Get started in Google Cloud

Cloud Volumes ONTAP

NetApp
November 17, 2022
Table of Contents

Get started in Google Cloud ................................................................. 1
  Quick start for Cloud Volumes ONTAP in Google Cloud .................. 1
  Plan your Cloud Volumes ONTAP configuration in Google Cloud ....... 2
  Networking requirements for Cloud Volumes ONTAP in GCP ............ 5
  Planning for VPC Service Controls in GCP ....................................... 16
  Create a service account for data tiering and backups .................... 18
  Using customer-managed encryption keys with Cloud Volumes ONTAP ... 21
  Set up licensing for Cloud Volumes ONTAP in Google Cloud ............ 22
  Launching Cloud Volumes ONTAP in GCP ....................................... 27
Get started with Cloud Volumes ONTAP for GCP in a few steps.

1. **Create a Connector**
   If you don’t have a Connector yet, an Account Admin needs to create one. [Learn how to create a Connector in GCP](#).

   When you create your first Cloud Volumes ONTAP working environment, BlueXP (formerly Cloud Manager) prompts you to deploy a Connector if you don’t have one yet.

2. **Plan your configuration**
   BlueXP offers preconfigured packages that match your workload requirements, or you can create your own configuration. If you choose your own configuration, you should understand the options available to you.

   [Learn more about planning your configuration](#).

3. **Set up your networking**
   a. Ensure that your VPC and subnets will support connectivity between the Connector and Cloud Volumes ONTAP.
   b. If you plan to enable data tiering, [configure the Cloud Volumes ONTAP subnet for Private Google Access](#).
   c. If you’re deploying an HA pair, ensure that you have four VPCs, each with their own subnet.
   d. If you’re using a shared VPC, provide the Compute Network User role to the Connector service account.
   e. Enable outbound internet access from the target VPC so the Connector and Cloud Volumes ONTAP can contact several endpoints.

   This step is important because the Connector can’t manage Cloud Volumes ONTAP without outbound internet access. If you need to limit outbound connectivity, refer to the list of endpoints for the Connector and Cloud Volumes ONTAP.

   [Learn more about networking requirements](#).

4. **Set up a service account**
   Cloud Volumes ONTAP requires a Google Cloud service account for two purposes. The first is when you enable data tiering to tier cold data to low-cost object storage in Google Cloud. The second is when you enable the Cloud Backup Service to back up volumes to low-cost object storage.

   You can set up one service account and use it for both purposes. The service account must have the Storage Admin role.

   [Read step-by-step instructions](#).
Enable Google Cloud APIs

Enable the following Google Cloud APIs in your project. These APIs are required to deploy the Connector and Cloud Volumes ONTAP.

- Cloud Deployment Manager V2 API
- Cloud Logging API
- Cloud Resource Manager API
- Compute Engine API
- Identity and Access Management (IAM) API

Launch Cloud Volumes ONTAP using BlueXP

Click Add Working Environment, select the type of system that you would like to deploy, and complete the steps in the wizard. Read step-by-step instructions.

Related links
- Creating a Connector from BlueXP
- Installing the Connector software on a Linux host
- What BlueXP does with GCP permissions

Plan your Cloud Volumes ONTAP configuration in Google Cloud

When you deploy Cloud Volumes ONTAP in Google Cloud, you can choose a preconfigured system that matches your workload requirements, or you can create your own configuration. If you choose your own configuration, you should understand the options available to you.

Choose a Cloud Volumes ONTAP license

Several licensing options are available for Cloud Volumes ONTAP. Each option enables you to choose a consumption model that meets your needs.

- Learn about licensing options for Cloud Volumes ONTAP
- Learn how to set up licensing

Choose a supported region

Cloud Volumes ONTAP is supported in most Google Cloud regions. View the full list of supported regions.

Choose a supported machine type

Cloud Volumes ONTAP supports several machine types, depending on the license type that you choose.

Supported configurations for Cloud Volumes ONTAP in GCP
Understand storage limits

The raw capacity limit for a Cloud Volumes ONTAP system is tied to the license. Additional limits impact the size of aggregates and volumes. You should be aware of these limits as you plan your configuration.

Storage limits for Cloud Volumes ONTAP in GCP

Size your system in GCP

Sizing your Cloud Volumes ONTAP system can help you meet requirements for performance and capacity. You should be aware of a few key points when choosing a machine type, disk type, and disk size:

Machine type

Look at the supported machine types in the Cloud Volumes ONTAP Release Notes and then review details from Google about each supported machine type. Match your workload requirements to the number of vCPUs and memory for the machine type. Note that each CPU core increases networking performance.

Refer to the following for more details:

- Google Cloud documentation: N1 standard machine types
- Google Cloud documentation: Performance

GCP disk type

When you create volumes for Cloud Volumes ONTAP, you need to choose the underlying cloud storage that Cloud Volumes ONTAP uses for a disk. The disk type can be any of the following:

- **Zonal SSD persistent disks**: SSD persistent disks are best for workloads that require high rates of random IOPS.
- **Zonal Balanced persistent disks**: These SSDs balance performance and cost by providing lower IOPS per GB.
- **Zonal Standard persistent disks**: Standard persistent disks are economical and can handle sequential read/write operations.

For more details, see Google Cloud documentation: Zonal Persistent disks (Standard and SSD).

GCP disk size

You need to choose an initial disk size when you deploy a Cloud Volumes ONTAP system. After that you can let BlueXP manage a system’s capacity for you, but if you want to build aggregates yourself, be aware of the following:

- All disks in an aggregate must be the same size.
- Determine the space that you need, while taking performance into consideration.
- The performance of persistent disks scales automatically with disk size and the number of vCPUs available to the system.

Refer to the following for more details:

- Google Cloud documentation: Zonal Persistent disks (Standard and SSD)
- Google Cloud documentation: Optimizing Persistent Disk and Local SSD Performance
View default system disks

In addition to the storage for user data, BlueXP also purchases cloud storage for Cloud Volumes ONTAP system data (boot data, root data, core data, and NVRAM). For planning purposes, it might help for you to review these details before you deploy Cloud Volumes ONTAP.

- View the default disks for Cloud Volumes ONTAP system data in Google Cloud.
- Google Cloud docs: Resource quotas

Google Cloud Compute Engine enforces quotas on resource usage so you should ensure that you haven’t reached your limit before you deploy Cloud Volumes ONTAP.

The Connector also requires a system disk. View details about the Connector’s default configuration.

Collect networking information

When you deploy Cloud Volumes ONTAP in GCP, you need to specify details about your virtual network. You can use a worksheet to collect the information from your administrator.

Network information for a single-node system

<table>
<thead>
<tr>
<th>GCP information</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region</td>
<td></td>
</tr>
<tr>
<td>Zone</td>
<td></td>
</tr>
<tr>
<td>VPC network</td>
<td></td>
</tr>
<tr>
<td>Subnet</td>
<td></td>
</tr>
<tr>
<td>Firewall policy (if using your own)</td>
<td></td>
</tr>
</tbody>
</table>

Network information for an HA pair in multiple zones

<table>
<thead>
<tr>
<th>GCP information</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region</td>
<td></td>
</tr>
<tr>
<td>Zone for Node 1</td>
<td></td>
</tr>
<tr>
<td>Zone for Node 2</td>
<td></td>
</tr>
<tr>
<td>Zone for the mediator</td>
<td></td>
</tr>
<tr>
<td>VPC-0 and subnet</td>
<td></td>
</tr>
<tr>
<td>VPC-1 and subnet</td>
<td></td>
</tr>
<tr>
<td>VPC-2 and subnet</td>
<td></td>
</tr>
<tr>
<td>VPC-3 and subnet</td>
<td></td>
</tr>
<tr>
<td>Firewall policy (if using your own)</td>
<td></td>
</tr>
</tbody>
</table>
Network information for an HA pair in a single zone

<table>
<thead>
<tr>
<th>GCP information</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region</td>
<td></td>
</tr>
<tr>
<td>Zone</td>
<td></td>
</tr>
<tr>
<td>VPC-0 and subnet</td>
<td></td>
</tr>
<tr>
<td>VPC-1 and subnet</td>
<td></td>
</tr>
<tr>
<td>VPC-2 and subnet</td>
<td></td>
</tr>
<tr>
<td>VPC-3 and subnet</td>
<td></td>
</tr>
<tr>
<td>Firewall policy (if using your own)</td>
<td></td>
</tr>
</tbody>
</table>

Choose a write speed

BlueXP enables you to choose a write speed setting for Cloud Volumes ONTAP, except for high availability (HA) pairs in Google Cloud. Before you choose a write speed, you should understand the differences between the normal and high settings and risks and recommendations when using high write speed. [Learn more about write speed.]

