Manage high availability groups

StorageGRID

NetApp
October 03, 2025

This PDF was generated from https://docs.netapp.com/us-en/storagegrid-116/admin/managing-high-availability-groups.html on October 03, 2025. Always check docs.netapp.com for the latest.

Table of Contents

Manage high availability groups . . . 1
- Manage high availability (HA) groups: Overview . . . 1
  - What is an HA group? . . . 1
  - How do you create an HA group? . . . 1
  - What is the active interface? . . . 1
  - View the current HA group status of a node . . . 2
  - What happens when the active interface fails? . . . 3
- How are HA groups used? . . . 3
  - Limitations of using HA groups with Grid Manager or Tenant Manager . . . 4
  - Limitations of using HA groups with the CLB service . . . 4
- Configuration options for HA groups . . . 4
- Configure high availability groups . . . 6
  - Create a high availability group . . . 6
  - Edit a high availability group . . . 10
  - Remove a high availability group . . . 12

Manage high availability groups

Manage high availability (HA) groups: Overview

You can group the network interfaces of multiple Admin and Gateway Nodes into a high availability (HA) group. If the active interface in the HA group fails, a backup interface can manage the workload.

What is an HA group?

You can use high availability (HA) groups to provide highly available data connections for S3 and Swift clients or to provide highly available connections to the Grid Manager and the Tenant Manager.

Each HA group provides access to the shared services on the selected nodes.

- HA groups that include Gateway Nodes, Admin Nodes, or both provide highly available data connections for S3 and Swift clients.
- HA groups that include only Admin Nodes provide highly available connections to the Grid Manager and the Tenant Manager.
- An HA group that includes only SG100 or SG1000 appliances and VMware-based software nodes can provide highly available connections for S3 tenants that use S3 Select. HA groups are recommended when using S3 Select, but not required.

How do you create an HA group?

1. You select a network interface for one or more Admin Nodes or Gateway Nodes. You can use a Grid Network (eth0) interface, Client Network (eth2) interface, VLAN interface, or an access interface you have added to the node.

   > ⓘ You cannot add an interface to an HA group if it has a DHCP-assigned IP address.

2. You specify one interface to be the Primary interface. The Primary interface is the active interface unless a failure occurs.
3. You determine the priority order for any Backup interfaces.
4. You assign one to 10 virtual IP (VIP) addresses to the group. Clients applications can use any of these VIP addresses to connect to StorageGRID.

For instructions, see Configure high availability groups.

What is the active interface?

During normal operation, all of the VIP addresses for the HA group are added to the Primary interface, which is the first interface in the priority order. As long as the Primary interface remains available, it is used when clients connect to any VIP address for the group. That is, during normal operation, the Primary interface is the “active” interface for the group.

Similarly, during normal operation, any lower priority interfaces for the HA group act as “backup” interfaces. These backup interfaces are not used unless the Primary (currently active) interface becomes unavailable.

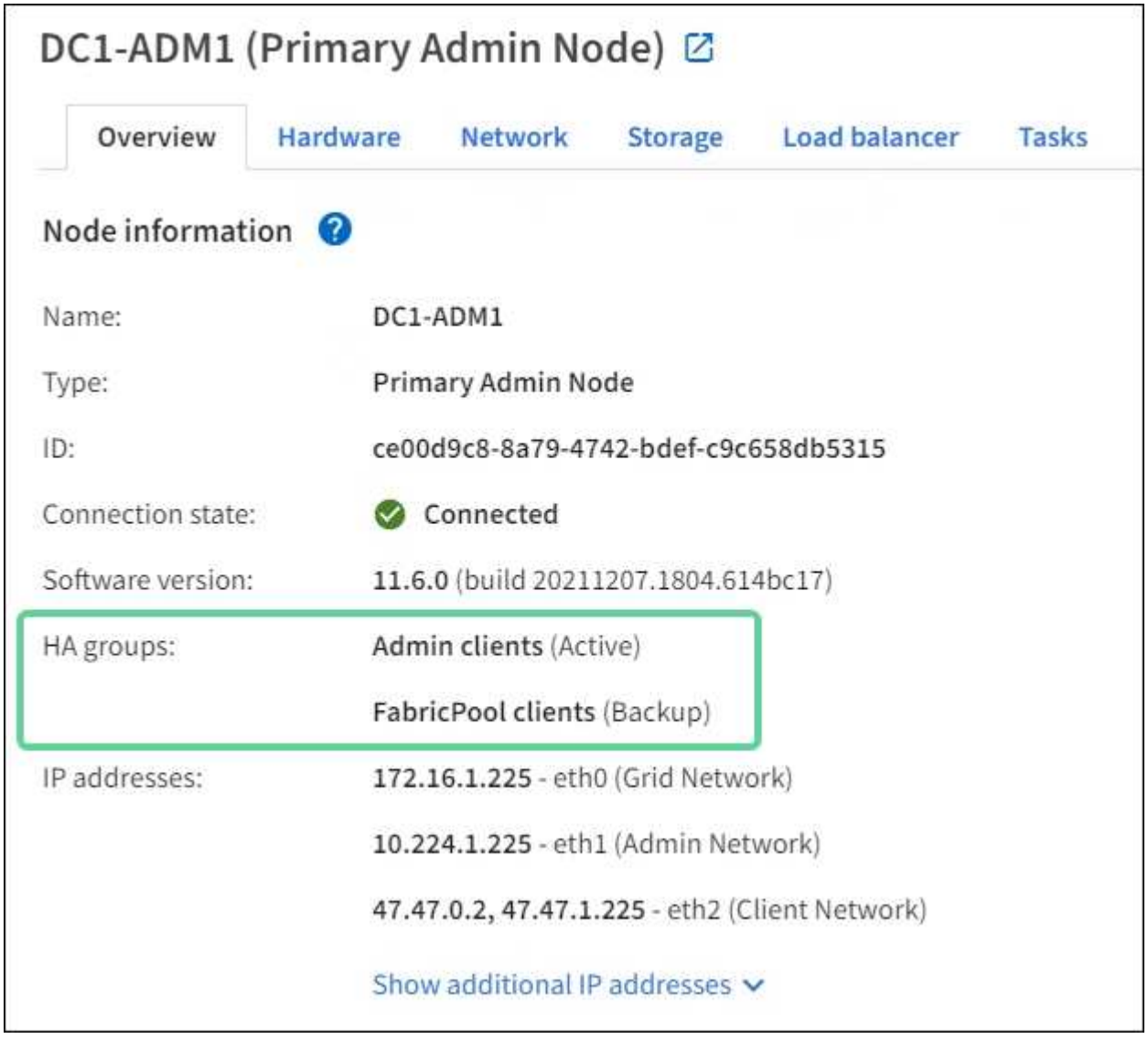
View the current HA group status of a node

