FortiNAC

High Availability

Version: 8.3, 8.5, 8.6, 8.7, 8.8, 9.1
Date: November 29, 2021
Rev: Q

FORTINET DOCUMENT LIBRARY
http://docs.fortinet.com

FORTINET VIDEO GUIDE
http://video.fortinet.com

FORTINET KNOWLEDGE BASE
http://kb.fortinet.com

FORTINET BLOG
http://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
http://support.fortinet.com

FORTINET COOKBOOK
http://cookbook.fortinet.com

NSE INSTITUTE
http://training.fortinet.com

FORTIGUARD CENTER
http://fortiguard.com

FORTICAST
http://forticast.fortinet.com

END USER LICENSE AGREEMENT
http://www.fortinet.com/doc/legal/EULA.pdf

Contents

Overview 5
What it Does 5
How it Works 5
Terminology 6
Combining Virtual Machines and Hardware Appliances 6
Requirements 6
Where to Install the Secondary Server 7
Configuration Options 8
Layer 2 (L2) High Availability 9
Layer 3 (L3) High Availability 10
Configuration 11
Network Infrastructure Overview 11
Layer 2 11
Layer 3 13
High Availability Configuration 15
Considerations 15
Procedure 15
Validate Configuration 19
Confirm Appliance Status and Licensing 19
Confirm Database Replication 21
Failover Test 22
Troubleshooting 25
Determine Which Appliance Has the Shared IP (Layer 2 HA) 25
Shared IP Missing After Network Service Restart 25
Re-Add Shared IP Address 26
Verify License Key Configuration 27
Validating Processes – CLI 29
High Availability Concepts 30
"Normal" Control Status 30
Failover Control Status 31
Startup High Availability 32
Primary Server Startup Process 32
Secondary Server Startup Process 32
Management Process 32

Control Sequence 33
Required Processes 33
Determining Whether the Secondary Needs to Take Control 33
Failover Scenarios Due to Network Communication Issues 35
Recovery 36
Appendix 37
Control/Application Server Pair IP Addressing 37
Connectivity Configuration 38
Access Secondary Server Wizard Post HA Configuration 38
Sponsor Approval Email Links 39
Configure Links for HTTPS 39
Embed Server FQDN 39
Stopping and Restarting Processes 41
What Happens When Processes are Stopped 41
Procedures 41
Alarms and Events 45
Process Down Events 45
Process Started Events 45
Other High Availability Events 46
Modify Ping Retry Count 46
Remove High Availability Configuration 48
Considerations 48
Configuration Removal Procedure 48
Access Secondary Server Configuration Wizard in L2 High Availability 56
Log Output Examples 57
System Software Updates 58
Operating System Updates 58

Overview

This document provides the steps necessary for configuring High Availability. It is intended to be used in conjunction with the **Deployment Guide** in the Fortinet Document Library.

Note:

- Individual Control Server/Application Server appliances referenced in this document are no longer available for purchase
- High Availability not available for FortiNAC Reporter/Analytics (no longer available)

What it Does

The FortiNAC High Availability solution is used for disaster recovery: ensuring redundancy for FortiNAC. This is achieved through active and passive appliances where the passive (backup) appliance becomes active when the main appliance is no longer functioning normally.

Important: The process that activates the backup appliance, as well as re-activates the main appliance, takes approximately **10-15 minutes** to complete. During this time, FortiNAC processes are not running.

How it Works

The High Availability solution consists of the following components. For more details see High Availability Concepts:

- **1-to-1 active/passive configuration:** for each appliance running (active), there is an appliance in standby (passive).
    - **Primary Server** - The appliance(s) of the high availability pair that is in control by default. Sometimes referred to as the Master.
    - **Secondary Server** - The "backup" appliance(s) that takes control when the Primary fails. Sometimes referred to as the Slave.

- **High Availability Management Process** - Provides messaging between the primary and secondary appliances. The process mirrors critical information, controls services, and performs system maintenance functions on all appliances. Database synchronization/replication is handled by MySql replication to provide complete data integrity. For additional information on the MySql replication see http://dev.mysql.com/doc/refman/4.1/en/replication.html.

  The management process also manages and determines which server is in control. It starts the secondary appliances in the event the primary appliances are no longer able to perform all the necessary services and tasks (referred to as “failover”). Additionally, it starts the primary appliances and other required tasks when the primary appliances resume control (referred to as “recovery”).

- **Supporting Scripts** - Determine whether the database replication is working. These scripts are also used to restore the database and/or files from the secondary to the primary and restart the Primary Server.

Terminology

Term	Definition
Primary	The active server or servers of the high availability pair that is in control by default. Sometimes referred to as the Master.
Secondary	The "backup" server or servers that take control when the primary fails. Sometimes referred to as the Slave.
Loader	The process that runs on the FortiNAC Server in Control: Principal (FortiNAC Server and Control Server) Nessus (FortiNAC Server and Application Server) Control Manager (FortiNAC Control Manager (NCM))
Management Process (Control Process)	The process which manages and determines which server is in control.
Idle	High Availability state in which the management process is functional, but the Secondary Server will not take control even if connectivity is lost with the Primary Server.

Combining Virtual Machines and Hardware Appliances

Customers have implemented the following configurations in a High Availability environment with no known issues:

- Combination of physical and virtual appliances for Primary and Secondary Servers
- Combination of physical and virtual appliances within a pair of Control and Application Server appliances

There are no known requirements for the virtual appliance to be all Hyper-V or VMware in an HA configuration.

Requirements

- The following have been completed for **both** appliances (see **Deployment Guide**)
  - Appliance Installation
    - VMware Appliances: If a VM was cloned for use as the Secondary, follow the instructions in section **Change the MySQL UUID file of Cloned VMs** of the **VMware Installation Guide** before proceeding.
  - Appliance Configuration
    - Configured for Layer 3 Network Type (required for L3 High Availability). See **Configuration Wizard** reference manual.
    - Eth1 must be configured with an IP address and DHCP scope. See Required Processes for additional information.
  - Operating System Updates

- Appliances can ping each other and establish SSH communication.

- If using Rogue DHCP Server Detection:
  - Both the primary and Secondary Servers/Application Servers must have the same Interface setting.
  - The ports to which the Interfaces connect must be added to the **System**

DHCP Port group. For instructions, see section **Modify a Group** of the **Administration Guide** in the Fortinet Document Library.

- In the event of a failover, it is important that these fields be setup correctly or DHCP monitoring will not run. For details, see section **Rogue DHCP Server Detection** of the **Administration Guide** in the Fortinet Document Library.

Where to Install the Secondary Server

When choosing the Secondary Server location, network bandwidth and traffic flow change must be taken into account.

- Starting latency and bandwidth recommendations (L2 & L3 configurations):
  - Latency between remote data nodes must not exceed 20 milliseconds
  - Bandwidth of the network link must be a minimum of 4.8 Mbps

  Fortinet recommends using the "Database Replication Error" event and the corresponding alarm action to notify administrators when an error occurs. There are two possible causes for this error:
  - There was a momentary network outage that caused the failure.
  - If the event happens continuously, then network speed of the must be increased.

- Communication between Primary and Secondary Servers
  - Database replication
  - Primary Server control resume process (large amounts of information are copied back to the Primary)

- Traffic redirected to the Secondary Server upon failover
  - Administration UI access
  - FortiNAC Agent communication
  - Infrastructure device communication (e.g. routers, switches, Controllers/AP's)
    - SNMP
    - SSH
    - RADIUS (if Proxy mode, includes communication with RADIUS server)
    - API
    - SSO

Example: RADIUS authentication traffic flow
Primary in Control
client ← → Wireless Controller/Access Point/Switch ← → Primary FortiNAC ← → RADIUS Server

Failover (Secondary in control):
client ← → Wireless Controller/Access Point/Switch ← → Secondary FortiNAC ← → RADIUS Server

Configuration Options

There are two possible High Availability configurations:

- **Layer 2 High Availability**: Both Primary and Secondary Servers reside on the same network. Layer 2 HA provides system redundancy in the event of an appliance failure.
- **Layer 3 High Availability**: Primary and Secondary Servers reside on different networks (e.g. Data Center and Disaster Recovery (DR) Data Center). This configuration not only provides system redundancy, but full disaster recovery in the event of a location outage.

Refer to the following pages for details.

Layer 2 (L2) High Availability

Uses a shared IP address (Virtual IP or VIP) and host name that is moved between appliances during a failover and recovery. This provides the administrator with a single point of management access regardless of which appliance is in control. To use a shared IP address, all of the appliances must be in the same subnet on the network. See section Network Infrastructure - Layer 2.

In a FortiNAC Control Server and Application Server configuration, the FortiNAC Application Server appliances are separate standbys from the FortiNAC Control Server appliances.

For example:

- If the primary FortiNAC Control Server fails, the secondary FortiNAC Control Server communicates with whichever FortiNAC Application Server is in control (either the primary or the secondary).
- If the primary FortiNAC Application Server fails, the primary FortiNAC Control Server communicates whichever FortiNAC Application Server is in control.

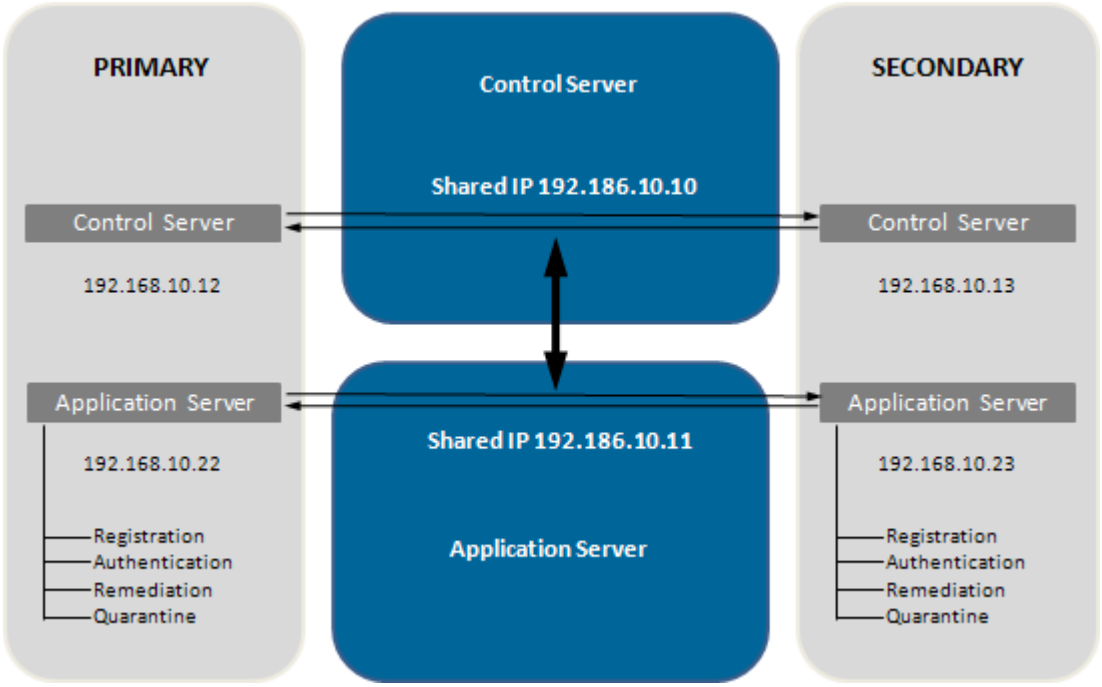


Figure 1: Shared IP - Servers On Same Subnet (L2)

Layer 3 (L3) High Availability

Primary and secondary appliances in a Layer 3 High Availability configuration are on different subnets. Unlike Layer 2 High Availability, Layer 3 does not use a Shared IP and hostname. See section Network Infrastructure - Layer 3.

Requirement: FortiNAC appliances must be configured for the **L3 Network Type**. This configWizard option is used when Isolation Networks are separated from the FortiNAC Appliance's eth1 interface by a router.

In a FortiNAC Control Server and Application Server configuration, the appliances failover in pairs.

For example:

- If the primary FortiNAC Control Server fails, the primary FortiNAC Application Server is also brought down and the Secondary pair of appliances take control.
- If the primary FortiNAC Application Server fails, the primary FortiNAC Control Server is also brought down and the Secondary pair of appliances take control.