Choose a volume usage profile

ONTAP includes several storage efficiency features that can reduce the total amount of storage that you need. When you create a volume in BlueXP, you can choose a profile that enables these features or a profile that disables them. You should learn more about these features to help you decide which profile to use.

NetApp storage efficiency features provide the following benefits:

**Thin provisioning**
- Presents more logical storage to hosts or users than you actually have in your physical storage pool.
- Instead of preallocating storage space, storage space is allocated dynamically to each volume as data is written.

**Deduplication**
- Improves efficiency by locating identical blocks of data and replacing them with references to a single shared block. This technique reduces storage capacity requirements by eliminating redundant blocks of data that reside in the same volume.

**Compression**
- Reduces the physical capacity required to store data by compressing data within a volume on primary, secondary, and archive storage.

Networking requirements for Cloud Volumes ONTAP in GCP

Set up your Google Cloud Platform networking so Cloud Volumes ONTAP systems can operate properly. This includes networking for the Connector and Cloud Volumes ONTAP.

If you want to deploy an HA pair, you should [learn how HA pairs work in GCP.](#)
Requirements for Cloud Volumes ONTAP

The following requirements must be met in GCP.

Internal load balancers

BlueXP automatically creates four Google Cloud internal load balancers (TCP/UDP) that manage incoming traffic to the Cloud Volumes ONTAP HA pair. No setup is required from your end. We’ve listed this as a requirement simply to inform you of the network traffic and to mitigate any security concerns.

One load balancer is for cluster management, one is for storage VM (SVM) management, one is for NAS traffic to node 1, and the last is for NAS traffic to node 2.

The setup for each load balancer is as follows:

- One shared private IP address
- One global health check
  
  By default, the ports used by the health check are 63001, 63002, and 63003.
- One regional TCP backend service
- One regional UDP backend service
- One TCP forwarding rule
- One UDP forwarding rule
- Global access is disabled

Even though global access is disabled by default, enabling it post deployment is supported. We disabled it because cross region traffic will have significantly higher latencies. We wanted to ensure that you didn’t have a negative experience due to accidental cross region mounts. Enabling this option is specific to your business needs.

One or multiple zones for HA pairs

You can ensure the high availability of your data by deploying an HA configuration across multiple or in a single zone. BlueXP will prompt you to choose multiple zones or a single zone when you create the HA pair.

- Multiple zones (recommended)

  Deploying an HA configuration across three zones ensures continuous data availability if a failure occurs within a zone. Note that write performance is slightly lower compared to using a single zone, but it’s minimal.

- Single zone

  When deployed in a single zone, a Cloud Volumes ONTAP HA configuration uses a spread placement policy. This policy ensures that an HA configuration is protected from a single point of failure within the zone, without having to use separate zones to achieve fault isolation.

  This deployment model does lower your costs because there are no data egress charges between zones.

Four Virtual Private Clouds for HA pairs

Four Virtual Private Clouds (VPCs) are required for an HA configuration. Four VPCs are required because
GCP requires that each network interface resides in a separate VPC network.

BlueXP will prompt you to choose four VPCs when you create the HA pair:

- VPC-0 for inbound connections to the data and nodes
- VPC-1, VPC-2, and VPC-3 for internal communication between the nodes and the HA mediator

**Subnets for HA pairs**

A private subnet is required for each VPC.

If you place the Connector in VPC-0, then you will need to enable Private Google Access on the subnet to access the APIs and to enable data tiering.

The subnets in these VPCs must have distinct CIDR ranges. They can’t have overlapping CIDR ranges.

**One Virtual Private Cloud for single node systems**

One VPC is required for a single node system.

**Shared VPCs**

Cloud Volumes ONTAP and the Connector are supported in a Google Cloud shared VPC and also in standalone VPCs.
For a single node system, the VPC can be either a shared VPC or a standalone VPC.

For an HA pair, four VPCs are required. Each of those VPCs can be either shared or standalone. For example, VPC-0 could be a shared VPC, while VPC-1, VPC-2, and VPC-3 could be standalone VPCs.

A shared VPC enables you to configure and centrally manage virtual networks across multiple projects. You can set up shared VPC networks in the host project and deploy the Connector and Cloud Volumes ONTAP virtual machine instances in a service project. Google Cloud documentation: Shared VPC overview.

Review the required shared VPC permissions covered in Connector deployment

Packet mirroring in VPCs

Packet mirroring must be disabled in the Google Cloud VPC in which you deploy Cloud Volumes ONTAP. Cloud Volumes ONTAP can’t operate properly if packet mirroring is enabled.

Outbound internet access for Cloud Volumes ONTAP

Cloud Volumes ONTAP requires outbound internet access for NetApp AutoSupport, which proactively monitors the health of your system and sends messages to NetApp technical support.

Routing and firewall policies must allow HTTP/HTTPS traffic to the following endpoints so Cloud Volumes ONTAP can send AutoSupport messages:

- https://support.netapp.com/aods/asupmessage
- https://support.netapp.com/asupprod/post/1.0/postAsup

If an outbound internet connection isn’t available to send AutoSupport messages, BlueXP automatically configures your Cloud Volumes ONTAP systems to use the Connector as a proxy server. The only requirement is to ensure that the Connector’s firewall allows inbound connections over port 3128. You’ll need to open this port after you deploy the Connector.

If you defined strict outbound rules for Cloud Volumes ONTAP, then you’ll also need to ensure that the Cloud Volumes ONTAP firewall allows outbound connections over port 3128.

After you’ve verified that outbound internet access is available, you can test AutoSupport to ensure that it can send messages. For instructions, refer to ONTAP docs: Set up AutoSupport.

If you’re using an HA pair, the HA mediator doesn’t require outbound internet access.

If BlueXP notifies you that AutoSupport messages can’t be sent, troubleshoot your AutoSupport configuration.

Private IP addresses

BlueXP allocates the following number of private IP addresses to Cloud Volumes ONTAP in GCP:

- **Single node**: 3 or 4 private IP addresses

You can skip creation of the storage VM (SVM) management LIF if you deploy Cloud Volumes ONTAP using the API and specify the following flag:

```plaintext
skipSvmManagementLif: true
```

A LIF is an IP address associated with a physical port. A storage VM (SVM) management LIF is required for management tools like SnapCenter.
• **HA pair**: 14 or 15 private IP addresses
  ◦ 7 or 8 private IP addresses for VPC-0

You can skip creation of the storage VM (SVM) management LIF if you deploy Cloud Volumes ONTAP using the API and specify the following flag:

```
skipSvmManagementLif: true
```

◦ Two private IP addresses for VPC-1
◦ Two private IP addresses for VPC-2
◦ Three private IP addresses for VPC-3

**Firewall rules**

You don’t need to create firewall rules because BlueXP does that for you. If you need to use your own, refer to the firewall rules listed below.

Note that two sets of firewall rules are required for an HA configuration:

• One set of rules for HA components in VPC-0. These rules enable data access to Cloud Volumes ONTAP. [Learn more](#).

• Another set of rules for HA components in VPC-1, VPC-2, and VPC-3. These rules are open for inbound & outbound communication between the HA components. [Learn more](#).

**Connection from Cloud Volumes ONTAP to Google Cloud Storage for data tiering**

If you want to tier cold data to a Google Cloud Storage bucket, the subnet in which Cloud Volumes ONTAP resides must be configured for Private Google Access (if you’re using an HA pair, this is the subnet in VPC-0). For instructions, refer to [Google Cloud documentation: Configuring Private Google Access](#).

For additional steps required to set up data tiering in BlueXP, see [Tiering cold data to low-cost object storage](#).

**Connections to ONTAP systems in other networks**

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

For instructions, refer to [Google Cloud documentation: Cloud VPN overview](#).

