Exinda How To Guide:

Clusters and High Availability

Exinda ExOS Version 6.4

exinda

Copyright

Document Built on August-15-13 at 10:43 AM

Using this guide

Before using this guide, become familiar with the Exinda documentation system.

- "Exinda documentation conventions" on page 2
- "Notes, Tips, Examples, and Cautions" on page 3

Exinda documentation conventions

The Exinda documentation uses the following conventions in the documentation.

Graphical interface conventions

The following is a summary of the conventions used for graphic interfaces such as those in the Exinda Web UI and the Central Management Technical Preview UI.

Convention	Definition
bold	Interface element such as buttons or menus. For example: Select the **Enable** checkbox.
Italics	Reference to other documents. For example: Refer to the *Exinda Application List*.
>	Separates navigation elements. For example: Select **File > Save**.

Command line conventions

The following is a summary of the syntax used for the CLI commands.

```
(config)# command <user input> keyword {list|of|options|to|select|from} [optional
parameter]
```

Convention	Definition
`monospace text`	Command line text or file names
`<courier italics>`	Arguments for which you use values appropriate to your environment.
courier bold	Commands and keywords that you enter exactly as shown.
`[x]`	Enclose an optional keyword or argument.
`{x}`	Enclose a required element, such as a keyword or argument.
`|`	Separates choices within an optional or required element.
`[x {y | z}]`	Braces and vertical lines (pipes) within square brackets indicate a required choice within an optional element.
`command with many parameters that wrap onto two lines in the documentation`	Underlined CLI commands may wrap on the page, but should be entered as a single line.

Notes, Tips, Examples, and Cautions

Throughout the manual the following text styles are used to highlight important points:

- **Notes** include useful features, important issues. They are identified by a light blue background.

  Note Note text

- **Tips** include hints and shortcuts. They are identified by a light blue box.

  Tip Tip text

- **Examples** are presented throughout the manual for deeper understanding of specific concepts. Examples are identified by a light gray background.

  Example

  Text

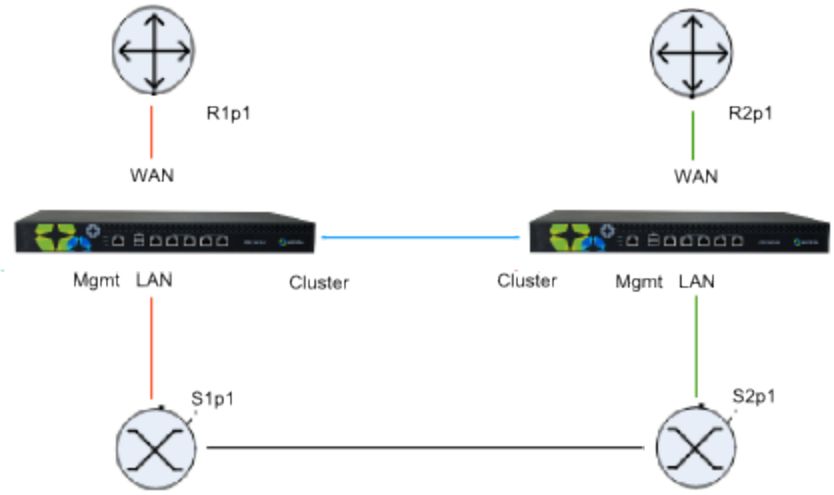
- **Cautions** and warnings that can cause damage to the device are included when necessary, and are highlighted in yellow.

  Caution Caution text

Table of Contents

Chapter 1: Cluster and High Availability

Clustering allows multiple Exinda appliances to operate as if they were a single appliance. This allows for seamless deployment into High Availability and Load Balanced environments. A typical deployment topology is illustrated below.



In this example, there are two physical links. An Exinda appliance is deployed between each switch and router, and a cable is connected between the two appliances for synchronization.

