. For newly created users, the system requires a password reset when the user logs in to the Azure portal.

Next Steps

After you deploy your Microsoft Entra DS instance and connect ANQ to it, you can configure SAML Single Sign-On (SSO) for your ANQ instance (page 22).

Creating and Managing Directory Quotas in Qumulo Core

This section explains how to create, modify, and delete directory quotas by using the Qumulo Core Web UI and how to use the Cluster Alerts for Qumulo script to manage cluster quota notifications.

Performance Characteristics and Default Service Limits of Azure Native Qumulo v2

This section describes the performance characteristics and default service limits of Azure Native Qumulo (ANQ) v2.

ANQ v2 introduces a file system architecture that offers improved performance and flexibility for file systems of any size. For this reason, we eliminated the concept of *total available capacity.* You pay only for the data you store and, separately, for the throughput you use.

> **Note**
>
> - We describe the performance of your ANQ v2 instance in terms of throughput (bytes per second), IOPS, and operation latency.
> - Because ANQ v2 is a distributed file system, it is very effective for servicing multi-stream workloads with multiple clients or threads. The throughput and IOPS for single-stream and low-concurrency workloads might be lower than the performance characteristics listed in this section.

Throughput Performance

ANQ v2 instances can perform at above 100 Gbps with high-concurrency, multi-stream workloads. However, when you provision an ANQ v2 instance, Qumulo sets a default service limit of about 4 GBps. If you have a workload that needs higher sustained or peak throughput peak, email Azure Native Qumulo Support to raise this service limit.

> **Note**
> The default service limit isn't a hard cap. In certain scenarios, it might be possible to reach a throughput higher than 4 GBps with default configuration.

IOPS Performance

By default, ANQ v2 is optimized for high-throughput (rather than high-IOPS) workloads.

For workloads with IOPS sensitivity, email Azure Native Qumulo Support for a technical consultation.

Supported Configurations and Known Limits for Qumulo Core

This section provides an overview of supported configurations and known limits for Qumulo Core.

Replication Version Requirements for Qumulo Core

This section explains the relationship between the version of Qumulo Core that a cluster runs and data replication between it and other clusters.

Authentication

Configuring SAML Single Sign-On (SSO) for Your Qumulo Cluster

This section explains how to integrate your Qumulo cluster with your organization's single sign-on (SSO) service by configuring Security Assertion Markup Language (SAML) 2.0 for Qumulo Core 5.2.5.1 (and higher).

Configuring the Search Trusted Domains Option in Active Directory for a Qumulo Cluster

This section explains how to restrict the scope of LDAP queries by using the Search Trusted Domains configuration option for a Qumulo cluster joined to an Active Directory (AD) domain.

Authorization

Managing Cross-Protocol Permissions (XPP) in Qumulo Core

This section explains how Cross-Protocol Permissions (XPP) work in Qumulo Core and how to enable, disable, and check the status of XPP by using the `qq` CLI.

External Services

Using Qumulo Core Access Tokens

This section explains how to create and use access tokens—by using the Qumulo REST API, Python SDK, and `qq` CLI—to authenticate external services to Qumulo Core.

Connecting Your Kubernetes Cluster to Your Qumulo Cluster by Using the Qumulo Container Storage Interface (CSI) Driver

This section introduces the Qumulo Container Storage Interface (CSI) driver and explains how you can connect your Kubernetes cluster to your Qumulo cluster by using the Qumulo CSI driver.

Network Configuration

Required Networking Ports for Qumulo Core

This section explains which inbound and outbound networking ports Qumulo Core requires.

Connecting to Multiple Virtual Networks in Qumulo Core

This section explains how to connect a Qumulo cluster to multiple virtual networks by using VLAN tagging.

Web UI

Setting the Qumulo Core Web UI Login Banner

This section explains how to set a login banner for the Qumulo Core Web UI.

Setting the Qumulo Core Web UI Inactivity Timeout

This section explains how to set an inactivity timeout for the Qumulo Core Web UI.

qq CLI

Enabling Autocomplete for the qq CLI

This section explains how to enable automatic command completion for the qq CLI and for command aliases.

Metadata

Managing User-Defined Metadata in Qumulo Core

This section explains how to create, retrieve, list, and delete user-defined metadata in Qumulo Core by using the `qq` CLI.

Snapshots

How Snapshots Work in Qumulo Core

This section explains snapshots, their storage usage, and their locking functionality in Qumulo Core.

Managing Snapshots in Qumulo Core

This section explains how to create on-demand snapshots and snapshot policies, view and search for existing snapshots, and delete snapshots by using the Qumulo Core Web UI. It also explains how to create snapshots on a schedule, create a snapshot with an expiration time, and modify a snapshot's expiration time.

Locking and Unlocking Snapshots in Qumulo Core

This section explains how to lock or unlock a snapshot by using a key located in the Qumulo file system key store and the `qq` CLI. In addition, it explains how to lock policy-created snapshots for local policies and for policies that are part of a replication target relationship.

Recovering Files by Using Snapshots

This section explains how to use snapshots to recover files.