To see if a node is assigned to an HA group and determine its current status, select **NODES** > ***node***.

If the **Overview** tab includes an entry for **HA groups**, the node is assigned to the HA groups listed. The value after the group name is the current status of the node in the HA group:

- **Active**: The HA group is currently being hosted on this node.
- **Backup**: The HA group is not currently using this node; this is a backup interface.
- **Stopped**: The HA group cannot be hosted on this node because the High Availability (keepalived) service has been stopped manually.
- **Fault**: The HA group cannot be hosted on this node because of one or more of the following:
  - The Load Balancer (nginx-gw) service is not running on the node.
  - The node's eth0 or VIP interface is down.
  - The node is down.

In this example, the primary Admin Node has been added to two HA groups. This node is currently the active interface for the Admin clients group and a backup interface for the FabricPool clients group.



What happens when the active interface fails?

The interface that currently hosts the VIP addresses is the active interface. If the HA group includes more than one interface and the active interface fails, the VIP addresses move to the first available backup interface in the priority order. If that interface fails, the VIP addresses move to the next available backup interface, and so on.

Failover can be triggered for any of these reasons:

- The node on which the interface is configured goes down.
- The node on which the interface is configured loses connectivity to all other nodes for at least 2 minutes.
- The active interface goes down.
- The Load Balancer service stops.
- The High Availability service stops.

> Failover might not be triggered by network failures external to the node that hosts the active interface. Similarly, failover is not triggered by the failure of the CLB service (deprecated) or services for the Grid Manager or the Tenant Manager.

The failover process generally takes only a few seconds and is fast enough that client applications should experience little impact and can rely on normal retry behaviors to continue operation.

When failure is resolved and a higher priority interface becomes available again, the VIP addresses are automatically moved to the highest priority interface that is available.

How are HA groups used?

You can use high availability (HA) groups to provide highly available connections to StorageGRID for object data and for administrative use.

- An HA group can provide highly available administrative connections to the Grid Manager or the Tenant Manager.
- An HA group can provide highly available data connections for S3 and Swift clients.
- An HA group that contains only one interface allows you to provide many VIP addresses and to explicitly set IPv6 addresses.

An HA group can provide high availability only if all nodes included in the group provide the same services. When you create an HA group, add interfaces from the types of nodes that provide the services you require.

- **Admin Nodes**: Include the Load Balancer service and enable access to the Grid Manager or the Tenant Manager.
- **Gateway Nodes**: Include the Load Balancer service and the CLB service (deprecated).

Purpose of HA group	Add nodes of this type to the HA group
Access to Grid Manager	• Primary Admin Node (**Primary**) • Non-primary Admin Nodes **Note:** The primary Admin Node must be the Primary interface. Some maintenance procedures can only be performed from the primary Admin Node.
Access to Tenant Manager only	• Primary or non-primary Admin Nodes
S3 or Swift client access — Load Balancer service	• Admin Nodes • Gateway Nodes
S3 client access for S3 Select	• SG100 or SG1000 appliances • VMware-based software nodes **Note**: HA groups are recommended when using S3 Select, but not required.
S3 or Swift client access — CLB service **Note:** The CLB service is deprecated.	• Gateway Nodes

Limitations of using HA groups with Grid Manager or Tenant Manager

If a Grid Manager or Tenant Manager service fails, HA group failover is not triggered.

