FortiNAC - High Availability - FortiNACOS

Version F 7.2.2

FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO GUIDE

https://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM

https://www.fortinet.com/training-certification

NSE INSTITUTE

https://training.fortinet.com

FORTIGUARD CENTER

https://www.fortiguard.com

END USER LICENSE AGREEMENT

https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdoc@fortinet.com

TABLE OF CONTENTS

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: This document applies to appliances running on the FortiNAC-OS platform.

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.

Time duration to change control: The process that activates the backup appliance (fail over), as well as re-activates the main appliance (resume control), takes approximately 10-15 minutes to complete. During this time, FortiNAC processes are not running.

Availability Percentage: Between 99% ("two nines") and 99.5% ("two and a half nines").

Reference:

https://en.wikipedia.org/wiki/High_availability

https://interworks.com/blog/rclapp/2010/05/06/what-does-availabilityuptime-mean-real-world/

High Availability Solutions versus Fault Tolerant Solutions

A fault tolerant environment has no service interruption but a significantly higher cost. A highly available environment has a minimal service interruption.

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.
  - **Secondary Server** - The "backup" appliance(s) that takes control when the Primary fails.
- **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.

  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.
Secondary	The "backup" server or servers that take control when the primary fails.
Loader	The process that runs on the FortiNAC Server in Control: Principal (FortiNAC Server) Nessus (FortiNAC 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.

Requirements

- Both FortiNAC servers must be the same model (FNC-CAX-xx or FNC-MX-xx). A mixed FortiNAC-OS and CentOS High Availability configuration is not supported.
- The following have been completed for both appliances (see Deployment Guide)
  - 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.
- Appliances can ping the default gateway for their eth0 interface. For details see Determine Gateway IP Addresses.
- If using Rogue DHCP Server Detection:
  - Both the primary and Secondary 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 set up correctly or DHCP monitoring will not

run. For details, see section Rogue DHCP Server Detection of the Administration Guide in the Fortinet Document Library.

Considerations

The Primary Server does not automatically resume control under any circumstance. It must be done manually.

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 bandwidth 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

FortiNAC F 7.2.2 High Availability - FortiNACOS
Fortinet Inc.

7

Configuration Options

There are two possible High Availability configurations:

- **Layer 2 High Availability:**
    - Optional Virtual/Shared IP address (VIP))
        - Available for GUI access convenience
        - UI access to the Primary and Secondary Server IPs is not supported when VIP is configured
        - Secondary Server UI access can be temporarily enabled to access Configuration Wizard (see Appendix)
        - When the IP address of the appliances are required in network device and agent configurations, it is recommended to use the physical IP address of the Primary and Secondary servers.
    - Both Primary and Secondary Servers reside on the same network. For more details see section Design - Layer 2
    - Provides system redundancy in the event of an appliance failure
- **Layer 3 High Availability:**
    - **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.
    - Does not use a Virtual/Shared IP address
    - Primary and Secondary Servers reside on different networks (e.g. Data Center and Disaster Recovery (DR) Data Center). For more details see section Design - Layer 3
    - Provides system redundancy in the event of an appliance failure
    - Full disaster recovery in the event of a location outage

Step 1: Design

Layer 2

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

  FortiNAC Manager (FNC-MX-xx)

  a. Shared IP Address

  b. Primary Server eth0

  c. Secondary Server eth0

  Example

  Shared IP Address: 192.168.100.10/24

  Primary Server eth0: 192.168.100.8/24

  Secondary Server eth0: 192.168.100.9/24

  FortiNAC Server (FNC-CAX-xx)

  a. Shared IP Address

  b. Primary Server eth0

  c. Primary Server eth1 (including isolation interface IPs)

  d. Secondary Server eth0

  e. Secondary Server eth1 (use same isolation interface IPs as Primary eth1)

    Example

    Shared IP Address: 192.168.100.4/24

    Primary Server eth0: 192.168.100.2/24

    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: 192.168.100.3/24

    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

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

- RADIUS Servers - Configure RADIUS servers to use both the primary and secondary FortiNAC 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:

  a. Primary RADIUS server = primary FortiNAC Server (use eth0 IP address). Do not use the Shared IP address.

  b. Secondary RADIUS server = secondary FortiNAC 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 Fully Qualified Domain Names (not the Shared name). Refer to Persistent Agent Deployment and Configuration Tips in the Documentation Library for details.

