



# CHAPTER 9

## Configuring High Availability

---

High Availability (or fault tolerance) uses a maximum of two ACE appliances to ensure that your network remains operational even if one of the appliances becomes unresponsive. Redundancy ensures that your network services and applications are always available.



**Note**

---

Redundancy is not supported between an ACE appliance and an ACE module operating as peers. Redundancy must be of the same ACE device type and software release.

---

### Related Topics

- [Understanding ACE Redundancy, page 9-1](#)
- [Configuring High Availability Overview, page 9-5](#)
- [Configuring High Availability Peers, page 9-7](#)
- [Configuring ACE High Availability Groups, page 9-10](#)
- [Switching Over a High Availability Group, page 9-13](#)
- [Deleting ACE High Availability Groups, page 9-15](#)
- [High Availability Tracking and Failure Detection Overview, page 9-16](#)
- [Tracking VLAN Interfaces for High Availability, page 9-16](#)
- [Tracking Hosts for High Availability, page 9-17](#)
- [Configuring Host Tracking Probes, page 9-18](#)
- [Configuring Peer Host Tracking Probes, page 9-20](#)

## Understanding ACE Redundancy

Redundancy provides seamless switchover of flows in case an ACE appliance becomes unresponsive or a critical host or interface fails. Redundancy supports the following network applications that require fault tolerance:

- Mission-critical enterprise applications
- Banking and financial services
- E-commerce
- Long-lived flows such as FTP and HTTP file transfers

The following overview topics describe high availability as performed by the ACE appliance:

- [Redundancy Protocol, page 9-2](#)
- [Stateful Failover, page 9-3](#)
- [Fault-Tolerant VLAN, page 9-4](#)
- [Configuration Synchronization, page 9-4](#)
- [Redundancy Configuration Requirements and Restrictions, page 9-5](#)

#### Related Topics

- [Configuring High Availability Overview, page 9-5](#)
- [Configuring High Availability Peers, page 9-7](#)
- [Configuring ACE High Availability Groups, page 9-10](#)

## Redundancy Protocol

You can configure a maximum of two ACE appliances (peers) for redundancy. Each peer appliance can contain one or more fault-tolerant (FT) groups. Each FT group consists of two members: one active context and one standby context. An FT group has a unique group ID that you assign.

One virtual MAC address (VMAC) is associated with each FT group. The format of the VMAC is: 00-0b-fc-fe-1b-*groupID*. Because a VMAC does not change upon switchover, the client and server ARP tables does not require updating. The ACE selects a VMAC from a pool of virtual MACs available to it. For more information, see [Configuring Virtual Contexts, page 2-4](#).

Each FT group acts as an independent redundancy instance. When a switchover occurs, the active member in the FT group becomes the standby member and the original standby member becomes the active member. A switchover can occur for the following reasons:

- The active member becomes unresponsive.
- A tracked host or interface fails.
- You force a switchover for a high availability group by clicking **Switchover** in the ACE HA Groups table (see [Switching Over a High Availability Group, page 9-13](#)).

To outside nodes (clients and servers), the active and standby FT group members appear as one node with respect to their IP addresses and associated VMAC. The ACE provides active-active redundancy with multiple contexts only when there are multiple FT groups configured on each appliance and both appliances contain at least one active group member (context). With a single context, the ACE supports active-backup redundancy and each group member is an Admin context.

The ACE sends and receives all redundancy-related traffic (protocol packets, configuration data, heartbeats, and state replication packets) on a dedicated FT VLAN. You cannot use this dedicated VLAN for normal traffic.

To optimize the transmission of heartbeat packets for multiple FT groups and to minimize network traffic, the ACE sends and receives heartbeat messages using a separate process. The ACE uses the heartbeat to probe the peer ACE, rather than probe each context. When an ACE does not receive a heartbeat from the peer ACE, all the contexts in the standby state become active. The ACE sends heartbeat packets over UDP. You can set the frequency with which the ACE sends heartbeat packets as part of the FT peer configuration. For details about configuring the heartbeat, see [Configuring High Availability Peers, page 9-7](#).

The election of the active member within each FT group is based on a priority scheme. The member configured with the higher priority is elected as the active member. If a member with a higher priority is found after the other member becomes active, the new member becomes active because it has a higher priority. This behavior is known as preemption and is enabled by default. You can override this default behavior by disabling preemption. To disable preemption, use the `Preempt` parameter. Enabling `Preempt` causes the member with the higher priority to assert itself and become active. For details about configuring preemption, see [Configuring ACE High Availability Groups, page 9-10](#).

