Master-L3-Redundancy

10:00 GMT | 11:00 CET | 14:00 GST
FEB 6th, 2018

Presenter: Abdul Ali Irfaan
abdal.ali.irfaan@hpe.com
Agenda

• Introduction
• Functionality
• Topology
• Configuration
• Troubleshooting
• Debugging
• Caveats
• Changes from Earlier Versions
• Demo
INTRODUCTION
Introduction

Why Layer-3 Redundancy?

• The L3 Redundancy Requirement primarily comes from customers who want to handle the complete Data Center Failure during natural disasters or other catastrophic events.

• ArubaOS 8.2.0.0 introduces support for a redundant pair of Mobility Masters.

• L3 redundancy will prevent a scenario where a Mobility Master acts as a single point of failure if the link to the Mobility Master goes down, or a co-located standby Mobility Master controller pair fails due to a data center failure or a local natural disaster.
Introduction

- Configuration and databases are synced automatically from the primary to secondary data center.
- Managed Devices detect a failure in the primary data center and automatically switch to the secondary data center.
- The switchover event in the managed device will have minimal service impact if any.
- With Centralized licensing, a single license can be used for both primary and secondary data centers.
- Layer-2 and Layer-3 redundancy will work together.
- When the primary data center comes back up all managed devices will switch back to primary data center with minimal service impact if any.
FUNCTIONALITY
Functionality

• The L3 Redundancy Feature supports Active-Standby model.
• The L3 Redundancy role is driven by explicit user configuration at both ends. There are 3 roles: Primary, Secondary, None (default).
• The L3 Redundancy role will determine:
  • If the user can make the config changes
  • If the sync will be initiated.
• When the redundancy Role is “Primary”, user config changes will be allowed on MM and initiates DB/config sync.
• If the redundancy Role is “Secondary”, user config changes will not be allowed and sync from primary will be accepted and acted upon.
• On the Secondary Master, config changes are allowed only on /mm/mynode.
• L3 redundant peers can either be switch IP or VRRP IP of L3 peers.
Functionality

• There are 4 sets of data that will be synced across L3 peers:
  • Databases
  • Certificates
  • Captive Portal Files (Custom images)
  • Configurations
Functionality

• Config sync is periodic and is based on configured l3-sync-timer (default 2 hours).

• If L2 redundancy is configured in primary and secondary DC then DB sync is initiated from Primary active to Secondary active.

• DB/config sync will not take place between MM’s if both are configured with role as primary or both configured with role as secondary.
Functionality

• MDs can be configured with secondary master IP during the initial setup, ZTP or as partial configuration from MM.

• Each MD will interface with HCM which will provide the reachability information of both Primary and Secondary MM.

• If MDs directly terminate on MM, then MDs probe the primary and secondary MM IP to detect primary data center failure.

• If MDs connect to MM via VPNC, then MDs probe the primary and secondary VPNC IP (if any) to detect primary data center failure.

• When MD detects that it cannot reach primary MM for 15 minutes, it triggers L3 Switchover.
Functionality

• The MDs will have management tunnel with only one MM at any given time.

• When MD detects that Primary Data Center is down and Secondary Data Center is up, MD will tear down the tunnel with Primary DC (or VPNC1) and attempt to establish IPSec tunnel with its Secondary DC (or VPNC2).

• Secondary MM will accept MDs only if it detects its tunnel with Primary MM is down.

• The MDs can connect to the Secondary Master and it will show up as a connected device in “show switches” in the Secondary master and can stay on it as long as Primary is down. As soon as the Primary is up, the tunnel with MDs will be torn down and MDs will switch back to primary MM.
CONFIGURATION
### Configuration