Layer 3

L3 HA - Multiple Isolation Network Configuration - Registration, Remediation and DeadEnd Separates Unkown, At Risk and Disabled devices
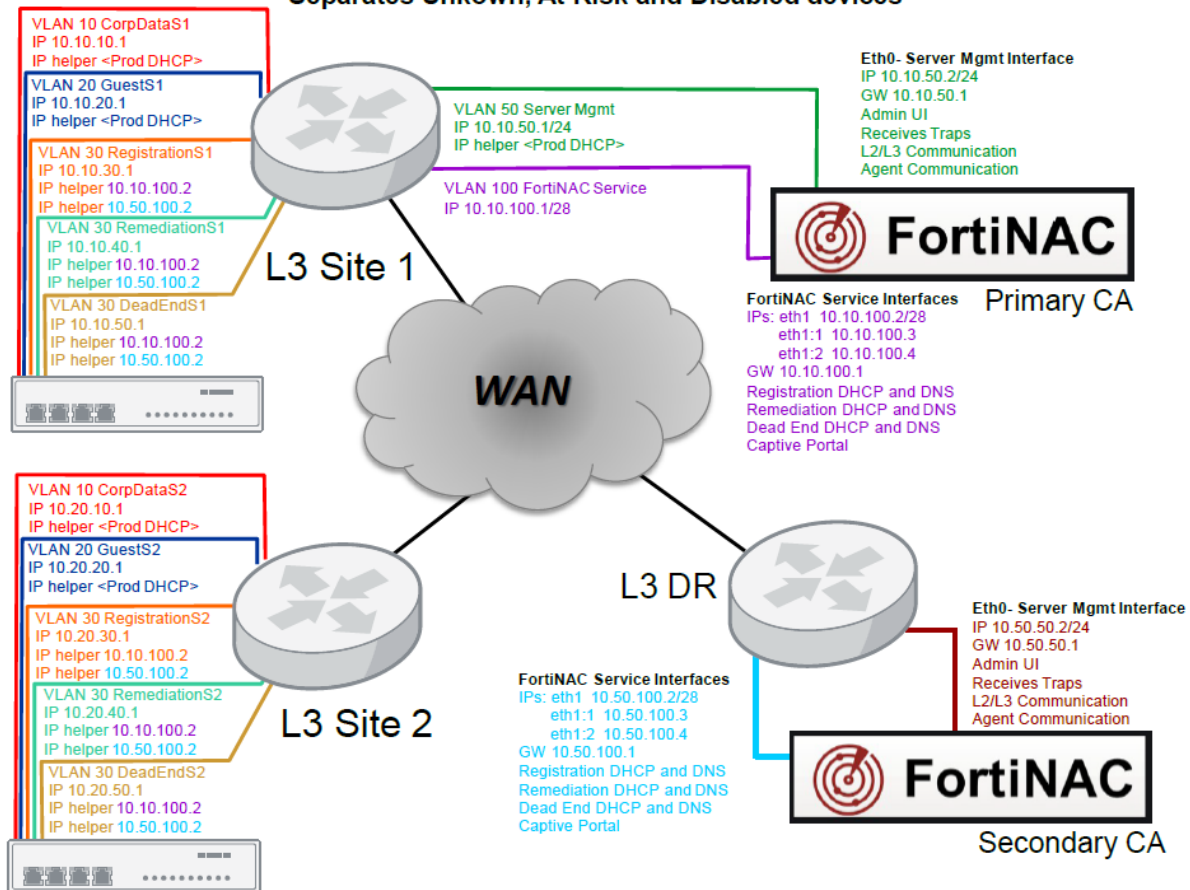
- IP Addressing - Determine the IP addresses to be used for FortiNAC appliances.

FortiNAC Control Manager (FNC-MX-xx)

a. Primary Server eth0

b. 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 (FNC-CAX-xx)

Primary Server eth0

a. Primary Server eth1 (including isolation interface IPs)

b. Secondary Server eth0 (different subnet than Primary eth0)

c. 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

- 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 eth0 IP addresses.
- RADIUS Servers - Configure RADIUS servers to use both the primary and secondary FortiNAC Server eth0 IP addresses.
- Devices Using FortiNAC as RADIUS Server (Wireless Controllers, Access Points, etc) - Configure a primary and secondary RADIUS server:

  a. Primary RADIUS server = primary FortiNAC Server (use eth0 IP address).

  b. Secondary RADIUS server = secondary FortiNAC 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 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 Sponsor Approval Email Links - Embed Server FQDN.

Determine Gateway IP Addresses

The Gateway IP address is the IP address pinged by the appliances to determine if network connectivity is still available. Failover behavior is dependent upon the IP address used for the Gateway IP Address value in the High Availability configuration. See below for options.

Note: Do not use FortiNAC IP addresses for the Gateway IP address entry.

Gateway Definition Options

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.