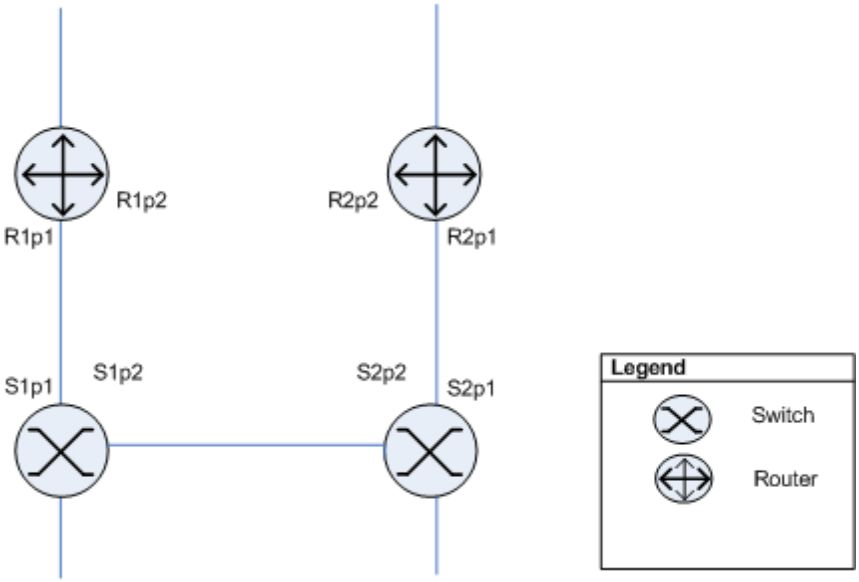
The appliances share configuration, monitoring information, and optimizer and acceleration policies, as if they were a single appliance.

Refer to the following topics for example topologies:

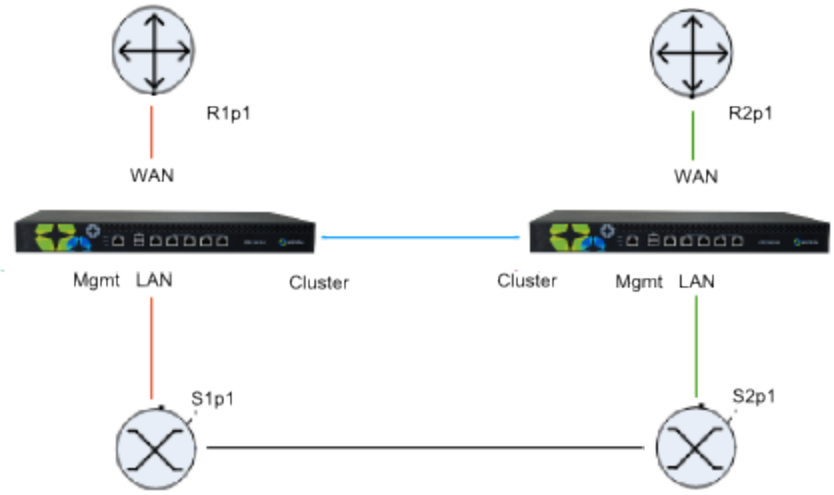
- "Redundancy through multiple Exinda appliances" on page 5
- "Load balancing and fail-over with multiple Exinda appliances" on page 7
- "High availability mode" on page 9

Redundancy through multiple Exinda appliances

The clustering feature allows two Exinda appliances to be connected in a redundant topology.



With the Exinda appliances installed the above topology will appear as below:



The two appliances are directly connected to each other. Both appliances will capture the same data. The appliance that receives the data directly will forward the traffic to the other appliance which will monitor it the same way. However, the copied traffic will not be forwarded onto the LAN.

Exinda's Clustering/HA framework is also responsible for automatically synchronizing configuration settings between the two appliances.

All platforms support this topology.

Installation

1. On each Exinda, assign an interface for cluster internal use and an interface to manage the appliance.
2. Connect the cluster interfaces on each Exinda with a crossover cable.