## Stateful Failover

The ACE replicates flows on the active FT group member to the standby group member per connection for each context. The replicated flows contain all the flow-state information necessary for the standby member to take over the flow if the active member becomes unresponsive. If the active member becomes unresponsive, the replicated flows on the standby member become active when the standby member assumes mastership of the context. The active flows on the former active member transition to a standby state to fully back up the active flows on the new active member.



---

**Note**

By default, connection replication is enabled in the ACE appliance.

---

After a switchover occurs, the same connection information is available on the new active member. Supported end-user applications do not need to reconnect to maintain the same network session.

The state information passed to the standby appliance includes the following data:

- Network Address Translation (NAT) table based on information synchronized with the connection record
- All Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) connections not terminated by the ACE appliance
- HTTP connection states (Optional)
- Sticky table



---

**Note**

In a user context, the ACE appliance allows a switchover only of the FT group that belongs to that context. In the Admin context, the ACE appliance allows a switchover of all FT groups in all configured contexts in the appliance.

---

To ensure that bridge learning occurs quickly upon a switchover in a Layer 2 configuration in the case where a VMAC moves to a new location, the new active member sends a gratuitous ARP on every interface associated with the active context. Also, when there are two VLANs on the same subnet and servers need to send packets to clients directly, the servers must know the location of the gateway on the client-side VLAN. The active member acts as the bridge for the two VLANs. In order to initiate learning of the new location of the gateway, the new active member sends an ARP request to the gateway on the client VLAN and bridges the ARP response onto the server VLAN.

## Fault-Tolerant VLAN

Redundancy uses a dedicated fault-tolerant VLAN between redundant ACEs to transmit flow-state information and the redundancy heartbeat. Do not use this dedicated VLAN for normal network traffic. You must configure this same VLAN on both peer appliances. You also must configure a different IP address within the same subnet on each appliance for the fault-tolerant VLAN.

The two redundant appliances constantly communicate over the fault-tolerant VLAN to determine the operating status of each appliance. The standby member uses the heartbeat packet to monitor the health of the active member. The active member uses the heartbeat packet to monitor the health of the standby member. Communications over the switchover link include the following data:

- Redundancy protocol packets
- State information replication data
- Configuration synchronization information
- Heartbeat packets

For multiple contexts, the fault-tolerant VLAN resides in the system configuration data. Each fault-tolerant VLAN on the ACE has one unique MAC address associated with it. The ACE uses these device MAC addresses as the source or destination MACs for sending or receiving redundancy protocol state and configuration replication packets.

**Note**

---

The IP address and the MAC address of the fault-tolerant VLAN do not change at switchover.

---

## Configuration Synchronization

For redundancy to function properly, both members of an fault-tolerant group must have identical configurations. Ensure that both ACE appliances include the same bandwidth software license (2G or 1G) and the same virtual context software license. If there is a mismatch in software license between the two ACE appliances in an FT group, the following operational behavior can occur:

- If there is a mismatch in virtual context software license, synchronization between the active ACE and standby ACE may not work properly.
- If both the active and the standby ACE appliances have the same virtual content software license but have a different bandwidth software license, synchronization will work properly but the standby ACE may experience a potential loss of traffic on switchover from the 2G ACE appliance to the 1G ACE appliance.

See the *Cisco 4700 Series Application Control Engine Appliance Administration Guide* for details about the available ACE software licenses.

The ACE automatically replicates the active configuration on the standby member using a process called *configuration synchronization* (config sync). Config sync automatically replicates any changes made to the configuration of the active member to the standby member. After the ACE synchronizes the redundancy configuration from the active member to the standby peer, it disables configuration mode on the standby. See [Synchronizing High Availability Configurations with ACE Appliance Device Manager](#), page 9-6.

## Redundancy Configuration Requirements and Restrictions

Follow these requirements and restrictions when configuring the redundancy feature.

- In bridged mode (Layer 2), two contexts cannot share the same VLAN.
- To achieve active-active redundancy, a minimum of two contexts and two fault-tolerant groups are required on each ACE.
- When you configure redundancy, the ACE keeps all interfaces that do not have an IP address in the Down state. The IP address and the peer IP address that you assign to a VLAN interface should be in the same subnet, but different IP addresses. For more information about configuring VLAN interfaces, see [Configuring Virtual Context VLAN Interfaces](#), page 8-6.

## Configuring High Availability Overview

The tasks involved with configuring high availability are described in [Table 9-1](#).