If you are signed in to the Grid Manager or the Tenant Manager when failover occurs, you are signed out and must sign in again to resume your task.

Some maintenance procedures cannot be performed when the primary Admin Node is unavailable. During failover, you can use the Grid Manager to monitor your StorageGRID system.

Limitations of using HA groups with the CLB service

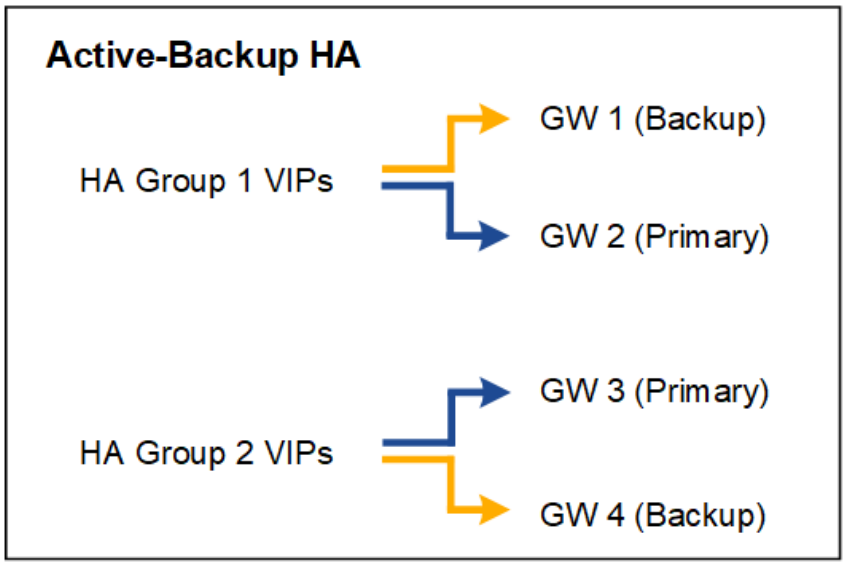
The failure of the CLB service does not trigger failover within the HA group.

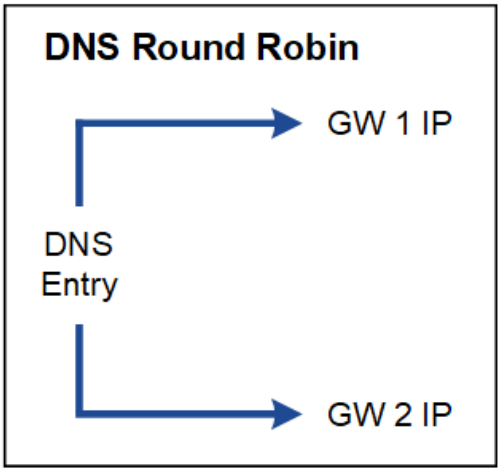
The CLB service is deprecated.

Configuration options for HA groups

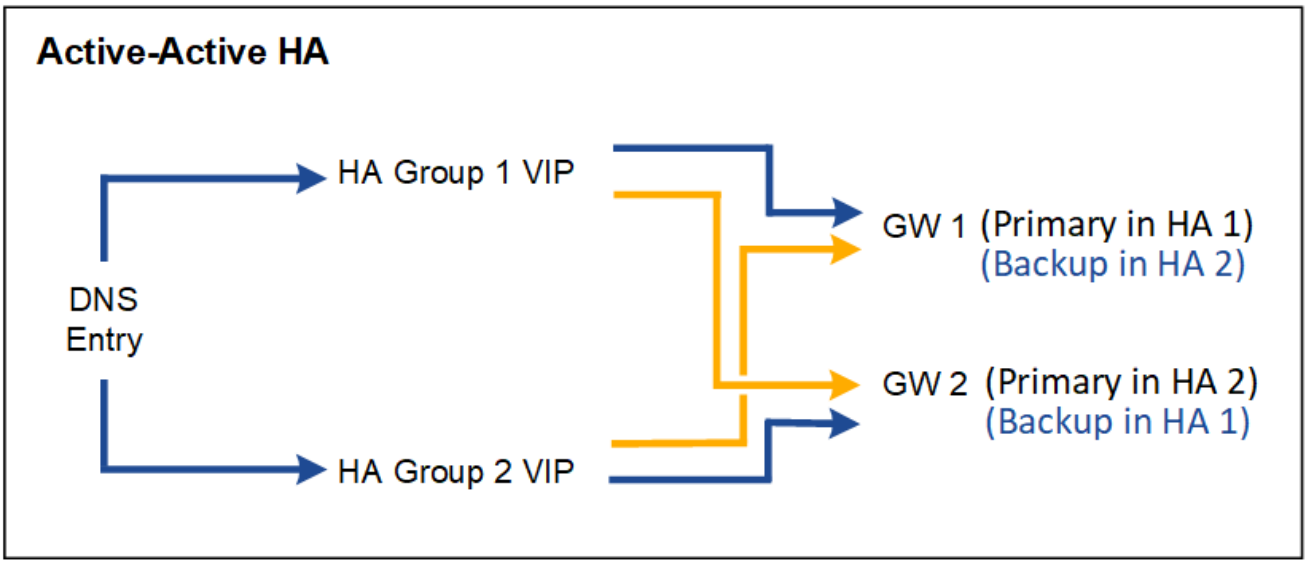
The following diagrams provide examples of different ways you can configure HA groups. Each option has advantages and disadvantages.