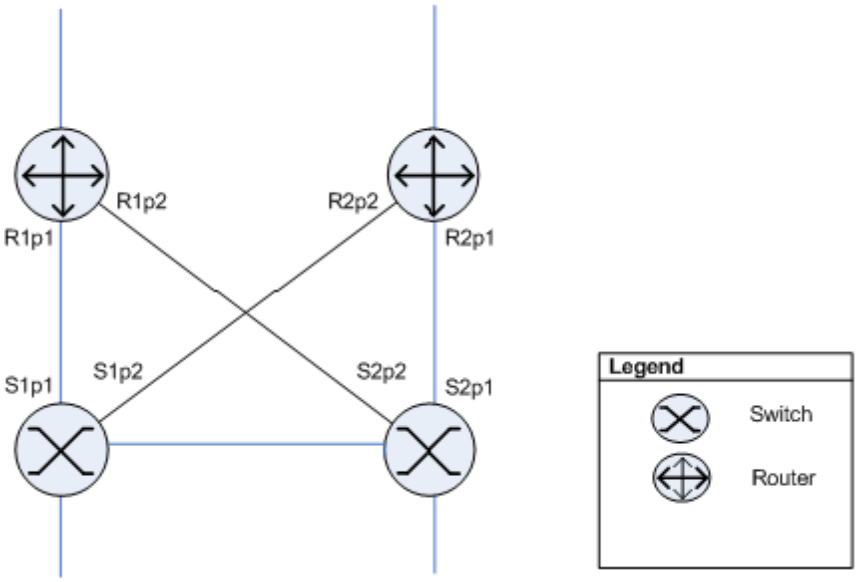
3. Power up Exinda 1. After 1 minute power up Exinda 2.
4. Connect Exinda 1 LAN into switch 1 (S1p1).
5. Connect Exinda 1 WAN into router 1 (R1p1).
6. Connect Exinda 2 LAN into switch 2 (S2p1).
7. Connect Exinda 2 WAN into router 2 (R2p1).
8. Connect Exinda 1 management interface into switch 2 (S2p2)
9. Connect Exinda 2 management interface into switch 1 (S1p2)

Capabilities

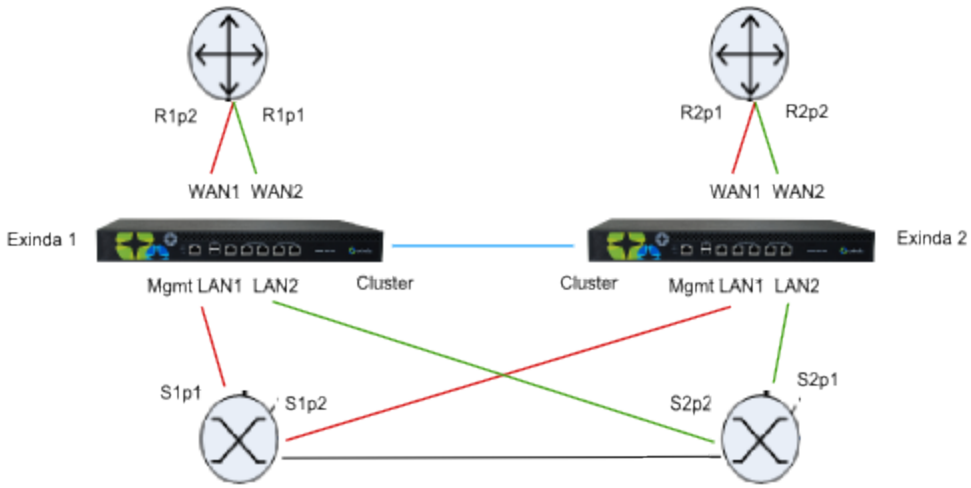
- Monitoring of both links.
- Optimization of both links.
- Redundancy of Exinda appliances.

Load balancing and fail-over with multiple Exinda appliances

Similar to the previous topology but in this case the routers are configured for load balancing. Both links in this topology act as fail-over and load balancing.



With Exinda appliances installed the above topology will appear as below:



In this topology both Exinda appliances are connected to both routers. As with the "Redundancy through multiple Exinda appliances" on page 5 case, direct traffic reaching one appliance is copied to the second appliance for monitoring and optimization, but is not forwarded on.

Platforms that support this topology include the 4060[1], 4061[1], 5000, 6010, 6060[1], 7000 and 10060[1].

