Networking requirements for Cloud Volumes ONTAP in Azure

You must set up your Azure networking so Cloud Volumes ONTAP systems can operate properly.

Looking for the list of endpoints to which Cloud Manager requires access? They're now maintained in a single location. Click here for details.

Outbound internet access for Cloud Volumes ONTAP

Cloud Volumes ONTAP requires outbound internet access to send messages to NetApp AutoSupport, which proactively monitors the health of your storage.

Routing and firewall policies must allow Azure HTTP/HTTPS traffic to mysupport.netapp.com so Cloud Volumes ONTAP can send AutoSupport messages.

Security groups

You do not need to create security groups because Cloud Manager does that for you. If you need to use your own, refer to Security group rules.

Connection from Cloud Volumes ONTAP to Azure Blob storage for data tiering

If you want to tier cold data to Azure Blob storage, you do not need to set up a VNet service endpoint as long as Cloud Manager has the required permission:

"Microsoft.Network/virtualNetworks/subnets/write",

That permission is included in the latest Cloud Manager policy. For details about providing permissions, see Granting Azure permissions.

For details about setting up data tiering, see Tiering cold data to low-cost object storage.

If your network configuration uses route tables, then Cloud Manager also requires the following permission: Microsoft.Network/routeTables/join/action

Connections to ONTAP systems in other networks

To replicate data between a Cloud Volumes ONTAP system in Azure and ONTAP systems in other networks, you must have a VPN connection between the Azure VNet and the other network—for example, an AWS VPC or your corporate network.

For instructions, refer to Microsoft Azure Documentation: Create a Site-to-Site connection in the Azure portal.