Azure Native Qumulo Scalable File Service Guide

Table of Contents

Azure Native Qumulo Scalable File Service Guide

How Azure Native Qumulo Scalable File Service (ANQ) Works

This section gives an overview of deploying ANQ; lists the Azure regions and compliance postures that the service supports; and explains the differences between this service, Qumulo on AWS as an AMI, and Qumulo on premises.

This fully managed service deploys and manages resources on your behalf, runs Qumulo Core, and provides the same interfaces and functionality as Qumulo on premises.

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

ANQ lets you configure file protocols, quotas, replication, and other features regardless of underlying infrastructure or storage and without requiring the tracking of resource quotas and costs. It receives the latest updates and features continuously and, when issues occur, replaces compute and storage resources automatically.

For instructions on deploying the service in Azure, see Getting Started with ANQ (page 7).

> **Note**
> For help with expanding the capacity of ANQ, email azure@qumulo.com.

Deploying Azure Native Qumulo Scalable File Service

This section outlines the process of configuring and deploying the service.

1. You specify the following configuration.
    - **Regional Settings:** The availability zone and region; for more information, see Supported Azure Regions (page 3)
    - **Networking Settings:** A virtual network in the same region; for more information, see Configuring Virtual Networking (page 5)
    - **Usable Capacity:** Actual required capacity; on this platform, this value isn't restricted by architecture
2. Qumulo deploys and configures the following resources in an environment that it manages.
    - **Managed Resource Group:** This group contains the networking resources that the service deploys.

- **Delegated Subnet:** The delegated subnet that the service uses to provision endpoints for your virtual network.
- **Qumulo Service Resource:** The Azure resource that represents one instance of the service. You can use this resource to manage the service and view configuration details.
- **Marketplace SaaS Resource:** The SaaS resource from the Qumulo Marketplace offer that you choose. Azure uses this resource for billing purposes.

> **Tip**
> Automated deployments let you create ANQ instances for long-term use cases and for short-term components of automated storage workflows.

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 for SMB. To allow the `admin` user to authenticate over the SMB protocol, change the `admin` user's password. When the password change is complete, the `admin` user can authenticate over the SMB protocol.

  > **Note**
  > An incompatibility in data formats between the SMB protocol and Qumulo's integration with Azure causes this limitation.

- **Namespaces Larger than 1 PB:** To deploy namespaces larger than 1 PB through the Azure Portal, email azure@qumulo.com.

Supported Azure Regions

ANQ supports all public U.S. regions. For more information, see Azure Geographies.

Feature Comparison with Qumulo on Other Platforms

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

> **Note**
> Although Qumulo manages the service fully, direct access to hosts with SSH is unavailable. You can configure the service by using the `qq` CLI from a remote machine or by using any of the IP addresses of the service to log in to the Web UI.

Feature	ANQ	Qumulo on AWS as an AMI	Qumulo on Premises
Automatic Deployment	✓		
Automatic Updates	✓		
Available in Cloud Marketplace	✓	✓	
Customer Support	✓	✓	✓
Automatic Infrastructure Replacement	✓	✓	
Incremental Sizing	✓		
Pay as You Go	✓	✓	
Portal Integration	✓		
Qumulo Core Features	✓	✓	✓
Simple, Fast Deployment Under 15 Minutes	✓		

Qumulo Compliance Posture

For more information about third-party attestations that Qumulo has achieved, including SOC 2 Type II and FIPS 140-2 Level 1, see Qumulo Compliance Posture in the Qumulo Core Administrator Guide.

Configuring Virtual Networking for Azure Native Qumulo Scalable File Service (ANQ)

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

The underlying storage of the service resides in Qumulo's Azure tenant. This storage system connects to your Azure subscription by using *VNet injection*, a process that establishes a direct connection between your resources and the service resources without using VNet peering. You can use VNet injection to apply routing and security policies to your service endpoints.

To create endpoints for accessing ANQ, Qumulo creates network interfaces (NICs) and inserts them into your subnet. To allow VNet injection to operate correctly, you must create and configure a new subnet within your virtual network.

Prerequisites for Configuring Virtual Networking

This section explains the prerequisites for configuring virtual networking for ANQ.

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.

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 service.

To Create a Dedicated Subnet

1. Identify the region in which you want to subscribe to the service.
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-Balanced Endpoints

Every endpoint created for the service appears as a NIC, with an IP address that you can use to access the service. To hold these endpoints, Qumulo creates a manage resource group under your Azure subscription. To view links to your managed resource group and NICs, see the **Portal** view of your `Qumulo.Storage/fileSystems` resource.

Qumulo provisions multiple endpoints to allow access to the service. To avoid the bandwidth limits of individual endpoints, use round-robin DNS to distribute your workload traffic across the endpoints available to you.

Configuring Virtual Networking

This section explains how to configure virtual networking for ANQ.

> ⚠ 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 NICs or to entire subnets. Because it is possible to create or remove NICs from the, we recommend assigning security groups to a delegated subnet.

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

Configuring Route Tables

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

Common configuration scenarios for a route table 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 platform uses a *split-networking configuration* in which different NICs handle back-end and front-end traffic. Changes that impact one traffic type have no impact on the other traffic type. In this way, split networking lets you configure firewalls and security groups without having to consider back-end connectivity requirements.

Getting Started with Azure Native Qumulo Scalable File Service (ANQ)

This section explains how to deploy ANQ, view information about your service, and connect to the Web UI.

To Deploy Azure Native Qumulo Scalable File Service

This section explains how to deploy the service in Azure.

1. Log in to the Azure Portal and search for `Azure Native Qumulo Scalable File Service`.
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.
    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 3).
    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 an estimated pay-as-you-go price, see the Pricing and Performance Calculator.
- For up-front pricing plans and free trials, email azure@qumulo.com.

7. On the **Networking** tab, in the **Configure virtual network** section:
   a. Select the **Virtual network** for hosting your service. For more information, see Configuring Virtual Networking for ANQ (page 5).
   b. Select an existing delegated subnet to associate with your service.

   > **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 Web UI

When Azure finishes creating your service, you can view information about the service and use the Web UI.

Viewing the IP Addresses of Your Service

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

To Log in to the Web UI

To log in to the 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 (page 7).

For more information about working with Qumulo Core and the Web UI, see the Qumulo Administrator Guide.

Connecting Azure Native Qumulo Scalable File Service (ANQ) to Azure Active Directory Domain Services

This section explains how to connect ANQ to Azure Active Directory Domain Services (AD DS).

Azure AD 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 Azure AD DS.

- For information about joining ANQ to standard AD, see Join Your Qumulo Cluster to Active Directory on Qumulo Care.
- For information about joining Azure AD DS, see the following resources in the Azure AD Domain Services documentation.
    - Tutorial: Configure virtual networking for an Azure Active Directory Domain Services managed domain
    - Tutorial: Join a Windows Server virtual machine to an Azure Active Directory Domain Services managed domain

To Configure Azure Active Directory Domain Services (AD DS)

1. Create an instance of Azure AD 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 is a routable or non-routable domain suffix.
    - **VNet:** A VNet and a resource group for your Azure 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 have specified.
2. Configure DNS for your managed domain.
    a. Log in to the Azure portal and search for `azure active directory 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 Azure AD Domain Services documentation.

3. (Optional) If the Azure AD 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 Azure AD 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 Azure AD 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 Azure AD DS instance and connect ANQ to it, you can configure SAML SSO for ANQ. For more information, see Configuring SAML Single Sign-On (SSO) for Your Qumulo Cluster in the Qumulo Administrator Guide.