Step 2: Configure

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

Considerations

- All appliances in the configuration must be restarted after High Availability is configured in the UI. 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 (FNC-MX-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. Log in to the CLI of both appliances.
2. Exchange SSH keys between the Primary and Secondary servers.
   a. In the Primary Server CLI, type

   ```
   get system public-key
   ```

   b. Copy the output to buffer. This is the Primary Server SSH key.

   c. In the Secondary Server CLI, add the Primary Server SSH key. Type

   ```
   config system ha

   set public-key add <Primary Server SSH key>

   end

   get system public-key
   ```

   d. Copy the output of the last command to buffer. This is the Secondary Server SSH key.

   e. In the Primary Server CLI, add the Secondary Server SSH key. Type

   ```
   config system ha

   set public-key add <Secondary Server SSH key>

   end
   ```

3. Ensure both appliances are configured to allow inter-system communication over eth0 (port1).
   a. In both appliances type

   ```
   show system interface port1
   ```

   b. Confirm the command set allowaccess includes both nac-ipc and ssh.

Example:

```
set allowaccess https-adminui ssh ping radius radius-acct snmp nac-ipc
```

c. If these need to be added, copy the existing set allowaccess line command to buffer. **Important**: Ensure all protocols listed are copied (depending upon what's currently configured, this command may be multiple lines in length).

d. Modify the access list. Type

```
config system interface port1
```

```
<Paste set allowaccess command copied to buffer> nac-ipc
```

```
end
```

e. Review the entry to confirm the protocols were added.

```
show system interface port1
```

f. Confirm the appliances can connect to each other via SSH. Type:

```
execute ssh admin@<IP address>
```

4. Create the Allowed Serial Numbers list in the Primary Server. This list is required to allow communication between servers.

   a. In the Primary Server CLI, type:

```
execute enter-shell
```

   Hit <ENTER>

   b. Include the serial numbers of both FortiNAC Servers. Type:

```
globaloptiontool -name security.allowedserialnumbers -setRaw
"<Primaryserialnumber>,<Secondaryserialnumber>"
```

   Example

```
globaloptiontool -name security.allowedserialnumbers -setRaw "FNVM-
CAxxxxxxx1,FNVM-CAxxxxxxx2"
```

   Note:

   - The message "Warning: There is no known option with name: security.allowedserialnumbers" may appear. This is normal.
   - Database replication will copy the configuration to the Secondary Server.

   c. Confirm entry by typing:

```
globaloptiontool -name security.allowedserialnumbers
```

5. Restart FortiNAC services. Type:

```
shutdownNAC
```

```
<wait 30 seconds>
```

```
startupNAC
```

6. Log out of the CLI of both servers. In each CLI type:

```
exit
```

```
exit
```

FortiNAC F 7.2.2 High Availability - FortiNACOS
Fortinet Inc.

14

7. Connect to the Administration UI of the Primary Server. Configure High Availability using the instructions in the High availability section of the Administration Guide.

8. The chart below lists the components that will be set.

L2 High Availability Configuration	L3 High Availability Configuration
Shared IP/Virtual IP (optional) • Shared IP address • Shared Subnet Mask • Shared Host Name	Shared IP/Virtual IP N/A
Primary Appliance • IP address • Gateway IP address	Primary Appliance • IP address • Gateway IP address
Secondary Appliance • IP address • Host Name • Gateway IP address	Secondary Appliance • IP address • Host Name • Gateway IP address

Step 3: Validate

1: Confirm Appliance Status and Licensing

Administration UI Method

1. Log in to the Primary Server Administration UI.

   The **System Summary** widget 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.

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. License Key detail is populated based upon the configuration:

   Primary Server is installed with Endpoint License Key: Both appliances display information in the License Key Detail and Server Detail sections.

   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.

2: 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 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 the database is replicating properly.

Administration UI Method

1. Navigate to **Logs > Events & Alarms**and click**Update**.

   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 > Events & Alarms > Mappings**.

CLI Method

1. Log in and type

   ```
   diagnose tail -F output.processManager
   ```
2. Look for the entry slave is active. This means the database is replicating.

   Example:

   ```
   yams.CampusManager INFO :: 2022-10-18 15:57:22:047 :: #1 :: fnac-rdc2-ca-s-
   loki.supportlab.fortinac.com(Slave) Master In Control Idle(false) Max Memory
   (KBytes) 699,392 Free Memory (KBytes) 682,128 Threads: 4 Up Time: 12 Days 2 Hours
   23 Minutes 8 Seconds Time Zone: EDT (UTC-0400)

   yams.CampusManager INFO :: 2022-10-18 15:57:22:130 :: #1 :: sendPacket()
   10.12.240.100 verb Ping retval = Running - In Control
   ```

FortiNAC F 7.2.2 High Availability - FortiNACOS
Fortinet Inc.