**Table 9-1 High Availability Task Overview**

	Task	Reference
Step 1	Create a fault-tolerant VLAN and identify peer IP addresses and configure peer appliances for heartbeat count and interval.	<a href="#">Configuring High Availability Peers</a> , page 9-7
Step 2	Create a fault-tolerant group, assign peer priorities, associate the group with a context, place the group in service, and enable automatic synchronization.	<a href="#">Configuring ACE High Availability Groups</a> , page 9-10
Step 3	Configure tracking for switchover.	<a href="#">High Availability Tracking and Failure Detection Overview</a> , page 9-16

### Related Topics

- [Understanding ACE Redundancy](#), page 9-1
- [High Availability Polling](#), page 9-6
- [Synchronizing High Availability Configurations with ACE Appliance Device Manager](#), page 9-6
- [Configuring High Availability Peers](#), page 9-7
- [Configuring ACE High Availability Groups](#), page 9-10
- [High Availability Tracking and Failure Detection Overview](#), page 9-16

## High Availability Polling

Approximately every two minutes, the ACE appliance Device Manager issues the **show ft group** command to the ACE appliance to gather the redundancy statistics of each virtual context. The state information is displayed in the HA State and HA Peer State fields when you click **Config > Virtual Context**. The possible states are:

- Active—Local member of the FT group is active and processing flows.
- Standby Cold—Indicates if the FT VLAN is down but the peer device is still alive, or the configuration or application state synchronization failed. When a context is in this state and a switchover occurs, the transition to the ACTIVE state is stateless.
- Standby Bulk—Local standby context is waiting to receive state information from its active peer context. The active peer context receives a notification to send a snapshot of the current state information for all applications to the standby context.
- Standby Hot—Local standby context has all the state information it needs to statefully assume the active state if a switchover occurs.
- Standby Warm—Allows the configuration and state synchronization process to continue on a best-effort basis when you upgrade or downgrade the ACE software.



### Note

When you upgrade or downgrade the ACE from one software version to another, there is a point in the process when the two ACEs have different software versions and, therefore, a software incompatibility. When the Standby Warm state appears, this means that the active ACE will continue to synchronize configuration and state information to the standby even though the standby may not recognize or understand the software commands or state information. This standby state allows the standby ACE to come up with best-effort support.

## Synchronizing High Availability Configurations with ACE Appliance Device Manager

When two ACE appliances are configured as high availability peers, their configurations must be synchronized at all times so that the standby ACE peer can seamlessly take over for the active ACE peer. As the active and standby ACEs synchronize, the configuration on the standby ACE appliance can become out of synchronization with the ACE Appliance Device Manager-maintained configuration data for that ACE appliance.

When an ACE appliance is in a standby state, if you make configuration changes on the active ACE appliance this change is also synchronized with the standby ACE appliance. However, when you access the Device Manager GUI you will not observe the configuration changes on the standby ACE. Yet, if you access the CLI on the standby ACE and display redundancy configurations using the **show running-config ft** command in Exec mode, you will see these configuration changes.

As a result, it is important for you to manually synchronize the ACE Appliance Device Manager on the standby appliance to observe the entire configuration. See the [“Manually Synchronizing Individual Virtual Context Configurations”](#) section on page 2-53.

When the ACE appliance performs a context failover (proceeds from the Standby Warm state or Standby Hot state) to the Active state), the new active ACE appliance auto-synchronizes the configuration and updates the ACE appliance Device Manager GUI.

In a high availability pair, the two configured virtual contexts synchronize with each other as part of their ongoing communications. However, their copies do not synchronize in ACE Appliance Device Manager and the configuration on the standby member can become out of sync with the configuration on the ACE appliance.

After the active member of a high availability pair fails and the standby member becomes active, ACE Appliance Device Manager on the newly active member detects any out-of-sync virtual context configurations and reports that status in the All Virtual Contexts table so that you can synchronize the virtual context configurations.

For information on synchronizing some or all virtual context configurations, see:

- [Manually Synchronizing Individual Virtual Context Configurations, page 2-53](#)
- [Manually Synchronizing All Virtual Context Configurations, page 2-53](#)

#### Related Topics

- [High Availability Polling, page 9-6](#)
- [Configuring High Availability Peers, page 9-7](#)
- [Configuring ACE High Availability Groups, page 9-10](#)
- [Manually Synchronizing Individual Virtual Context Configurations, page 2-53](#)
- [Manually Synchronizing All Virtual Context Configurations, page 2-53](#)

## Configuring High Availability Peers



#### Note

---

This functionality is available for only Admin contexts.

---

Fault-tolerant peers use a fault-tolerant VLAN to transmit and receive heartbeat packets and state and configuration replication packets. The standby member uses the heartbeat packet to monitor the health of the active member, while the active member uses the heartbeat packet to monitor the health of the standby member. When the heartbeat packets are not received from the active member when expected, switchover occurs and the standby member assumes all active communications previously on the active member.

Use this procedure to:

- Identify the two members of a high availability pair.
- Assign IP addresses to the peer ACE appliances.
- Assign a fault-tolerant VLAN to high availability peers and bind a physical gigabit Ethernet interface to the FT VLAN.
- Configure heartbeat frequency and count on the ACE appliances in a fault-tolerant VLAN.