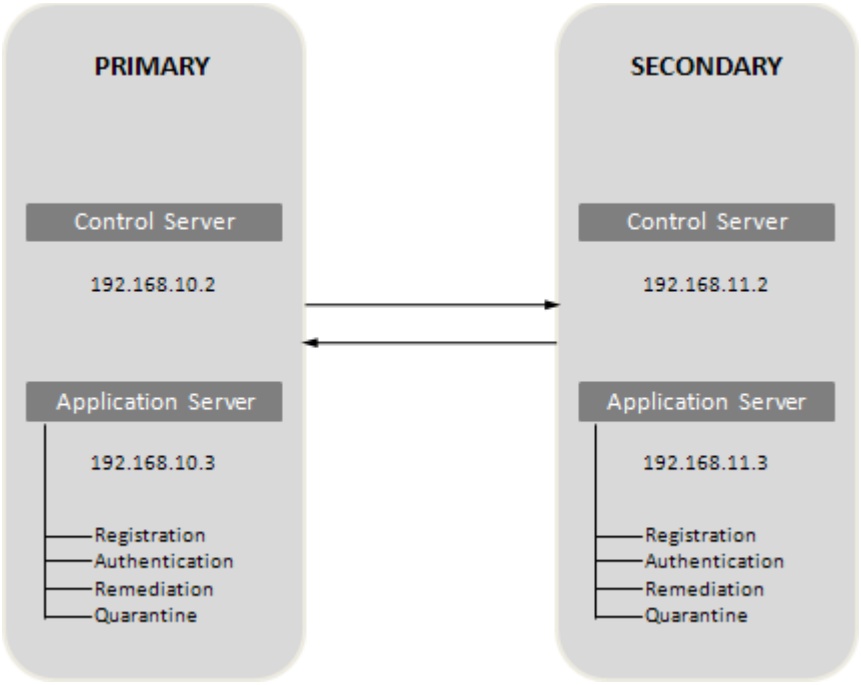


Figure 2: No Shared IP - Servers In Different Subnets (L3)

Configuration

Network Infrastructure Overview

Layer 2

- **IP Addressing -** Determine the IP addresses to be used. (Examples shown are with appliances using Layer 3 Network Type)

FortiNAC Control Manager (NCM)

1. Shared IP Address
2. Primary Server eth0
3. Secondary Server eth0

Example
Shared IP Address: 192.168.00.10/24
Primary Server eth0: 192.168.00.8/24
Secondary Server eth0: 192.168.00.9/24

FortiNAC Server (NS500CA, NS600CA)

1. Shared IP Address
2. Primary Server eth0
3. Primary Server eth1 (including isolation interface IP's)
4. Secondary Server eth0
5. Secondary Server eth1 (use same isolation interface IP's as Primary eth1)

Example
Shared IP Address: 192.168.00.4/24
Primary Server eth0: 192.168.00.2/24
Primary Server eth1 Registration: 192.168.200.20/28
Primary Server eth1 Remediation: 192.168.200.21/28
Primary Server eth1 DeadEnd: 192.168.200.22/28

Secondary Server eth0: 192.168.00.3/24
Secondary Server eth1 Registration: 192.168.200.20/28
Secondary Server eth1 Remediation: 192.168.200.21/28
Secondary Server eth1 DeadEnd: 192.168.200.22/28

For Control Server/Application Server pairs, see Appendix.

- **Network Device Traps -** Configure all network devices to send traps to both the primary and secondary FortiNAC Server/Control Server eth0 IP addresses (do not use Shared IP address).

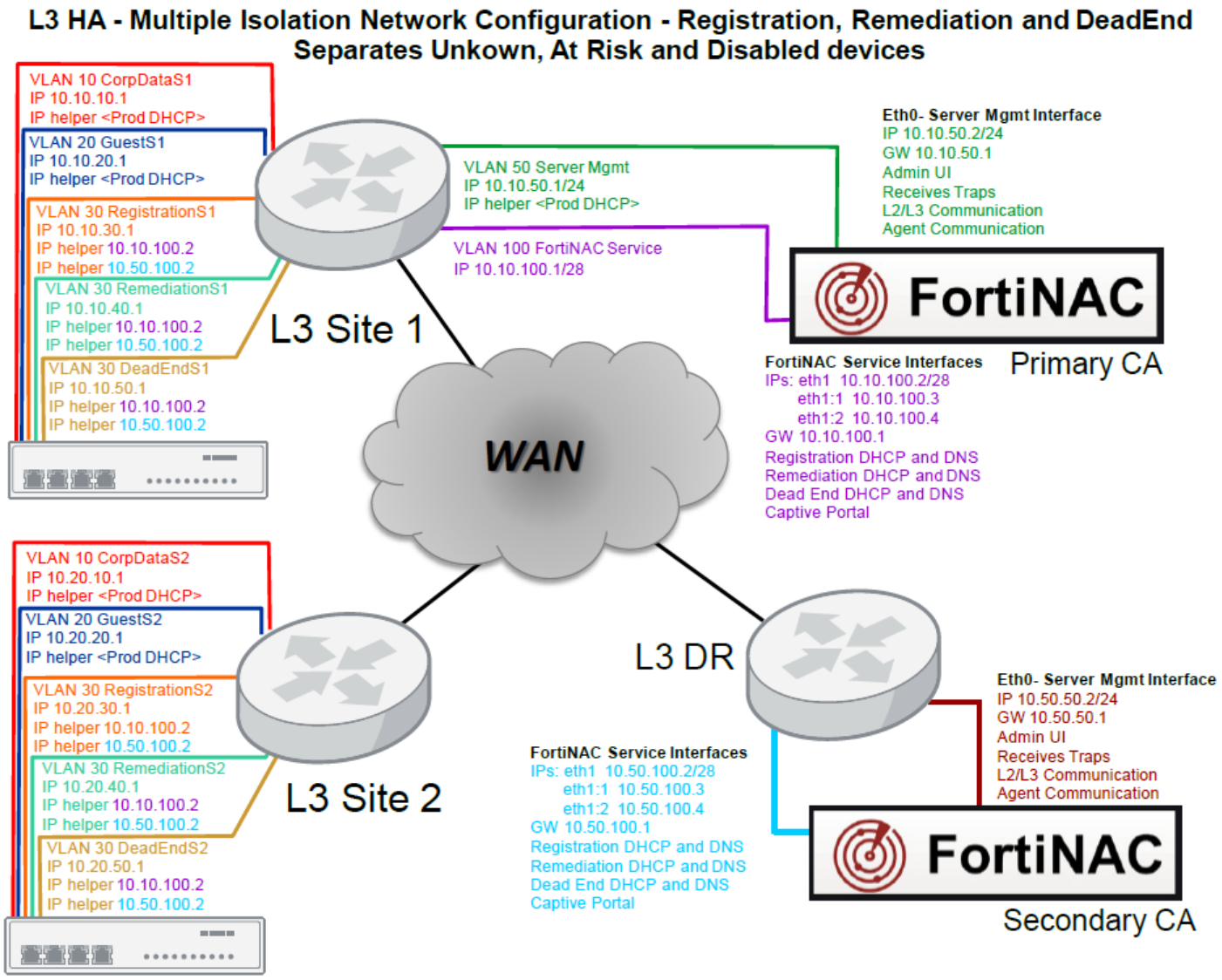
- **RADIUS Servers -** Configure RADIUS servers to use both the primary and secondary FortiNAC Server/Control Server eth0 IP addresses (do not use Shared IP address).

- **Devices Using FortiNAC as RADIUS Server (Wireless Controllers, Access Points, etc) -** Configure a primary and secondary RADIUS server:
    1. Primary RADIUS server = primary FortiNAC Server/Control Server (use eth0 IP address). Do not use the Shared IP address.
    2. Secondary RADIUS server= secondary FortiNAC Server/Control Server (use eth0 IP address). Do not use the Shared IP address.

  Regardless of the environment, consider setting up the actual RADIUS server to be used in the event that none of the FortiNAC appliances can be reached. This would allow users to access the network, but they would not be controlled by FortiNAC.

- **Persistent Agent -** Use the primary and secondary FortiNAC Server/Application Server Fully Qualified Domain Names (not the Shared name). Refer to Persistent Agent Deployment and Configuration Tips in the Documentation Library for details.

Layer 3



- **IP Addressing -** Determine the IP addresses to be used for FortiNAC appliances.

  <u>FortiNAC Control Manager (NCM)</u>

  1. Primary Server eth0
  2. Secondary Server eth0 (different subnet than Primary eth0)

  Example
  Primary Server eth0: 10.10.50.8/24
  Secondary Server eth0: 10.50.50.8/24

FortiNAC Server

1. Primary Server eth0
2. Primary Server eth1 (including isolation interface IP's)
3. Secondary Server eth0 (different subnet than Primary eth0)
4. Secondary Server eth1 (different subnet than Primary eth1)

Example
Primary Server eth0: 10.10.50.2/24
Primary Server eth1 Registration: 10.10.100.2/28
Primary Server eth1 Remediation: 10.10.100.3/28
Primary Server eth1 DeadEnd: 10.10.100.4/28

Secondary Server eth0: 10.50.50.2/24
Secondary Server eth1 Registration: 10.50.100.2/28
Secondary Server eth1 Remediation: 10.50.100.3/28
Secondary Server eth1 DeadEnd: 10.50.100.4/28

For Control Server/Application Server pairs, see Appendix.

- **Network Communication** - Make sure that communication between the subnets is configured in advance.

- **DHCP Helpers** – FortiNAC returns two DNS servers for isolation VLANs. Therefore, for each isolation VLAN, configure DHCP Helpers for both Primary and Secondary eth1 IP addresses. If multiple isolation VLANs are configured, use the main eth1 IP address.

- **Isolated hosts will have two DNS entries for use**: primary and secondary eth1. Upon failover, should the host stay in isolation longer than the DHCP time to live, the host will fail to renew its IP from the primary. It will redo DHCP discovery and get an IP address from the secondary. The secondary will have responded with two DNS servers (secondary eth1 and primary eth1).

- **Network Device Traps** - Configure all network devices to send traps to both the primary and secondary FortiNAC Server/Control Server eth0 IP addresses.

- **RADIUS Servers** - Configure RADIUS servers to use both the primary and secondary FortiNAC Server/Control Server eth0 IP addresses.

- **Devices Using FortiNAC as RADIUS Server (Wireless Controllers, Access Points, etc)** - Configure a primary and secondary RADIUS server:
    1. Primary RADIUS server = primary FortiNAC Server/Control Server (use eth0 IP address).
    2. Secondary RADIUS server = secondary FortiNAC Server/Control Server (use eth0 IP address).

  Regardless of the environment, consider setting up the actual RADIUS server to be used in the event that none of the FortiNAC appliances can be reached. This would allow users to access the network, but they would not be controlled by FortiNAC.

- **Persistent Agent** – Use the primary and secondary FortiNAC Server/Application Server Fully Qualified Domain Names. Refer to Persistent Agent Deployment and Configuration Tips in the Customer Portal for details.

- **Self-Registration Email Settings** - If using the Guest Self-Registration feature, configure settings to generate the correct links in the emails sent to Sponsors when a guest requests access. See section Configure Email Links To Use HTTPS And Server FQDN.

High Availability Configuration

Configure the appliances to work as a High Availability pair using the Administration UI.

Considerations

- All appliances in the configuration are restarted and placed into High Availability mode when **Save Settings** is clicked. FortiNAC services will be interrupted during this time.
- Use the **High Availability** view for all changes to the configuration. If files on the appliance are manually edited, values in the files will not be reflected in this view.
- **Appliances Managed by Manager (FNAC-M-xx)**: High Availability can be configured before or after the Primary Server has been added to the Manager's Server List. The Server List will automatically update with the Secondary Server once the configuration is complete.

Procedure

1. **Appliances Managed by Manager (FNAC-M-xx):** If the appliance becoming the Secondary Server is in the Manager's Server List, remove before configuring High Availability.

2. Login to the Administration UI of the FortiNAC server that will become the Primary Server.

3. Navigate to **System > Settings > System Management > High Availability**.

4. Fill in the appropriate fields using the table below. For L2 HA configurations, click the **Use Shared IP Address** checkbox and enter the Shared IP Address information.

Field	Description
Shared IP Configuration	
Use Shared IP Address	Enables the use of a shared IP address in the High Availability configuration. If enabled, the administrator can manage whichever appliance that is in control with the shared IP address instead of the actual machine IP address. If your primary and Secondary Servers are not in the same subnet, do not use a shared IP address.

Shared IP Address	The shared IP address for the High Availability configuration. Added to the **/etc/hosts** file when the configuration is saved.
Shared Subnet Mask (bits)	The shared subnet mask in bits. For example, 255.255.255.0 = 24 bits. If you are using a Shared IP Address, this field is required.
Shared Host Name	Part of the entry in the **/etc/hosts** file for the shared IP address. Admin users can access the UI using either the Shared IP address or the shared host name.
Server Configuration	
Primary Appliance	**IP Address**—IP address assigned to eth0 for the primary. **Gateway IP Address***—IP address pinged by the appliances to determine if network connectivity is still available. **Note**: Do not use FortiNAC IP addresses for this entry. **CLI/SSH root Password [User:root]**—root password on the appliance itself. Allows settings to be written to the appliance. **Retype root CLI/SSH Password [User:root]**—retype the password entered in the CLI/SSH root Password field for confirmation.
Secondary Appliance	**IP Address**—IP address assigned to eth0 for the secondary. **Host Name** — Name assigned to the secondary. **Gateway IP Address***—IP Address pinged by the appliances to determine if network connectivity is still available. **Note**: Do not use FortiNAC IP addresses for this entry. **CLI/SSH root Password [User:root]**—root password on the appliance itself. Allows settings to be written to the appliance. **Retype root CLI/SSH Password [User:root]**—retype the password entered in the CLI/SSH root Password field for confirmation.