**Requirements for the Connector**

Set up your networking so that the Connector can manage resources and processes within your public cloud environment. The most important step is ensuring outbound internet access to various endpoints.

If your network uses a proxy server for all communication to the internet, you can specify the proxy server from the Settings page. Refer to [Configuring the Connector to use a proxy server](#).

**Connection to target networks**

A Connector requires a network connection to the VPCs in which you want to deploy Cloud Volumes ONTAP. If you’re deploying an HA pair, then the Connector needs a connection to VPC-0 only.

If you plan to deploy Cloud Volumes ONTAP in a VPC separate from the Connector, then you’ll need to set up
VPC Network Peering. Learn more about VPC Network Peering

Outbound internet access

The Connector requires outbound internet access to manage resources and processes within your public cloud environment.

<table>
<thead>
<tr>
<th>Endpoints</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://support.netapp.com">https://support.netapp.com</a></td>
<td>To obtain licensing information and to send AutoSupport messages to NetApp support.</td>
</tr>
<tr>
<td>https://*.cloudmanager.cloud.netapp.com</td>
<td>To provide SaaS features and services within BlueXP.</td>
</tr>
<tr>
<td><a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a></td>
<td></td>
</tr>
<tr>
<td><a href="https://cloudmanagerinfraprod.azurecr.io">https://cloudmanagerinfraprod.azurecr.io</a></td>
<td>To upgrade the Connector and its Docker components.</td>
</tr>
<tr>
<td>https://*.blob.core.windows.net</td>
<td></td>
</tr>
</tbody>
</table>

Firewall rules for Cloud Volumes ONTAP

BlueXP creates GCP firewall rules that include the inbound and outbound rules that Cloud Volumes ONTAP needs to operate successfully. You might want to refer to the ports for testing purposes or if you prefer your to use own firewall rules.

The firewall rules for Cloud Volumes ONTAP requires both inbound and outbound rules.

If you’re deploying an HA configuration, these are the firewall rules for Cloud Volumes ONTAP in VPC-0.

Inbound rules

When you create a working environment, you can choose the source filter for the predefined firewall policy during deployment:

- **Selected VPC only**: the source filter for inbound traffic is the subnet range of the VPC for the Cloud Volumes ONTAP system and the subnet range of the VPC where the Connector resides. This is the recommended option.
- **All VPCs**: the source filter for inbound traffic is the 0.0.0.0/0 IP range.

If you use your own firewall policy, ensure that you add all networks that need to communicate with Cloud Volumes ONTAP, but also ensure to add both address ranges to allow the internal Google Load Balancer to function correctly. These addresses are 130.211.0.0/22 and 35.191.0.0/16. For more information, refer to Google Cloud documentation: Load Balancer Firewall Rules.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>All ICMP</td>
<td>All</td>
<td>Pinging the instance</td>
</tr>
<tr>
<td>HTTP</td>
<td>80</td>
<td>HTTP access to the System Manager web console using the IP address of the cluster management LIF</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>Connectivity with the Connector and HTTPS access to the System Manager web console using the IP address of the cluster management LIF</td>
</tr>
</tbody>
</table>
### Protocol

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH</td>
<td>22</td>
<td>SSH access to the IP address of the cluster management LIF or a node management LIF</td>
</tr>
<tr>
<td>TCP</td>
<td>111</td>
<td>Remote procedure call for NFS</td>
</tr>
<tr>
<td>TCP</td>
<td>139</td>
<td>NetBIOS service session for CIFS</td>
</tr>
<tr>
<td>TCP</td>
<td>161-162</td>
<td>Simple network management protocol</td>
</tr>
<tr>
<td>TCP</td>
<td>445</td>
<td>Microsoft SMB/CIFS over TCP with NetBIOS framing</td>
</tr>
<tr>
<td>TCP</td>
<td>635</td>
<td>NFS mount</td>
</tr>
<tr>
<td>TCP</td>
<td>749</td>
<td>Kerberos</td>
</tr>
<tr>
<td>TCP</td>
<td>2049</td>
<td>NFS server daemon</td>
</tr>
<tr>
<td>TCP</td>
<td>3260</td>
<td>iSCSI access through the iSCSI data LIF</td>
</tr>
<tr>
<td>TCP</td>
<td>4045</td>
<td>NFS lock daemon</td>
</tr>
<tr>
<td>TCP</td>
<td>4046</td>
<td>Network status monitor for NFS</td>
</tr>
<tr>
<td>TCP</td>
<td>10000</td>
<td>Backup using NDMP</td>
</tr>
<tr>
<td>TCP</td>
<td>11104</td>
<td>Management of intercluster communication sessions for SnapMirror</td>
</tr>
<tr>
<td>TCP</td>
<td>11105</td>
<td>SnapMirror data transfer using intercluster LIFs</td>
</tr>
<tr>
<td>TCP</td>
<td>63001-63050</td>
<td>Load balance probe ports to determine which node is healthy (required for HA pairs only)</td>
</tr>
<tr>
<td>UDP</td>
<td>111</td>
<td>Remote procedure call for NFS</td>
</tr>
<tr>
<td>UDP</td>
<td>161-162</td>
<td>Simple network management protocol</td>
</tr>
<tr>
<td>UDP</td>
<td>635</td>
<td>NFS mount</td>
</tr>
<tr>
<td>UDP</td>
<td>2049</td>
<td>NFS server daemon</td>
</tr>
<tr>
<td>UDP</td>
<td>4045</td>
<td>NFS lock daemon</td>
</tr>
<tr>
<td>UDP</td>
<td>4046</td>
<td>Network status monitor for NFS</td>
</tr>
<tr>
<td>UDP</td>
<td>4049</td>
<td>NFS rquotad protocol</td>
</tr>
</tbody>
</table>

### Outbound rules

The predefined security group for Cloud Volumes ONTAP opens all outbound traffic. If that is acceptable, follow the basic outbound rules. If you need more rigid rules, use the advanced outbound rules.

#### Basic outbound rules

The predefined security group for Cloud Volumes ONTAP includes the following outbound rules.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>All ICMP</td>
<td>All</td>
<td>All outbound traffic</td>
</tr>
<tr>
<td>All TCP</td>
<td>All</td>
<td>All outbound traffic</td>
</tr>
<tr>
<td>All UDP</td>
<td>All</td>
<td>All outbound traffic</td>
</tr>
</tbody>
</table>
Advanced outbound rules

If you need rigid rules for outbound traffic, you can use the following information to open only those ports that are required for outbound communication by Cloud Volumes ONTAP.