17

```
yams.CampusManager INFO :: 2022-10-18 15:57:22:231 :: #1 :: replication status:
Slave_IO_Running: Yes

yams.CampusManager INFO :: 2022-10-18 15:57:22:231 :: #1 :: replication status:
Slave_SQL_Running: Yes

yams.CampusManager INFO :: 2022-10-18 15:57:22:232 :: #1 :: slave is active
```

3. **Ctrl-C** to stop tail.

   If "slave is inactive" is printed instead, database replication is not completing. See Troubleshooting or contact Support.

3: Perform 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.

Important: Verify the database is successfully replicating before proceeding. See Confirm Database Replication for instructions.

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).
- L3 HA
  - Upon failover, there may be a delay when the end station attempts to reach the registration portal. This is due to the order in which the DNS servers are contacted:
    - The end station attempts the primary DNS server first.
    - If this attempt has timed out, the secondary is contacted.

Trigger Failover

1. Log in to the Administration UI and add a new container named TEST in **Network > Inventory**.
2. Open SSH sessions to each Server (Primary and Secondary). Log in as root.
3. In both SSH sessions, begin tailing the processManager log.

   ```
   diagnose tail -F output.processManager
   ```

4. Simulate a condition on the Primary Server to trigger failover using one of the scenarios below.
   Scenario 1 - Network loss: Disconnect the eth0 interface of the Primary Server or admin down the switch port
   Scenario 2 – Appliance is down: In the Primary Server CLI, reboot the appliance. Type

   ```
   execute reboot
   ```

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 **(Secondary) Secondary In Control Idle(false).**This can take several minutes.

Refer to the Appendix for Log Output Examples.

Scenario 3 - Failover Script: For testing purposes only. This script is a tool for validating the failover configuration. The ping retry count is bypassed, decreasing the time it takes for the secondary to attempt to take over. In the Primary Server CLI type

```
execute enter-shell
hsForceFailover
```

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: Confirm Secondary Server is in Control

1. Connect to the Administration UI of the Secondary Server. L2 HA systems configured with shared IP must use the shared IP or name to access UI.
2. Scroll to the **System Summary** widget in the dashboard. Secondary Server status should now display **Running - In Control**.
3. Verify the TEST container created in Inventory appears. This is a simple method to verify database replication.
4. Navigate to **System > Settings > System Management > License Management**. Verify the **License Name** and **Concurrent Licenses** number matches the Primary Server.
5. If control has been configured, test enforcement - Rogue host is isolated and can register via normal means (Captive Portal, Persistent Agent, etc).
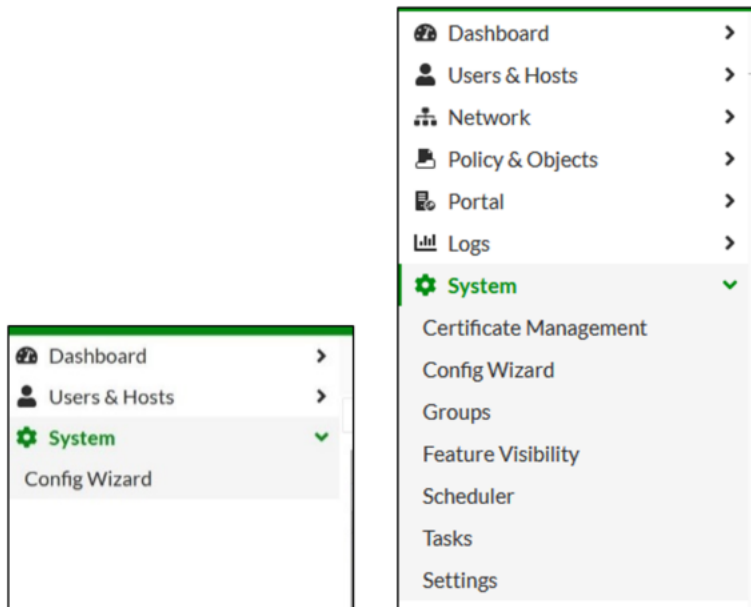
5: Resume Control to Primary Server

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

1. Either reconnect the Primary Server's eth0 interface (if disconnected) or restart. Verify the default gateway for eth0 is pingable.

2. Connect and log in to the Primary Server UI. Under the **System Summary** widget, confirm the Secondary Server shows **In Control**.

   Note: The server not in control will have limited UI menu options.

3. In the Secondary Server UI, click the **Resume Control**button in the **System Summary** Dashboard widget. This will take several minutes to complete.