*Represents the network gateway IP address of the Primary and Secondary Servers. If building appliances using Azure, see below.

Failover behavior will differ depending upon the option used.

Option1:
Primary Appliance Gateway IP Address: network gateway of the Primary Server.
Secondary Appliance Gateway IP Address: network gateway of the Secondary Server.

Option 2:
Primary Appliance Gateway IP Address: network gateway of the *Secondary Server*.
Secondary Appliance Gateway IP Address: network gateway of the *Primary Server*.

Option 2 can prevent both primary and secondary servers from being active at the same time. See section Failover Scenarios Due to Network Communication Issues for details.

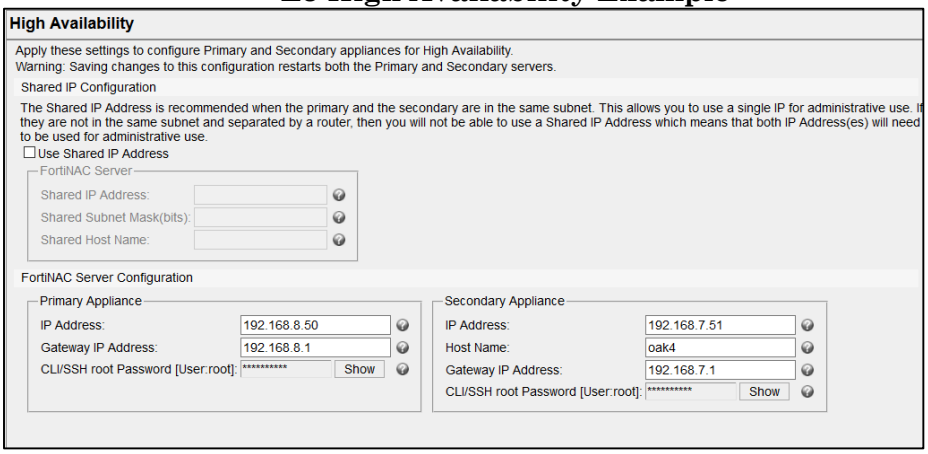
Defining Gateways for Azure Appliances

There is no specific "Gateway" when FortiNAC appliances are built using Azure. Therefore, another IP address must be used for this entry. Requirements:

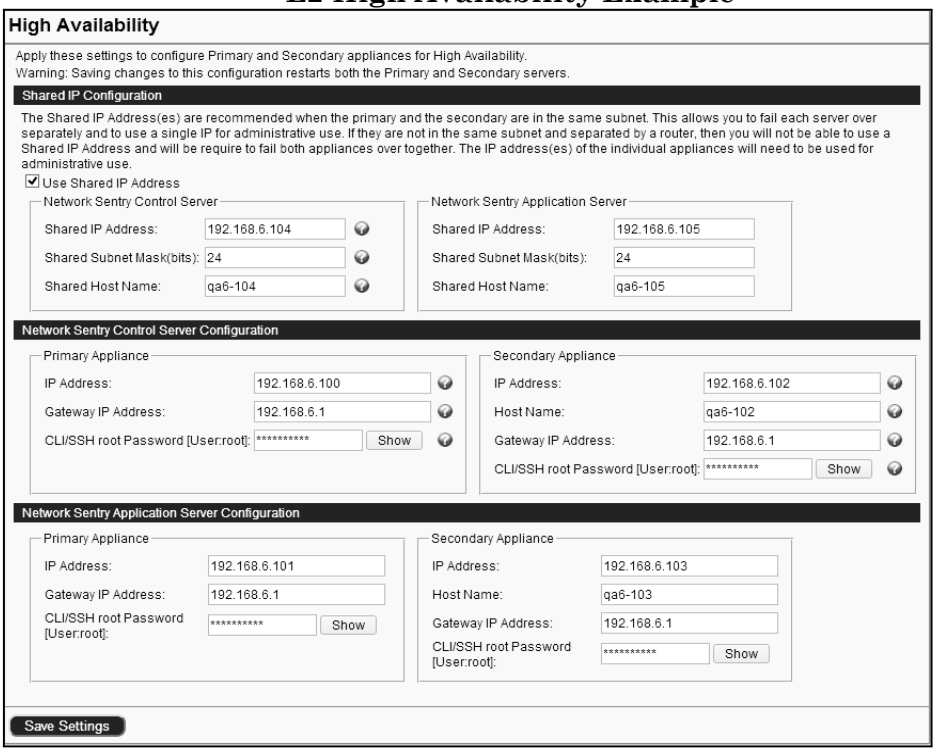
- IP address must respond to a PING request from the FortiNAC eth0 IP addresses.
- Device owning the IP address should always be available (e.g. a router interface)
- The PING test is used to determine whether the Secondary Server can reach the

network prior to taking control. Therefore, choose an interface that best suits this requirement based upon the local network design.

L3 High Availability Example



L2 High Availability Example



5. Click **Save Settings** to apply the configuration.

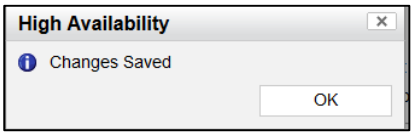
   The following message will appear:
   Applying Settings. This could take a few minutes. Please wait.

   This will take several minutes. The information entered into the view is written to files on all of the appliances involved, configures the SSH keys for all the specified appliances and configures mysql for replication. All appliances in the configuration are restarted and placed into High Availability mode.

   Note: When clicking **Save Settings**, the Primary Server tries to communicate with the secondary to ensure that the database will be replicated. If the Primary Server cannot communicate with the secondary, it continues to try until communication is established.

6. Click **Yes** to restart server when prompted.

7. Click **OK** again.



8. Wait several minutes to allow FortiNAC to restart management processes.

Proceed to **Validate Configuration**.

Validate Configuration

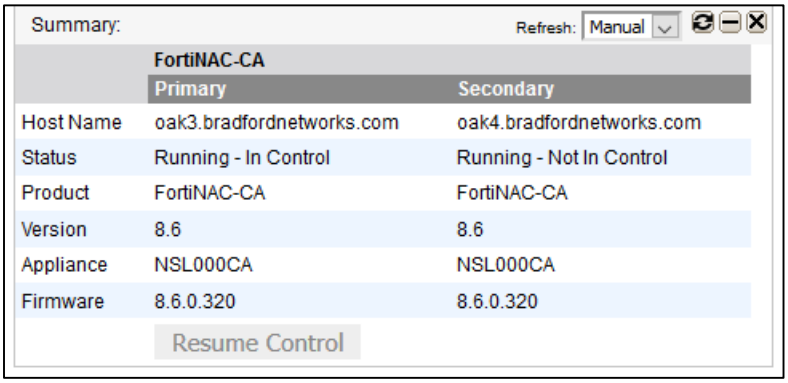
Confirm Appliance Status and Licensing

Administration UI Method

1. Login to the Primary Server Administration UI.

   The **Summary** panel on the Dashboard indicates the status of Primary and Secondary Servers. This information includes which appliance has control and whether or not an appliance is idle.

   Under normal conditions, the Primary Server should be in control and would display the following status:
   Primary Server(s): **Running - In Control**
   Secondary Server(s): **Running - Not In Control**

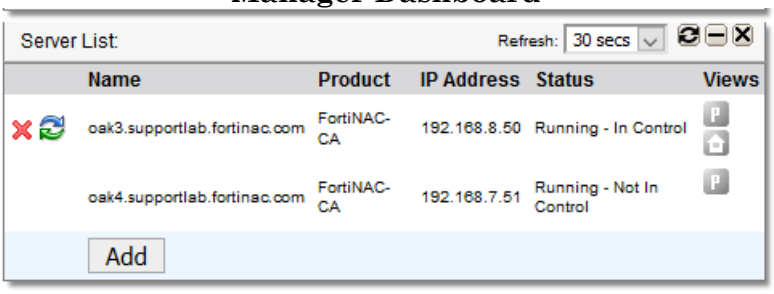


Systems Managed by Control Manager

If the High Availability pair is to be managed by a Manager, but not already part of the Manager's Server List, add the Primary Server at this time. For details and instructions, refer to the Control Manager Admin Guide in the Fortinet Document Library.

Once added to the Server List, similar information will display in the Manager UI.

Manager Dashboard

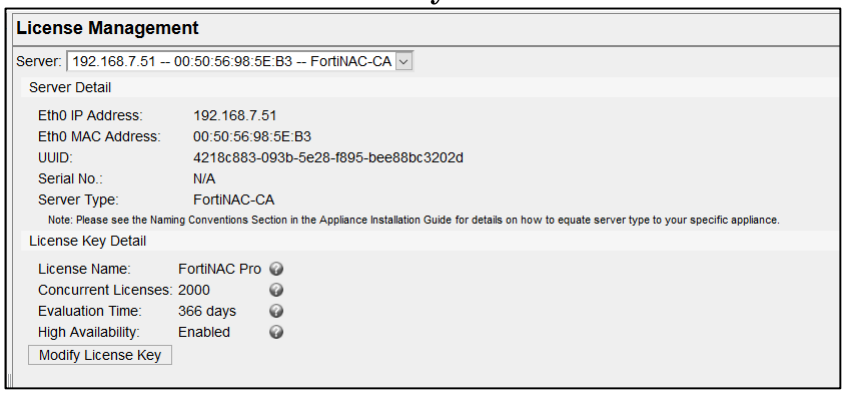


2. Verify the key information for both appliances. In the Primary Server Administration UI, navigate to **System > Settings > System Management > License Management** and select the Secondary Server from the drop-down menu.

   Primary Server is installed with Endpoint License Key (Example Below): Both appliances display information in the **License Key Detail** and **Server Detail** sections

Primary Server with License Key

Secondary Server



Pair is managed by a Manager:

- Primary Server displays information for both **License Key Detail** and **Server Detail** sections.
- Secondary Server displays information in the **Server Detail** only.

Confirm Database Replication

When the Primary Server is started, it attempts to communicate with the Secondary Server. It continues to attempt communication until it connects to the secondary and can begin replicating the database. When a change is made in the database of the Primary Server, the database replication process makes the same change in the database of the Secondary Server. Depending upon the size of the database and the network connection between Primary and Secondary Servers, replication can take several minutes. The Secondary Server does not perform mysql database replication back to the primary.

Important: If the database is not replicating properly, unexpected behavior can result should a failover occur. This behavior can vary depending upon the missing data. For example, isolation of recently registered hosts can occur if replication failed before those host records were copied. *Do not attempt to test the failover functionality until database is replicating properly.*

Administration UI Method

1. Navigate to **Logs > Events**.

   If the database copied successfully, the event **Database Replication Succeeded** should be listed. Otherwise, the **Database Replication Error** event will appear.
2. Ensure the **Database Replication Error** event is mapped to an alarm under **Logs > Alarm Mappings**.

CLI Method

Navigate to the **/bsc/campusMgr/bin/** directory on the Secondary. Run the following script:
hsIsSlaveActive

A response similar to the following should be returned:

```
root@Host Name:/bsc/campusMgr/bin
> hsIsSlaveActive Host Host Name
SQL version 5.0.18, slave is active
```

If the response contains the line **slave is active**, database replication is active.
If the response contains the line **slave is inactive**, database replication is not active.

Note: If for any reason the database is not replicated correctly on the secondary before failover, the recovery process gives the option of retaining the older database located on the primary.

Failover Test

Test the failover function to validate the High Availability feature is working properly. For Distributed Systems, the Secondary Server will not be updated with Endpoint Licenses until the first failover occurs after completing High Availability configuration. Once the Secondary Server is in control, the Manager pushes the licenses to the Secondary Server.

Considerations

- During a Failover test, FortiNAC processes will be down until the Secondary Server(s) take control. This takes approximately 10-15 minutes to complete. This is also true when resuming control of the Primary Server(s).
- L2 HA: If Control Server/Application Server pair, the corresponding Secondary Server takes control.
- L3 HA: If Control Server/Application Server pair, the entire Secondary Server pair takes control.

Trigger Failover

1. Login to Admin UI and add a new container named TEST in **Network Devices > Topology**.

2. Open SSH sessions to each Server (Primary and Secondary) and begin tailing the processManager log.
   logs
   tail –F output.processManager

3. Simulate a condition on the Primary Server to trigger failover using one of the scenarios below.

   Note: Issuing the commands "halt" or "poweroff" on the Primary Server will not trigger the secondary to take control. These commands trigger a clean shutdown which idles the Control process. It is not a valid network/power outage simulation test.

   Scenario 1 - Network loss: Disconnect the eth0 interface of the Primary Server or admin down the switch port

   Scenario 2 - Management processes down: In the Primary Server CLI, stop the management process without idling the Control process. Type **shutdownNAC -kill**

   The Secondary Server regularly attempts to poll the status of its corresponding Primary Server every 30 seconds. If the Primary Server does not respond after 5 consecutive attempts (or the number defined by the Ping Retry Count), the Secondary Server will attempt to take control.

