Warning - The high-availability Receivers feature is not FIPS compliant. If you are required to comply with FIPS regulations, it is recommended that you not use this feature.

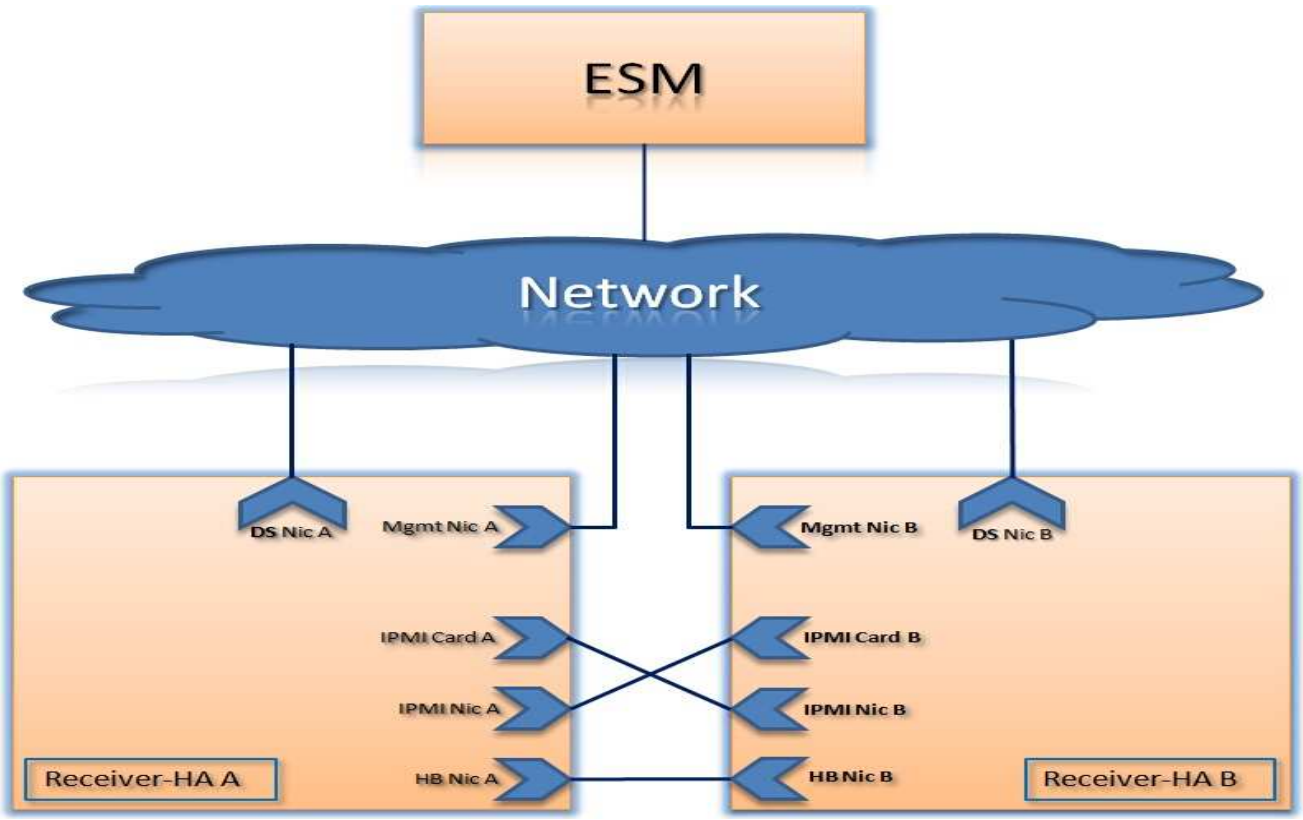
High-availability Receivers are used in primary/secondary mode so the secondary Receiver can swiftly take over functions when the primary Receiver fails, providing continuity of data collection that is significantly better than that provided by a single Receiver. This setup consists of two Receivers, either of which can act as the primary or secondary Receiver and can switch or be switched to the other role as needed. The secondary Receiver monitors the primary Receiver continuously. When the secondary determines that the primary has failed, the secondary receiver stops operations on the primary receiver and takes over as the primary. The new primary remains as the primary until you manually intervene to switch them back to their previous roles. You can swap roles between the primary and secondary as needed.