- The source is the interface (IP address) on the Cloud Volumes ONTAP system.
<table>
<thead>
<tr>
<th>Service</th>
<th>Protocol</th>
<th>Port</th>
<th>Source</th>
<th>Destination</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
<td>TCP</td>
<td>88</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>Kerberos V authentication</td>
</tr>
<tr>
<td></td>
<td>UDP</td>
<td>137</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>NetBIOS name service</td>
</tr>
<tr>
<td></td>
<td>UDP</td>
<td>138</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>NetBIOS datagram service</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>139</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>NetBIOS service session</td>
</tr>
<tr>
<td></td>
<td>TCP &amp; UDP</td>
<td>389</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>LDAP</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>445</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>Microsoft SMB/CIFS over TCP with NetBIOS framing</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>464</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>Kerberos V change &amp; set password (SET_CHANGE)</td>
</tr>
<tr>
<td></td>
<td>UDP</td>
<td>464</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>Kerberos key administration</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>749</td>
<td>Node management LIF</td>
<td>Active Directory forest</td>
<td>Kerberos V change &amp; set Password (RPCSEC_GSS)</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>88</td>
<td>Data LIF (NFS, CIFS)</td>
<td>Active Directory forest</td>
<td>Kerberos V authentication</td>
</tr>
<tr>
<td></td>
<td>UDP</td>
<td>137</td>
<td>Data LIF (NFS, CIFS)</td>
<td>Active Directory forest</td>
<td>NetBIOS name service</td>
</tr>
<tr>
<td></td>
<td>UDP</td>
<td>138</td>
<td>Data LIF (NFS, CIFS)</td>
<td>Active Directory forest</td>
<td>NetBIOS datagram service</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>139</td>
<td>Data LIF (NFS, CIFS)</td>
<td>Active Directory forest</td>
<td>NetBIOS service session</td>
</tr>
<tr>
<td></td>
<td>TCP &amp; UDP</td>
<td>389</td>
<td>Data LIF (NFS, CIFS)</td>
<td>Active Directory forest</td>
<td>LDAP</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>445</td>
<td>Data LIF (NFS, CIFS)</td>
<td>Active Directory forest</td>
<td>Microsoft SMB/CIFS over TCP with NetBIOS framing</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>464</td>
<td>Data LIF (NFS, CIFS)</td>
<td>Active Directory forest</td>
<td>Kerberos V change &amp; set password (SET_CHANGE)</td>
</tr>
<tr>
<td></td>
<td>UDP</td>
<td>464</td>
<td>Data LIF (NFS, CIFS)</td>
<td>Active Directory forest</td>
<td>Kerberos key administration</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>749</td>
<td>Data LIF (NFS, CIFS)</td>
<td>Active Directory forest</td>
<td>Kerberos V change &amp; set password (RPCSEC_GSS)</td>
</tr>
<tr>
<td>Service</td>
<td>Protocol</td>
<td>Port</td>
<td>Source</td>
<td>Destination</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------------</td>
<td>----------</td>
<td>------</td>
<td>----------------------</td>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>AutoSupport</td>
<td>HTTPS</td>
<td>443</td>
<td>Node management LIF</td>
<td>support.netapp.com</td>
<td>AutoSupport (HTTPS is the default)</td>
</tr>
<tr>
<td></td>
<td>HTTP</td>
<td>80</td>
<td>Node management LIF</td>
<td>support.netapp.com</td>
<td>AutoSupport (only if the transport protocol is changed from HTTPS to HTTP)</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>3128</td>
<td>Node management LIF</td>
<td>Connector</td>
<td>Sending AutoSupport messages through a proxy server on the Connector, if an outbound internet connection isn't available</td>
</tr>
<tr>
<td>Cluster</td>
<td>All traffic</td>
<td>All traffic</td>
<td>All LIFs on one node</td>
<td>All LIFs on the other node</td>
<td>Intercluster communications (Cloud Volumes ONTAP HA only)</td>
</tr>
<tr>
<td>DHCP</td>
<td>UDP</td>
<td>68</td>
<td>Node management LIF</td>
<td>DHCP</td>
<td>DHCP client for first-time setup</td>
</tr>
<tr>
<td>DHCPS</td>
<td>UDP</td>
<td>67</td>
<td>Node management LIF</td>
<td>DHCP</td>
<td>DHCP server</td>
</tr>
<tr>
<td>DNS</td>
<td>UDP</td>
<td>53</td>
<td>Node management LIF</td>
<td>DNS</td>
<td>DNS</td>
</tr>
<tr>
<td>NDMP</td>
<td>TCP</td>
<td>1860</td>
<td>Node management LIF</td>
<td>Destination servers</td>
<td>NDMP copy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0–18</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SMTP</td>
<td>TCP</td>
<td>25</td>
<td>Node management LIF</td>
<td>Mail server</td>
<td>SMTP alerts, can be used for AutoSupport</td>
</tr>
<tr>
<td>SNMP</td>
<td>TCP</td>
<td>161</td>
<td>Node management LIF</td>
<td>Monitor server</td>
<td>Monitoring by SNMP traps</td>
</tr>
<tr>
<td></td>
<td>UDP</td>
<td>161</td>
<td>Node management LIF</td>
<td>Monitor server</td>
<td>Monitoring by SNMP traps</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>162</td>
<td>Node management LIF</td>
<td>Monitor server</td>
<td>Monitoring by SNMP traps</td>
</tr>
<tr>
<td></td>
<td>UDP</td>
<td>162</td>
<td>Node management LIF</td>
<td>Monitor server</td>
<td>Monitoring by SNMP traps</td>
</tr>
<tr>
<td>SnapMirror</td>
<td>TCP</td>
<td>1110</td>
<td>Intercluster LIF</td>
<td>ONTAP intercluster LIFs</td>
<td>Management of intercluster communication sessions for SnapMirror</td>
</tr>
<tr>
<td></td>
<td>TCP</td>
<td>1110</td>
<td>Intercluster LIF</td>
<td>ONTAP intercluster LIFs</td>
<td>SnapMirror data transfer</td>
</tr>
<tr>
<td>Syslog</td>
<td>UDP</td>
<td>514</td>
<td>Node management LIF</td>
<td>Syslog server</td>
<td>Syslog forward messages</td>
</tr>
</tbody>
</table>

**Firewall rules for VPC-1, VPC-2, and VPC-3**

In GCP, an HA configuration is deployed across four VPCs. The firewall rules needed for the HA configuration in VPC-0 are listed above for Cloud Volumes ONTAP.
Meanwhile, the predefined firewall rules that BlueXP creates for instances in VPC-1, VPC-2, and VPC-3 enables ingress communication over all protocols and ports. These rules enable communication between HA nodes.

Communication from the HA nodes to the HA mediator takes place over port 3260 (iSCSI).

**Firewall rules for the Connector**

The firewall rules for the Connector requires both inbound and outbound rules.

**Inbound rules**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH</td>
<td>22</td>
<td>Provides SSH access to the Connector host</td>
</tr>
<tr>
<td>HTTP</td>
<td>80</td>
<td>Provides HTTP access from client web browsers to the local user interface</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>Provides HTTPS access from client web browsers to the local user interface</td>
</tr>
<tr>
<td>TCP</td>
<td>3128</td>
<td>Provides Cloud Volumes ONTAP with internet access to send AutoSupport messages to NetApp Support. You must manually open this port after deploying the Connector.</td>
</tr>
</tbody>
</table>

**Outbound rules**

The predefined firewall rules for the Connector opens all outbound traffic. If that is acceptable, follow the basic outbound rules. If you need more rigid rules, use the advanced outbound rules.

**Basic outbound rules**

The predefined firewall rules for the Connector includes the following outbound rules.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>All TCP</td>
<td>All</td>
<td>All outbound traffic</td>
</tr>
<tr>
<td>All UDP</td>
<td>All</td>
<td>All outbound traffic</td>
</tr>
</tbody>
</table>

**Advanced outbound rules**

If you need rigid rules for outbound traffic, you can use the following information to open only those ports that are required for outbound communication by the Connector.

<table>
<thead>
<tr>
<th>Service</th>
<th>Protocol</th>
<th>Port</th>
<th>Destination</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>API calls and AutoSupport</td>
<td>HTTP PS</td>
<td>44  3</td>
<td>Outbound internet and ONTAP cluster management LIF</td>
<td>API calls to GCP and ONTAP, to Cloud Data Sense, to the Ransomware service, and sending AutoSupport messages to NetApp</td>
</tr>
<tr>
<td>DNS</td>
<td>UDP</td>
<td>53</td>
<td>DNS</td>
<td>Used for DNS resolve by BlueXP</td>
</tr>
</tbody>
</table>

The source IP address is the Connector host.
Planning for VPC Service Controls in GCP

When choosing to lock down your Google Cloud environment with VPC Service Controls, you should understand how BlueXP and Cloud Volumes ONTAP interact with the Google Cloud APIs, as well as how to configure your service perimeter to deploy BlueXP and Cloud Volumes ONTAP.

VPC Service Controls enable you to control access to Google-managed services outside of a trusted perimeter, to block data access from untrusted locations, and to mitigate unauthorized data transfer risks. Learn more about Google Cloud VPC Service Controls.

How NetApp services communicate with VPC Service Controls

BlueXP communicates directly with the Google Cloud APIs. This is either triggered from an external IP address outside of Google Cloud (for example, from api.services.cloud.netapp.com), or within Google Cloud from an internal address assigned to the BlueXP Connector.

Depending on the deployment style of the Connector, certain exceptions may have to be made for your service perimeter.

Images

Both Cloud Volumes ONTAP and BlueXP use images from a project within GCP that is managed by NetApp. This can affect the deployment of the BlueXP Connector and Cloud Volumes ONTAP, if your organization has a policy that blocks the use of images that are not hosted within the organization.

You can deploy a Connector manually using the manual installation method, but Cloud Volumes ONTAP will also need to pull images from the NetApp project. You must provide an allowed list in order to deploy a Connector and Cloud Volumes ONTAP.