#### Enabling L3 redundancy (On primary and secondary MM) from /mm/mynode

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Primary-Master) [mynode] (config-submode)#master-l3redundancy</td>
<td>Enabling L3 redundancy</td>
</tr>
<tr>
<td>(Primary-Master) [mynode] (config-submode)#l3-peer-ip-address 10.17.204.171?</td>
<td>Primary Master setup</td>
</tr>
<tr>
<td>ipsec</td>
<td>IPSec secure communication between masters</td>
</tr>
<tr>
<td>ipsec-custom-cert</td>
<td>Custom-Cert-based IPSec secure communication between masters</td>
</tr>
<tr>
<td>ipsec-factory-cert</td>
<td>Factory-Cert-based IPSec secure communication between masters</td>
</tr>
<tr>
<td>(Primary-Master) [mynode] (config-submode)#l3-sync-state ?</td>
<td>L3 Sync state selection</td>
</tr>
<tr>
<td>None</td>
<td>No Sync state for L3 Redundancy</td>
</tr>
<tr>
<td>Primary</td>
<td>Set Sync state for L3 Redundancy as Primary</td>
</tr>
<tr>
<td>Secondary</td>
<td>Set Sync state for L3 Redundancy as Secondary</td>
</tr>
<tr>
<td>(Primary-Master) [mynode] (config-submode)#l3-sync-time 2</td>
<td>L3 Sync time configuration</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>(Primary-Master) [mynode] (config) #master-l3redundancy</td>
<td>Example of enabling L3 redundancy</td>
</tr>
<tr>
<td>(Primary-Master) [mynode] (config-submode)#l3-peer-ip-address 10.17.204.171 ipsec arub123</td>
<td>Primary Master setup with IPSec configuration</td>
</tr>
<tr>
<td>(Primary-Master) [mynode] (config-submode)#l3-sync-state Primary</td>
<td>Example of setting Sync state</td>
</tr>
<tr>
<td>(Primary-Master) [mynode] (config-submode)#l3-sync-time 2</td>
<td>Example of setting Sync time</td>
</tr>
</tbody>
</table>
Secondary master IP config for MDs (Using CLI under /md)

For MD:

secondary master-ip <ip/FQDN> ipsec <key> <optional-peer-mac-1> <optional-peer-mac-2>
secondary master-ip <ip/FQDN> ipsec-factory-cert <mac-1> <optional-peer-mac-2>
secondary master-ip <ip/FQDN> ipsec-custom-cert <mac-1> <optional-peer-mac-2> ca-cert <ca-cert-name/factory-cert> server-cert <server-cert-name/factory-cert> suite-b < gcm128/gcm256

Example:

secondary master-ip 10.17.204.171 ipsec aruba123

For BoC:

secondary master-ip <ip/FQDN> vpn-ip <ip/FQDN> ipsec <key> <optional-peer-mac-1> <optional-peer-mac-2>
secondary master-ip <ip/FQDN> vpn-ip <ip/FQDN> ipsec-factory-cert <mac-1> <optional-peer-mac-2>
secondary master-ip <ip/FQDN> vpn-ip <ip/FQDN> ipsec-custom-cert <mac-1> <optional-peer-mac-2> ca-cert <ca-cert-name/factory-cert> server-cert <server-cert-name/factory-cert> suite-b < gcm128/gcm256

Example:

secondary master-ip 10.17.204.171 vpn-ip 10.17.204.173 ipsec-factory-cert vpn-mac-1 00:50:56:9f:31:8b
Initial Setup in MD:

Full-setup:

Do you want to enable L3 Redundancy (Yes|No) [No]:
Enter Secondary Master switch IP address or FQDN:
Is this a VPN concentrator for managed device to reach Secondary Master switch (yes|no) [no]:
Enter IPSec Pre-shared Key:
Enter Secondary Master switch MAC address:
Enter Secondary Redundant Master switch MAC address [none]:
This device connects to Secondary Master switch via VPN concentrator (yes|no) [no]:
Enter VPN concentrator IP address or FQDN:
VPN concentrator Authentication method (FactoryCert|PSKwithMAC) [FactoryCert]:
Enter VPN concentrator MAC address:
Enter Redundant VPN concentrator MAC address [none]:
Enter IPSec Pre-shared Key:
Enter VPN concentrator MAC address:
Enter Redundant VPN concentrator MAC address [none]:
Is Secondary Master switch Virtual Mobility Master? (yes|no) [yes]:
Secondary Master switch Authentication method (PSKwithIP|PSKwithMAC) [PSKwithIP]:
Secondary Master switch Authentication method (PSKwithIP|PSKwithMAC|FactoryCert) [PSKwithIP]:
Enter IPSec Pre-shared Key:
Enter Secondary Master switch MAC address:
Enter Secondary Redundant Master switch MAC address [none]:
Configuration

Mini-setup:

Do you want to enable L3 Redundancy (Yes|No)? [No]:
Enter Secondary Master switch IP address or FQDN:
Enter VPN concentrator IP address or FQDN [none]:
Enter VPN concentrator MAC address:
Enter Redundant VPN concentrator MAC address [none]:
Enter Secondary Master switch MAC address:
Enter Secondary Redundant Master switch MAC address [none]:
TROUBLESHOOTING
Troubleshooting

- Verify L3-sync role, L3 peer IP, Pre-Shared Key on the Primary and Secondary MM
- On Primary MM:

  (Primary-Master-DC1) [mynode] #show master-l3redundancy

  L3 Sync Role:Primary
  L3 Redundant Peer IP:10.17.204.171
  IKE PSK: aruba123
  (Primary-Master-DC1) [mynode] #

- On Secondary MM:

  (Secondary-Master-DC2) [mynode] #show master-l3redundancy

  L3 Sync Role:Secondary
  L3 Redundant Peer IP:10.17.160.175
  IKE PSK: aruba123
  (Secondary-Master-DC2) [mynode] #
- Verify crypto ipsec sa between Primary and Secondary MM

```
(Primary-Master-DCl) [mynode] #show crypto ipsec sa

IPSEC SA (V2) Active Session Information

<table>
<thead>
<tr>
<th>Initiator IP</th>
<th>Responder IP</th>
<th>SPI(IN/OUT)</th>
<th>Flags</th>
<th>Start Time</th>
<th>Inner IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.17.160.172</td>
<td>10.17.160.171</td>
<td>e4223700/d2a9a600</td>
<td>T2</td>
<td>Feb 5 01:31:22</td>
<td>-</td>
</tr>
<tr>
<td>10.17.204.171</td>
<td>10.17.160.175</td>
<td>82bcb500/4f42f300</td>
<td>T2</td>
<td>Feb 5 01:31:19</td>
<td>-</td>
</tr>
<tr>
<td>10.17.170.80</td>
<td>10.17.160.175</td>
<td>1fde500 /cdebae00</td>
<td>UT2</td>
<td>Feb 5 01:31:44</td>
<td>-</td>
</tr>
<tr>
<td>10.17.204.173</td>
<td>10.17.160.175</td>
<td>e5fabe00/fe6b9f00</td>
<td>UT2</td>
<td>Feb 5 01:31:43</td>
<td>-</td>
</tr>
</tbody>
</table>

Flags: T = Tunnel Mode; E = Transport Mode; U = UDP Encap
L = L2TP Tunnel; N = Nortel Client; C = Client; Z = IKEv2
Total IPSEC SAs: 4
```

(Primary-Master-DCl) [mynode] #
Troubleshooting

- Crypto ipsec sa on Secondary MM

```
(Secondary-Master-DC2) [mynode] #show crypto ipsec sa

IPSEC SA (V2) Active Session Information
________________________________________
Initiator IP  Responder IP  SPI(IN/OUT)  Flags  Start Time  Inner IP
-----------------  ------------  ----------  ------  -----------  -------
10.17.204.171   10.17.160.175  4f42f300/82bcb500  T2  Feb 5 14:01:47  -

Flags: T = Tunnel Mode; E = Transport Mode; U = UDP Encap
       L = L2TP Tunnel; N = Nortel Client; C = Client; Z = IKEv2

Total IPSEC SAs: 1
(Secondary-Master-DC2) [mynode] #
```
• Verify database sync between Primary and Secondary MM

```
(Primary-Master-DC1) [mynode] # show database synchronize

Last L2 manual synchronization time: Wed Jan 31 23:49:01 2018
Last L3 synchronization time: Mon Feb 5 01:22:07 2018
To Master Switch at 10.17.160.172: succeeded
To Secondary Master Switch at 10.17.204.171: succeeded
WMS Database backup file size: 30297 bytes
Local User Database backup file size: 30934 bytes
Global AP Database backup file size: 12706 bytes
IAP Database backup file size: 3750 bytes
Airgroup Database backup file size: 3052 bytes
License Database backup file size: 3107 bytes
CPSec Database backup file size: 3224 bytes
Bomgr Database backup file size: 6016 bytes
L2 Synchronization took 3 second
L3 Synchronization took 1 second
1 L2 synchronization attempted
0 L2 synchronization have failed
50 L3 synchronization attempted
1 L3 synchronization have failed
L2 Periodic synchronization is disabled
L3 Periodic synchronization is enabled and runs every 120 minutes
Synchronization doesn't include Captive Portal Custom data
Airmatch database gets synchronized periodically. Last synchronization time: 2019-02-05 01:45:44
(Primary-Master-DC1) [mynode] #
```
Troubleshooting

- Verify config sync between Primary and Secondary MM

```
(Secondary-Master-DC2) [mynode] #show master-l3redundancy config-sync status
L3 Config-Sync Status
Sync Success: 53
Sync Failures: 0
Last Sync Start: Mon Feb 5 13:52:36 2018
Last Sync Finish: Mon Feb 5 13:52:37 2018
Last Sync Success: Mon Feb 5 13:52:37 2018

(Secondary-Master-DC2) [mynode] #
```
Troubleshooting