#### Assumption

- At least one fault-tolerant VLAN has been configured.



#### Note

---

A fault-tolerant VLAN cannot be used for other network traffic.

---

**Procedure**

- Step 1** Select **Config > Virtual Contexts > High Availability (HA) > Setup**. The ACE HA Management window appears with two columns: One for the selected ACE appliance and one for a peer ACE appliance.
- Step 2** Click **Edit**, then enter the information for the primary appliance and the peer appliance as described in [Table 9-2](#).

**Table 9-2 ACE High Availability Management Configuration Attributes**

Field	This Appliance	Peer Appliance
VLAN	Specify a fault-tolerant VLAN to be used for this high availability pair. Valid entries are integers from 2 to 4094.  <b>Note</b> This VLAN cannot be used for other network traffic.	Not applicable.
Interface	Select the interface (specified by <i>slot_number/port_number</i> where <i>slot_number</i> is the physical slot on the ACE appliance, and <i>port_number</i> is the physical Ethernet data port on the ACE appliance) or the port channel.	Not applicable.
IP Address	Enter an IP address for the fault-tolerant VLAN in dotted-decimal format, such as 192.168.11.2.	Enter the IP address of the peer interface in dotted-decimal format so that the peer appliance can communicate on the fault-tolerant VLAN.
Netmask	Select the subnet mask that is to be used for the fault-tolerant VLAN.	Not applicable.
Management IP Address	Enter the IP address for the ACE.	Enter the Management IP Address of the peer appliance. When you enter this information, you can click on the HA Peer hyperlink in the <b>Config &gt; Virtual Contexts</b> screen.
Query VLAN	Select the VLAN that the standby appliance is to use to determine whether the active appliance is down or if there is a connectivity problem with the fault-tolerant VLAN.	Not applicable.
Heartbeat Count	Enter the number of heartbeat intervals that must occur with no heartbeat packet received by the standby appliance before the standby appliance determines that the active member is not available. Valid entries are integers from 10 to 50.	Not applicable.

**Table 9-2** ACE High Availability Management Configuration Attributes (continued)

Field	This Appliance	Peer Appliance
Heartbeat Interval	Enter the number of milliseconds that the active appliance is to wait between each heartbeat it sends to the standby appliance. Valid entries are integers from 100 to 1000.	Not applicable.
Interface Enabled	Select the Interface Enabled check box to enable the high availability interface. Clear the check box to disable the high availability interface.	Not applicable.
HA State	This is a read-only field with the current state of high availability on the ACE appliance.	Not applicable.

**Step 3** Click:

- **Deploy Now** to save your entries and to continue with configuring high availability groups. The ACE HA Management screen appears at the top of the content area and the ACE HA Groups table appears at the bottom. See [Configuring ACE High Availability Groups, page 9-10](#) to configure a high availability group.
- **Cancel** to exit this procedure without saving your entries and to view the ACE HA Management screen.

**Related Topics**

- [Understanding ACE Redundancy, page 9-1](#)
- [Configuring ACE High Availability Groups, page 9-10](#)
- [Tracking VLAN Interfaces for High Availability, page 9-16](#)

## Clearing High Availability Pairs

**Note**

This functionality is available for only Admin contexts.

Use this procedure to remove a high availability link between two ACE appliances.

**Procedure**

- Step 1** Select **Config > Virtual Contexts > High Availability (HA) > Setup**. The ACE HA Management screen appears.
- Step 2** Select the ACE appliance pair whose high availability configuration you want to remove, then click **Clear**. A message appears asking you to confirm the clearing of the high availability link.

**Step 3** Click:

- **OK** to confirm the removal of this high availability link and to return to the ACE HA Management screen.
- **Cancel** to exit this procedure without removing this high availability link and to return to the ACE HA Management screen.

**Related Topics**

- [Understanding ACE Redundancy, page 9-1](#)
- [Configuring High Availability Peers, page 9-7](#)
- [Editing ACE High Availability Groups, page 9-11](#)
- [High Availability Tracking and Failure Detection Overview, page 9-16](#)
- [Tracking VLAN Interfaces for High Availability, page 9-16](#)
- [Tracking Hosts for High Availability, page 9-17](#)

## Configuring ACE High Availability Groups

**Note**

This functionality is available for only Admin contexts.

A fault-tolerant group consists of a maximum of two contexts: One active context on one appliance and one standby context on the peer appliance. You can create multiple fault-tolerant groups on each ACE appliance up to a maximum of 251 groups (250 user contexts and 1 Admin context).

Use this procedure to configure high availability groups.

**Assumption**

At least one high availability pair has been configured. (See [Configuring High Availability Peers, page 9-7](#).)