The following Receiver models can be purchased with high-availability functionality:

- 1225-HA
- 2230-HA
- 2250-HA
- 4245-HA
- 4500-HA

These models include an Intelligent Platform Management Interface (IPMI) port as well as at least 4 NICs, which are necessary for HA functionality.

The basic architecture of a Receiver-HA setup is shown in the following diagram:



.

Diagram Key	
Abbreviation	**Meaning**
DS NIC	Data Source NIC
ESM	Enterprise Security Manager
HB NIC	Heartbeat NIC
IPMI	Intelligent Platform Management Interface
IPMI Card	Daughter card or motherboard sub-system to implement IPMI, includes its own NIC
IPMI NIC	NIC used to operate the IPMI card on the other receiver
MGMT NIC	Management NIC
NIC	Network Interface Card

Before you get started make sure you have the following:

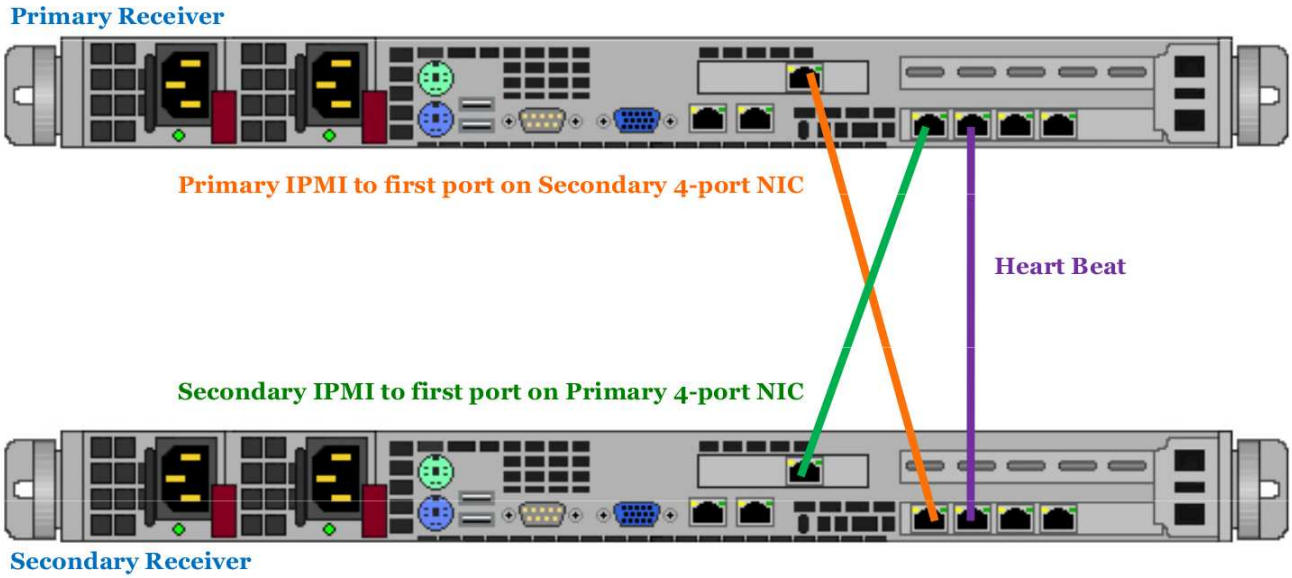
- 3 – IP addresses. One each for the management of the Receivers in the HA pair and one used as the shared data source IP between the pair.

- 3 – CAT 5, CAT 5e or CAT 6 UTP cables. These are to be used for connections between the HA Receivers. Maximum length for these is 3 ft (100m). If y choose to g to the max, use CAT 6 as it has extra shielding on a few of the wire pairs. However, if the receivers are located next to each other, use the shortest cable available to reduce noise susceptibility. These cables can be straight thru or cross over.