   Failover is complete once the appropriate Secondary Server(s) taking control display status **(Slave) Slave In Control Idle(false).** This can take several minutes.

   Refer to the Appendix for Log Output Examples.

Scenario 3 - DHCP service down: In the Primary Server CLI, stop the DHCP service.
1. Admin shut down eth1. Type
ifconfig eth1 down
2. Stop the dhcpd service. In Primary server CLI type
service dhcpd stop

Note: Eth1 must be shut down first to prevent FortiNAC from successfully restarting the service automatically.

Primary Server attempts to restart the service. If the service does not start, 3 additional attempts are made. If the service remains stopped, the Primary Server triggers the failover. Refer to the Appendix for Log Output Examples.

Failover is complete once the appropriate Secondary Server(s) taking control display status **(Slave) Slave In Control Idle(false).**

Distributed Systems - Control Manager

a. Once the system has failed over, the Control Manager will lose communication with the Primary Server. At which point, it will attempt communication with the Secondary Server.
b. Once the Secondary Server control process is up, the Secondary starts responding to polls from the Manager.
c. Upon the next UI panel refresh, the **Server List** Dashboard panel should display the Secondary Server with a status of **Running – In Control**.

Note: Once a HA pair is added to the Server List, the Manager's endpoint license key file is copied to the Secondary Server during the initial failover event. For more information on License Distribution, refer to the **Deployment Guide** in the Fortinet Document Library.

4. Reconnect to the Administration UI of the Secondary Server/Control Server (use shared IP or name if L2 HA). Scroll to the **Summary** panel in the dashboard.

   L2 HA: Secondary Server that is now in control should display status **Running - In Control**.

   L3 HA: Secondary Server that is now in control should display status **Running - In Control**.

   If Control Server/Application Server pair, both Secondary Servers should display status **Running - In Control**.

5. Navigate to **System > Settings > System Management > License Management**. Verify the **License Name** and **Concurrent Licenses** number matches the Primary Server.

6. Verify the following:
    - TEST container created in Topology appears. This is a simple method to verify database replication.
    - If control has been configured, test enforcement - Rogue host is isolated and can register via normal means (Captive Portal, Persistent Agent, etc)

Resume Control

Once testing with the Secondary Server(s) has completed, restore control to the Primary Server(s).

1. Reconnect the eth0 interface of the Primary Server (if disconnected). And verify the default gateway for eth0 is pingable (if not, resume will fail).

2. In Administration UI, click the **Resume Control** button in the **Summary** Dashboard panel. This will take several minutes to complete.

3. Look for the following lines to appear to verify resume has completed:
   Primary Servers: **(Master) Master In Control Idle(false)**
   Secondary Servers: **(Slave) Master In Control Idle(false)**

4. Reconnect to the Administration UI using IP address of the Primary Control Server (use shared IP if L2 HA). Scroll to the **Summary** panel in the dashboard and verify appliance status.
   Primary Servers should display status **Running - In Control**.
   Secondary Servers should display status **Running - Not In Control**.

If assistance is needed contact FortiNAC Support.

Troubleshooting

Note: Prior to configuring High Availability, ensure that all appliances are able to communicate via SSH (i.e. firewall is not blocking communication).

Use these troubleshooting tips to:

- Determine which appliance has the shared IP address (Layer 2 HA only).
- Verify whether the license key is configured for High Availability.

Determine Which Appliance Has the Shared IP (Layer 2 HA)

Enter **ip addr sh dev eth0** at the command prompt and look at the output to determine which eth0 interface has the Shared IP Address (eth0 of the primary or eth0 of the secondary). In the belowexample, the Shared IP Address is 192.168.8.25. The eth0 on the primary has the Shared IP Address.

Primary Server

```
> ip addr sh dev eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP
qlen 1000
    link/ether 00:50:56:ac:2e:82 brd ff:ff:ff:ff:ff:ff
    inet 192.168.8.23/24 brd 192.168.8.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet 192.168.8.25/24 scope global secondary eth0  ← Shared IP
       valid_lft forever preferred_lft forever
```

Secondary Server

```
> ip addr sh dev eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP
qlen 1000
    link/ether 00:50:56:ac:08:4e brd ff:ff:ff:ff:ff:ff
    inet 192.168.8.26/24 brd 192.168.8.255 scope global eth0
       valid_lft forever preferred_lft forever
```

Shared IP Missing After Network Service Restart

Shared IP association to eth0 is not persistent through network service restarts on the appliance in control. Example after running "service network restart" on the Primary Server:

```
> ip addr sh dev eth0
2: eth0: <BROADCAST,MULTICAST,UP,10000> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:30:48:f9:9e:b6 brd ff:ff:ff:ff:ff:ff
    inet 10.1.1.208/16 brd 10.1.255.255 scope global eth0
    inet6 fe80::230:48ff:fef9:9eb6/64 scope link
       valid_lft forever preferred_lft forever
```

If network services are restarted on the appliance in control, re-add the Shared IP.

Re-Add Shared IP Address

Use one of the options below to re-add the Shared IP address.

Option 1 (Does not require a restart of FortiNAC services)

Login to the CLI as root of the appliance in control and type
hsIP ADD <Virtual IP address> <mask CIDR format> eth0
Example:

```
> hsIP ADD 192.168.8.25 24 eth0
```

Option 2: Restart FortiNAC services on the appliance in control

Login to the appliance CLI as root and type
shutdownNAC

<wait 30 seconds>

startupNAC

Option 3: Reboot Appliance via UI

1. In the Administration UI, navigate to **System > Settings > System Management > Power Management**.
2. Select the appliance in control and click **Reboot**.

Verify Shared IP
Confirm the Shared IP entry has been re-added to eth0 via the CLI. Type
ip addr sh dev eth0

Example:

```
> ip addr sh dev eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP
qlen 1000
    link/ether 00:50:56:ac:2e:82 brd ff:ff:ff:ff:ff:ff
    inet 192.168.8.23/24 brd 192.168.8.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet 192.168.8.25/24 scope global secondary eth0  ← Shared IP
       valid_lft forever preferred_lft forever
```

Verify License Key Configuration

Hot Standby Functionality

The license key on both the Primary and Secondary appliances must be configured to be High Availability capable. The High Availability feature is included in BASE, PLUS and PRO licenses.

In the FortiNAC Server/Control Server command prompt, enter the following:
DumpKey

Look for Plugins: **Hot-Standby-Capable**

License Entitlements

The license can be verified using the command **licensetool**.

Example:

```
> licensetool
EFFECTIVE:
serial = xxxxx
type = NetworkControlApplicationServer
level = PRO
count = 100000
expiration = 31622400000
expired = false
mac = 00:50:56:98:34:73
uuid = 4218e64a-d8f1-39e3-471f-46e2c5f027df
certificates = [xxxx]
```

```
> licensetool
EFFECTIVE:
serial = xxxxxx
type = NetworkControlApplicationServer
level = PRO
count = 2000
expiration = 31622400000
expired = false
mac = 00:50:56:98:5E:B3
uuid = 4218c883-093b-5e28-f895-bee88bc3202d
certificates = [xxxx]
```

To view both Primary and Secondary Server licenses at once, login to the Secondary Server CLI and type
licensetool -key APPLIANCE -key PRIMARY

Example (Output of system with Primary Server in control):

```
> licensetool -key EFFECTIVE -key APPLIANCE -key PRIMARY -key MANAGER
EFFECTIVE:      <--- Key of server in control (Primary Server)
serial = xxxxx
type = NetworkControlApplicationServer
level = PRO
count = 100000
expiration = 31622400000
expired = false
mac = 00:50:56:98:34:73
uuid = 4218e64a-d8f1-39e3-471f-46e2c5f027df
certificates = [xxxx]


APPLIANCE:   <--- Secondary Server
serial = xxxxxx
type = NetworkControlApplicationServer
level = PRO
count = 100000
expiration = 31622400000
expired = false
mac = 00:50:56:98:5E:B3
uuid = 4218c883-093b-5e28-f895-bee88bc3202d
certificates = [xxxx]


PRIMARY:    <--- Primary Server
serial = xxxxx
type = NetworkControlApplicationServer
level = PRO
count = 100000
expiration = 31622400000
expired = false
mac = 00:50:56:98:34:73
uuid = 4218e64a-d8f1-39e3-471f-46e2c5f027df
certificates = [xxxx]
```

Validating Processes – CLI

CampusManager - Management Process that runs on all appliances regardless of control status.
Yams - Loader that runs when the appliance status is "Running - In Control."

To verify if these processes are running, use the "jps" command.

FortiNAC Server

```
> jps
3828 Yams
2885 CampusManager
4055 Yams
7976 Jps
1400 TomcatAdmin
1548 TomcatPortal
```

FortiNAC Control Server

```
> jps
12131 Yams
14387 jar
12874 TomcatAdmin
8491 Jps
3103 CampusManager
```

FortiNAC Application Server

```
> jps
2371 TomcatPortal
5893 Jps
3305 CampusManager
30463 Yams
```

Login to each appliance as root and type
tail –F /bsc/logs/output.processManager | grep "In Control Idle"

The following message indicates Primary is in control:
Primary Server: **(Master) Master In Control Idle(false)**
Secondary Server: **(Slave) Master In Control Idle(false)**

High Availability Concepts

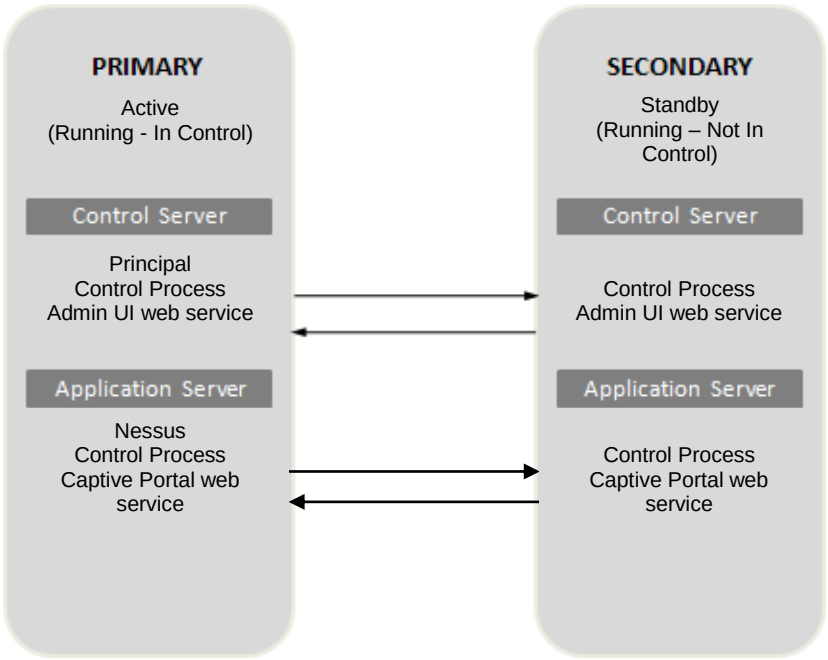
High Availability operations include:

- Primary and Secondary Server communication
- Startup procedures
- Change of Control sequences

The combination of these processes monitor the state of the Primary and Secondary Servers, and execute the steps necessary for the activating the backup when necessary.

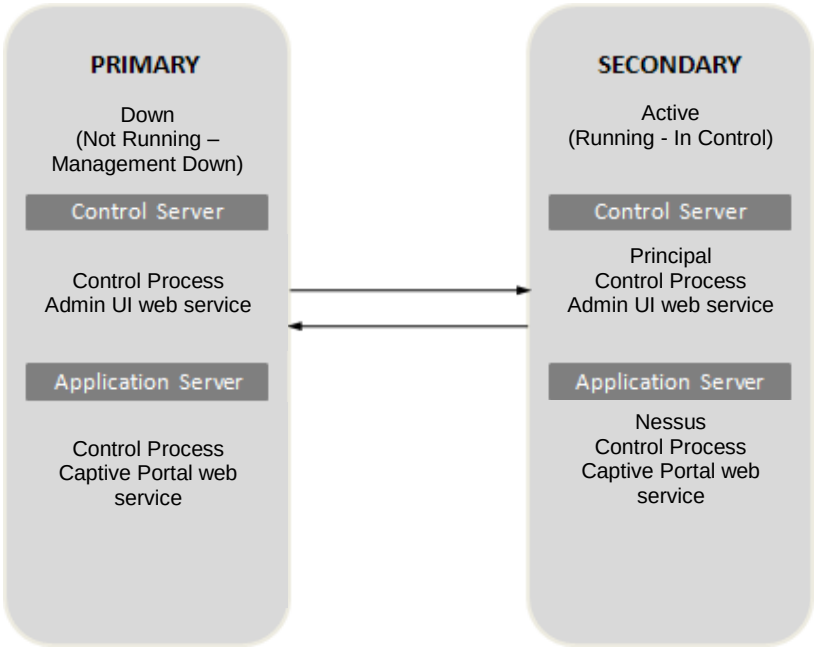
"Normal" Control Status

During normal operation, the Primary Server is in control while the Secondary Server is in standby. The Primary and Secondary Servers communicate with each other to ensure they are functioning normally. The Management Process is running on all servers, but the loaders (Principal, Nessus or Control Manager) only run on the Primary Servers.