**Procedure**

- 
- Step 1** **Config > Virtual Contexts > High Availability (HA) > Setup.** The ACE HA Management screen appears at the top of the content area and the ACE HA Groups table appears at the bottom.
- Step 2** In the ACE HA Groups table, click **Add** to add a new high availability group. The table refreshes with the configurable fields.
- Step 3** Select the Enabled check box to enable the high availability group. Clear the Enabled check box to disable the high availability group.
- Step 4** In the Context field, select the virtual context to associate with this high availability group.
- Step 5** In the Priority (Actual) field, enter the priority you want to assign to the first appliance in the group. Valid entries are integers from 1 to 255.

A member of a fault-tolerant group becomes the active member through a process based on the priority assigned. In this process, the group member with the higher priority becomes the active member. When you set up a fault-tolerant pair, use a higher priority for the group where the active member initially resides.

**Step 6** Select the Preempt check box to indicate that the group member with the higher priority is to always assert itself and become the active member. Clear the Preempt check box to indicate that you do not want the group member with the higher priority to always become the active member.

**Step 7** In the Peer Priority (Actual) field, enter the priority you want to assign to the peer appliance in the group. Valid entries are integers from 1 to 255.

A member of a fault-tolerant group becomes the active member through a process based on the priority assigned. In this process, the group member with the higher priority becomes the active member. When you set up a fault-tolerant pair, use a higher priority for the group where the active member initially resides.

**Step 8** Select the Autosync Run check box to enable automatic synchronization of the running configuration files. Clear the Autosync Run check box to disable automatic synchronization of the running configuration files. If you disable automatic synchronization, you need to update the configuration of the standby context manually.

**Step 9** Select the Autosync Startup check box to enable automatic synchronization of the startup configuration files. Clear the Autosync Run check box to disable automatic synchronization of the startup configuration files. If you disable automatic synchronization, you need to update the configuration of the standby context manually. See [Manually Synchronizing Individual Virtual Context Configurations](#), page 2-53.

**Step 10** Click:

- **Deploy Now** to accept your entries. The ACE HA Groups table refreshes with the new high availability group.
- **Cancel** to exit this procedure without saving your entries and to return to the ACE HA Management screen and ACE HA Groups table.

---

#### Related Topics

- [Configuring High Availability Peers](#), page 9-7
- [Editing ACE High Availability Groups](#), page 9-11
- [High Availability and Virtual Context Configuration Status](#), page 2-52
- [Tracking VLAN Interfaces for High Availability](#), page 9-16
- [Tracking Hosts for High Availability](#), page 9-17

## Editing ACE High Availability Groups



#### Note

---

This functionality is available for only Admin contexts.

---

Use this procedure to modify the attributes of a high availability group.

**Note**

If you need to modify a fault-tolerant group, take the group out of service before making any other changes (see [Taking a High Availability Group Out of Service, page 9-12](#)). When you finish making all changes, place the group back into service (see [Enabling a High Availability Group, page 9-13](#)).

**Procedure**

- 
- Step 1** Select **Config > Virtual Contexts > High Availability (HA) > Setup**. The ACE HA Management screen appears at the top of the content area and the ACE HA Groups table appears at the bottom.
- Step 2** In the ACE HA Groups table, select the high availability group you want to modify, then click **Edit**. The table refreshes with configurable fields.
- Step 3** Modify the fields as desired. For information on these fields, see [Configuring ACE High Availability Groups, page 9-10](#).
- Step 4** When you finish modifying this group, click:
- **Deploy Now** to accept your entries and to return to the ACE HA Groups table.
  - **Cancel** to exit this procedure without saving your entries and to return to the ACE HA Management screen.
- 

**Related Topics**

- [Taking a High Availability Group Out of Service, page 9-12](#)
- [Enabling a High Availability Group, page 9-13](#)
- [Configuring High Availability Peers, page 9-7](#)
- [High Availability Tracking and Failure Detection Overview, page 9-16](#)
- [Tracking VLAN Interfaces for High Availability, page 9-16](#)
- [Tracking Hosts for High Availability, page 9-17](#)

## Taking a High Availability Group Out of Service

**Note**

This functionality is available for only Admin contexts.

If you need to modify a fault-tolerant group, you must first take the group out of service before making any other changes. Use this procedure to take a high availability group out of service.

**Procedure**

- 
- Step 1** Select **Config > Virtual Contexts > High Availability (HA) > Setup**. The ACE HA Management screen appears at the top of the content area and the ACE HA Groups table appears at the bottom.
- Step 2** In the ACE HA Groups table, select the high availability group you want to take out of service, then click **Edit**. The table refreshes with configurable fields.
- Step 3** Clear the **Enabled** check box.