Deploying a Connector

The user who deploys a Connector needs to be able to reference an image hosted in the projectId netapp-cloudmanager and the project number 14190056516.

Deploying Cloud Volumes ONTAP

• The BlueXP service account needs to reference an image hosted in the projectId netapp-cloudmanager and the project number 14190056516 from the service project.

• The service account for the default Google APIs Service Agent needs to reference an image hosted in the projectId netapp-cloudmanager and the project number 14190056516 from the service project.

Examples of the rules needed for pulling these images with VPC Service Controls are defined below.

VPC Service Controls perimeter policies

Policies allow exceptions to the VPC Service Controls rule sets. For more information about policies, please visit the GCP VPC Service Controls Policy Documentation.

To set the policies that BlueXP requires, navigate to your VPC Service Controls Perimeter within your organization and add the following policies. The fields should match the options given in the VPC Service Controls policy page. Also note that all rules are required and the OR parameters should be used in the rule
Ingress rules

Rule 1

From:
   Identities:
      [User Email Address]
      Source > All sources allowed
To:
   Projects =
      [Service Project]
   Services =
      Service name: iam.googleapis.com
      Service methods: All actions
      Service name: compute.googleapis.com
      Service methods: All actions

OR

Rule 2

From:
   Identities:
      [User Email Address]
      Source > All sources allowed
To:
   Projects =
      [Host Project]
   Services =
      Service name: compute.googleapis.com
      Service methods: All actions

OR
Create a service account for data tiering and backups

Cloud Volumes ONTAP requires a Google Cloud service account for two purposes. The first is when you enable data tiering to tier cold data to low-cost object storage in Google Cloud. The second is when you enable the Cloud Backup Service to back up volumes to low-cost object storage.

Cloud Volumes ONTAP uses the service account to access and manage one bucket for tiered data and another bucket for backups.

You can set up one service account and use it for both purposes. The service account must have the Storage Admin role.

Steps
1. In the Google Cloud console, go to the Service accounts page.
2. Select your project.
3. Click **Create service account** and provide the required information.
   a. **Service account details**: Enter a name and description.
   b. **Grant this service account access to project**: Select the **Storage Admin** role.
   c. **Grant users access to this service account**: Add the Connector service account as a **Service Account User** to this new service account.

This step is required for data tiering only. It’s not required for the Cloud Backup Service.
What's next?

You'll need to select the service account later when you create a Cloud Volumes ONTAP working environment.
Using customer-managed encryption keys with Cloud Volumes ONTAP

While Google Cloud Storage always encrypts your data before it’s written to disk, you can use the BlueXP API to create a Cloud Volumes ONTAP system that uses customer-managed encryption keys. These are keys that you generate and manage in GCP using the Cloud Key Management Service.

Steps

1. Ensure that the BlueXP Connector service account has the correct permissions at the project level, in the project where the key is stored.

   The permissions are provided in the Connector service account permissions by default, but may not be applied if you use an alternate project for the Cloud Key Management Service.

   The permissions are as follows:

   - cloudkms.cryptoKeyVersions.useToEncrypt
   - cloudkms.cryptoKeys.get
   - cloudkms.cryptoKeys.list
   - cloudkms.keyRings.list

2. Ensure that the service account for the Google Compute Engine Service Agent has Cloud KMS
Encrypter/Decrypter permissions on the key.

The name of the service account uses the following format: "service-[service_project_number]@compute-system.iam.gserviceaccount.com".

**Google Cloud Documentation: Using IAM with Cloud KMS - Granting roles on a resource**

3. Obtain the "id" of the key by invoking the get command for the /gcp/vsa/metadata/gcp-encryption-keys API call or by choosing "Copy Resource Name" on the key in the GCP console.

4. If using customer-managed encryption keys and tiering data to object storage, BlueXP attempts to utilize the same keys that are used to encrypt the persistent disks. But you'll first need to enable Google Cloud Storage buckets to use the keys:
   a. Find the Google Cloud Storage service agent by following the Google Cloud Documentation: Getting the Cloud Storage service agent.
   b. Navigate to the encryption key and assign the Google Cloud Storage service agent with Cloud KMS Encrypter/Decrypter permissions.
   
   For more information, refer to Google Cloud Documentation: Using customer-managed encryption keys

5. Use the "GcpEncryption" parameter with your API request when creating a working environment.

**Example**

```
"gcpEncryptionParameters": {
   "key": "projects/project-1/locations/us-east4/keyRings/keyring-1/cryptoKeys/generatedkey1"
}
```

Refer to the BlueXP automation docs for more details about using the "GcpEncryption" parameter.

**Set up licensing for Cloud Volumes ONTAP in Google Cloud**

After you decide which licensing option you want to use with Cloud Volumes ONTAP, a few steps are required before you can choose that licensing option when creating a new working environment.

**Freemium**

Select the Freemium offering to use Cloud Volumes ONTAP free of charge with up to 500 GiB of provisioned capacity. Learn more about the Freemium offering.

**Steps**

1. From the left navigation menu, select **Storage > Canvas**.

2. On the Canvas page, click **Add Working Environment** and follow the steps in BlueXP.
   a. On the **Details and Credentials** page, click **Edit Credentials > Add Subscription** and then follow the prompts to subscribe to the pay-as-you-go offering in the Google Cloud Marketplace.

   You won't be charged through the marketplace subscription unless you exceed 500 GiB of provisioned...
capacity, at which time the system is automatically converted to the Essentials package.

b. After you return to BlueXP, select Freemium when you reach the charging methods page.

![Select Charging Method]


**Capacity-based license**

Capacity-based licensing enables you to pay for Cloud Volumes ONTAP per TiB of capacity. Capacity-based licensing is available in the form of a package: the Essentials package or the Professional package.

The Essentials and Professional packages are available with the following consumption models:

- A license (BYOL) purchased from NetApp
- An hourly, pay-as-you-go (PAYGO) subscription from the Google Cloud Marketplace
- An annual contract

Learn more about capacity-based licensing.

The following sections describe how to get started with each of these consumption models.

**BYOL**

Pay upfront by purchasing a license (BYOL) from NetApp to deploy Cloud Volumes ONTAP systems in any cloud provider.

**Steps**

1. Contact NetApp Sales to obtain a license
2. Add your NetApp Support Site account to BlueXP

BlueXP automatically queries NetApp’s licensing service to obtain details about the licenses associated with your NetApp Support Site account. If there are no errors, BlueXP automatically adds the licenses to the Digital Wallet.

Your license must be available from the Digital Wallet before you can use it with Cloud Volumes ONTAP. If needed, you can manually add the license to the Digital Wallet.
3. On the Canvas page, click **Add Working Environment** and follow the steps in BlueXP.
   a. On the **Details and Credentials** page, click **Edit Credentials > Add Subscription** and then follow the prompts to subscribe to the pay-as-you-go offering in the Google Cloud Marketplace.

   The license that you purchased from NetApp is always charged first, but you’ll be charged from the hourly rate in the marketplace if you exceed your licensed capacity or if the term of your license expires.

   b. After you return to BlueXP, select a capacity-based package when you reach the charging methods page.

![Select Charging Method]

**View step-by-step instructions to launch Cloud Volumes ONTAP in Google Cloud.**

**PAYGO subscription**

Pay hourly by subscribing to the offer from your cloud provider’s marketplace.

When you create a Cloud Volumes ONTAP working environment, BlueXP prompts you to subscribe to the agreement that’s available in the Google Cloud Marketplace. That subscription is then associated with the working environment for charging. You can use that same subscription for additional working environments.

**Steps**

1. From the left navigation menu, select **Storage > Canvas**.

2. On the Canvas page, click **Add Working Environment** and follow the steps in BlueXP.
   
   a. On the **Details and Credentials** page, click **Edit Credentials > Add Subscription** and then follow the prompts to subscribe to the pay-as-you-go offering in the Google Cloud Marketplace.

   b. After you return to BlueXP, select a capacity-based package when you reach the charging methods page.

You can manage the Google Cloud Marketplace subscriptions associated with your accounts from the Settings > Credentials page. Learn how to manage your Google Cloud credentials and subscriptions

Annual contract

Pay for Cloud Volumes ONTAP annually by purchasing an annual contract.

