



Thunder Configuration Guide for Dell® Series

August 2021

A10

Information in this document is subject to change without notice.

PATENT PROTECTION

A10 Networks products are protected by patents in the U.S. and elsewhere. The following website is provided to satisfy the virtual patent marking provisions of various jurisdictions including the virtual patent marking provisions of the America Invents Act. A10 Networks' products, including all Thunder Series products, are protected by one or more of U.S. patents and patents pending listed at:

<https://www.a10networks.com/company/legal-notices/a10-virtual-patent-marking>

TRADEMARKS

A10 Networks trademarks are listed at:

<https://www.a10networks.com/company/legal-notices/a10-trademarks>

CONFIDENTIALITY

This document contains confidential materials proprietary to A10 Networks, Inc. This document and information and ideas herein may not be disclosed, copied, reproduced or distributed to anyone outside A10 Networks, Inc. without prior written consent of A10 Networks, Inc.

A10 NETWORKS INC. SOFTWARE LICENSE AND END USER AGREEMENT

Software for all A10 Networks products contains trade secrets of A10 Networks and its subsidiaries and Customer agrees to treat Software as confidential information.

Anyone who uses the Software does so only in compliance with the terms of the End User License Agreement (EULA), provided later in this document or available separately. Customer shall not:

1. Reverse engineer, reverse compile, reverse de-assemble, or otherwise translate the Software by any means.
2. Sub-license, rent, or lease the Software.

DISCLAIMER

This document does not create any express or implied warranty about A10 Networks or about its products or services, including but not limited to fitness for a particular use and non-infringement. A10 Networks has made reasonable efforts to verify that the information contained herein is accurate, but A10 Networks assumes no responsibility for its use. All information is provided "as-is." The product specifications and features described in this publication are based on the latest information available; however, specifications are subject to change without notice, and certain features may not be available upon initial product release. Contact A10 Networks for current information regarding its products or services. A10 Networks' products and services are subject to A10 Networks' standard terms and conditions.

ENVIRONMENTAL CONSIDERATIONS

Some electronic components may possibly contain dangerous substances. For information on specific component types, please contact the manufacturer of that component. Always consult local authorities for regulations regarding proper disposal of electronic components in your area.

FURTHER INFORMATION

For additional information about A10 products, terms and conditions of delivery, and pricing, contact your nearest A10 Networks location, which can be found by visiting www.a10networks.com.

Table of Contents

| | |
|---|-----------|
| GETTING STARTED | 5 |
| OEM Solution | 6 |
| HARDWARE INFORMATION | 9 |
| Mounting | 9 |
| Hardware Specifications | 10 |
| Front View | 11 |
| Rear View | 14 |
| Status LED indicators | 19 |
| Service Tag Location | 20 |
| ASSIGNING MANAGEMENT IP TO DELL HOST | 21 |
| iDRAC IP Configuration | 21 |
| ACOS UTILITIES COMMAND REFERENCE | 23 |
| Configuration | 23 |
| a10-config | 23 |
| a10-show | 24 |
| a10-update | 25 |
| a10-gui | 25 |
| a10-ifconfig | 26 |
| LICENSE MANAGEMENT | 27 |
| License Activation | 27 |
| VTHUNDER INITIAL CONFIGURATION | 29 |
| Configuration Mode | 29 |
| Management Interface Configuration | 30 |
| Password Management | 31 |
| Saving Changes | 31 |
| SLB CONFIGURATIONS | 33 |
| Real Server | 33 |

- Service Group.....34
- Virtual Server and Virtual IP (VIP).....36
- Wild-card VIPs, Ports, and Virtual Ports.....37
- SSL CONFIGURATION 39**
 - SSL Offload40
 - Configure SSL Offload using CLI40
 - Configure SSL Offload using GUI41
 - SSL Templates42
 - Managing CAs and CSRs43
 - Certificate and Key44
 - Importing Individual Files44
 - Generating a SSL Certificate45
 - Generating a Certificate Signing Request (CSR)46
 - Generating a Self-Signed Certificate and Key47
 - Installing the Certificate48
 - Request and Install a CA-Signed Certificate48
 - Install a Self-Signed Certificate50
- DEPLOYMENT MODE 51**
 - Gateway (Router) Mode52
- ADVANCED FEATURES 61**
 - High Availability61
 - Cluster Configuration Management61
 - Reference61
- ACRONYMS 63**

GETTING STARTED

A10 Thunder® on Dell Technologies is turnkey software and hardware solutions that provide flexibility and rapid deployment for multi-cloud infrastructures.