In the diagrams, blue indicates the primary interface in the HA group and yellow indicates the backup interface in the HA group.





GW = Gateway Node
VIP = Virtual IP address



The table summarizes the benefits of each HA configuration shown in the diagram.

Configuration	Advantages	Disadvantages
Active-Backup HA	• Managed by StorageGRID with no external dependencies. • Fast failover.	• Only one node in an HA group is active. At least one node per HA group will be idle.
DNS Round Robin	• Increased aggregate throughput. • No idle hosts.	• Slow failover, which could depend on client behavior. • Requires configuration of hardware outside of StorageGRID. • Needs a customer-implemented health check.

Configuration	Advantages	Disadvantages
Active-Active HA	• Traffic is distributed across multiple HA groups. • High aggregate throughput that scales with the number of HA groups. • Fast failover.	• More complex to configure. • Requires configuration of hardware outside of StorageGRID. • Needs a customer-implemented health check.

Configure high availability groups

You can configure high availability (HA) groups to provide highly available access to the services on Admin Nodes or Gateway Nodes.

What you'll need

- You are signed in to the Grid Manager using a supported web browser.
- You have the Root access permission.
- If you plan to use a VLAN interface in an HA group, you have created the VLAN interface. See Configure VLAN interfaces.
- If you plan to use an access interface for a node in an HA group, you have created the interface:
  - **Red Hat Enterprise Linux or CentOS (before installing the node)**: Create node configuration files
  - **Ubuntu or Debian (before installing the node)**: Create node configuration files
  - **Linux (after installing the node)**: Linux: Add trunk or access interfaces to a node
  - **VMware (after installing the node)**: VMware: Add trunk or access interfaces to a node

Create a high availability group

When you create a high availability group, you select one or more interfaces and organize them in priority order. Then, you assign one or more VIP addresses to the group.

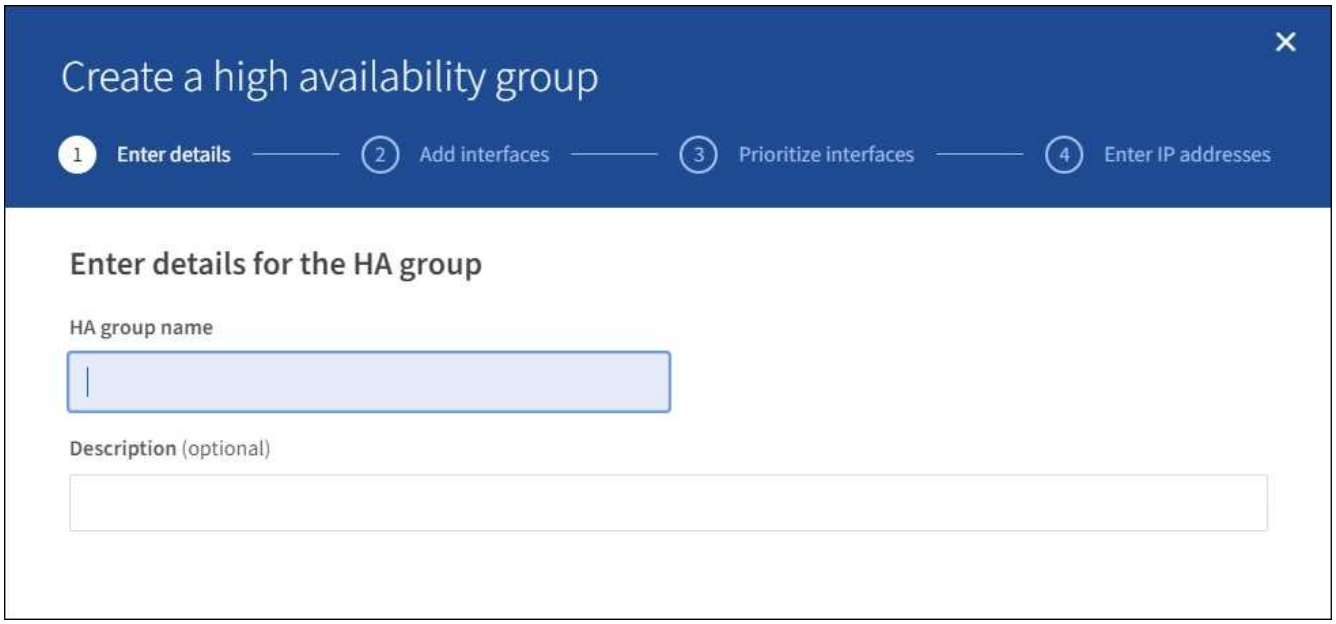
An interface must be for a Gateway Node or an Admin Node to be included in an HA group. An HA group can only use one interface for any given node; however, other interfaces for the same node can be used in other HA groups.