[1] Network expansion modules are required.

Installation

1. On each Exinda, assign an interface for cluster internal use and an interface for managing the appliance.
2. Connect the cluster interfaces on each Exinda with a crossover cable.
3. Power up Exinda 1. After 1 minute power up Exinda 2.
4. Connect Exinda 1 LAN2 into switch 1 (S1p2).
5. Connect Exinda 1 WAN2 into router 1 (R2p2).
6. Connect Exinda 1 LAN1 into switch 1 (S1p1).
7. Connect Exinda 1 WAN2 into router 1 (R1p1).
8. Connect Exinda 2 LAN2 into switch 2 (S2p1).
9. Connect Exinda 2 WAN2 into router 2 (R2p1).
10. Connect Exinda 2 LAN1 into switch 2 (S2p2).
11. Connect Exinda 2 WAN1 into router 2 (R1p2).
12. Connect Exinda 1 MGMT into switch 2.
13. Connect Exinda 2 MGMT into switch 1.

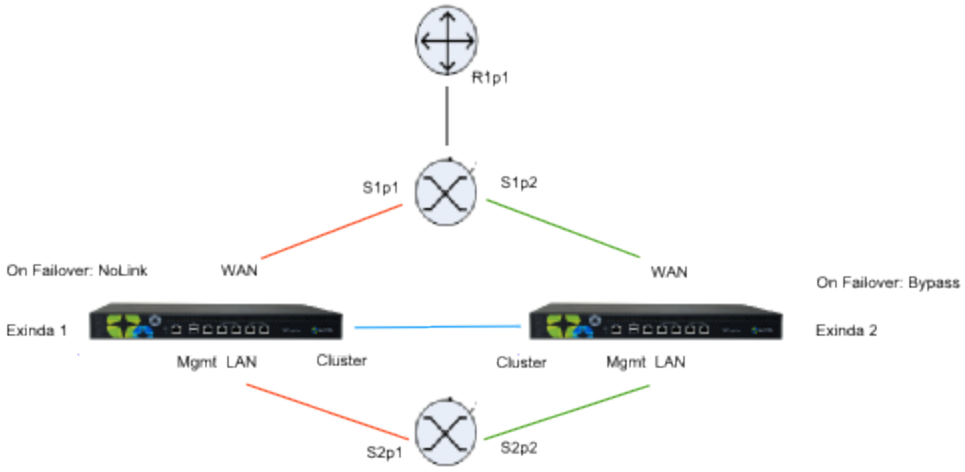
Capabilities

- Monitoring of both links.
- Optimization of both links.
- Redundancy of Exinda appliances.

High availability mode

When Router Redundancy is not present but you would still like to configure the Exinda solution in High Availability mode, use the configuration below.

With Exinda appliances installed the above topology will appear as below:



In this topology, both Exinda appliances are connected via a WAN switch. As with the "Redundancy through multiple Exinda appliances" on page 5 case, direct traffic reaching one appliance is copied to the second appliance for monitoring, but is not forwarded.

> **Note** Your WAN switch and LAN switch must support the Spanning Tree Protocol (STP) Configure STP with S2p1 higher priority then S2p2. If the link at S2p1 goes down (e.g. Exinda 1 loses power) then the switch will enable S2p2. Exinda1 should configure NoLink as the bridge failover option, Exinda 2 should configure Bypass.
>
> Active Path: S2p1 to S1p1
>
> Standby Path: S2p2 to S1p2

All platforms support this topology.

Installation

1. On each Exinda, assign an interface for cluster internal use and an interface for managing the appliance.
2. Connect the cluster interfaces on each Exinda with a crossover cable.
3. Power up Exinda 1. After 1 minute power up Exinda 2.
4. Connect Exinda 1 LAN into switch 1 (S1p1).
5. Connect Exinda 1 WAN into switch 2 (S2p1).
6. Connect Exinda 2 LAN into switch 1 (S1p2).
7. Connect Exinda 2 WAN into switch 2 (S2p2).
8. Connect the management interface of Exinda 1 into switch 1.
9. Connect the management interface of Exinda 2 into switch 1.