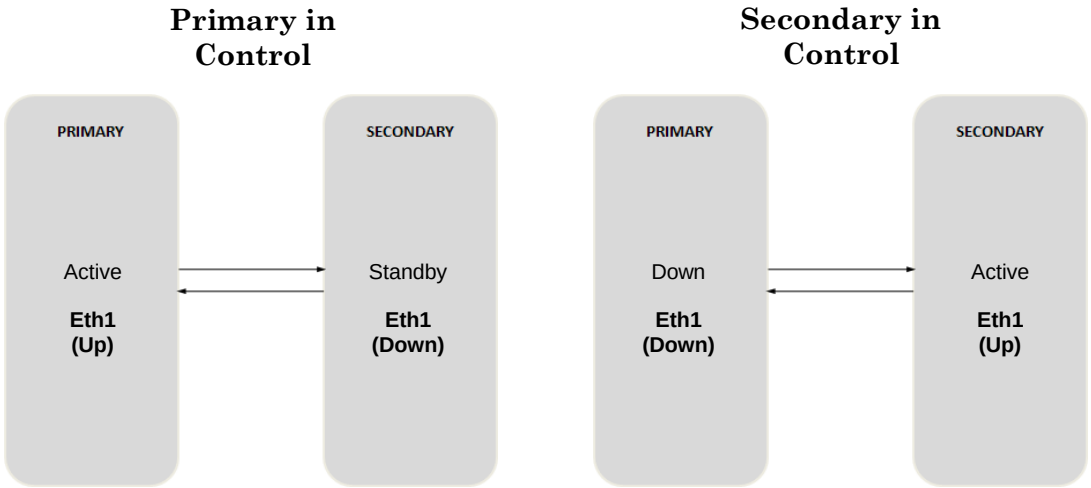


Failover Control Status

When a failover is triggered, the loader(s) start on the Secondary Server. In most cases, the loader(s) on the Primary Server stop. For more details on the failover process and the scenarios that can trigger it, see section Control Sequence.



Note: In L2 HA configurations, both primary and secondary eth1 interfaces are configured with the same IP addresses. Therefore, in order to prevent duplicate IP addresses on the network, eth1 is disabled on the FortiNAC Server/Application Server that is not in control.



Startup High Availability

Primary Server Startup Process

1. The management process starts up.
2. The status of the Secondary Server is checked.
3. If the secondary is **in control**, the secondary retains control until a manual recovery is performed to return control to the Primary Server. See section Recovery.
4. If the secondary is **not in control**, the startup of the primary continues and the primary is in control.

Note: If any of the following processes do not start, the appliance is not in control: httpd, dhcpd, named, mysqld, SSHd, TomcatAdmin and TomcatPortal. If any of these processes fail, then failover from primary to secondary is started.

Secondary Server Startup Process

1. The management process starts up.
2. The status of the Primary Server is checked.
3. If the primary is **in control**, database replication is started. Other processes are not started on the secondary.
4. If the primary is **not in control** and the secondary is not idle then the startup of the secondary continues.
5. The secondary remains in control until a manual recovery is performed that returns control to the Primary Server.

Management Process

The Management process starts when the appliance is booted up or by running the following command:
startupNAC

If the appliance is in control the appropriate processes are started.

Note: If any of the following processes does not start, the appliance is not in control: httpd, dhcpd, named, mysqld, SSHd, TomcatAdmin and TomcatPortal. If any of these processes fail, then failover from primary to secondary is started.

Control Sequence

Required Processes

In a High Availability environment, the primary fails over to the secondary when certain processes don't start or fail while running. If any process listed in the table below fails on the primary, then the secondary attempts to take control. Depending on the appliance and platform being used, different processes are required. See the table below for additional information.

Important: FortiNAC Server appliances to be set up for High Availability must have eth1 configured. If eth1 is not present or disabled, some of the required processes in the chart below will not start. This will prevent the High Availability configuration from completing. Should eth1 be removed, disabled or not present on the primary, the primary will not remain in control.

Required Process	FortiNAC Control Manager	FortiNAC Control Server	FortiNAC Application Server	FortiNAC Server
mysql	X	X		X
SSHd	X	X	X	X
dhcpd			X	X
httpd			X	X
named			X	X
tomcat-admin	X	X		X
tomcat-portal			X	X

Determining Whether the Secondary Needs to Take Control

The Secondary Server polls the status of the Primary Server every 30 seconds to determine whether the primary is still in control. If the secondary does not receive a response from a poll, it will re-attempt to communicate 5 additional times (every 30 seconds) by default.

The messaging in the output.processManager is similar to the entries below, where "Ping retval = null" indicate the Primary Server did not respond to the poll.

```
sendPacket() <Primary Server IP> verb Ping retval = Running - In Control
sendPacket() <Primary Server IP> verb Ping retval = Running - In Control
sendPacket() <Primary Server IP> verb Ping retval = Running - In Control
sendPacket() <Primary Server IP> verb Ping retval = null
**** Failed to talk to master **** PingRetryCnt = 1 pingRetries = 5
**** Failed to talk to master **** PingRetryCnt = 2 pingRetries = 5
**** Failed to talk to master **** PingRetryCnt = 3 pingRetries = 5
**** Failed to talk to master **** PingRetryCnt = 4 pingRetries = 5
**** Failed to talk to master **** PingRetryCnt = 5 pingRetries = 5
**** Failed to talk to master **** PingRetryCnt exceeded!
```

If the secondary does not receive a response, the secondary pings the "Secondary Appliance Gateway IP Address" configured in the High Availability Tab. See section Primary And Secondary Server Configuration.

- If the gateway is reachable, the secondary takes control, since the primary is assumed to be isolated from the network. If, however, the Secondary Server's Management Process has been running for less than 10 minutes, the secondary waits 10 minutes for any further communication from the primary. If still no response, the secondary takes control.
- If the gateway is not reachable, the secondary will not take control since the secondary is assumed to be isolated from the network and the primary could be functioning properly.

Important: If the secondary is Idle, it does not take control. For example, the secondary can be set to Idle when Reboot and Shutdown commands are run on the primary.

The number of ping retries can be modified from the default of 5 attempts. For detail, see Modify Ping Retry Count in the Appendix.

Failover Scenarios Due to Network Communication Issues

There are situations when portions of the network may fail, preventing communication between the Primary and Secondary Servers. In those cases, the resulting failover behavior can vary. The following scenarios have been observed to occur predominantly in Layer 3 High Availability (HA) configurations. Note that these scenarios are also possible in Layer 2 HA configurations, but less likely to occur.

Scenario 1: Servers Fail to Communicate - Gateways Reachable

- All FortiNAC processes are functioning normal on primary and secondary.
- Primary and secondary are communicating to their defined gateways.
- The network is basically functioning but communications between just the primary and secondary are down.

Scenario 1 Failover Behavior:

1. Primary stays active. Loader(s) remain running.
2. Secondary becomes active and starts its loader(s). **Both FortiNAC Control Servers are now running.**
3. After restoring the network communication between primary and secondary, the primary loader(s) immediately shut down. Secondary Server remains active.

Scenario 2: Servers Fail to Communicate – Primary's Gateway Unreachable

- All FortiNAC processes are functioning normal on primary and secondary.
- The network is basically functioning but communications between primary and secondary are down.
- Primary's network communication to its defined gateway is also down.

Scenario 2 Failover Behavior:

1. Primary stays active. Loader(s) remain running.
2. Secondary becomes active and starts its loader(s). **Both FortiNAC Control Servers are now running.**
3. After restoring the network communication between primary and secondary, the primary loader(s) immediately shut down. Secondary Server remains active.

Scenario 3: Servers Fail to Communicate – Secondary's Gateway Unreachable

- All FortiNAC processes are functioning normal on primary and secondary.
- The network is basically functioning but communications between primary and secondary are down.
- Secondary's communication to its defined gateway is also down.

Scenario 3 Failover Behavior:

1. Primary stays active. Loader(s) remain running.
2. The secondary goes through the failure routine but does NOT start the loader(s).
3. After restoring the network communication between the primary, secondary and gateway:
    - Primary remains active.
    - Secondary returns to a 'not in control' mode.
    - Database replication is restarted on the secondary.

Configuration Considerations

To prevent scenarios where both servers are running when a wide area network failure occurs, the following can be used when configuring High Availability:

Primary Appliance Gateway IP Address: the actual network gateway of the *secondary* system.
Secondary Appliance Gateway IP Address: the actual network gateway of the *primary* system.

With this configuration, if there is a wide area network failure, the secondary will fail to reach both the gateway and primary (as in scenario 3) and the secondary loader(s) will not start.

Recovery

If High Availability (HA) has been implemented and a failover has occurred, correct the reason for the failover. Once corrected, resume control of the Primary Server(s).

Important: Resuming control is not an automatic process and must be done manually

Restart The Primary Server

Under normal operation, the **Resume Control** button on the Dashboard Summary panel is grayed out. Once a failover has occurred, this button becomes "hot". Use the **Resume Control** button to initiate the process of transitioning control from the Secondary Server(s) back to the Primary Server(s). For FortiNAC Server, FortiNAC Control Server and FortiNAC Control Manager appliances, the database is also copied.

Control Server and Application Server pairs in a Layer 2 HA configuration failover individually, and therefore, control is resumed individually. Two **Resume Control** buttons will be displayed (Primary Control Server and Primary Application Server).

Control Server and Application Server pairs in a Layer 3 HA configuration will failover as a pair, and therefore, control is resumed as a pair. When the **Resume Control** button is clicked, the process of transitioning control starts for both servers.

Note: If for any reason the database was not replicated correctly on the secondary before failover, the recovery process gives the option of retaining the older database located on the primary.

1. Navigate to **Bookmarks > Dashboard**.
2. Scroll to the **Summary** panel.
3. Click the **Resume Control** button for the server that should resume control.
4. The Primary Server restarts. Database and configuration files are copied from the secondary to the primary. Processes are started on the primary. Then the Secondary Server relinquishes control.

Note: If for any reason the database was not replicated correctly on the secondary before failover, the recovery process gives the option of retaining the older database located on the primary. To restart the primary via CLI, see CLI Control Scripts.

Appendix

Control/Application Server Pair IP Addressing

Layer 2

1. Shared IP Address for Control Server
2. Shared IP Address for Application Server
3. Primary Control Server eth0
4. Primary Application Server eth0
5. Primary Application Server eth1 (including isolation interface IP's)
6. Secondary Control Server eth0
7. Secondary Application Server eth0
8. Secondary Application Server eth1 (use same isolation interface IP's as Primary eth1)

Example
Shared IP Address for Control Server: 192.168.00.4/24
Primary Control Server eth0: 192.168.00.2/24
Primary Application Server eth0: 192.168.00.3/24
Primary Application Server eth1 Registration: 192.168.200.20/28
Primary Application Server eth1 Remediation: 192.168.200.21/28
Primary Application Server eth1 DeadEnd: 192.168.200.22/28

Shared IP Address for Application Server: 192.168.00.7/24
Secondary Control Server eth0: 192.168.00.5/24
Secondary Application Server eth0: 192.168.00.6/24
Secondary Application Server eth1 Registration: 192.168.200.20/28
Secondary Application Server eth1 Remediation: 192.168.200.21/28
Secondary Application Server eth1 DeadEnd: 192.168.200.22/28

Layer 3

1. Primary Control Server eth0
2. Primary Application Server eth0
3. Primary Application Server eth1 (including isolation interface IP's)
4. Secondary Control Server eth0 (different subnet than Primary eth0)
5. Secondary Application Server eth0 (different subnet than Primary eth0)
6. Secondary Application Server eth1 (different subnet than Primary eth1)

Example
Primary Control Server eth0: 192.168.00.2/24
Primary Application Server eth0: 192.168.00.3/24
Primary Application Server eth1 Registration: 192.168.200.20/28
Primary Application Server eth1 Remediation: 192.168.200.21/28
Primary Application Server eth1 DeadEnd: 192.168.200.22/28

Secondary Control Server eth0: 192.168.10.2/24
Secondary Application Server eth0: 192.168.10.3/24
Secondary Application Server eth1 Registration: 192.168.230.20/28
Secondary Application Server eth1 Remediation: 192.168.230.21/28
Secondary Application Server eth1 DeadEnd: 192.168.230.22/28

Connectivity Configuration

To access the Admin user interface that is available through a web browser, the appliances use the "nac" alias to identify which IP Address/hostname will be allowed in the URL.

In High Availability configurations, entries for the "nac" alias are entered automatically in the **/etc/hosts** file for the FortiNAC Server appliances. Each of the appliances in the High Availability configuration must be resolvable in the DNS.

Consider the following for the nac alias:

1. If the appliance is a FortiNAC Control Manager there should be no nac alias entry in the /etc/hosts file. Use either the shared or individual IP address to access this server.