Access the wizard

1. Select **CONFIGURATION** > **Network** > **High availability groups**.
2. Select **Create**.

Enter details for the HA group

1. Provide a unique name for the HA group.

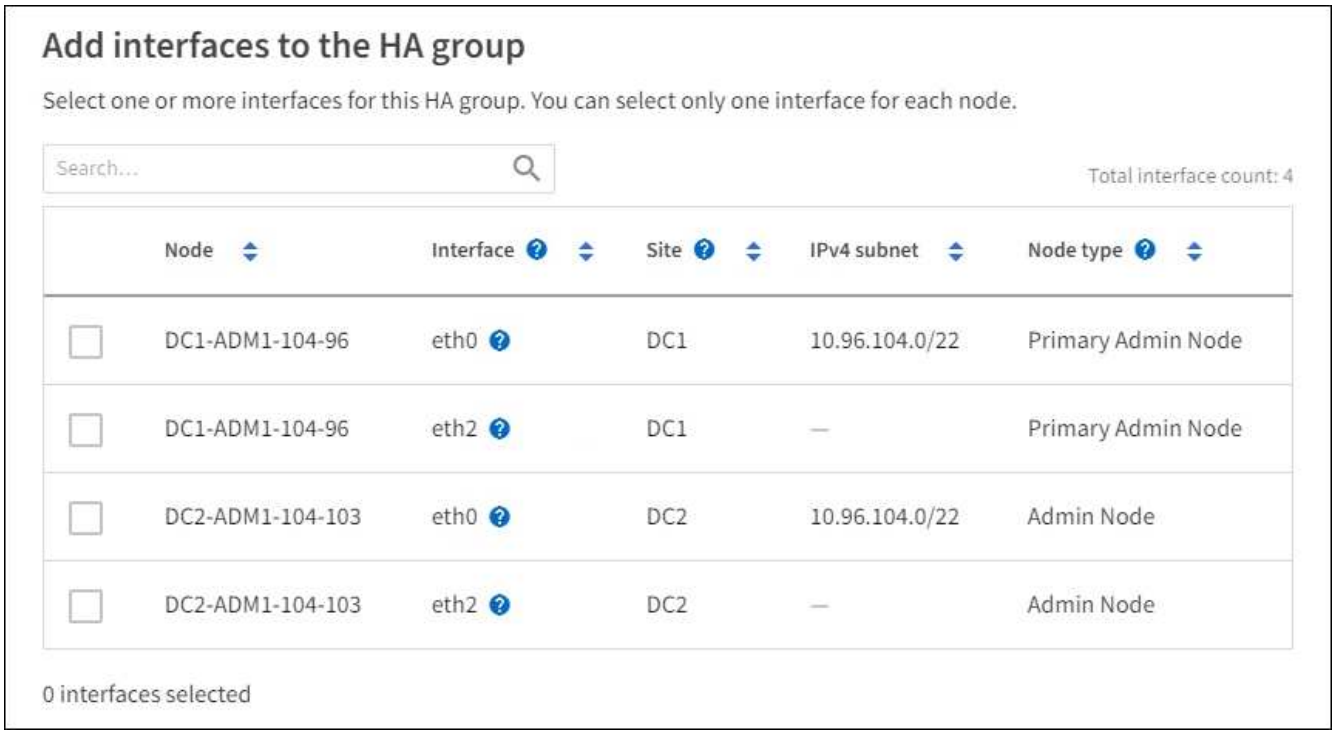


2. Optionally, enter a description for the HA group.
3. Select **Continue**.

Add interfaces to the HA group

1. Select one or more interfaces to add to this HA group.

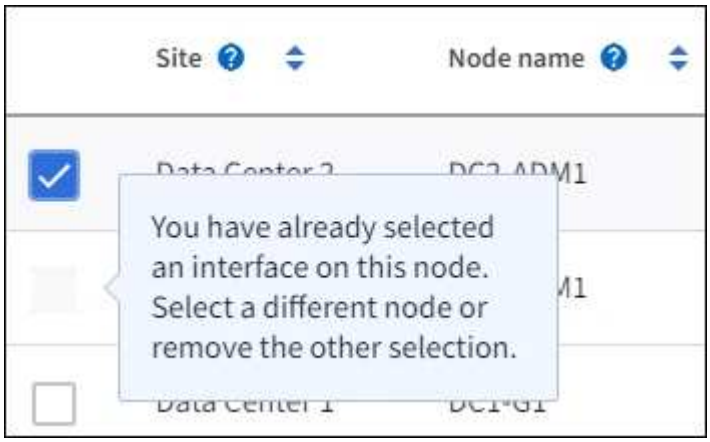
   Use the column headers to sort the rows, or enter a search term to locate interfaces more quickly.