4. Look for the following lines to appear to verify resume has completed:

   Primary Servers: **(Primary) Primary In Control Idle(false)**

   Secondary Servers: **(Secondary) Primary In Control Idle(false)**

5. Reconnect to the Administration UI using IP address of the Primary Server (use shared IP if L2 HA). Scroll to the **System Summary**widget in the dashboard and verify appliance status.

   Primary Servers should display status **Running - In Control.**

   Secondary Servers should display status **Running - Not In Control.**

6. Verify UI access to the Secondary Server.

   Layer 2 HA without Shared IP/VIP & Layer 3 HA

   Browse to the Secondary Server IP address or hostname

   ```
   https://<FortiNAC eth0 IPAddress or hostname>:8443/
   ```

   Layer 2 HA configurations with Shared IP/VIP
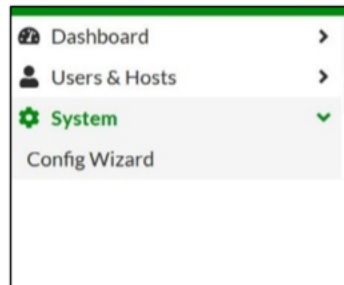
   By default, Secondary Server UI is not accessible unless a failover occurs. To access the Secondary Server's UI while the primary is in control, see Access Configuration Wizard (Post HA Configuration): VIP.

   The appliance not in control will have limited options in the UI. See below.

FortiNAC F 7.2.2 High Availability - FortiNACOS
Fortinet Inc.

20
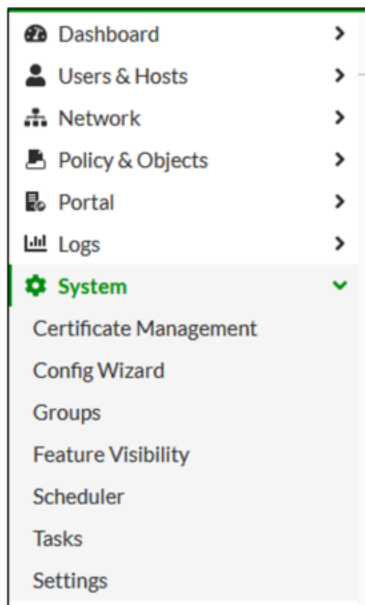
If assistance is needed, contact FortiNAC Support.

Troubleshooting

Verify License Key Configuration

The High Availability feature is included in BASE, PLUS and PRO licenses.

For more information on licensing, refer to the License Upgrade Guide in the Document Library.

License Entitlements

The license can be verified using the command **get system license**.

Example:

```
> get system license

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]
```

To view both Primary and Secondary Server licenses at once, log in to the **Secondary Server CLI** and type

```
get system license -key APPLIANCE -key PRIMARY
```

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

```
> get system license -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

Log in to each appliance and type