2. If the High Availability appliances are being managed by the FortiNAC Control Manager, verify that none of the appliances have an entry for nac alias in the /etc/hosts file. Using nac alias in this configuration would stop the FortiNAC Control Manager from accessing the appliances it manages. To access the managed appliances, use either the direct or shared IP address.

3. If the High Availability appliances are not being managed by the FortiNAC Control Manager use these guidelines:
    - If the appliance is a FortiNAC Server, verify that the nac alias is mapped to the shared IP address. Use the shared IP address (or shared host name) in the URL.
    - If the appliance is the FortiNAC Control Server or FortiNAC Control Manager, verify that the nac alias has been removed from the **/etc/hosts** file and use the shared or the individual IP addresses (or host names) in the URL.

Note: The "nac" alias must not be included in DNS. For example, do not use an alias like "nac.abc.def.com" anywhere in DNS.

Access Secondary Server Wizard Post HA Configuration

In order to access configWizard on the Secondary Server, use the physical IP address/host name of the Secondary Server (not the Virtual IP or name if L2 HA configuration).

Example:
`https://oak2.bradfordnetworks.com:8443/configWizard/`

In older versions of FortiNAC, the Secondary Server IP address or host name may not respond to HTTP/HTTPS requests by default in a L2 HA configuration. If unable to reach the secondary via HTTP/HTTPS, review the Secondary Server's **/etc/hosts** file. If the /etc/hosts file has the "nac" entry on the same line as the VIP:

```
192.168.8.25    oak.bradfordnetworks.com        oak cm nac
```

Then it will be necessary to modify the file in order to access the Secondary Server.

Modifying Hosts file for Secondary Server HTTP/HTTPS Access in L2 HA

1. In the CLI of the Secondary Server, edit **/etc/hosts**.
2. Locate the line containing the "nac" entry. This should be the line with the virtual IP address.
3. Remove "nac" from the line and save.
4. Restart tomcat-admin service:
   service tomcat-admin restart
5. Connect on the Secondary Server via configWizard using actual eth0 IP.

Note: Once configWizard has been run, the /etc/hosts file will be restored automatically.

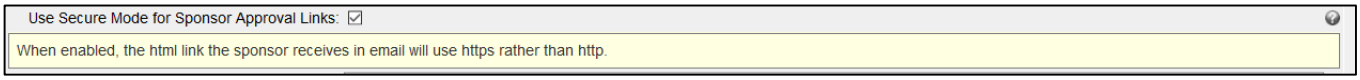
Sponsor Approval Email Links

In Guest Manager when Self Registration Requests are sent to sponsors, the email messages contain links for the sponsor to either automatically accept/deny the request, or to login to the Admin UI to do this. The default links provided use non-secure http access. If using an SSL certificate to secure the FortiNAC Admin UI and access to http for Admin Users is blocked, these links must use https.

Configure Links for HTTPS

Note: Applies to versions 8.6.x and lower.

1. Navigate to **System > Portal Configuration**
2. Enable **Use Secure Mode for Sponsor Approval Links** in the Self-Registration Login page.



Embed Server FQDN

The link contained in the email is composed by FortiNAC. The link contains the URL of the FortiNAC Server or Control Server. In a High Availability environment with an L3 configuration where redundant FortiNAC servers do not use a shared IP address, the URL should contain the FQDN of the correct FortiNAC Server or Control Server. Typically, FortiNAC can determine the FQDN, however if there is an issue, the FQDN can be configured.

To configure FortiNAC to use the FQDN of the server in the email links, a property file must be modified on the FortiNAC Server. Modify the property file as follows on both Primary and Secondary Servers:

1. Log into the CLI as root on your FortiNAC Server or Control Server.
2. Navigate to the following directory:
   /bsc/campusMgr/master_loader/
3. Using vi or another editor, open the **.masterPropertyFile** file.
4. At the top of the file there is a sample entry that is commented out. Follow the syntax of the sample entry to create your own changes using one of the following examples:

FQDN for Links Using HTTPS (Port 8443)
To configure email links to use the FQDN of the FortiNAC Server or Control Server and use https and port 8443 add the information to the EmailLink Host property.

```
FILE_NAME=./properties_plugin/selfRegRequest.properties
{
com.bsc.plugin.guest.SelfRegRequestServer.EmailLinkHost=
https://mySpecialHost.Fortinetnetworks.com:8443
}
```

FQDN for Links Using HTTP (Port 8080)
To configure email links to use the FQDN of the FortiNAC Server or Control Server add the information to the EmailLinkHost property.

```
FILE_NAME=./properties_plugin/selfRegRequest.properties
{
com.bsc.plugin.guest.SelfRegRequestServer.EmailLinkHost=
http://mySpecialHost.Fortinetnetworks.com:8080
}
```

5. Save the changes to the file.

6. Restart the FortiNAC Server.
   shutdownNAC

   <wait 30 seconds>

   startupNAC

   When the server restarts, the changes listed in the **.masterPropertyFile** are written to the **selfRegRequest.properties** file.

Verify:

1. Log into the CLI of the FortiNAC Server or Control Server and navigate to the following directory:
   /bsc/campusMgr/master_loader/properties_plugin/

2. View the contents of **selfRegRequest.properties** and verify that the changes have been written to the file. At the prompt type
   cat selfRegRequest.properties

Stopping and Restarting Processes

What Happens When Processes are Stopped

When the **shutdownNAC** command is run on the appliance in control, the following occurs:

- If Primary Server(s) are in control, the management process sets the secondary state to "Idle." This prevents a failover from occurring.
- The loaders are stopped on the appliance in control. In a Control/Application Server pair, when the loaders are stopped on the Control Server, the loaders are also stopped on the Application Server in control.
- FortiNAC does not switch VLANs, serve Captive Portal pages or respond to RADIUS requests.
- In L2 HA configurations, the Virtual IP address stops responding.
- Primary and Secondary Server eth0 IP addresses are still reachable via normal means (e.g. ICMP, SSH, etc).

The **shutdownNAC -kill** command stops the Management Process on the appliance the command is run.

Important: Running **shutdownNAC -kill** on the primary without running **shutdownNAC** first will cause a failover.

Procedures

Restart Processes without Causing Failover

Used for routine maintenance and quick restart.
Important: For L2 HA configurations, do not use the Virtual IP for connecting to CLI.

1. SSH as root to the Primary Control Server or Primary Control/Application Server and type
   shutdownNAC
2. Type
   jps
   (use the jps command until you no longer see any "Yams" process running, this could take 10 - 30 seconds)
3. Start back up the loaders. Type
   startupNAC

Note: The startup could take anywhere between roughly 5-10 minutes. Suggest waiting that long before attempting to access the Administrative UI.

Stopping All Processes (FortiNAC Servers e.g NS500/550/600/700)

Stop processes in order to:

- Restart management processes
- Reboot or power down appliances

Important: For L2 HA configurations, do not use the Virtual IP for connecting to CLI.

1. SSH as root to the Primary Server and type
   shutdownNAC
2. Type
   jps
   (use the jps command until you no longer see any "Yams" process running, this could take 10 - 30 seconds)
3. Type
   shutdownNAC -kill
4. SSH as root to the Secondary Server and type
   shutdownNAC -kill

Option1: Restart Management Processes

1. In Primary Server CLI type
   startupNAC
2. Wait until the Primary Server is up and running (by confirming you have Administration UI access).
   Note: The startup could take anywhere between roughly 5-10 minutes. Suggest waiting that long before attempting to access the Administrative UI.
3. Once Primary is running, in Secondary Server CLI type
   startupNAC

   Note: The Administration UI will display "Processes are Down" unless the appliance is in control.

Option 2: Reboot Appliances

1. In Primary Server CLI type
   reboot
2. Wait until the Primary Server is up and running (by confirming you have SSH access and Admin UI access).
   Note: The startup could take anywhere between roughly 5-10 minutes. Suggest waiting that long before attempting to access the Administrative UI.
3. Once Primary is running, in Secondary Server CLI type
   reboot

Option 3: Power Down Appliances

1. Shutdown and halt the system. In both Primary and Secondary Server CLI type
   shutdown -h now
2. Power down the appliance.

- Virtual machines: select the server from the list and click the Power Off button. This process may take 30 seconds.
- Physical appliances: push the power button.

Stopping All Processes (FortiNAC Control Server/Application Server Pair)

Stop processes in order to:

- Restart management processes
- Reboot or power down appliances

Important: For L2 HA configurations, do not use the Virtual IP for access to the CLI.

1. SSH as root to the Primary Control Server and type
   shutdownNAC
2. Type
   jps
   (use the jps command until you no longer see any "Yams" process running, this could take 10 - 30 seconds)
3. Type
   shutdownNAC -kill
4. SSH as root to the Primary Application Server and type
   jps
   (use the jps command to validate there are no "Yams" process running.)
5. Type
   shutdownNAC –kill
6. Repeat steps 4-5 for Secondary Control and Primary and Secondary Application Servers.

Option 1: Restart Management Processes

1. In the Primary Control Server CLI type
   startupNAC
2. Wait until the Primary Control and Application Servers are up and running by confirming Admin UI access.
   Note: The startup could take anywhere between roughly 5-10 minutes. Suggest waiting that long before attempting to access the Administrative UI.
3. In Secondary Application Server CLI type
   reboot
4. Wait 30 seconds
5. In the Secondary Control Server CLI type
   startupNAC

   Note: The Administration UI will display “Processes are Down” unless the appliance is in control.

Option 2: Reboot Appliances

1. In Primary Application Server CLI type
   reboot
2. Wait 30 seconds
3. In the Primary Control Server CLI type
   reboot
4. Wait until the Primary Control Server is up and running (by confirming you have SSH access and Admin UI access).
   Note: The startup could take anywhere between roughly 5-10 minutes. Suggest waiting that long before attempting to access the Administrative UI.
5. In Secondary Application Server CLI type
   reboot
6. Wait 30 seconds
7. In the Secondary Control Server CLI type
   reboot

   Note: The Administration UI will display "Processes are Down" unless the appliance is in control.

Option 3: Power Down Appliances

1. Shutdown and halt the system. In both Primary and Secondary Server(s) CLI type
   shutdown -h now
2. Power down the appliance.
   - Virtual machines: select the server from the list and click the Power Off button. This process may take 30 seconds.
   - Physical appliances: push the power button.

Alarms and Events

Process Down Events

FortiNAC generates events and alarms whenever any of the required processes fails or does not start as expected. FortiNAC tries to restart the process every 30 seconds. In a High Availability environment failover occurs after the fourth failed restart attempt. These events are enabled by default and each event has a corresponding alarm.

In the Event View, event messages for failed processes include the name of the process and the IP address of the machine where the process failed. For example, if the **named** process failed you would see the following message associated with the event.

```
A critical service (/bsc/services/named/sbin/named) on 192.168.5.228
was not running.
```

Events for failed processes include:
Service Down - Tomcat Admin
Service Down - Tomcat Portal
Service Down - dhcpd
Service Down - httpd
Service Down - mysqld
Service Down - named
Service Down - SSHd

Process Started Events

FortiNAC generates events whenever any of the required processes is started. These events are enabled by default and each event has a corresponding alarm. Alarms for process started events are not typically enabled. They can be enabled manually using Alarm Mappings.

In the Event View, event messages for started processes include the name of the process and the IP address of the machine where the process started. For example, if the **named** process started you would see the following message associated with the event.

```
A critical service (/bsc/services/named/sbin/named) on 192.168.5.228
was not running and has been  started.
```

Events for started processes include:
Service Started - Tomcat Admin
Service Started - Tomcat Portal
Service Started - dhcpd
Service Started - httpd
Service Started - mysqld
Service Started - named
Service Started - SSHd

Other High Availability Events

Important: These events are not generated for the FortiNAC Control Manager.

An Event appears in the Events view and can have an alarm configured to send email to you when it occurs.

Database Replication Error - This event is generated if the database on the secondary appliance is not replicating.
System Failover - This event is generated when a failover occurs.

Modify Ping Retry Count

The Secondary Server polls the status of the Primary Server every 30 seconds to determine whether the primary is still in control. If the secondary does not receive a response from a poll, it will re-attempt to communicate 5 additional times (every 30 seconds) by default. The Ping Retry Count defines the number of re-attempts FortiNAC makes after the first poll failure.

The Ping Retry Count can be modified to a higher or lower number. Setting the value lower will cause the Secondary Server to wait fewer ping retries before executing the failover process. Depending on where the failure occurs in the 30 second poll cycle, a failover minimum time is somewhere between 31 and 60 seconds when the Ping Retry Count = 1.

Important: Care should be taken when modifying this value. Setting the value too low can cause an unnecessary failover. Consider the following when determining how low to change the count:

- A brief interruption of communication (like a restart of network equipment for maintenance purposes) between the appliances
- Intermittent ping loss due to the bandwidth between appliances
- Rebooting the FortiNAC Primary Server

The Ping Retry Count should be high enough to allow for the above conditions to occur without triggering a failover. In order to determine if there is intermittent ping loss, a review of the Secondary Server **/bsc/logs/output.processManager** log for failed ping attempts should be done prior to the change.