> After creating a VLAN interface, wait up to 5 minutes for the new interface to appear in the table.

Guidelines for selecting interfaces

- You must select at least one interface.
- You can select only one interface for a node.
- If the HA group is for HA protection of Admin Node services, which include the Grid Manager and the Tenant Manager, select interfaces on Admin Nodes only.
- If the HA group is for HA protection of S3 or Swift client traffic, select interfaces on Admin Nodes, Gateway Nodes, or both.
- If the HA group is for HA protection of the deprecated CLB service, select interfaces on Gateway Nodes only.
- If you select interfaces on different types of nodes, an informational note appears. You are reminded that if a failover occurs, services provided by the previously active node might not be available on the newly active node. For example, a backup Gateway Node cannot provide HA protection of Admin Node services. Similarly, a backup Admin Node cannot perform all of the maintenance procedures that the primary Admin Node can provide.
- If you cannot select an interface, its check box is disabled. The tool tip provides more information.



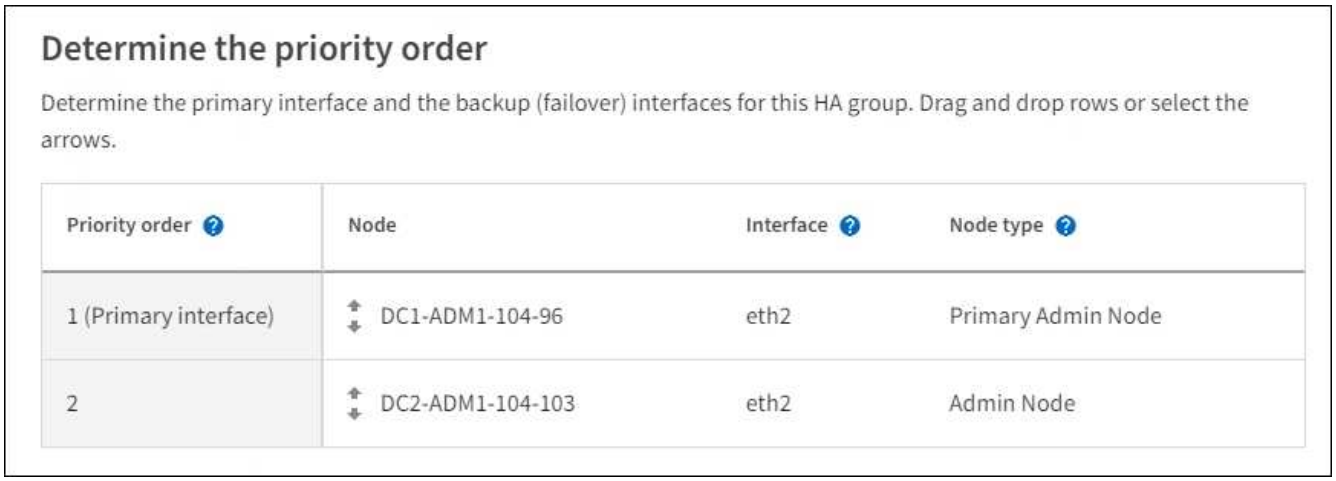
- You cannot select an interface if its subnet value or gateway conflicts with another selected interface.
- You cannot select a configured interface if it does not have a static IP address.

2. Select **Continue**.

Determine the priority order

1. Determine the Primary interface and any Backup (failover) interfaces for this HA group.

   Drag and drop rows to change the values in the **Priority order** column.



If the HA group provides access to the Grid Manager, you must select an interface on the primary Admin Node to be the Primary interface. Some maintenance procedures can only be performed from the primary Admin Node.

The first interface in the list is the Primary interface. The Primary interface is the active interface unless a failure occurs.

If the HA group includes more than one interface and the Primary interface fails, the VIP addresses move to the highest priority interface that is available. If that interface fails, the VIP addresses move to the next highest priority interface that is available, and so on.