Steps

1. Contact your NetApp sales representative to purchase an annual contract.

   The contract is available as a private offer in the Google Cloud Marketplace.

   After NetApp shares the private offer with you, you can select the annual plan when you subscribe from the Google Cloud Marketplace during working environment creation.

2. On the Canvas page, click Add Working Environment and follow the steps in BlueXP.
   
   a. On the Details and Credentials page, click Edit Credentials > Add Subscription and then follow the prompts to subscribe to the annual plan in the Google Cloud Marketplace.
   
   b. In Google Cloud, select the annual plan that was shared with your account and then click Subscribe.
   
   c. After you return to BlueXP, select a capacity-based package when you reach the charging methods page.

**Keystone Flex Subscription**

A Keystone Flex Subscription is a pay-as-you-grow subscription-based service. Learn more about Keystone Flex Subscriptions.

**Steps**

1. If you don’t have a subscription yet, contact NetApp
2. Contact NetApp to authorize your BlueXP user account with one or more Keystone Flex Subscriptions.
3. After NetApp authorizes your account, link your subscriptions for use with Cloud Volumes ONTAP.
4. On the Canvas page, click Add Working Environment and follow the steps in BlueXP.
   a. Select the Keystone Flex Subscription charging method when prompted to choose a charging method.

**Launching Cloud Volumes ONTAP in GCP**

You can launch Cloud Volumes ONTAP in a single-node configuration or as an HA pair in Google Cloud Platform.

**Before you get started**

You need the following to create a working environment.

- A Connector that’s up and running.
  - You should have a Connector that is associated with your workspace.
  - You should be prepared to leave the Connector running at all times.
  - The service account associated with the Connector should have the required permissions
- An understanding of the configuration that you want to use.

You should have prepared by choosing a configuration and by obtaining GCP networking information from your administrator. For details, see Planning your Cloud Volumes ONTAP configuration.

- An understanding of what’s required to set up licensing for Cloud Volumes ONTAP.
  
  Learn how to set up licensing.
Google Cloud APIs should be **enabled in your project**:
- Cloud Deployment Manager V2 API
- Cloud Logging API
- Cloud Resource Manager API
- Compute Engine API
- Identity and Access Management (IAM) API

**Launching a single-node system in GCP**

Create a working environment in BlueXP to launch Cloud Volumes ONTAP in GCP.

**Steps**

1. From the left navigation menu, select **Storage > Canvas**.
2. On the Canvas page, click **Add Working Environment** and follow the prompts.
3. **Choose a Location**: Select **Google Cloud** and **Cloud Volumes ONTAP**.
4. If you’re prompted, **create a Connector**.
5. **Details & Credentials**: Select a project, specify a cluster name, optionally select a service account, optionally add labels, and then specify credentials.

The following table describes fields for which you might need guidance:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Working Environment Name</td>
<td>BlueXP uses the working environment name to name both the Cloud Volumes ONTAP system and the GCP VM instance. It also uses the name as the prefix for the predefined security group, if you select that option.</td>
</tr>
<tr>
<td>Service Account Name</td>
<td>If you plan to use data tiering or Cloud Backup with Cloud Volumes ONTAP, then you need to enable <strong>Service Account</strong> and select a service account that has the predefined Storage Admin role. Learn how to create a service account.</td>
</tr>
<tr>
<td>Add Labels</td>
<td>Labels are metadata for your GCP resources. BlueXP adds the labels to the Cloud Volumes ONTAP system and GCP resources associated with the system.</td>
</tr>
<tr>
<td></td>
<td>You can add up to four labels from the user interface when creating a working environment, and then you can add more after its created. Note that the API does not limit you to four labels when creating a working environment. For information about labels, refer to Google Cloud Documentation: Labeling Resources.</td>
</tr>
<tr>
<td>User name and password</td>
<td>These are the credentials for the Cloud Volumes ONTAP cluster administrator account. You can use these credentials to connect to Cloud Volumes ONTAP through System Manager or its CLI. Keep the default admin user name or change it to a custom user name.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Edit Project</td>
<td>Select the project where you want Cloud Volumes ONTAP to reside. The default project is the project where BlueXP resides. If you don’t see any additional projects in the drop-down list, then you haven’t yet associated the BlueXP service account with other projects. Go to the Google Cloud console, open the IAM service, and select the project. Add the service account with the BlueXP role to that project. You’ll need to repeat this step for each project.</td>
</tr>
</tbody>
</table>

This is the service account that you set up for BlueXP, as described on this page.

Click **Add Subscription** to associate the selected credentials with a subscription.

To create a pay-as-you-go Cloud Volumes ONTAP system, you need to select a GCP project that’s associated with a subscription to Cloud Volumes ONTAP from the GCP Marketplace.

The following video shows how to associate a pay-as-you-go Marketplace subscription to your GCP project. Alternatively, follow the steps to subscribe located in the Associating a Marketplace subscription with GCP credentials section.

6. **Services**: Select the services that you want to use on this system. In order to select Cloud Backup, or to use Tiering, you must have specified the Service Account in step 3.

7. **Location & Connectivity**: Select a location, choose a firewall policy, and confirm network connectivity to Google Cloud storage for data tiering.

The following table describes fields for which you might need guidance:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connectivity verification</td>
<td>To tier cold data to a Google Cloud Storage bucket, the subnet in which Cloud Volumes ONTAP resides must be configured for Private Google Access. For instructions, refer to Google Cloud Documentation: Configuring Private Google Access.</td>
</tr>
<tr>
<td>Generated firewall policy</td>
<td>If you let BlueXP generate the firewall policy for you, you need to choose how you'll allow traffic:</td>
</tr>
<tr>
<td></td>
<td>• If you choose <strong>Selected VPC only</strong>, the source filter for inbound traffic is the subnet range of the selected VPC and the subnet range of the VPC where the Connector resides. This is the recommended option.</td>
</tr>
<tr>
<td></td>
<td>• If you choose <strong>All VPCs</strong>, the source filter for inbound traffic is the 0.0.0.0/0 IP range.</td>
</tr>
<tr>
<td>Use existing firewall policy</td>
<td>If you use an existing firewall policy, ensure that it includes the required rules. Learn about firewall rules for Cloud Volumes ONTAP.</td>
</tr>
</tbody>
</table>

8. **Charging Methods and NSS Account**: Specify which charging option would you like to use with this system, and then specify a NetApp Support Site account.

- Learn about licensing options for Cloud Volumes ONTAP.
- Learn how to set up licensing.

9. **Preconfigured Packages**: Select one of the packages to quickly deploy a Cloud Volumes ONTAP system, or click *Create my own configuration*.

   If you choose one of the packages, you only need to specify a volume and then review and approve the configuration.

10. **Licensing**: Change the Cloud Volumes ONTAP version as needed and select a machine type.

    If a newer Release Candidate, General Availability, or patch release is available for the selected version, then BlueXP updates the system to that version when creating the working environment. For example, the update occurs if you select Cloud Volumes ONTAP 9.10.1 and 9.10.1 P4 is available. The update does not occur from one release to another—for example, from 9.6 to 9.7.

11. **Underlying Storage Resources**: Choose settings for the initial aggregate: a disk type and the size for each disk.

    The disk type is for the initial volume. You can choose a different disk type for subsequent volumes.

    The disk size is for all disks in the initial aggregate and for any additional aggregates that BlueXP creates.
when you use the simple provisioning option. You can create aggregates that use a different disk size by using the advanced allocation option.

For help choosing a disk type and size, see Sizing your system in GCP.

12. **Write Speed & WORM**: Choose **Normal** or **High** write speed, and activate write once, read many (WORM) storage, if desired.

Choosing a write speed is supported with single node systems only.

Learn more about write speed.

WORM can’t be enabled if data tiering was enabled.

Learn more about WORM storage.

13. **Data Tiering in Google Cloud Platform**: Choose whether to enable data tiering on the initial aggregate, choose a storage class for the tiered data, and then either select a service account that has the predefined Storage Admin role (required for Cloud Volumes ONTAP 9.7 or later), or select a GCP account (required for Cloud Volumes ONTAP 9.6).