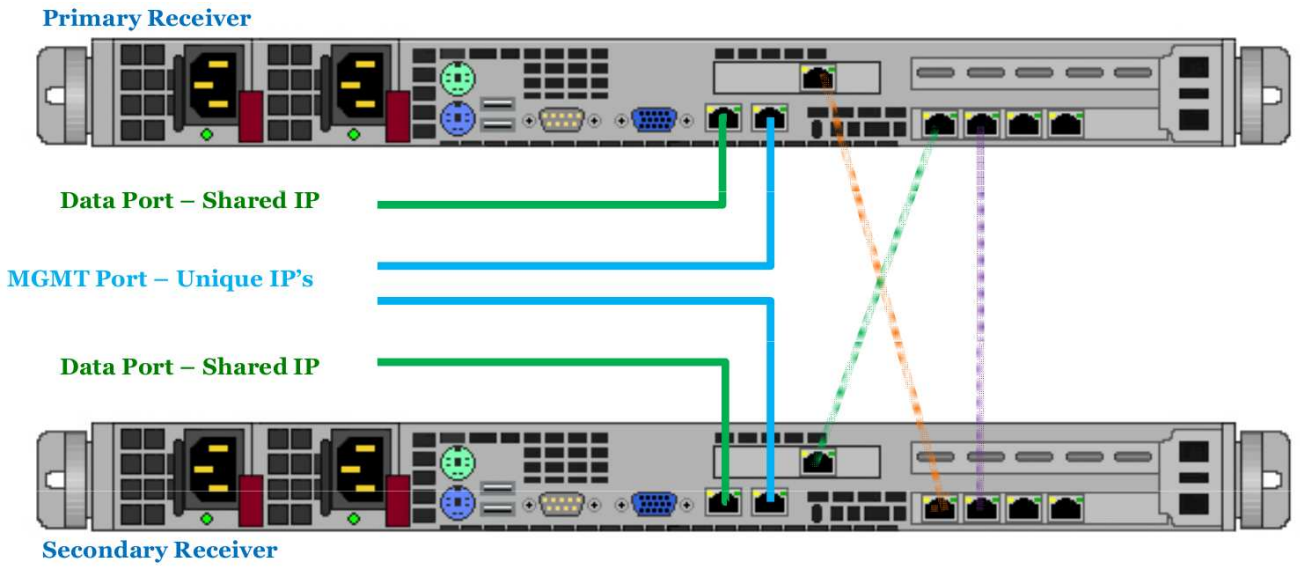
- 4 – CAT 5, CAT 5e or CAT 6 UTP cables. These will be used to connect the traditional MGMT1 and MGMT2 ports to a network switch. All 4 ports need to be able to communicate with the ESM. MGMT1 on Both Receivers, which will act as the shared IP address, will need to be accessible by all the data sources that the HA pair will be collecting information from from.

Wiring Setup

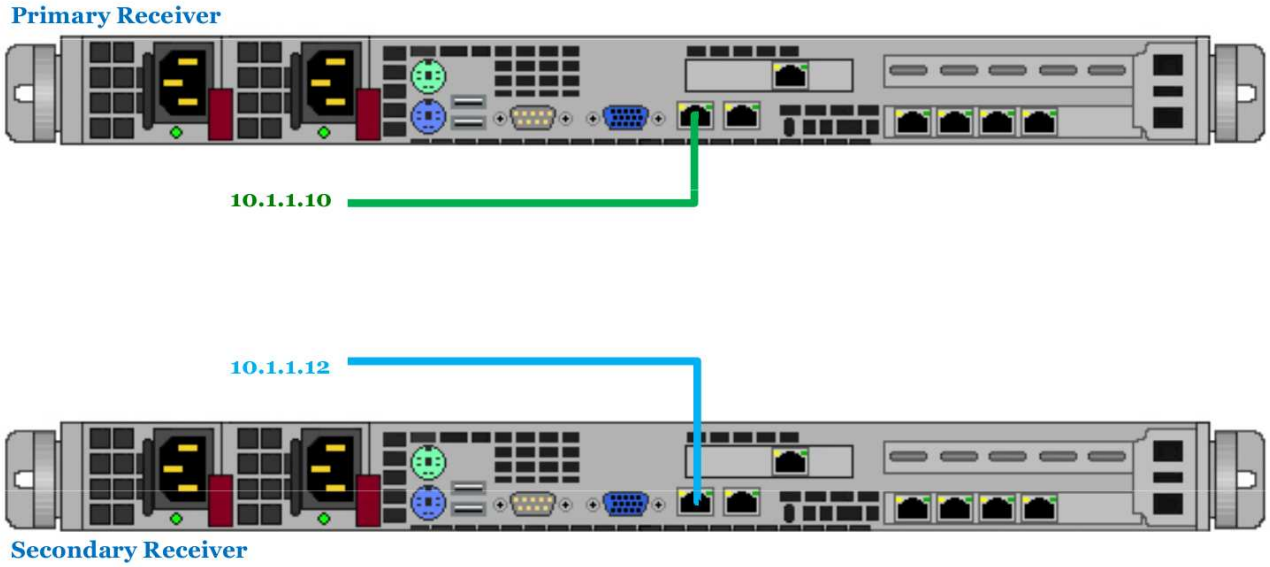
Using the color coded diagram below, connect the 2 IPMI ports between the Receiver pairs in a cross-over pattern and connect the heart-beat ports.