**Step 4** Click **Deploy Now** to take the high availability group out of service and to return to the ACE HA Groups table.

You can now make the necessary modifications to the high availability group. To put the high availability group back in service, see [Enabling a High Availability Group, page 9-13](#).

---

**Related Topic**

- [Enabling a High Availability Group, page 9-13](#)

## Enabling a High Availability Group



**Note**

This functionality is available for only Admin contexts.

---

After you take a high availability group out of service to modify it, you need to reenable the group. Use the following procedure to put a high availability group back in service.

**Procedure**

---

- Step 1** Select **Config > Virtual Contexts > High Availability (HA) > Setup**. The ACE HA Management screen appears at the top of the content area and the ACE HA Groups table appears at the bottom.
- Step 2** In the ACE HA Groups table, select the high availability group you want to take out of service, then click **Edit**. The table refreshes with configurable fields.
- Step 3** Select the **Enabled** check box.
- Step 4** Click **Deploy Now** to put the high availability group in service and to return to the ACE HA Groups table.
- 

**Related Topic**

- [Taking a High Availability Group Out of Service, page 9-12](#)

## Switching Over a High Availability Group



**Note**

This functionality is available for only Admin contexts.

---

You may need to cause a switchover when you want to make a particular context the standby (for example, for maintenance or a software upgrade on the currently active context). If the standby group member can statefully become the active member of the high availability group, a switchover occurs.

Use this procedure to force the failover of a high availability group.

**Procedure**

- 
- Step 1** Select **Config > Virtual Contexts > High Availability (HA) > Setup**. The ACE HA Management screen appears at the top of the content area and the ACE HA Groups table appears at the bottom.
- Step 2** In the ACE HA Groups table, select the group you want to switch over, then click **Switchover**. The standby group member becomes active, while the previously active group member becomes the standby member.
-

**Related Topics**

- [Understanding ACE Redundancy, page 9-1](#)
- [Configuring High Availability Peers, page 9-7](#)
- [Configuring ACE High Availability Groups, page 9-10](#)
- [Tracking VLAN Interfaces for High Availability, page 9-16](#)

## Deleting ACE High Availability Groups

**Note**

---

This functionality is available for only Admin contexts.

---

Use this procedure to remove a high availability group from ACE Appliance Device Manager management.

**Procedure**

- 
- Step 1** Select **Config > Virtual Contexts > High Availability (HA) > Setup**. The ACE HA Management screen appears at the top of the content area and the ACE HA Groups table appears at the bottom.
- Step 2** In the ACE HA Groups table, select the high availability group that you want to remove, then click **Delete**. A message appears asking you to confirm the deletion.
- Step 3** Click:
- **Deploy Now** to delete the high availability group and to return to the ACE HA Groups table. The selected group no longer appears.
  - **Cancel** to exit this procedure without deleting the high availability group and to return to the ACE HA Groups table.
- 

**Related Topics**

- [Configuring High Availability Peers, page 9-7](#)
- [Configuring ACE High Availability Groups, page 9-10](#)
- [Tracking VLAN Interfaces for High Availability, page 9-16](#)

# High Availability Tracking and Failure Detection Overview

The tracking and detection of failures ensures that switchover occurs as soon as the criteria are met (see [Configuring High Availability Peers, page 9-7](#)). With the ACE Appliance Device Manager, you can track and detect failures on:

- Hosts—See [Tracking Hosts for High Availability, page 9-17](#).
- Interfaces—See [Tracking VLAN Interfaces for High Availability, page 9-16](#).

When the active member of a fault-tolerant group becomes unresponsive, the following occurs:

1. The active member's priority is reduced by 10.
2. If the resulting priority value is less than that of the standby member, the active member switches over and the standby member becomes the new active member. All active flows continue uninterrupted.
3. When the failed member comes back up, its priority is incremented by 10.
4. If the resulting priority value is greater than that of the currently active member, a switchover occurs again, returning the flows to the originally active member.



## Note

In a user context, the ACE appliance allows a switchover only of the fault-tolerant groups belonging to that context. In an Admin context, the ACE appliance allows a switchover of all fault-tolerant groups on all configured contexts on the appliance.

## Related Topics

- [Configuring ACE High Availability Groups, page 9-10](#)
- [Tracking VLAN Interfaces for High Availability, page 9-16](#)
- [Tracking Hosts for High Availability, page 9-17](#)

## Tracking VLAN Interfaces for High Availability

Use this procedure to configure a tracking and failure detection process for a VLAN interface.