10. On Exinda 1, select "NoLink" for the LAN/WAN bridge failover mode.
11. On Exinda 2, select "Bypass" for the LAN/WAN bridge failover mode.

> **Note** S2p2 should have the highest STP priority.

Capabilities

- Monitoring data available on both Exinda appliances.
- Optimization available via Exinda 1 or Exinda 2.
- Redundancy of Exinda appliances.

Cluster Interfaces

Before configuring clustering, the Exinda appliances must be correctly cabled. It is recommended that each appliance in the cluster be connected and configured with a dedicated management port.

In addition, clustering requires a dedicated interface for cluster internal traffic. Any interface that is not bridged or in use for another role (e.g. Mirror or WCCP) may be used.

The table below lists the suggested cluster interface for each hardware series.

Hardware Series	Cluster Interface
2000/4000	eth1 (with Bridge 0 disabled)
4060/4061	eth2
5000	eth1
6000	eth5 (with Bridge 2 disabled)
6010	eth1
6060	eth2
7000	eth1
8060	eth2
10060	eth2

Where there are two appliances in a cluster, the cluster interfaces may be connected directly to each other with a CAT 5 cross-over cable.

Where there are more than two appliances in a cluster, each appliance's cluster interface must be connected to a single, dedicated switch - such that each appliance can communicate with every other appliance without requiring a route (must be on the same Layer 2 LAN segment).

Cluster Failover

In the event that a node in the cluster fails, is rebooted or powered off, it will enter bypass mode and traffic will pass though unaffected. When the appliance is brought back online, the node will be updated with the latest configuration settings from the Cluster Master and normal operation will continue. Monitoring and reporting information during the downtime will not be synchronized retrospectively.

In the event that the Cluster Master fails, is rebooted or powered off, a new Cluster Master will be automatically elected and the offline node will be treated a regular offline node. When it is brought back online, it won't necessarily become the Cluster Master again.

Cluster Terminology

Cluster—A group of Exinda appliances (cluster nodes) configured to operate as a single Exinda appliance.

Cluster External IP—An IP address assigned to the management port of the cluster master. Whichever node is the cluster master has this IP address assigned to it's management port.

Cluster Node—An Exinda appliance that is a member of a cluster.

Cluster Interface—The physical interface that a node in the cluster uses to connect to other cluster nodes (also referred to as the HA or AUX interface).

Cluster Internal IP—A private IP address assigned to each cluster node's, cluster interface for the purposes of communicating with other nodes in the cluster.

Cluster Master—The node responsible for synchronizing configuration changes with all other cluster nodes. Configuration changes should only be made from the cluster master.

ID—The node's cluster assigned unique identifier.

Management IP—The clusters management (alias) address. The cluster is always reachable at this address as long as at least one node is online.

Role—The current 'role' of node within the cluster (master or standby).

State—The node state (online or offline)

Create a cluster of Exinda appliances

Configuring the appliances in the network to behave as a cluster, allowing for high availability and failover, involves two steps:

1. "Add Exinda appliances to the cluster" on page 13
2. "Specify what data is synchronized between cluster members" on page 14

After the appliances have been configured, all appliances in the cluster can be monitored. See "View the status of all members of the cluster" on page 15.

Add Exinda appliances to the cluster

Configure the appliances with an internal IP address used within the cluster, as well as the IP address of the cluster master.

1. Click **System > Network > IP Address**.
2. In eth1, type the management port IP address of the appliance in the **Static Addresses** field.
3. In eth2, select **Cluster**, and type the internal IP address for this node of the cluster in the **Static Addresses** field.

   Note The Cluster Internal IP for each appliance in the cluster must be in the same subnet and should be an isolated and unused subnet within the network. The cluster subnet is used exclusively for communications between cluster nodes so should be private and not publicly routable.

4. In the Cluster Master Settings area, select eth1 and type the external address used to access the appliances.
5. Repeat these steps all each Exinda appliance joining the cluster.