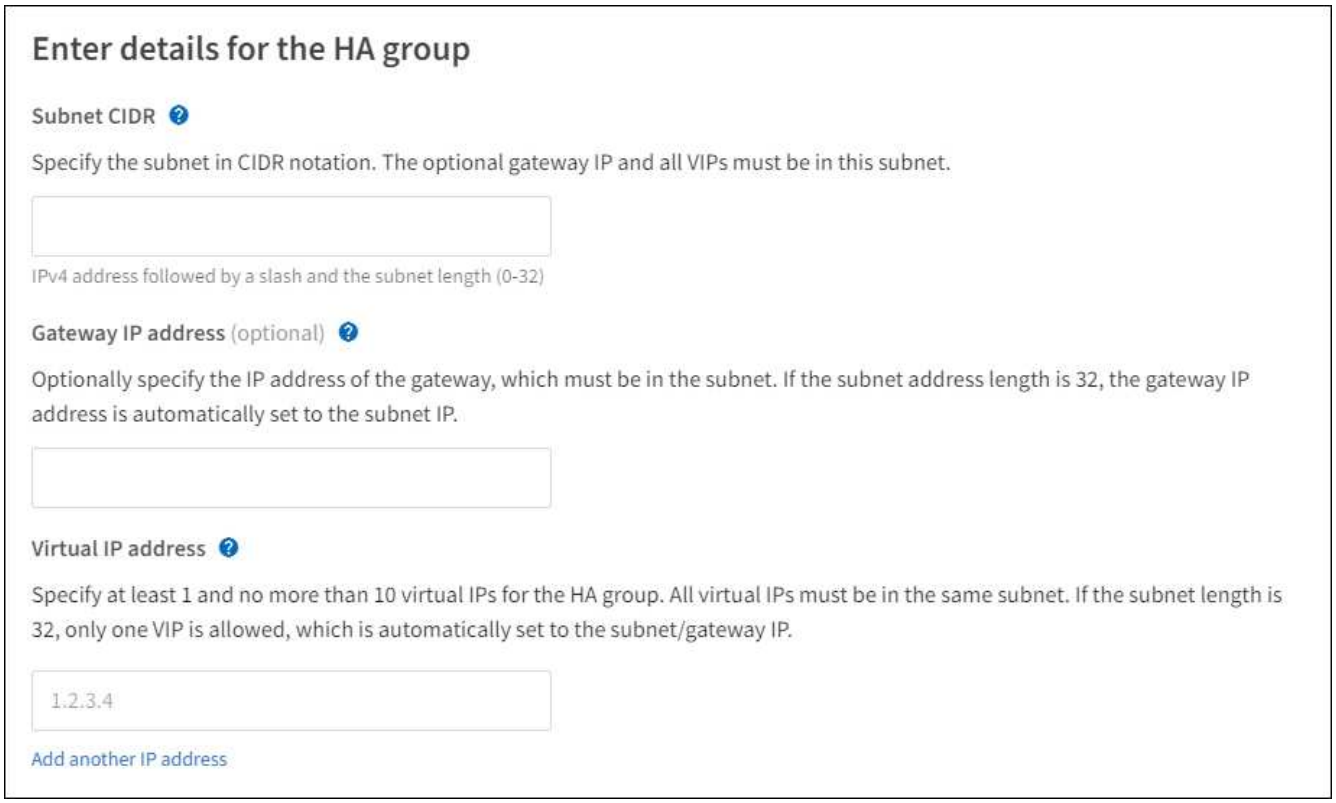
2. Select **Continue**.

Enter IP addresses

1. In the **Subnet CIDR** field, specify the VIP subnet in CIDR notation—an IPv4 address followed by a slash and the subnet length (0-32).

   The network address must not have any host bits set. For example, `192.16.0.0/22`.

   If you use a 32-bit prefix, the VIP network address also serves as the gateway address and the VIP address.



2. Optionally, if any S3, Swift, administrative or tenant clients will access these VIP addresses from a different subnet, enter the **Gateway IP address**. The gateway address must be within the VIP subnet.

   Client and admin users will use this gateway to access the virtual IP addresses.

3. Enter one or more **virtual IP addresses** for the HA group. You can add up to 10 IP addresses. All VIPs must be within the VIP subnet.

   You must provide at least one IPv4 address. Optionally, you can specify additional IPv4 and IPv6 addresses.

4. Select **Create HA group** and select **Finish**.

   The HA Group is created, and you can now use the configured virtual IP addresses.

Wait up to 15 minutes for changes to an HA group to be applied to all nodes.

Next steps

If you will use this HA group for load balancing, create a load balancer endpoint to determine the port and network protocol and to attach any required certificates. See Configure load balancer endpoints.