Next, wire the receivers MGMT ports to the switches. The wiring here is slightly different that what is usually done for a standalone receiver. In an HA configuration, MGMT1 is for the shared IP address and MGMT2 is the unique IP that the ESM will use to interact with each Receiver.



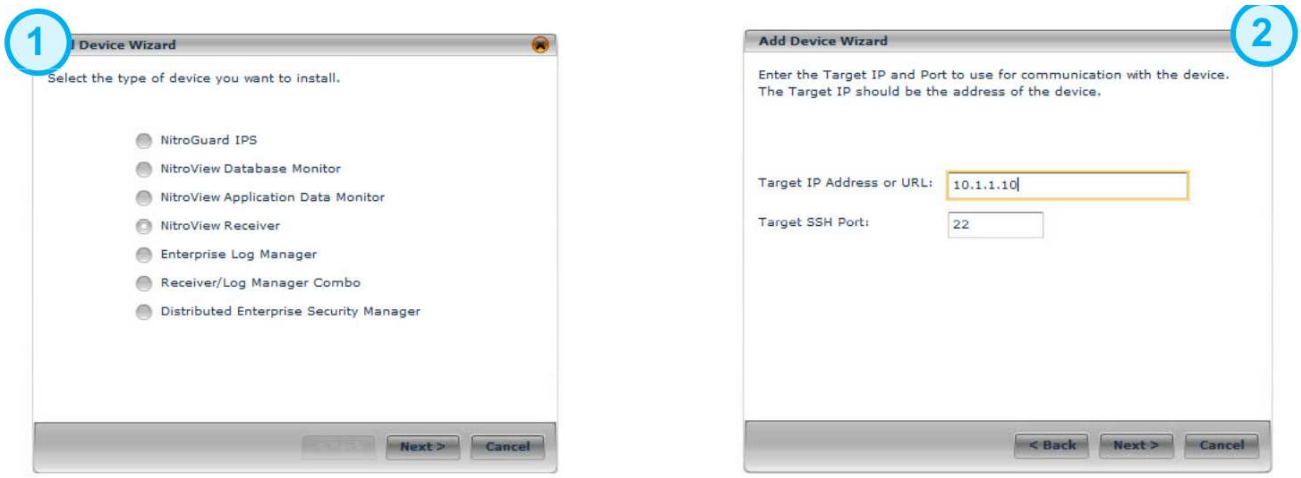
Now its time to set the initial IP's using just 2 of the 3 unique IP addresses that an HA Receiver pair require. In this example, lets say you have 10.1.1.10, 10.1.1.11 & 10.1.1.12. Where 10.1.1.10 is the shared IP address and .11 & .12 are the unique management IP addresses.


Primary Receiver
10.1.1.10
10.1.1.12
Secondary Receiver

Assuming the ESM has been booted and all initial configuration items (FIPS Rules Time, etc) have been completed, login into ESM.

Next, Add a Device using the standard steps to add a NitroView Receiver (image 1). Then, in the Target IP dialog (image 2), enter the IP address that you set for the Receiver that will act as the Primary. In this example, that would be 10.1.1.10. After you enter the IP, complete this process as you would a normal Receiver.