Example:

```
**** Failed to talk to master **** PingRetryCnt = 1 pingRetries = 5
**** Failed to talk to master **** PingRetryCnt = 2 pingRetries = 5
```

Contact Support for assistance.

Procedure

1. Login as root to the Secondary Server CLI
2. Modify **/bsc/campusMgr/bin/.networkConfig**
3. Add the following line:
   PingRetries=x

   Where "x" is the number of desired retries. The default value is 5.

Example:

```
NetworkApplicationServerPrimary=192.168.8.24
yamsrc=/bsc/campusMgr/master_loader/.yamsrc
PrimaryServer=192.168.8.23
logFile=/bsc/logs/processManager/output.processManager
NetworkApplicationServerSecondary=192.168.8.27
NetworkControlServerSecondary=192.168.8.26
Status=1
Gateway=192.168.8.1
NetworkControlManagerPrimary=
Debug=true
NetworkControlServerPrimary=192.168.8.23
StandbyServer=192.168.8.26
NetworkControlManagerSecondary=
PingRetries=3
```

4. Save the file.

5. Restart management processes on the Secondary Server for the changes to take affect
   shutdownNAC –kill
   <wait 30 seconds>
   startupNAC

6. Test to verify failover occurs after x number of retries based upon the new value. See Failover Test.

   Example of entries printed in output.processManager log based upon new entry "PingRetries=3":

```
sendPacket() <Primary Server IP> verb Ping retval = null
**** Failed to talk to master **** PingRetryCnt = 1 pingRetries = 5
**** Failed to talk to master **** PingRetryCnt = 2 pingRetries = 5
**** Failed to talk to master **** PingRetryCnt = 3 pingRetries = 5
**** Failed to talk to master **** PingRetryCnt exceeded!
```

7. Resume control of the Primary Server.

8. Reboot FortiNAC Primary Server and verify a failover does not occur.

9. Restart an infrastructure device within the path between the Primary and Secondary Server and verify a failover does not occur.

10. If a failover occurs as a result of either step 8 or 9, increase the PingRetries value in .**networkConfig** and retest.

Remove High Availability Configuration

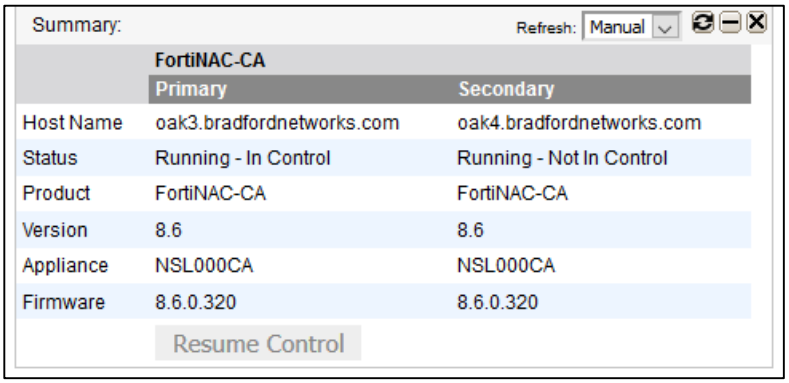
The following procedure removes the High Availability settings to enable the Primary and Secondary Servers to act independently of one another. The Primary Server will continue to manage the network, while the Secondary Server can be either shut down or moved to be used in a different configuration.

Considerations

- This procedure should be performed during a maintenance window.
- If managed by a Manager (FNAC-M-xx), endpoint licensing will be temporarily removed from the Primary Server.
- Both Primary and Secondary Servers are restarted during this procedure.
- A different License Key will be required if re-using the Secondary Server.
- The data stored in the Secondary Server's database (configurations made through the Administration UI and information regarding network infrastructure and endpoints) will be erased.
- The Secondary Server eth1 interface(s) will be disabled. Should the Secondary server be re-licensed, this prevents the server from potentially delivering incorrect DHCP addresses prior to proper configuration.
- This procedure *does not* change the following Secondary Server Configuration Wizard settings:
  - CLI and Configuration Wizard passwords
  - Interface eth0 settings

Configuration Removal Procedure

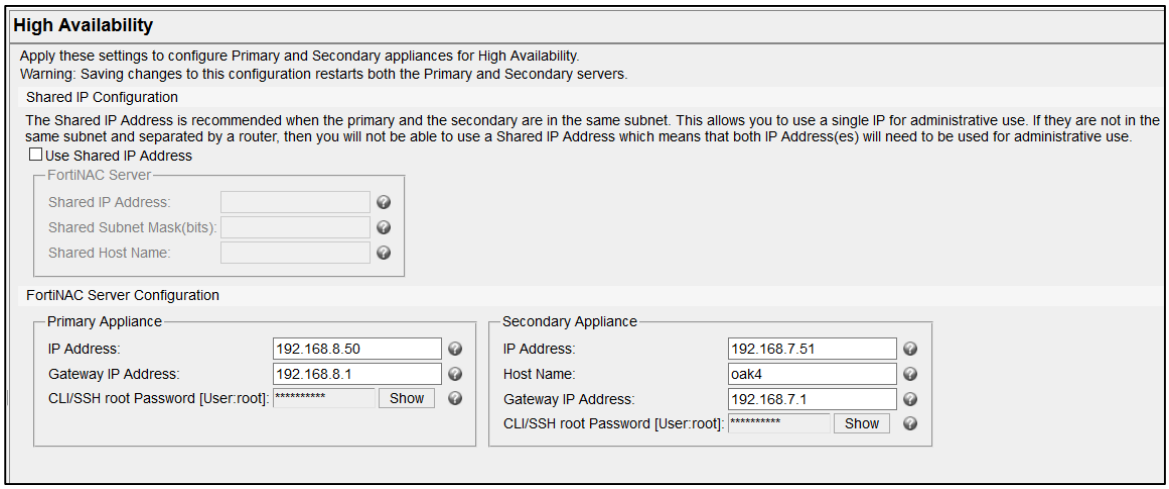
1. Login to the Administration UI and verify the Primary Server is in control by reviewing the **Summary** Dashboard panel. (This window can be left open). If Primary Server is not in control, *do not* proceed until control had been resumed to the Primary Server. Contact Support if assistance is required.



2. If High Availability pair is managed by a Manager (FNAC-M-xx), remove the Primary Server from the **Server List** Dashboard panel in the Manager UI. **Note:** This will remove the endpoint license from the Primary Server.

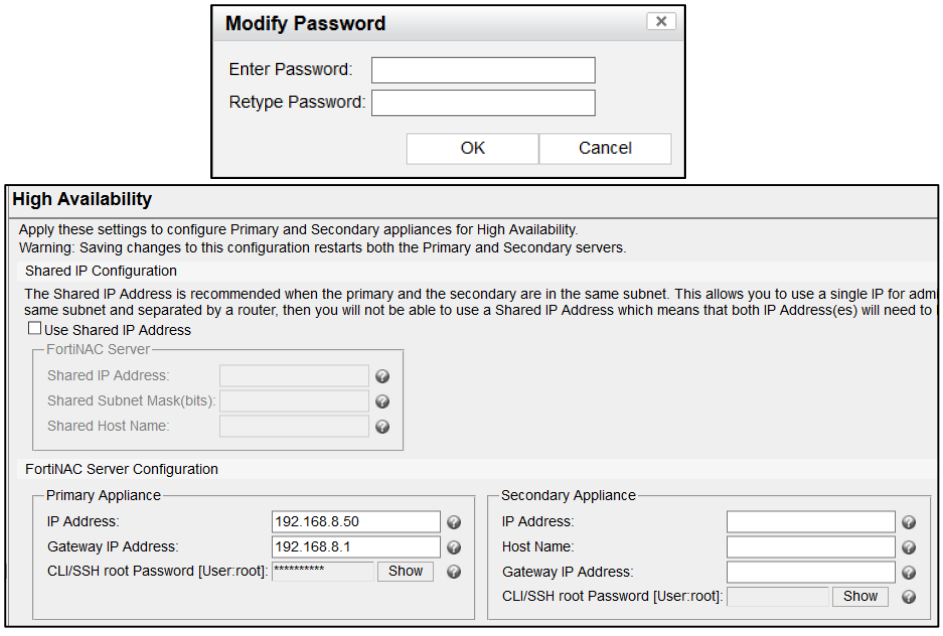
a. Login to the Manager Administration UI.
b. In the **Server List** Dashboard panel, click the **X** next to the Primary Server. Both the Primary and Secondary Servers will be removed from the list.

3. In the Primary Server Administration UI, navigate to **System > Settings > System Management > High Availability**



4. Clear the shared and Secondary Appliance information and leave the Primary Appliance information filled in. Make sure "Use Shared IP address" is de-selected.

5. Clear secondary password by clicking on the password (as if to modify), leave fields blank and click **OK**.

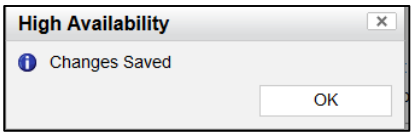


6. Click **Save Settings**.

The following message will appear:
Applying Settings. This could take a few minutes. Please wait.

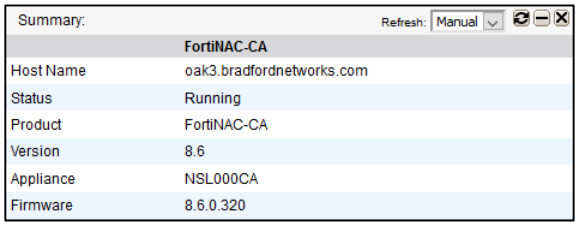
7. Click **Yes** to restart server when prompted.

8. Click **OK** again.

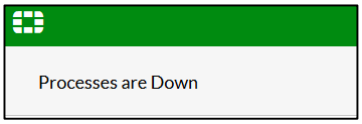


9. Wait several minutes to allow FortiNAC to restart management processes.

10. Login to the Primary Server UI. Verify only one server now displays in the Summary panel of the Dashboard. Logout.



11. Connect to the Secondary Server UI. The page should show processes are down.



Important: Do not reboot or restart processes on the Secondary Server until the following steps have been completed. These steps prevent the Secondary Server from attempting to control the network or serve DHCP addresses to isolated endpoints.

12. Login to the Secondary Server CLI as root.

13. Remove the license key file copied from the Primary Server.

    cd /bsc/campusMgr/

    rm .licenseKeyPrimary

14. If managed by a Manager (FNAC-M-xx), remove the license key copied from the Manager.

    rm .licenseKeyNCM

15. Shutdown management processes
    shutdownNAC -kill

16. Reinitialize the Secondary Server's current database. Type

    cd /bsc/campusMgr/master_loader/mysql

    ydb_initialize

17. When prompted to drop the 'bsc' database, enter "y".

    Example:

```
> ydb_initialize
  Dropping the database is potentially a very bad thing to do.
  Any data stored in the database will be destroyed.

  Do you really want to drop the 'bsc' database [y/N] y
  Database "bsc" dropped
```