- Verify config-id on Primary and Secondary MM

- On Primary:

```
(Primary-Master-DC1) [mynode] (config) #show switches

All Switches

<table>
<thead>
<tr>
<th>IP Address</th>
<th>IPv6 Address</th>
<th>Name</th>
<th>Location</th>
<th>Type</th>
<th>Model</th>
<th>Version</th>
<th>Status</th>
<th>Configuration State</th>
<th>Config Sync Time (sec)</th>
<th>Config ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.17.160.171</td>
<td>None</td>
<td>Primary-Master-DC1</td>
<td>Building1.floor1</td>
<td>master</td>
<td>ArubaMM-VA</td>
<td>8.2.0.2_62929</td>
<td>up</td>
<td>UPDATE SUCCESSFUL</td>
<td>0</td>
<td>33</td>
</tr>
<tr>
<td>10.17.160.172</td>
<td>None</td>
<td>Primary-StandBy-DC1</td>
<td>Building1.floor1</td>
<td>standby</td>
<td>ArubaMM-VA</td>
<td>8.2.0.2_62929</td>
<td>up</td>
<td>UPDATE SUCCESSFUL</td>
<td>0</td>
<td>33</td>
</tr>
<tr>
<td>10.17.160.173</td>
<td>None</td>
<td>VPNC-DC1</td>
<td>Building1.floor1</td>
<td>MD</td>
<td>ArubaMC-VA</td>
<td>8.2.0.2_62929</td>
<td>up</td>
<td>UPDATE SUCCESSFUL</td>
<td>0</td>
<td>33</td>
</tr>
<tr>
<td>192.168.100.1</td>
<td>None</td>
<td>BoC</td>
<td>Building1.floor1</td>
<td>MD</td>
<td>Aruba7000</td>
<td>8.2.0.2_62929</td>
<td>up</td>
<td>UPDATE SUCCESSFUL</td>
<td>0</td>
<td>33</td>
</tr>
<tr>
<td>10.17.170.80</td>
<td>None</td>
<td>MD1</td>
<td>Building1.floor1</td>
<td>MD</td>
<td>Aruba7000</td>
<td>8.2.0.2_62929</td>
<td>up</td>
<td>UPDATE SUCCESSFUL</td>
<td>0</td>
<td>33</td>
</tr>
</tbody>
</table>

Total Switches: 6
(Primary-Master-DC1) [mynode] (config) #
```

- On Secondary:

```
(Secondary-Master-DC2) [mynode] (config) #show switches

All Switches

<table>
<thead>
<tr>
<th>IP Address</th>
<th>IPv6 Address</th>
<th>Name</th>
<th>Location</th>
<th>Type</th>
<th>Model</th>
<th>Version</th>
<th>Status</th>
<th>Configuration State</th>
<th>Config Sync Time (sec)</th>
<th>Config ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.17.204.171</td>
<td>None</td>
<td>Secondary-Master-DC2</td>
<td>Building1.floor1</td>
<td>master</td>
<td>ArubaMM-VA</td>
<td>8.2.0.1_62115</td>
<td>up</td>
<td>UPDATE SUCCESSFUL</td>
<td>0</td>
<td>33</td>
</tr>
</tbody>
</table>

Total Switches: 1
(Secondary-Master-DC2) [mynode] #
```
Troubleshooting

- Verify the status of MMs on the MDs

```
(MD1) #show master-13redundancy status

L3 Redundancy Status
---------------------
Role       IP Address       Status
--------   ---------------   ------
Master     10.17.160.175    Down
Secondary Master 10.17.204.171 Up
```

```
(MD1) #show ip health-check

IP Health-check Entries
-----------------------
Probe IP     Src Interface State     Probe-Profile  Avg RTT(in ms)
-----------   --------------    -----        ---------------  --------
10.17.160.175        --      Down     default         0.000
10.17.204.171        --       Up      default         0.650
(MD1) #
```
Troubleshooting

Manual config sync:

On Secondary MM:
master-l3redundancy config-sync

Manual L3 switchover:

On MD:
master-l3redundancy switchover
Troubleshooting

- Verify if the MDs have failed over to the Secondary MM
Debugging

Dbsync related issues
logging system process dbsync level debugging

Config Sync related issues
logging system process cfgm  level debugging
logging system process cfgdist level debugging

Ike related issues :
logging security process crypto level debugging

Health check and failover issues
logging system process fpapps level debugging
logging system process hcm level debugging
Changes from earlier versions

• In 6.4.4, L3 Redundancy Support was added for BoC Controllers. It had some limitations like
  • User had to explicitly do the sync across L3 peers manually
  • MDs rebooted when the Master IP changed
  • Separate licenses had to be manually installed on the Secondary Master.

• In 8.x , L3 redundancy:
  • Config DB’s and captive portal files are automatically synced between primary and secondary.
  • MD’s do not reboot during master IP change.
  • Licenses are synced between Primary and secondary MM.
Caveats

- No UI support for configuring L3 redundancy in this release
- No v6 support for L3 peers.
- L3 redundancy is not supported in standalone topology and MCM topology.
- L3 redundancy and Centralized licensing in multiple mobility master are mutually exclusive.
QUESTIONS?
THANK YOU!