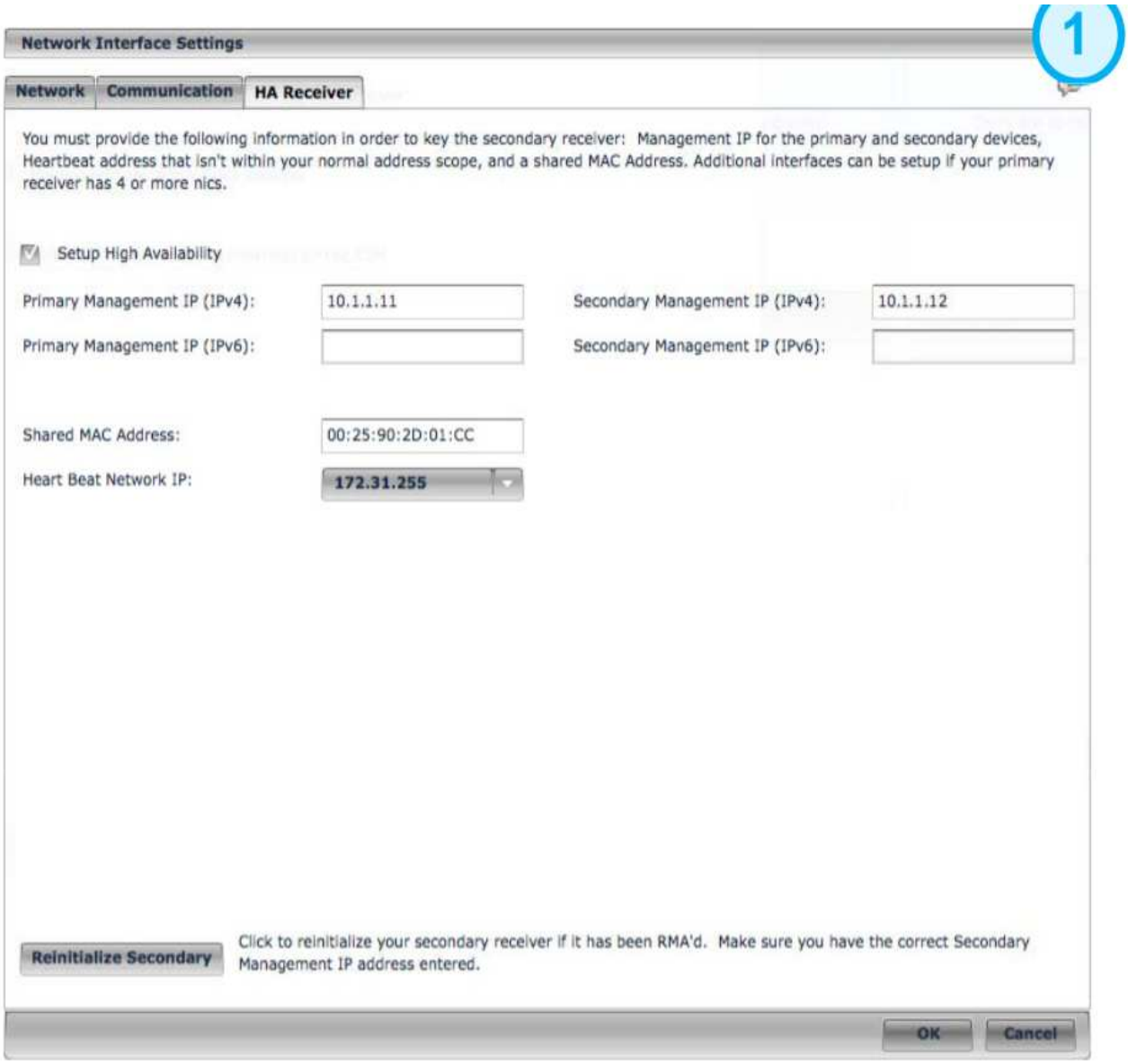
NOTE: We use this address because it was set as the MGMT1 address for the Receiver that would act as the Primary in the HA pair. This will be automatically altered in coming steps.



Once the Keying process has finished successfully, open the Receiver Properties dialog, select Receiver Configuration and then click the Interface button. You will see an HA tab in addition to Network and Communication. Select the HA tab and the dialog below will appear.