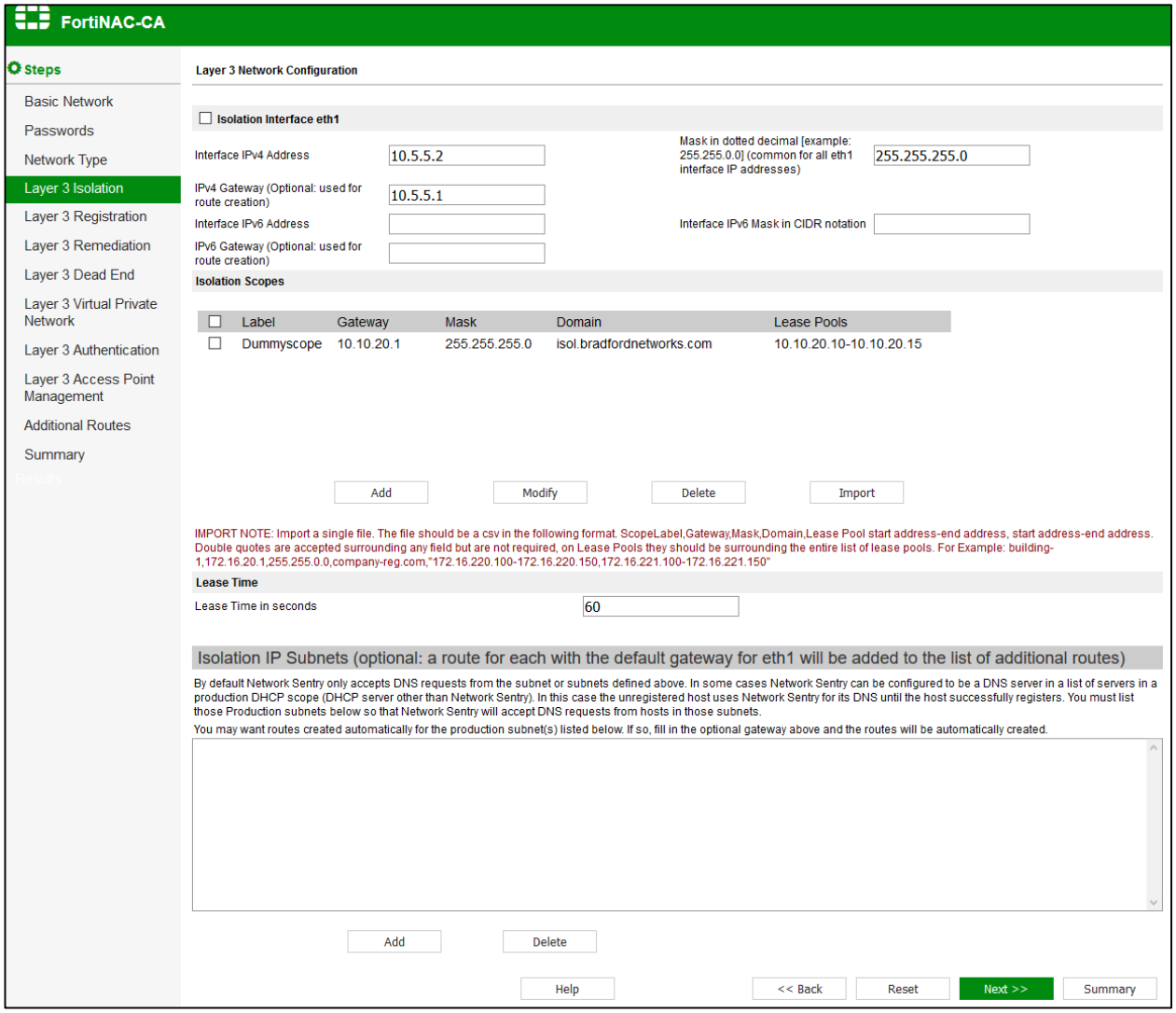
18. Logout of the CLI.

    logout

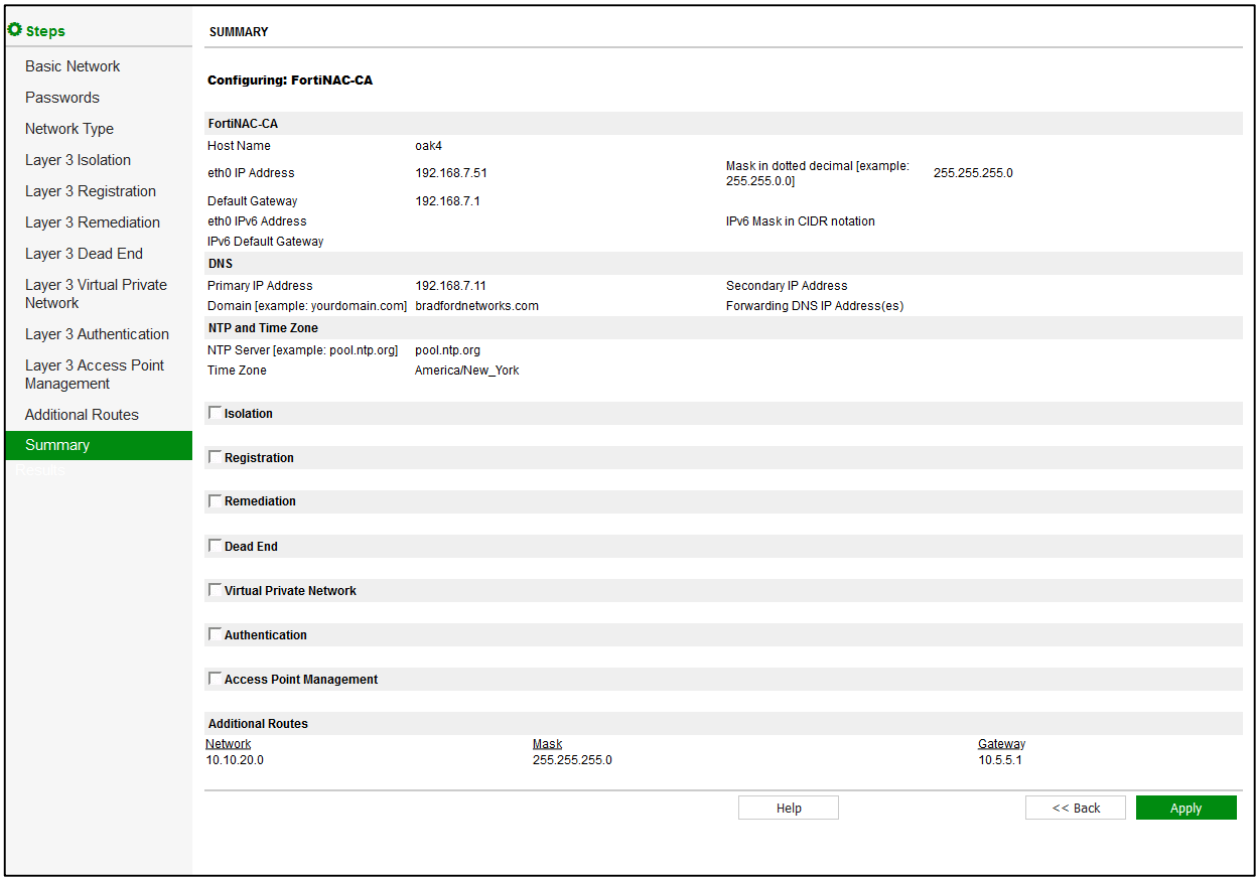
19. Login to the **Secondary** Server Configuration Wizard using the below URL:

    https://<*name or IP of Secondary Server*>:8443/configWizard/

20. Disable all eth1 interfaces by de-selecting the check box for each active interface (Isolation, Registration, etc.). The configuration can also be removed at this time.



21. Once changes are completed, click **Summary.** None of the eth1 interfaces should be selected.



22. Review changes then click **Apply**.

After a few moments, the Results will display.

Note: The following lines may be seen and are normal:

Warning: Line subnet BN_EMPTY_DHCP_IP netmask 255.255.255.0 { was not substituted in /etc/dhcp/dhcpd.conf.test due to a missing tag. If you are configuring in monitor mode this may not be an issue.

Warning: /etc/dhcp/dhcpd.conf.test was not written in full due to a missing tag in empty scope. If you are configuring in monitor mode this may not be an issue.

23. Click **Reboot**.

24. When the Secondary Server has booted, login to the Secondary Server Administration UI. Verify the database is now empty by attempting to login using credentials previously configured. They should no longer work. Use the following credentials:

Username: **root**

Password: **YAMS**

25. Review the UI and verify there are no entries in the various panels:
    - Dashboard: Summary panel should not list the Primary Server.
    - Dashboard: Alarms, Network Device Summary, and Host Summary should be empty.
    - **Network Devices > Topology** should no longer have device data.

26. Logout of UI and login to the Secondary Server CLI.

27. Verify DHCP is not running (failed status).

    service dhcpd status

```
> service dhcpd status
Redirecting to /bin/systemctl status dhcpd.service
● dhcpd.service - DHCPv4 Server Daemon
   Loaded: loaded (/usr/lib/systemd/system/dhcpd.service; enabled;
   vendor preset: disabled)
   Active: failed (Result: exit-code) since Tue 2020-04-21 17:33:48
   EDT; 5min ago
```

28. Backup the current license key.

    cd /bsc/campusMgr/

    cp .licenseKey .licenseKey.old<date>

    Example

```
cp .licenseKey .licenseKey.old_4_20_2020
```

29. Deactivate the License Key. Modify **.licenseKey** and remove contents. Save file.

30. Shutdown management processes

    shutdownNAC

    <wait 30 seconds>

    shutdownNAC –kill

    The Secondary UI should show **Processes are Down**

    The appliance can now be shut down or re-keyed as needed. To shut down, type **shutdown -h now**

31. If High Availability pair is managed by a Manager (FNAC-M-xx), add the Primary Server back to the Manager's **Server List**. This will re-distribute the Endpoint License to the Primary Server.
    a. Login to the Manager Administration UI.
    b. In the **Server List** Dashboard panel, click **Add.**
    c. Enter the Primary Server eth0 IP address and click **OK**.
    d. Once the Primary Server is re-added, login to the Primary Server Administration UI and verify the **License Key Detail** is updated under **System > Settings > System Management > License Management.**

To apply a new key and change eth0 and eth1 configurations on the former Secondary Server, access Configuration Wizard using passwords previously configured. Refer to the proper installation guide in the Fortinet Document Library for instructions. Contact Support for assistance.

Access Secondary Server Configuration Wizard in L2 High Availability

Once L2 High Availability is configured, the Secondary Server may no longer be accessible via port 8443 unless a failover occurs. This is dependent upon the location of the “nac” entry in the **/etc/hosts** file. The "nac" entry redirects web access to the applied eth0 IP address.

In some systems, the “nac” entry may be on the same line as the Virtual IP (VIP) entry. Only access to the VIP is allowed in this configuration.

Example

```
> vi /etc/hosts
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6

<...>

<Virtual IP>     nac
```

In other systems, it is listed at the bottom next to the default entry "0.0.0.0". This entry allows access to the VIP as well as the Primary and Secondary eth0 IP addresses.

Example

```
> vi /etc/hosts
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6

<...>

0.0.0.0     nac
```

For systems whose “nac” entry is applied to the VIP, perform the following steps to access the Secondary Server's Configuration Wizard:

1. Login to the Secondary Server CLI as root and modify **/etc/hosts.**

2. Remove the "nac" entry from the applicable line.
   Example
   ```
   cat /etc/hosts
   127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
   ::1         localhost localhost.localdomain localhost6 localhost6.localdomain6

   <...>

   <Virtual IP>
   ```

3. Restart the web service. Type
   service tomcat-admin restart

4. Access the Secondary Server Configuration Wizard using the following URL
   `https://<Secondary Server name or IP>:8443/configWizard`

5. Once access to Configuration Wizard is no longer required, modify **/etc/hosts** and replace the "nac" entry.

```
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6

<...>

<Virtual IP>   nac
```

6. Restart the web service.
   service tomcat-admin restart

Log Output Examples

Primary Server Management Processes Down

Example of entries printed in Secondary Server **/bsc/logs/output.processManager** (appear roughly 30 seconds apart). Failover triggered after 5 communication attempts.

```
**** Failed to talk to master **** PingRetryCnt = 1 pingRetries = 5
**** Failed to talk to master **** PingRetryCnt = 2 pingRetries = 5
**** Failed to talk to master **** PingRetryCnt = 3 pingRetries = 5
**** Failed to talk to master **** PingRetryCnt = 4 pingRetries = 5
**** Failed to talk to master **** PingRetryCnt = 5 pingRetries = 5

**** Failed to talk to master **** PingRetryCnt exceeded!
```

Primary Server DHCP Services Down

Primary Server attempts to restart the service. If the service does not start, 3 additional attempts are made. If the service remains stopped, the Primary Server triggers the failover.

Example of entries printed in Primary Server /bsc/logs/output.processManager (appear roughly 30 seconds apart):

```
dhcpd is not running!
Restarting dhcpd (retries = 0)
<…>
dhcpd is not running!
Restarting dhcpd (retries = 1)
<…>
dhcpd is not running!
Restarting dhcpd (retries = 2)
<…>
dhcpd is not running!
Restarting dhcpd (retries = 3)
<…>
dhcpd is not running!
******* System Check Failed! *******
******* Changing status to - Slave In Control *******
Sending Force Failover to trigger other servers
```

Control Manager Log Entries During Failover

If monitoring the logs **/bsc/logs/output.mom** in Manager, the following can be observed:

Manager can no longer communicate with Primary Server (management process stopped).

```
2020-04-07 13:55:59:453 :: Polled primaryserver.company.com-00:0C:29:19:A2:5A Lost
```

Secondary Server has taken control but control process is not yet fully started.

```
2020-04-07 13:57:49:526 :: Polled secondaryserver.company.com-00:0C:29:72:B6:EA
Management_Lost
2020-04-07 13:59:49:593 :: Polled secondaryserver.company.com-00:0C:29:72:B6:EA
Management_Lost
```

Secondary Server control process is up and is responding to polls from the Manager.

```
2020-04-07 14:01:49:660 :: Polled secondaryserver.company.com-00:0C:29:72:B6:EA Established
```

Upon the next panel refresh, the **Server List** Dashboard panel should display the Secondary Server with a status of **Running – In Control**.

System Software Updates

When updating FortiNAC appliances in a High Availability, the Primary Server automatically updates the Secondary Server. In managed environments, the FortiNAC Control Manager can be used to update all the managed appliances.

Refer to the **Upgrade Instructions and Considerations** guide in the Fortinet Document Library for details.

Operating System Updates

In a High Availability environment, all of the servers can be updated from the **Operating System Updates** panel. If a server cannot be reached, an error message displays in the table along with the IP address of the server. For instructions, see **Updating CentOS** in the Fortinet Document Library.