Once these settings are saved, the appliances will auto-discover each other and one will be elected as the Cluster Master. All configuration must be done on the Cluster Master, so when accessing the cluster, it is best to use the Cluster Master IP address when managing a cluster.

Cluster configuration through the CLI

Configuration using the CLI is very similar to that of the Web UI.

1. Configure a Cluster Internal address. Any interface not bound to a bridge or used in another role (e.g. Mirror or WCCP) may be used. This command will need to be run on each node in the cluster, and each with a unique Cluster Internal address.

```
(config) # cluster interface eth2
(config)# interface eth2 ip address 192.168.1.1 /24
```

This command will need to be run on each node in the cluster, and each with a unique Cluster Internal IP.

2. Configure, the Cluster External IP. This command should be executed on all cluster nodes.

```
(config) # cluster master interface eth1
(config) # cluster master address vip 192.168.0.160 /24
```

The same Cluster External IP should be configured on each cluster node.

3. Enable the cluster.

```
(config) # cluster enable
```

4. As with the Web UI, the role of the node currently logged into will be displayed in the CLI prompt as shown below. Configuration changes should only be made on the Cluster Master node.

```
exinda-091cf4 [exinda-cluster: master] (config) #
```

5. It is possible to view the status of the cluster from the CLI by issuing the following command.

```
(config)# show cluster global brief
Global cluster state summary
==============================
Cluster ID: exinda-default-cluster-id
Cluster name: exinda-cluster
Management IP: 192.168.0.160/24
Cluster master IF: eth1
Cluster node count: 2
ID  Role     State    Host         External Addr    Internal Addr
-------------------------------------------------------------------
1*  master   online   exinda-A     192.168.0.161    192.168.1.1
2   standby  online   exinda-B     192.168.0.162    192.168.1.2
```

Specify what data is synchronized between cluster members

As part of normal cluster operations, the Cluster Master synchronizes parts of the system configuration to all other nodes in the cluster. Some configuration is specific to an individual appliance (for example IP addressing and licensing), however, most of the system configuration is synchronized throughout the cluster, including:

- Optimizer Policies (see note below)
- Network Objects
- Protocol and VLAN Objects
- Applications and Application Groups
- Optimizer Schedules
- Monitoring and Reporting Settings
- SDP and Remote SQL Settings

- Time-zone and NTP Settings
- Logging Settings
- Email and SNMP Notification Settings

Similarly, most monitoring information is shared across the cluster. Some reports don't make sense to share (e.g. Interface reports); however, most reports are synchronized, including:

- Realtime
- Network
- AQS
- Applications and URLs
- Hosts
- Conversations
- Subnets

> **Note** Optimizer policies are also implemented globally across all cluster nodes. For example, if there were a single policy to restrict all traffic to 1Mbps, this would be applied across all cluster nodes. So, the sum of all traffic through all cluster nodes would not exceed 1Mbps.

The following CLI commands can be used to control how data is synchronized between cluster members:

`(config)# [no] cluster sync {all|acceleration|monitor|optimizer}`

`all` - Acceleration, monitor and optimizer data are synchronized. This is disabled by default.

`acceleration` - Synchronize acceleration data only

`monitor` - Synchronize monitor data only

`optimizer` - Synchronize optimizer data only

View the status of all members of the cluster

Identify the roles of each appliances in the cluster, and see basic statistics about the appliances in the Exinda Web UI.

1. Click **System > Maintenance > Clustering**.

   All appliances in the cluster are displayed.

Clustering State									
Host ID	External IPv4 Address	Internal IPv4 Address	Status	Role	Uptime	Version	Memory	Operation	
0024e83dcaed	192.168.0.161	192.168.1.1	☑	Master	1h 1m 23s	6.1.0.16836	2050.5MB	Shutdown	Reboot
bc305bd453a8	192.168.0.162	192.168.1.2	☑	Standby	1h 1m 25s	6.1.0.16836	2050.5MB	Shutdown	Reboot

2. To identify the cluster master, the role is displayed in the list of all appliances.

   When logged into the Web UI of a cluster node, the role of the node is also shown in the header of the user interface as shown below.