### Procedure

- Step 1** Select **Config > Virtual Contexts > HA Tracking and Failure Detection > Interfaces**. The Track Interface table appears.
- Step 2** Click **Add** to add a new tracking process to this table, or select an existing entry, then click **Edit** to modify it. The Track Interface configuration screen appears.
- Step 3** In the Track Object Name field, enter a unique identifier for the tracking process. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
- Step 4** In the Priority field, enter the priority for the interface on the active member. Valid entries are integers from 1 to 255 with higher values indicating higher priorities. The values that you enter here and in the Interface Peer Priority field (see [Step 6](#)) reflect the point at which you want switchover to occur. If the tracked interface goes down, the priority of that fault-tolerant group is decremented by the value entered in the Priority field. If the priority of the fault-tolerant group on the active member falls below that of the standby member, a switchover occurs.

- Step 5** In the VLAN Interface field, select the fault-tolerant VLAN that you want the active member to track.
- Step 6** In the Interface Peer Priority field, enter the priority for the interface on the standby member. Valid entries are integers from 1 to 255 with higher values indicating higher priorities. The values that you enter here and in the Priority field (See [Step 4](#)) reflect the point at which you want switchover to occur. If the tracked interface goes down, the priority of that fault-tolerant group is decremented by the value entered in the Interface Peer Priority field. If the priority of the fault-tolerant group on the active member falls below that of the standby member, a switchover occurs.
- Step 7** In the Peer VLAN Interface field, enter the identifier of an existing fault-tolerant VLAN that you want the standby member to track. Valid entries are integers from 1 to 4096.
- Step 8** Click:
- **Deploy Now** to save your entries and to return to the Track Interface table.
  - **Cancel** to exit this procedure without saving your entries and to return to the Track Interface table.
  - **Next** to save your entries and to configure the next entry in the Track Interface table.
- 

#### Related Topics

- [Configuring High Availability Peers, page 9-7](#)
- [Configuring ACE High Availability Groups, page 9-10](#)
- [Tracking Hosts for High Availability, page 9-17](#)

## Tracking Hosts for High Availability

Use this procedure to configure a tracking and failure detection process for a gateway or host.

#### Procedure

---

- Step 1** Select **Config > Virtual Contexts > HA Tracking and Failure Detection > Hosts**. The Track Host table appears.
- Step 2** Click **Add** to add a new tracking process to the table, or select an existing entry, then click **Edit** to modify it. The Track Host configuration screen appears.
- Step 3** In the Track Object Name field, enter a unique identifier for the tracking process. Valid entries are unquoted text strings with no spaces and a maximum of 64 alphanumeric characters.
- Step 4** In the Track Host/IP Address field, enter the IP address or hostname of the gateway or host that you want the active member of the high availability group to track. Enter the IP address in dotted-decimal format, such as 192.168.11.2.
- Step 5** In the Priority field, enter the priority of the probe sent by the active member. Valid entries are integers from 1 to 255. Higher values indicate higher priorities. Assign a priority value based on the relative importance of the host that the probe is tracking. If the probe goes down, the ACE appliance decrements the priority of the fault-tolerant group on the active member by the value in the Priority field.
- Step 6** In the Peer Host/IP Address field, enter the IP address or hostname of the host that you want the standby member to track. Enter the IP address using dotted-decimal notation, such as 192.168.11.2.

- Step 7** In the Peer Priority field, enter the priority of the probe sent by the standby member. Valid entries are integers from 1 to 255. Higher values indicate higher priorities. Assign a priority value based on the relative importance of the host that the probe is tracking. If the probe goes down, the ACE appliance decrements the priority of the fault-tolerant group on the standby member by the value in the Priority field.
- Step 8** Click:
- **Deploy Now** to save your entries and to continue with configuring track host probes. See [Configuring Host Tracking Probes, page 9-18](#).
  - **Cancel** to exit this procedure without saving your entries and to return to the Track Host table.
  - **Next** to save your entries and to configure another tracking process.
- 

#### Related Topics

- [Configuring Host Tracking Probes, page 9-18](#)
- [Configuring High Availability Peers, page 9-7](#)
- [Configuring ACE High Availability Groups, page 9-10](#)
- [Tracking VLAN Interfaces for High Availability, page 9-16](#)

## Configuring Host Tracking Probes

Use this procedure to configure probes on the active high availability group member to track the health of the gateway or host.

#### Assumptions

- At least one host tracking process for high availability has been configured (see [Tracking Hosts for High Availability, page 9-17](#).)
- At least one health monitoring probe has been configured (see [Configuring Health Monitoring for Real Servers, page 4-24](#)).

#### Procedure

- 
- Step 1** Select **Config > Virtual Contexts > HA Tracking and Failure Detection > Hosts**. The Track Host table appears.
- Step 2** Select the tracking process you want to configure a probe for, then select the Track Host Probe tab. The Track Host Probe table appears.
- Step 3** In the Track Host Probe table, click **Add** to add a track host probe, or select an existing track host probe, then click **Edit** to modify it. The Track Host Probe configuration screen appears.
- Step 4** In the Probe Name field, select the name of the probe to be used for the host tracking process.