Note the following:

- BlueXP sets the service account on the Cloud Volumes ONTAP instance. This service account provides permissions for data tiering to a Google Cloud Storage bucket. Be sure to add the Connector service account as a user of the tiering service account, otherwise, you can’t select it from BlueXP.
- For help with adding a GCP account, see Setting up and adding GCP accounts for data tiering with 9.6.
- You can choose a specific volume tiering policy when you create or edit a volume.
- If you disable data tiering, you can enable it on subsequent aggregates, but you’ll need to turn off the system and add a service account from the GCP console.

Learn more about data tiering.

14. **Create Volume**: Enter details for the new volume or click **Skip**.

Learn about supported client protocols and versions.

Some of the fields in this page are self-explanatory. The following table describes fields for which you might need guidance:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size</td>
<td>The maximum size that you can enter largely depends on whether you enable thin provisioning, which enables you to create a volume that is bigger than the physical storage currently available to it.</td>
</tr>
<tr>
<td>Access control (for NFS only)</td>
<td>An export policy defines the clients in the subnet that can access the volume. By default, BlueXP enters a value that provides access to all instances in the subnet.</td>
</tr>
<tr>
<td>Permissions and Users / Groups (for CIFS only)</td>
<td>These fields enable you to control the level of access to a share for users and groups (also called access control lists or ACLs). You can specify local or domain Windows users or groups, or UNIX users or groups. If you specify a domain Windows user name, you must include the user’s domain using the format domain\username.</td>
</tr>
</tbody>
</table>
A Snapshot copy policy specifies the frequency and number of automatically created NetApp Snapshot copies. A NetApp Snapshot copy is a point-in-time file system image that has no performance impact and requires minimal storage. You can choose the default policy or none. You might choose none for transient data: for example, tempdb for Microsoft SQL Server.

Select an NFS version for the volume: either NFSv3 or NFSv4.

Initiator groups and IQNs (for iSCSI only) are tables of iSCSI host node names and control which initiators have access to which LUNs.

iSCSI targets connect to the network through standard Ethernet network adapters (NICs), TCP offload engine (TOE) cards with software initiators, converged network adapters (CNAs) or dedicated host bus adapters (HBAs) and are identified by iSCSI qualified names (IQNs).

When you create an iSCSI volume, BlueXP automatically creates a LUN for you. We’ve made it simple by creating just one LUN per volume, so there’s no management involved. After you create the volume, use the IQN to connect to the LUN from your hosts.

The following image shows the Volume page filled out for the CIFS protocol:

15. **CIFS Setup**: If you chose the CIFS protocol, set up a CIFS server.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Primary and Secondary IP Address</td>
<td>The IP addresses of the DNS servers that provide name resolution for the CIFS server. The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the CIFS server will join.</td>
</tr>
<tr>
<td></td>
<td>If you’re configuring Google Managed Active Directory, AD can be accessed by default with the 169.254.169.254 IP address.</td>
</tr>
<tr>
<td>Active Directory Domain to join</td>
<td>The FQDN of the Active Directory (AD) domain that you want the CIFS server to join.</td>
</tr>
<tr>
<td>Credentials authorized to join the domain</td>
<td>The name and password of a Windows account with sufficient privileges to add computers to the specified Organizational Unit (OU) within the AD domain.</td>
</tr>
<tr>
<td>CIFS server NetBIOS name</td>
<td>A CIFS server name that is unique in the AD domain.</td>
</tr>
<tr>
<td>Organizational Unit</td>
<td>The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers.</td>
</tr>
<tr>
<td></td>
<td>To configure Google Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, enter <strong>OU=Computers,OU=Cloud</strong> in this field.</td>
</tr>
<tr>
<td></td>
<td><em>Google Cloud Documentation: Organizational Units in Google Managed Microsoft AD</em></td>
</tr>
<tr>
<td>DNS Domain</td>
<td>The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.</td>
</tr>
<tr>
<td>NTP Server</td>
<td>Select <strong>Use Active Directory Domain</strong> to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the <em>BlueXP automation docs</em> for details.</td>
</tr>
<tr>
<td></td>
<td>Note that you can configure an NTP server only when creating a CIFS server. It’s not configurable after you create the CIFS server.</td>
</tr>
</tbody>
</table>

16. **Usage Profile, Disk Type, and Tiering Policy**: Choose whether you want to enable storage efficiency features and change the volume tiering policy, if needed.

   For more information, see **Understanding volume usage profiles** and **Data tiering overview**.

17. **Review & Approve**: Review and confirm your selections.

   a. Review details about the configuration.
   
   b. Click **More information** to review details about support and the GCP resources that BlueXP will purchase.
   
   c. Select the **I understand...** check boxes.
   
   d. Click **Go**.

**Result**

BlueXP deploys the Cloud Volumes ONTAP system. You can track the progress in the timeline.
If you experience any issues deploying the Cloud Volumes ONTAP system, review the failure message. You can also select the working environment and click Re-create environment.

For additional help, go to NetApp Cloud Volumes ONTAP Support.

**After you finish**

- If you provisioned a CIFS share, give users or groups permissions to the files and folders and verify that those users can access the share and create a file.
- If you want to apply quotas to volumes, use System Manager or the CLI.

Quotas enable you to restrict or track the disk space and number of files used by a user, group, or qtree.

**Launching an HA pair in GCP**

Create a working environment in BlueXP to launch Cloud Volumes ONTAP in GCP.

**Steps**

1. From the left navigation menu, select Storage > Canvas.
2. On the Canvas page, click Add Working Environment and follow the prompts.
3. **Choose a Location**: Select Google Cloud and Cloud Volumes ONTAP HA.
4. **Details & Credentials**: Select a project, specify a cluster name, optionally select a Service Account, optionally add labels, and then specify credentials.

The following table describes fields for which you might need guidance:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Working Environment Name</td>
<td>BlueXP uses the working environment name to name both the Cloud Volumes ONTAP system and the GCP VM instance. It also uses the name as the prefix for the predefined security group, if you select that option.</td>
</tr>
<tr>
<td>Service Account Name</td>
<td>If you plan to use the Tiering or Cloud Backup services, you need to enable the Service Account switch and then select the Service Account that has the predefined Storage Admin role.</td>
</tr>
<tr>
<td>Add Labels</td>
<td>Labels are metadata for your GCP resources. BlueXP adds the labels to the Cloud Volumes ONTAP system and GCP resources associated with the system.</td>
</tr>
<tr>
<td></td>
<td>You can add up to four labels from the user interface when creating a working environment, and then you can add more after its created. Note that the API does not limit you to four labels when creating a working environment.</td>
</tr>
<tr>
<td></td>
<td>For information about labels, refer to Google Cloud Documentation: Labeling Resources.</td>
</tr>
<tr>
<td>User name and password</td>
<td>These are the credentials for the Cloud Volumes ONTAP cluster administrator account. You can use these credentials to connect to Cloud Volumes ONTAP through System Manager or its CLI. Keep the default admin user name or change it to a custom user name.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Edit Project</td>
<td>Select the project where you want Cloud Volumes ONTAP to reside. The default project is the project where BlueXP resides. If you don’t see any additional projects in the drop-down list, then you haven’t yet associated the BlueXP service account with other projects. Go to the Google Cloud console, open the IAM service, and select the project. Add the service account with the BlueXP role to that project. You’ll need to repeat this step for each project. This is the service account that you set up for BlueXP, as described on this page. Click Add Subscription to associate the selected credentials with a subscription. To create a pay-as-you-go Cloud Volumes ONTAP system, you need to select a GCP project that’s associated with a subscription to Cloud Volumes ONTAP from the GCP Marketplace.</td>
</tr>
</tbody>
</table>

The following video shows how to associate a pay-as-you-go Marketplace subscription to your GCP project. Alternatively, follow the steps to subscribe located in the Associating a Marketplace subscription with GCP credentials section.

5. **Services**: Select the services that you want to use on this system. In order to select Cloud Backup, or to use Tiering, you must have specified the Service Account in step 3.

6. **HA Deployment Models**: Choose multiple zones (recommended) or a single zone for the HA configuration. Then select a region and zones.

   Learn more about HA deployment models.

7. **Connectivity**: Select four different VPCs for the HA configuration, a subnet in each VPC, and then choose a firewall policy.

   Learn more about networking requirements.