```
diagnose tail -F output.processManager
```

The following message indicates Primary is in control:

Primary Server: **(Primary) Primary In Control Idle(false)**

Secondary Server: **(Secondary) Primary 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 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.
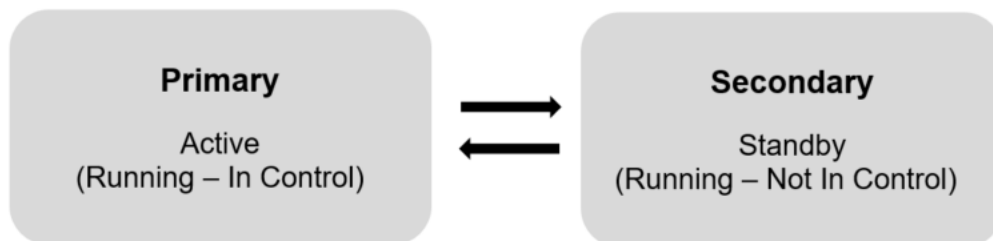

Failover Control Status

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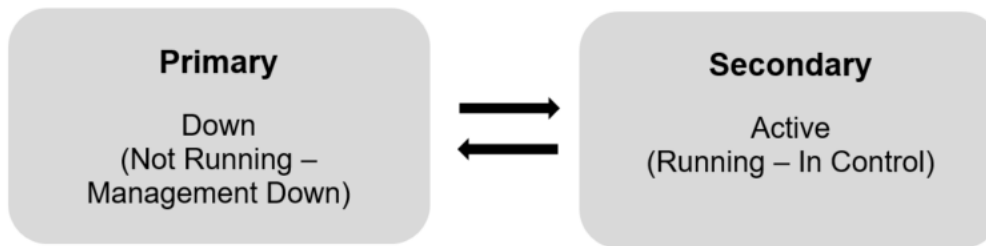
Note: In L2 HA configurations, both primary and secondary eth1 interfaces are configured with the same IP addresses. Therefore, in order to prevent duplicate IP addresses on the network, eth1 is disabled on the FortiNAC Server that is not in control.
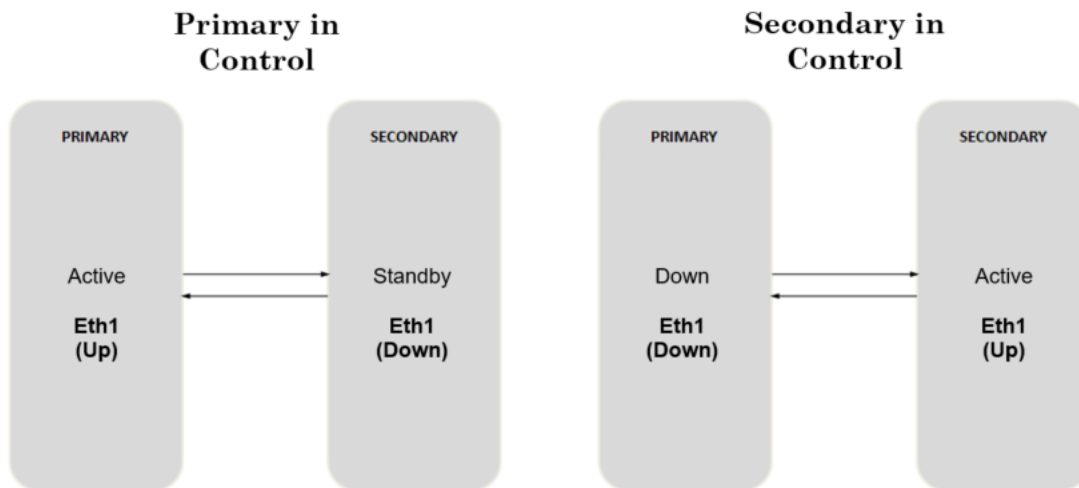
Startup High Availability

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 required processes do not start, then failover from primary to secondary is initiated.

FortiNAC F 7.2.2 High Availability - FortiNACOS
Fortinet Inc.

25

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 contro**l 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. If the appliance is in control, the appropriate processes are started.

Note: If any of the required processes do not start, then failover from primary to secondary is initiated.

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 Server
mysql	X	X
SSHd	X	X
dhcpd		X
httpd		X
named		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" indicates 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 Primary **** PingRetryCnt = 1 pingRetries = 5

**** Failed to talk to Primary **** PingRetryCnt = 2 pingRetries = 5

**** Failed to talk to Primary **** PingRetryCnt = 3 pingRetries = 5

**** Failed to talk to Primary **** PingRetryCnt = 4 pingRetries = 5

**** Failed to talk to Primary **** PingRetryCnt = 5 pingRetries = 5

**** Failed to talk to Primary **** 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 details, 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 as 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 Servers are now running.**

FortiNAC F 7.2.2 High Availability - FortiNACOS
Fortinet Inc.

27

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 as 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 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 as 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.

FortiNAC F 7.2.2 High Availability - FortiNACOS
Fortinet Inc.

28

Restart The Primary Server

Under normal operation, the **Resume Control** button on the Dashboard **System Summary** widget is grayed out. Once a failover has occurred, this button becomes enabled. Use the **Resume Control** button to initiate the process of transitioning control from the Secondary Server(s) back to the Primary Server(s). The database is also copied.

1. Navigate to **Dashboard**.
2. Scroll to the **System Summary** widget.
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 KB article 190414.

FortiNAC F 7.2.2 High Availability - FortiNACOS
Fortinet Inc.

29

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 the nac alias in the /etc/hosts file. Using the 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 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 Configuration Wizard (Post HA Configuration): No VIP

1. Browse to the appropriate appliance IP address or hostname

   ```
   https://<FortiNAC eth0 IP Address or hostname>:8443/
   ```

2. Navigate to System > Configuration Wizard.

Access Configuration Wizard (Post HA Configuration): VIP

By default, the Secondary Server is not accessible via port 8443 unless a failover occurs. The Secondary Server's admin UI web service must be started manually in order to access.

Secondary Server appliances where 'nac' appears on the shared IP entry in /etc/hosts file will not be accessible by default.

Example:

```
> cat /etc/hosts

127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4

::1 localhost localhost.localdomain localhost6 localhost6.localdomain6

<...>

<shared IP> <shared FQDN> <shared short name> nac <---

<secondary eth0 IP> <secondary FQDN> <secondary short name>
```

1. Log in to the Secondary Server CLI and type

   ```
   execute enter-shell

   cd /etc
   ```

2. With vi or some other text editor, modify **/etc/hosts**:

   Move the 'nac' entry from the shared IP entry to the Secondary server IP entry. This will enable the secondary server IP address to be accessible.

   Example

   ```
   > cat /etc/hosts

   127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4

   ::1 localhost localhost.localdomain localhost6 localhost6.localdomain6

   <...>

   <shared IP> <shared FQDN> <shared short name>

   <secondary eth0 IP> <secondary FQDN> <secondary short name> nac<---
   ```

3. Restart the web service. Type

   ```
   systemctl start nac-secondary-admingui
   ```

4. Access the Secondary Server Configuration Wizard using the following URL

   https://<Secondary Server name or IP>:8443

5. Navigate to **System > Config wizard**.

6. After configuration Wizard is run and changes are complete, stop the web service in the Secondary Server CLI.

```
systemctl stop nac-secondary-admingui
```

Important: If the service is not stopped, UI won't be accessible on fail-over.

Sponsor Approval Email Links - Embed Server FQDN

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 log in 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.

The link contained in the email is composed by FortiNAC. The link contains the URL of the FortiNAC 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. 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.
2. Navigate to the following directory:

```
execute enter-shell

cd /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 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, 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
```

```
startupNAC
```

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

Verify:

1. Navigate to **/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.
- 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 from.

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

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 Server and type

   ```
   execute enter-shell

   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 5-10 minutes to complete. Please wait at least 10 minutes before attempting to access the Administrative UI.

Stopping All Processes

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

   ```
   execute enter-shell

   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
   ```

Option 1: Restart Management Processes

1. In the Primary Server CLI type

   ```
   execute enter-shell

   startupNAC
   ```

2. Wait until the Primary Server is up and running (by confirming you have Administration UI access).

   Note: The startup could take 5-10 minutes to complete. Please wait at least 10 minutes before attempting to access the Administrative UI.

3. Once the Primary Server is running, in the Secondary Server CLI type

   ```
   execute enter-shell

   startupNAC
   ```

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

Reboot Appliances

1. In the Primary Server CLI type

   ```
   execute reboot
   ```

2. Wait until the Primary Server is up and running (by confirming you have SSH access and Administration UI access).

   Note: The startup could take 5-10 minutes to complete. Please wait at least 10 minutes before attempting to access the Administration UI.

3. Once the Primary Server is running, in the Secondary Server CLI type

   ```
   execute reboot
   ```

Power Down Appliances

1. Shut down and halt the system. In both the Primary and Secondary Server CLIs type

   ```
   execute shutdown
   ```

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 fail or do not start as expected. FortiNAC tries to restart the problematic 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 - 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 - 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.

FortiNAC F 7.2.2 High Availability - FortiNACOS
Fortinet Inc.

39

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 **output.processManager** log for failed ping attempts should be done prior to the change.

Example:

```
**** Failed to talk to Primary **** PingRetryCnt = 1 pingRetries = 5
```

```
**** Failed to talk to Primary **** PingRetryCnt = 2 pingRetries = 5
```

Contact Support for assistance.

Procedure

1. Log in to the Secondary Server CLI and type

    ```
    execute enter-shell
    cd /bsc/campusMgr/bin/
    ```

2. Modify **.networkConfig** and 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
```

3. Save the file.
4. Restart management processes on the Secondary Server for the changes to take affect

   ```
   shutdownNAC –kill
   ```

5. Wait 30 seconds then type

   ```
   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 Primary **** PingRetryCnt = 1 pingRetries = 5

   **** Failed to talk to Primary **** PingRetryCnt = 2 pingRetries = 5

   **** Failed to talk to Primary **** PingRetryCnt = 3 pingRetries = 5

   **** Failed to talk to Primary **** 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 either be shut down or moved for use in a different configuration.

Considerations

- This procedure should be performed during a maintenance window.
- If managed by a Manager (FNC-MX-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

Procedure

1. Log in to the Administration UI and verify the Primary Server is in control by reviewing the**SystemSummary**Dashboard widget. (This window can be left open). If the Primary Server is not in control, *do not*proceed until control has been resumed to the Primary Server. Contact Support if assistance is required.
2. If a High Availability pair is managed by a Manager (FNC-MX-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. Log in 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 the secondary password by clicking on the password (as if to modify), leave fields blank and click **OK**.
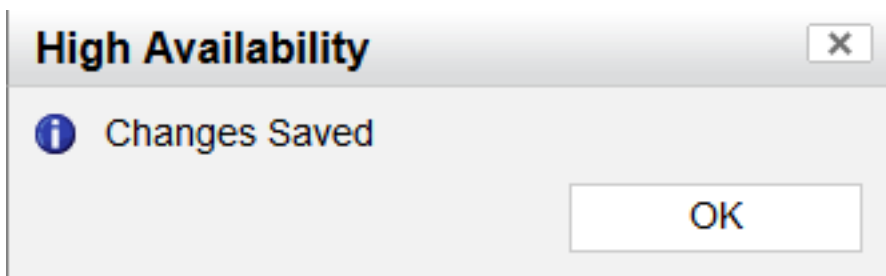

6. Click **Save Settings**.

   The following message will appear:

   Applying Settings. This could take a few minutes. Please wait.