A10 Thunder deployed on Dell EMC PowerEdge R640XL and R740XL servers, as well as Dell EMC Virtual Edge 4600 Platform enables:

- Availability to maintain uptime for web applications, data center, and cloud infrastructure
- Acceleration to deliver better user experience, maintain SLAs, and optimize server utilization
- Security to enhance the existing security infrastructure and protect against the latest threats, while providing SSL/TLS offload for encrypted server traffic

Thunder MVP enables multiple services, including Thunder ADC, Thunder CGN, and Thunder SSLi and provides other functionalities as well:

- Improves operational agility and flexibility by running multiple independent instances on a single optimized and accelerated hardware platform. Each instance can run a different ACOS version and can be booted separately
- Delivers Thunder ADC instances, providing increased uptime, faster user experience and attack prevention for highly available, accelerated, and secure applications
- Integrates Thunder SSLi instances, providing security devices with decrypted SSL/TLS traffic visibility to stop data leaks and end-user attacks, for a foundation for Zero-Trust. A10 URL filtering and threat intelligence options can be added for enhanced user security.

NOTE: Spanning Tree protocol (STP) is not supported on Thunder MVP.

A10 Thunder on Dell technologies is a Single Service Platform (SSP) consisting of A10's cloud-ready software and purpose-built Dell Technologies hardware. It is available for application delivery controller (ADC), carrier grade networking (CGN) or SSL Insight (SSLi).

- A10 Thunder ADC or CGN on Dell Technologies VEP4600
- A10 Thunder ADC, SSLi or CGN on Dell Technologies R640
- A10 Thunder ADC, SSLi or CGN on Dell Technologies R740

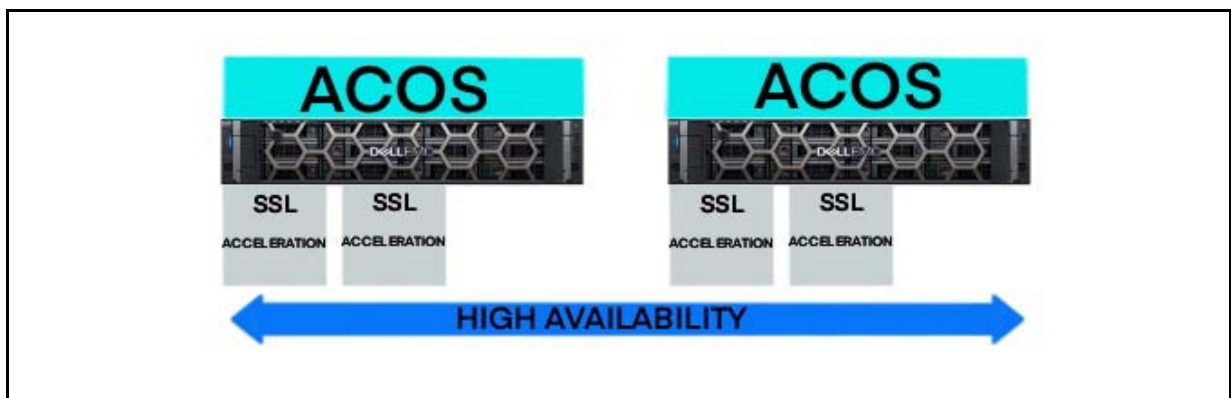
OEM Solution

The A10 Thunder on Dell Technologies OEM Solution bundles Thunder ADC, CGN, and SSLi on Dell Technologies. The single-service platform, and Thunder MVP on Dell Technologies, a Multi-tenant Virtual Platform (with Hypervisor) is available in the following bundles:

1. Single Service Platform (Thunder ADC, CGN, SSLi on Dell)

- VEP4600 (10Gbps) brings a unique Edge of Network (EON) device to provide ADC, CGN, and SSL to small enterprises and Edge deployments
- R640 (60Gbps) and R740 (100Gbps) appliances provide enterprise-grade hardware with field replaceable parts instead of full units. Faster recovery time, fewer parts stocking, easier RMA
- Dedicated hardware acceleration with Cavium.
- Thunder ADC, CGN, SSLi runs on enterprise-grade Dell EMC Servers, with TLS hardware acceleration.