The following table describes fields for which you might need guidance:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generated policy</td>
<td>If you let BlueXP generate the firewall policy for you, you need to choose how you’ll allow traffic:</td>
</tr>
<tr>
<td></td>
<td>• If you choose <strong>Selected VPC only</strong>, the source filter for inbound traffic is the subnet range of the selected VPC and the subnet range of the VPC where the Connector resides. This is the recommended option.</td>
</tr>
<tr>
<td></td>
<td>• If you choose <strong>All VPCs</strong>, the source filter for inbound traffic is the 0.0.0.0/0 IP range.</td>
</tr>
<tr>
<td>Use existing</td>
<td>If you use an existing firewall policy, ensure that it includes the required rules. Learn about firewall rules for Cloud Volumes ONTAP.</td>
</tr>
</tbody>
</table>

8. **Charging Methods and NSS Account**: Specify which charging option would you like to use with this system, and then specify a NetApp Support Site account.

   - Learn about licensing options for Cloud Volumes ONTAP.
   - Learn how to set up licensing.

9. **Preconfigured Packages**: Select one of the packages to quickly deploy a Cloud Volumes ONTAP system, or click **Create my own configuration**.

    If you choose one of the packages, you only need to specify a volume and then review and approve the configuration.

10. **Licensing**: Change the Cloud Volumes ONTAP version as needed and select a machine type.

    If a newer Release Candidate, General Availability, or patch release is available for the selected version, then BlueXP updates the system to that version when creating the working environment. For example, the update occurs if you select Cloud Volumes ONTAP 9.10.1 and 9.10.1 P4 is available. The update does not occur from one release to another—for example, from 9.6 to 9.7.

11. **Underlying Storage Resources**: Choose settings for the initial aggregate: a disk type and the size for each disk.

    The disk type is for the initial volume. You can choose a different disk type for subsequent volumes.
The disk size is for all disks in the initial aggregate and for any additional aggregates that BlueXP creates when you use the simple provisioning option. You can create aggregates that use a different disk size by using the advanced allocation option.

For help choosing a disk type and size, see Sizing your system in GCP.

12. **WORM**: Activate write once, read many (WORM) storage, if desired.

WORM can’t be enabled if data tiering was enabled. Learn more about WORM storage.

13. **Data Tiering in Google Cloud Platform**: Choose whether to enable data tiering on the initial aggregate, choose a storage class for the tiered data, and then select a service account that has the predefined Storage Admin role.

Note the following:

- BlueXP sets the service account on the Cloud Volumes ONTAP instance. This service account provides permissions for data tiering to a Google Cloud Storage bucket. Be sure to add the Connector service account as a user of the tiering service account, otherwise, you can’t select it from BlueXP.
- You can choose a specific volume tiering policy when you create or edit a volume.
- If you disable data tiering, you can enable it on subsequent aggregates, but you’ll need to turn off the system and add a service account from the GCP console.

Learn more about data tiering.

14. **Create Volume**: Enter details for the new volume or click **Skip**.

Learn about supported client protocols and versions.

Some of the fields in this page are self-explanatory. The following table describes fields for which you might need guidance:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size</td>
<td>The maximum size that you can enter largely depends on whether you enable thin provisioning, which enables you to create a volume that is bigger than the physical storage currently available to it.</td>
</tr>
<tr>
<td>Access control (for NFS only)</td>
<td>An export policy defines the clients in the subnet that can access the volume. By default, BlueXP enters a value that provides access to all instances in the subnet.</td>
</tr>
<tr>
<td>Permissions and Users / Groups (for CIFS only)</td>
<td>These fields enable you to control the level of access to a share for users and groups (also called access control lists or ACLs). You can specify local or domain Windows users or groups, or UNIX users or groups. If you specify a domain Windows user name, you must include the user’s domain using the format domain\username.</td>
</tr>
<tr>
<td>Snapshot Policy</td>
<td>A Snapshot copy policy specifies the frequency and number of automatically created NetApp Snapshot copies. A NetApp Snapshot copy is a point-in-time file system image that has no performance impact and requires minimal storage. You can choose the default policy or none. You might choose none for transient data: for example, tempdb for Microsoft SQL Server.</td>
</tr>
<tr>
<td>Advanced options (for NFS only)</td>
<td>Select an NFS version for the volume: either NFSv3 or NFSv4.</td>
</tr>
</tbody>
</table>
iSCSI storage targets are called LUNs (logical units) and are presented to hosts as standard block devices.

Initiator groups are tables of iSCSI host node names and control which initiators have access to which LUNs.

iSCSI targets connect to the network through standard Ethernet network adapters (NICs), TCP offload engine (TOE) cards with software initiators, converged network adapters (CNAs) or dedicated host bust adapters (HBAs) and are identified by iSCSI qualified names (IQNs).

When you create an iSCSI volume, BlueXP automatically creates a LUN for you. We’ve made it simple by creating just one LUN per volume, so there’s no management involved. After you create the volume, use the IQN to connect to the LUN from your hosts.

The following image shows the Volume page filled out for the CIFS protocol:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Primary and Secondary IP Address</td>
<td>The IP addresses of the DNS servers that provide name resolution for the CIFS server.</td>
</tr>
<tr>
<td></td>
<td>The listed DNS servers must contain the service location records (SRV) needed to locate the</td>
</tr>
<tr>
<td></td>
<td>Active Directory LDAP servers and domain controllers for the domain that the CIFS server will</td>
</tr>
<tr>
<td></td>
<td>join.</td>
</tr>
<tr>
<td></td>
<td>If you’re configuring Google Managed Active Directory, AD can be accessed by default with the</td>
</tr>
<tr>
<td></td>
<td>169.254.169.254 IP address.</td>
</tr>
<tr>
<td>Active Directory Domain to join</td>
<td>The FQDN of the Active Directory (AD) domain that you want the CIFS server to join.</td>
</tr>
<tr>
<td>Credentials authorized to join the domain</td>
<td>The name and password of a Windows account with sufficient privileges to add computers to the</td>
</tr>
<tr>
<td></td>
<td>specified Organizational Unit (OU) within the AD domain.</td>
</tr>
</tbody>
</table>

15. **CIFS Setup**: If you chose the CIFS protocol, set up a CIFS server.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIFS server NetBIOS name</td>
<td>A CIFS server name that is unique in the AD domain.</td>
</tr>
<tr>
<td>Organizational Unit</td>
<td>The organizational unit within the AD domain to associate with the CIFS server. The default is CN=Computers. To configure Google Managed Microsoft AD as the AD server for Cloud Volumes ONTAP, enter OU=Computers,OU=Cloud in this field. Google Cloud Documentation: Organizational Units in Google Managed Microsoft AD</td>
</tr>
<tr>
<td>DNS Domain</td>
<td>The DNS domain for the Cloud Volumes ONTAP storage virtual machine (SVM). In most cases, the domain is the same as the AD domain.</td>
</tr>
<tr>
<td>NTP Server</td>
<td>Select <strong>Use Active Directory Domain</strong> to configure an NTP server using the Active Directory DNS. If you need to configure an NTP server using a different address, then you should use the API. See the BlueXP automation docs for details. Note that you can configure an NTP server only when creating a CIFS server. It’s not configurable after you create the CIFS server.</td>
</tr>
</tbody>
</table>

16. **Usage Profile, Disk Type, and Tiering Policy**: Choose whether you want to enable storage efficiency features and change the volume tiering policy, if needed.

For more information, see **Understanding volume usage profiles** and **Data tiering overview**.

17. **Review & Approve**: Review and confirm your selections.
   a. Review details about the configuration.
   b. Click **More information** to review details about support and the GCP resources that BlueXP will purchase.
   c. Select the **I understand...** check boxes.
   d. Click **Go**.

**Result**

BlueXP deploys the Cloud Volumes ONTAP system. You can track the progress in the timeline.

If you experience any issues deploying the Cloud Volumes ONTAP system, review the failure message. You can also select the working environment and click **Re-create environment**.

For additional help, go to **NetApp Cloud Volumes ONTAP Support**.

**After you finish**

- If you provisioned a CIFS share, give users or groups permissions to the files and folders and verify that those users can access the share and create a file.
- If you want to apply quotas to volumes, use System Manager or the CLI.

Quotas enable you to restrict or track the disk space and number of files used by a user, group, or qtree.
Copyright information

Copyright © 2022 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.