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

Restart Server ☒

? The Server will need to be restarted for the new settings to take effect. Would you like to restart the Server now?

| Yes | No |

8. Click **OK** again.

High Availability ☒

ⓘ Changes Saved

OK
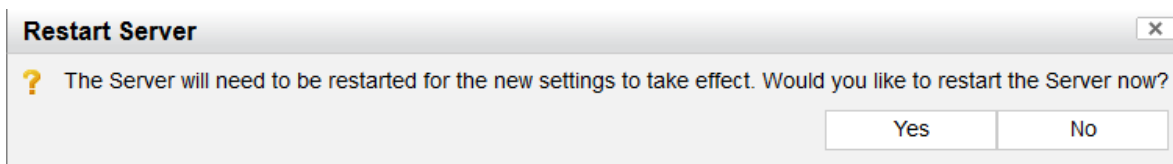
9. Wait several minutes to allow FortiNAC to restart management processes.
10. Log in to the Primary Server UI. Verify only one server now displays in the System Summary widget of the Dashboard. Log out.

Summary:		Refresh: Manual ☑ ⟳ ⊖ ☒
	FortiNAC-CA	
Host Name	oak3.bradfordnetworks.com	
Status	Running	
Product	FortiNAC-CA	
Version	8.6	
Appliance	NSL000CA	
Firmware	8.6.0.320	

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.

11. Log in to the Secondary Server CLI.
12. Shutdown management processes.

```
execute enter-shell

shutdownNAC -kill
```

13. Remove license key files copied from the Primary Server and Manager (FNC-MX-xx) (if any).

```
cd /bsc/campusMgr/

rm .licenseKeyPrimary

rm .licenseKeyNCM
```

14. Reinitialize the Secondary Server's current database.

```
cd/bsc/campusMgr/bin
```

```
ydb_initialize
```

15. 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
    ```

16. Log out of the CLI.

    ```
    exit

    exit
    ```

17. Log in to the **Secondary** Server UI and select **System > Config Wizard**.

18. 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.

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

20. 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.

21. Click **Reboot**.

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

    Username: **root**

    Password: **YAMS**

23. Review the UI and verify there are no entries in the various panels:

    - Dashboard: System Summary widget should not list the Primary Server.
    - Dashboard: Alarms, Network Device Summary, and Host Summary should be empty.
    - **Network > Inventory** should no longer have device data.

24. Logout of UI and log in to the Secondary Server CLI.

25. Backup the current license key.

    ```
    execute enter-shell

    cd /bsc/campusMgr/

    cp .licenseKey .licenseKey.old<date>
    ```

Example

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

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

27. Shut down management processes and return to the main prompt.

```
shutdownNAC -kill

exit
```

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

```
execute shutdown
```

28. If a High Availability pair is managed by a Manager (FNC-MX-xx), add the Primary Server back to the Manager's Server List. This will re-distribute the Endpoint License to the Primary Server.

a. Log in 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, log in to the Primary Server Administration UI and verify the **License Key Detai**l 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. See Guided Install in the Administration Guide for instructions.

Contact Support for assistance.

Log Output Examples

Primary Server Management Processes Down

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

```
**** Failed to talk to Primary **** PingRetryCnt = 1 pingRetries = 5

**** Failed to talk to Primary **** PingRetryCnt = 2 pingRetries = 5

**** Failed to talk to Primary **** PingRetryCnt = 3 pingRetries = 5

**** Failed to talk to Primary **** PingRetryCnt = 4 pingRetries = 5

**** Failed to talk to Primary **** PingRetryCnt = 5 pingRetries = 5


**** Failed to talk to Primary **** 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 the Primary server 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 - Secondary In Control *******

Sending Force Failover to trigger other servers
```

Control Manager Log Entries During Failover

If monitoring the logs **output.master** 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.**

FortiNAC F 7.2.2 High Availability - FortiNACOS
Fortinet Inc.

49

System Software Updates

When updating FortiNAC appliances in a High Availability environment, 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.