You now need to enter the management IP's for the HA pair. Using the IP's previously defined, enter 10.1.1.11 in the Primary IPv4 text box and 10.1.1.12 into the Secondary IPv4 text box. Do not modify the MAC or Heart Beat IP.

Once you click OK, a password dialog (image 2) will appear. The Secondary Receiver needs to be keyed and password added. Once entered, click OK.



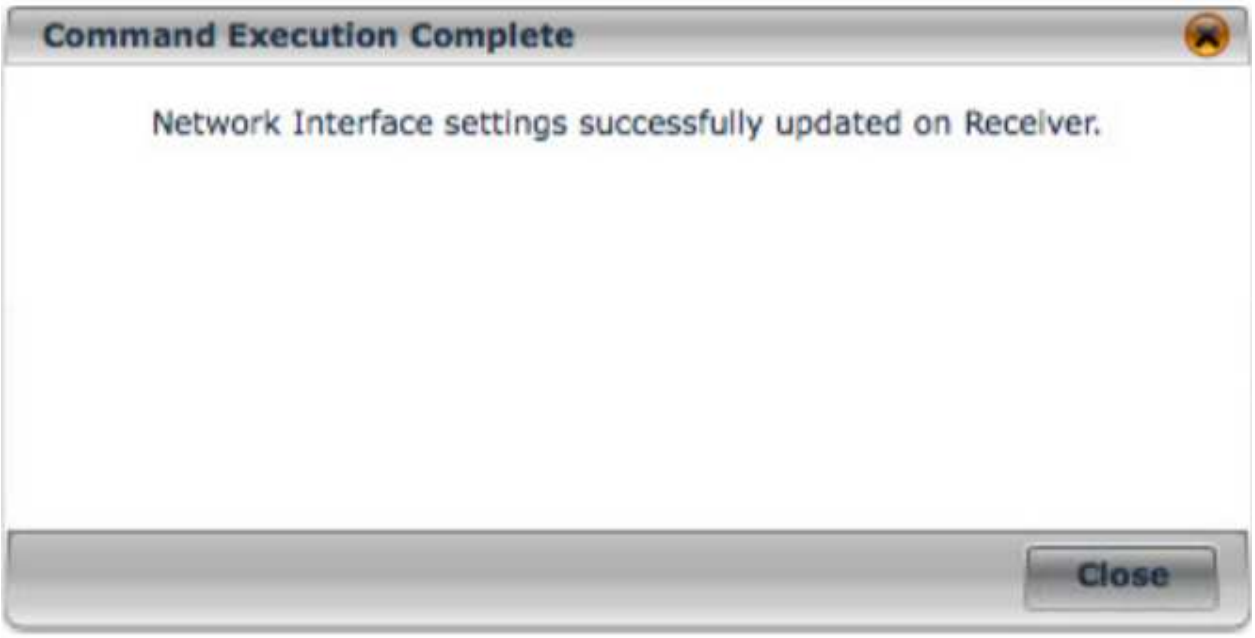
The process that is invoked after the Secondary Receiver password is entered changes the IP addresses that you originally set.

- It will set the Management IP's on MGMT2 for both Primary and Secondary Receivers

- It will configure the shared IP on MGMT1 for both Primary and Secondary Receivers
- It will install / invoke the code which manages the IPMI adapter & heartbeat process

This background configuration process will take approximately 10 to 20 minutes depending on the platforms. A number of dialogs will display indicating various steps has started or have completed. There are times when no dialog will display or very little information is presented. This is normal.

When finished, you will see the dialog below.



The IPMI cards eliminate the possibility of both DS NICs using the shared IP and MAC at the same time by shutting down the failed receiver. The IPMI cards are connected with a cross-over or straight-through cable to the other Receiver. The Receivers are connected with a cross-over or straight-through cable on the heartbeat NIC. There is a management NIC for communication with the ESM, and a data source NIC for collecting data.

The sections that follow discuss all possible HA operations. In addition, you can refer to the following sections:

- Setting up Receiver-HA Devices
- Configuring Receiver-HA Devices
- Receiver High Availability

Normal Operation

This section covers what is happening between the ESM, primary Receiver, and secondary Receiver during routine operations. The primary Receiver is running as it should and the secondary Receiver is in secondary mode. When in this mode:

- The Receivers communicate constantly over the dedicated heartbeat NIC and the

management NIC.