Edit a high availability group

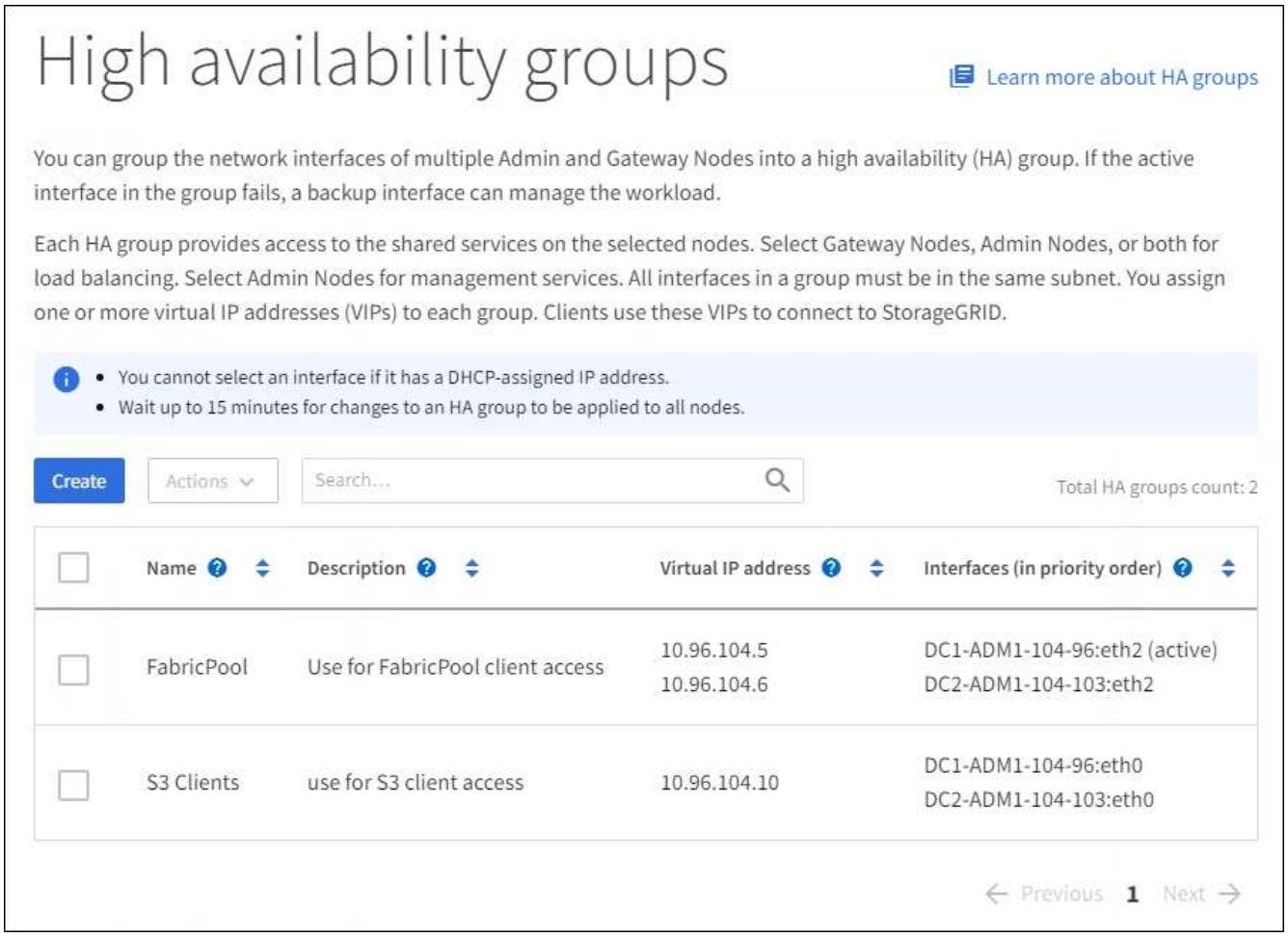
You can edit a high availability (HA) group to change its name and description, add or remove interfaces, change the priority order, or add or update virtual IP addresses.

For example, you might need to edit an HA group if you want to remove the node associated with a selected interface in a site or node decommission procedure.

Steps

1. Select **CONFIGURATION** > **Network** > **High availability groups**.

   The High availability groups page shows all existing HA groups.



2. Select the check box for the HA group you want to edit.
3. Do one of the following, based on what you want to update:
   - Select **Actions** > **Edit virtual IP address** to add or remove VIP addresses.
   - Select **Actions** > **Edit HA group** to update the group's name or description, add or remove interfaces, change the priority order, or add or remove VIP addresses.
4. If you selected **Edit virtual IP address**:
   a. Update the virtual IP addresses for the HA group.
   b. Select **Save**.
   c. Select **Finish**.
5. If you selected **Edit HA group**:
   a. Optionally, update the group's name or description.
   b. Optionally, select or unselect the check boxes to add or remove interfaces.

If the HA group provides access to the Grid Manager, you must select an interface on the primary Admin Node to be the Primary interface. Some maintenance procedures can only be performed from the primary Admin Node

c. Optionally, drag and drop rows to change the priority order of the Primary interface and any Backup interfaces for this HA group.

d. Optionally, update the virtual IP addresses.

e. Select **Save** and then select **Finish**.

Wait up to 15 minutes for changes to an HA group to be applied to all nodes.

Remove a high availability group

You can remove one or more high availability (HA) groups at a time. However, you cannot remove an HA group if it is bound to one or more load balancer endpoints.

To prevent client disruptions, update any affected S3 or Swift client applications before you remove an HA group. Update each client to connect using another IP address, for example, the virtual IP address of a different HA group or the IP address that was configured for an interface during installation.

Steps

1. Select **CONFIGURATION** > **Network** > **High availability groups**.
2. Select the check box for each HA group you want to remove. Then, select **Actions** > **Remove HA group**.
3. Review the message and select **Delete HA group** to confirm your selection.

   All HA groups you selected are removed. A green success banner appears on the High availability groups page.

Copyright information

Copyright © 2025 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.