Encryption and Data Security

Generating and Storing ECDSA Keys on a Qumulo Cluster

This section explains how to generate Elliptic Curve Digital Signature Algorithm (ECDSA) keys and ECDSA verification signatures that are compatible with the Qumulo file system key store.

Managing Security Keys in the Qumulo File System Key Store

This section explains how to manage security keys in the Qumulo file system key store by using the `qq` CLI.

Data Replication

Creating and Managing a Continuous Replication Relationship in Qumulo Core

This section explains how to create, authorize, modify, and delete a replication relationship by using the Qumulo Core Web UI.

Using Qumulo Shift-To to Copy Objects to Amazon S3

This section explains how to use Shift-To to copy objects from a directory in a Qumulo cluster to a folder in an Amazon Simple Storage Service (Amazon S3) bucket and how to manage Shift relationships.

Using Qumulo Shift-From to Copy Objects from Amazon S3

This section explains how to use Shift-From to copy objects from a folder in an Amazon Simple Storage Service (Amazon S3) bucket (cloud object store) to a directory in a Qumulo cluster and how to manage Shift relationships.

File System Changes

How File System Change Notifications Work in Qumulo Core

This section describes how file system change notifications work in Qumulo Core and explains request filtering, recursion, and the three configuration modes for notification requests.

Watching for File Attribute and Directory Changes by Using SMB2 CHANGE_NOTIFY

This section lists the completion filters that an SMB client can request and the corresponding actions that Qumulo Core returns for a matched change.

Watching for File Attribute and Directory Changes by Using REST

This section describes how to configure Qumulo Core and watch for file attribute and directory changes by using REST.

NFS

Creating and Managing an NFS Export in Qumulo Core

This section explains how to create, modify, and delete an NFS export by using the Qumulo Core Web UI.

Enabling and Using NFSv4.1 on a Qumulo Cluster

This section explains how to configure your cluster for a supported export configuration and enable or disable NFSv4.1 on your cluster.

Managing File Access Permissions by Using NFSv4.1 Access Control Lists (ACLs)

This section explains how to use Qumulo Core's implementation of NFSv4.1 with access control lists (ACLs) to manage access permissions for files.

Configuring and Troubleshooting Host Access Rules for NFS Exports in Qumulo Core

This section explains how host access rules work in Qumulo Core and how to configure and troubleshoot them.

NFSv4.1 with Kerberos

How NFSv4.1 Works with Kerberos in Qumulo Core

This section provides an overview of how NFSv4.1 works with Kerberos in Qumulo Core.

Prerequisites for Joining a Qumulo Cluster to Active Directory

This section describes the prerequisites for joining a Qumulo Cluster to Active Directory for using NFSv4.1 with Kerberos.

Configuring Active Directory for Use With Kerberos

This section describes the Active Directory Domain Controller (DC) configuration changes necessary for enabling NFSv4.1 with Kerberos.

Performing Additional Cluster Configuration after Joining Active Directory

This section describes additional Qumulo cluster configuration that can affect the behavior of NFSv4.1 with Kerberos.

Using Kerberos Permissions in the Qumulo File System

This section describes how NFSv4.1 interacts with the secure file permissions that Kerberos enables for the Qumulo Core file system.

Configuring a Linux Client for NFSv4.1 with Kerberos

This section describes how to configure a Linux client for using NFSv4.1 with Kerberos.

Configuring Cross-Domain Active Directory Trusts

This section describes how the configuration of cross-domain Active Directory (AD) trusts supports NFSv4.1 with Kerberos.

Troubleshooting NFSv4.1 with Kerberos

This section describes common troubleshooting procedures for configuring NFSv4.1 to work with Kerberos.

SMB

Creating and Managing an SMB Share in Qumulo Core

This section explains how to create, modify, and delete an SMB share by using the Qumulo Core Web UI.

S3 API

Configuring and Using the S3 API in Qumulo Core

This section explains how to configure and get started working with the S3 API. This API lets clients and applications interact with the Qumulo file system natively, by using the Amazon S3 API.

Creating and Managing S3 Access Keys in Qumulo Core

This section explains how to create and manage credentials that S3 API actions in Qumulo Core require to access file system resources, such as access key pairs that sign requests.

Creating and Managing S3 Buckets in Qumulo Core

This section explains how to create and manage S3 buckets for a Qumulo cluster. These buckets expose a part of your Qumulo file system to applications that use the Amazon S3 API.

Managing Access to S3 Buckets in a Qumulo Cluster

This section explains how to manage access to S3 buckets in a Qumulo cluster.

Managing Access Policies for S3 Buckets in a Qumulo Cluster

This section explains how to manage access policies for S3 buckets in a Qumulo cluster.

Managing Multipart S3 Uploads in Qumulo Core

This section explains how multipart S3 uploads affect usable capacity on a Qumulo cluster and how to abort and clean up multipart uploads manually or automatically.

Supported Functionality and Known Limits for S3 in Qumulo Core

This section documents Qumulo Core support for S3 API functionality and S3 API limits.

Monitoring and Metrics

Qumulo OpenMetrics API Specification

This section lists the names, types, labels, and descriptions for the metrics that Qumulo Core 5.3.0 (and higher) emits in OpenMetrics API format.