- Any certificates that are received, such as OPSEC or Estreamer, are passed to the other Receiver in the pair.
- All data sources use the data source NIC.
- Each Receiver monitors and reports its own health. This includes internal health items like disk errors, database freezes, and lost links on NICs.
- The ESM communicates with the receivers periodically to determine their status and health.
- Any new configuration information is sent to both the primary and secondary receiver.
- The ESM sends policy to both the primary and secondary receiver.
- Stop/Reboot/Terminal/Call Home apply to each receiver independently.

User-Initiated Switch Over

The user-initiated switch-over process allows you to switch the primary and secondary Receiver's roles. You may need to do this when upgrading a Receiver, preparing a Receiver to be returned to the manufacturer, or moving cables on a Receiver. Since neither Receiver is in a failure condition in these circumstances, this switch should minimize the amount of data lost.

1. Use the Fail-over button on the High Availability dialog to initiate a switch-over for the Receiver-HA.
2. The ESM instructs the secondary Receiver to start using the shared data source IP and collecting data.
3. The secondary Receiver issues Cluster Resource Manager (CRM) command to switch the shared IP and MAC, and starts the collectors.
4. The ESM pulls all alert and flow data from the primary Receiver.
5. The ESM marks the secondary Receiver as the primary and marks the primary Receiver as the secondary.

If necessary, you can then disconnect the secondary Receiver and suffer minimal loss of data, if any.

Primary Receiver Failure

Determination of primary Receiver failure is the responsibility of the secondary receiver. It must determine that failure quickly and accurately in order to minimize data loss. On fail-over, all data since the primary last sent data to the ESM and ELM is lost. The amount of data lost depends on the throughput of the Receiver and the rate at which the ESM pulls data from the Receiver. These competing processes must be carefully balanced to optimize data availability.

When the primary Receiver fails completely (power loss, CPU failure, etc.) there is no heartbeat communication with the primary Receiver. Corosync recognizes the loss of communication and marks the primary Receiver as failed. Pacemaker on the secondary Receiver requests that the IPMI card on the primary Receiver shut down the primary Receiver. The secondary Receiver then assumes the shared IP and MAC address, and starts all collectors.

Secondary Receiver Failure

The secondary failure process occurs when the secondary Receiver is no longer responding to the heartbeat communication. This means the system has been unable to communicate with the secondary Receiver after attempting to do so for a period of time using the management and heartbeat interfaces.

If the primary is unable to get heartbeat and integrity signals, corosync marks the secondary as failed and pacemaker uses the secondary's IPMI card to shut it down.

Primary Health Problem

The health of the primary receiver can be severely compromised. Severely compromised health would include a non-responsive database, an unresponsive data source interface, and excessive disk errors.

When the primary Receiver notices a healthmon alert for any of these conditions, it kills the corosync and pacemaker processes and sets a healthmon alert. Killing these processes causes the data collection duties to transfer to the secondary Receiver.

Secondary Health Problem

When the health of the secondary Receiver is severely compromised, the following occurs:

1. The secondary Receiver reports health problems to the ESM when queried and kills the corosync and pacemaker processes.
2. If the secondary receiver is still part of the cluster, it removes itself from the cluster and is unavailable in case of primary Receiver failure.
3. The health problem is analyzed and a repair attempted.
4. If the health problem is resolved the Receiver is returned to normal operation using the Return to Service procedure.
5. If the health problem is not resolved, the Replace Failed Receiver process is initiated.

Replace Failed Receiver

If a secondary Receiver has a health problem that cannot be resolved, it may be necessary to replace the Receiver. Once you replace the Receiver, you will need to key the new Receiver with the same key as the primary Receiver and then return it to service. For details regarding this process, refer to Replacing Failed Receiver section.

Return To Service

When a receiver is returned to service after a failure (e.g., restart after a power failure, hardware repair, network repair, etc.), the following will occur:

1. Receivers in high-availability mode will not start collecting data on start-up. They will assume they are in secondary mode until told differently.
2. If two Receivers indicate they are both unable to be primary, one selects itself to go to primary mode. It starts using the shared data source IP and collecting data.