Qumulo in the Cloud Guide

December 05, 2022

Table of Contents

Qumulo on Azure as a Service

Qumulo on Azure as a Service

Getting Started with Qumulo on Azure as a Service

This guide is a supplement to the Qumulo Getting Started Guide , where configuration steps and best practices differ from those we recommend for other platforms.

The next step after provisioning your file system is configuring it for your environment.

Networking Connectivity

The biggest difference between running Qumulo on Azure and on other platforms is connectivity to the file system through your network. This section guides you through network configuration specific to Qumulo on Azure as a Service.

Configuring Virtual Network Peering

Virtual Network (VNet) peering allows bidirectional connectivity between the file system and your infrastructure. This connectivity enables several Qumulo features, such as LDAP integration, audit logging, and Active Directory. Qumulo on Azure as a Service requires one or more VNet peering connections between the VNet provisioned for the Qumulo file system and the VNets in your infrastructure.

During the file system provisioning, you received the resource ID for the Qumulo on Azure as a Service VNet and one user from your organization was invited into the Qumulo tenancy with permissions necessary to configure VNet peering on that resource. To change who has this permission, contact Qumulo Care .

> **ⓘ Note**
> VNet peering isn't transitive. For example, if the three VNets A, B, and C are peered transitively (A ↔ B ↔ C), the infrastructure in VNet A won't be able to communicate transitively with infrastructure in VNet C. This has implications for Qumulo on Azure as a Service in the hub-and-spoke network topology , which Azure recommends as a best practice. If you have infrastructure that Qumulo must be able to reach (for example, a DNS server, a syslog audit log server, and so on) that lives in a hub VNet, you *must* peer the Qumulo on Azure as a Service VNet with your hub VNet and with any spoke VNets that must be able to connect to the file system.

Configuring DHCP Mode

> **⚠ Important**
> Configuring static networking results in an error.

Like other cloud platform implementations, you can configure Qumulo on Azure as a Service to run only in DHCP mode, where Azure assigns IP addresses to the file system automatically.

Configuring DNS

To resolve internal hostnames to IP addresses in your infrastructure, you must configure Qumulo Core to use a DNS server that can resolve the necessary hostnames. By default, the file system uses Azure's default DNS server (`168.63.129.16`) provided by DHCP.

Using Services on the Public Internet

For improved security, the Qumulo on Azure as a Service file system provisioned for you doesn't have access to the public Internet. Thus, you must proxy any connectivity between your file system and a service on the public Internet by using a VNet peer in your Azure subscription.

The following service require specific configuration for public Internet connectivity.

- **Audit:** Requires an Rsyslog server or proxy to a public Rsyslog server in a peered VNet.

- **Shift for S3:** Requires an S3 proxy in a peered VNet. You can configure this proxy on the **Advanced S3 Server Settings** panel when you create a copy job.

Using IP Failover with Floating IP Addresses

In on-premises configurations, and when running on AWS and GCP, Qumulo Core uses floating IPs that allow the file system to be be continuously available regardless of node failure.

Because the compute infrastructure that underlies Qumulo on Azure as a Service is more fluid than on other platforms, the concepts of file system *nodes* and the file system's *static* and *floating* IPs are irrelevant. Treat all IP addresses for Qumulo on Azure as a Service like floating IPs in a traditional Qumulo file system.

Upgrades

In addition to *host* upgrades, Qumulo performs *instant* Qumulo Core software upgrades on Qumulo on Azure as a Service file systems on your behalf. Upgrades take place in the week that follows the release of a new Qumulo Core version (typically, once every two weeks). During these upgrades, your file system experiences a brief downtime (usually, less than 30 seconds). For more information, see Qumulo Core Instant Software Upgrade on Qumulo Care.

Active Directory (AD) Domains

Like other cloud platform implementations, Qumulo on Azure as a Service lets the file system join an Active Directory domain for authentication and authorization.

- If you run a traditional Active Directory domain with domain controllers, follow the instructions in Join your Qumulo Cluster to Active Directory on Qumulo Care.

- If you use Azure AD in your environment, Qumulo Core requires enabling Azure Active Directory Domain Services in your tenancy. For more information, see What is Azure Active Directory Domain Services? in Azure documentation.

> **ⓘ Note**
> Currently, Qumulo core doesn't support Azure AD natively.

Remote Monitoring and Support

Qumulo on Azure as a Service doesn't require special remote monitoring configuration. All Qumulo on Azure as a Service file systems have remote monitoring enabled by default. You can't disable this functionality. Your Qumulo on Azure as a Service file systems display on Qumulo Trends alongside any other Qumulo systems you might have on other platforms. For more information, see Qumulo Trends Overview on Qumulo Care.

> **ⓘ Note**
> Remote Support VPN is always disabled for Qumulo on Azure as a Service. It isn't required for getting support for Qumulo on Azure as a Service.

Capacity and Performance Increases

Qumulo manages the addition of capacity and performance to your file system. For help with expanding your existing file system, contact a Qumulo sales representative .