- Step 5** In the Priority field, enter a priority for the host you are tracking by the active member of the high availability group. Valid entries are integers from 1 to 255 with higher values indicating higher priorities. Assign a priority value based on the relative importance of the gateway or host that the probes are tracking. If the host goes down, the ACE appliance decrements the priority of the high availability group on the active member by the value in this Priority field. If the resulting priority of the high availability group on the active member is less than the priority of the high availability group on the standby member, a switchover occurs.
- Step 6** Click:
- **Deploy Now** to save your entries and to return to the Track Host Probe table. The table includes the added probe.
  - **Cancel** to exit this procedure without saving your entries and to return to the Track Host Probe table.
  - **Next** to save your entries and to configure another track host probe.
- 

**Related Topics**

- [Configuring Peer Host Tracking Probes, page 9-20](#)
- [Configuring High Availability Peers, page 9-7](#)
- [Configuring ACE High Availability Groups, page 9-10](#)
- [Tracking VLAN Interfaces for High Availability, page 9-16](#)

## Deleting Host Tracking Probes

Use this procedure to remove a high availability host tracking probe.

**Procedure**

- 
- Step 1** Select **Config > Virtual Contexts > HA Tracking and Failure Detection > Hosts**. The Track Host table appears.
- Step 2** Select the tracking process you want to modify, then select the Track Host Probe tab. The Track Host Probe table appears.
- Step 3** In the Track Host table, select the probe you want to remove, then click **Delete**. The probe is deleted and the Track Host Probe table refreshes without the deleted probe.
- 

**Related Topics**

- [Configuring Peer Host Tracking Probes, page 9-20](#)
- [Configuring High Availability Peers, page 9-7](#)
- [Configuring ACE High Availability Groups, page 9-10](#)
- [Tracking VLAN Interfaces for High Availability, page 9-16](#)

# Configuring Peer Host Tracking Probes

Use this procedure to configure probes on the standby member of a high availability group to track the health of the gateway or host.

## Assumptions

- At least one host tracking process for high availability has been configured (see [Tracking Hosts for High Availability, page 9-17.](#))
- At least one health monitoring probe has been configured (see [Configuring Health Monitoring for Real Servers, page 4-24.](#))

## Procedure

- 
- Step 1** Select **Config > Virtual Contexts > HA Tracking and Failure Detection > Hosts**. The Track Host table appears.
- Step 2** Select the tracking process you want to modify, then select the Peer Track Host Probe tab. The Peer Track Host Probes table appears.
- Step 3** In the Peer Track Host Probes table, click **Add** to add a peer host tracking probe, or select an existing peer host tracking probe, then click **Edit** to modify it. The Peer Track Host Probes configuration screen appears.
- Step 4** In the Probe Name field, select the name of the probe to be used for the peer host tracking process.
- Step 5** In the Priority field, enter a priority for the host you are tracking by the standby member of the high availability group. Valid entries are integers from 1 to 255 with higher values indicating higher priorities. Assign a priority value based on the relative importance of the gateway or host that the probes are tracking. If the host goes down, the ACE appliance decrements the priority of the high availability group on the standby member by the value in this Priority field.
- Step 6** Click:
- **Deploy Now** to save your entries and to return to the Peer Track Host Probes table. The table includes the added probe.
  - **Cancel** to exit this procedure without saving your entries and to return to the Peer Track Host Probes table.
  - **Next** to save your entries and to configure another peer track host probe.
- 

## Related Topics

- [Configuring Host Tracking Probes, page 9-18](#)
- [Configuring High Availability Peers, page 9-7](#)
- [Configuring ACE High Availability Groups, page 9-10](#)
- [Tracking VLAN Interfaces for High Availability, page 9-16](#)

# Deleting Peer Host Tracking Probes

Use this procedure to remove a high availability peer host tracking probe.

### Procedure

---

- Step 1** Select **Config > Virtual Contexts > HA Tracking and Failure Detection > Hosts**. The Track Host table appears.
- Step 2** Select the tracking process you want to modify then, select the Peer Track Host Probe tab. The Peer Track Host Probes table appears.
- Step 3** In the Peer Track Host Probes table, select the probe you want to remove, then click **Delete**. The probe is deleted and the Peer Track Host Probes table refreshes without the deleted probe.
- 

### Related Topics

- [Configuring Peer Host Tracking Probes, page 9-20](#)
- [Configuring Host Tracking Probes, page 9-18](#)
- [Tracking VLAN Interfaces for High Availability, page 9-16](#)