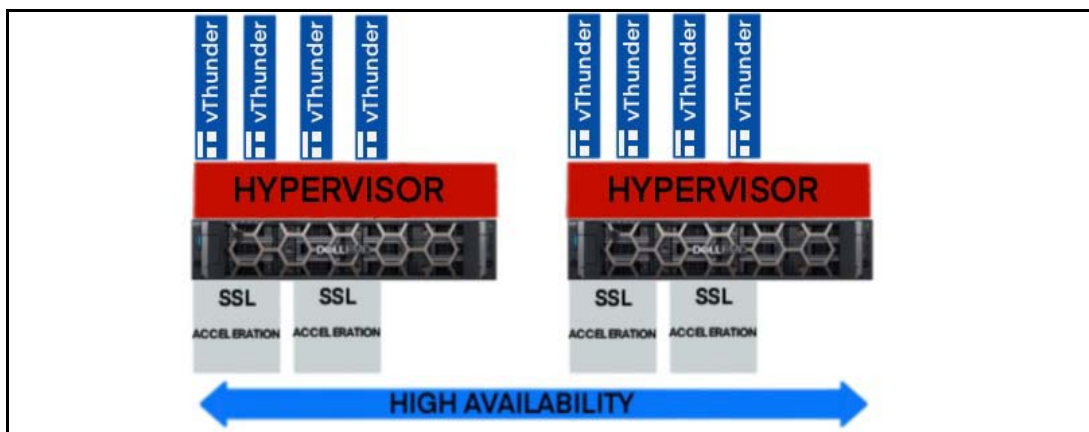
FIGURE 1 : Single Service Platform (Thunder ADC, CGN, SSLi on Dell)



2. Thunder Multi-tenant Virtual Platform (Thunder MVP)

- Consolidation of multiple vThunder instances to a single platform, for example, 4 Virtual ACOS instances on the R640 and 8 Virtual instances on the R740
- Enterprise-grade hardware with field replaceable parts instead of full units for faster recovery time, fewer parts stocking, and easier RMA
- Allows for flexible reboots, software versions, software features in one hardware platform
- Dedicated hardware acceleration
- Hypervisor based multi-tenant Thunder ADC, CGN, and SSLi solution that runs on enterprise-grade Dell EMC servers with embedded security processors for TLS/SSL transactions.

FIGURE 2 : Thunder Multi-tenant Virtual Platform (Thunder MVP)

**Limitation**

Additional Reference Information

For more information about the products, see the following guides:

- CGN guides
 - [IPv4-to-IPv6 Transition Solutions Guide](#)
 - [Traffic Logging Guide for IPv6 Migration](#)
- CLI reference guides
 - [Command Line Interface Reference for ADC](#)
 - [Command Line Interface Reference for CGN](#)
- SSLi guide
 - [SSL Insight \(SSLi\) Configuration Guide](#)
- SLB guide
 - [Application Delivery Controller Guide](#)

Acronyms

| | |
|----------|---|
| ADC | Application Delivery Controller |
| CRL | Certificate Revocation List |
| EON | Edge Of Network |
| ePSA | Enhanced Pre-Boot System Assessment |
| EST | Enterprise Service Tag |
| GLM | Global License Manager |
| iDRAC | Integrated Dell Remote Access Controller |
| MVP | Multi-tenant Virtual Platform |
| NDC | Network Daughter Card |
| NIC | Network Interface Card |
| OEM | Original Equipment Manufacturer |
| OMM | Open Manage Mobile |
| PCIe | Peripheral Component Interconnect Express |
| PSU | Power Supply Unit |
| SFP+ | Small Form-factor Pluggable |
| SLB | Server Load Balancing |
| SSD | Solid State Drive |
| SSL | Secure Socket Layer |
| SSLi | Secure Socket Layer Insight |
| TLS | Transport Layer Security |
| VGA | Video Graphics Array |
| vThunder | Virtual Thunder |

HARDWARE INFORMATION

This section provides complete Dell EMC PowerEdge R640, R740, and VEP4600 systems details.

The following topics are covered:

- [Mounting](#)
- [Hardware Specifications](#)
- [Front View](#)
- [Rear View](#)
- [Status LED indicators](#)
- [Service Tag Location](#)

Mounting

The rack rails are used for installing Dell PowerEdge devices in server racks. There are two types of hardware mounting options:

- **Static Rails:** Mounting servers in a rack without an option to move them after installation. If another server is mounted directly above, the system has to be unmounted for any work on the server hardware.
- **Sliding Rails:** Mounting servers in a rack with the option to work on the server hardware, even when another server is mounted directly above. The server can be pulled out of the rack from the front.

For more information on mounting instructions, refer to the [Server Rack Rails – Information and Resources](#) article.

Hardware Specifications

This section provides overview of dell hardware specifications for Dell EMC PowerEdge R640, R740, and VEP4600 systems.

TABLE 1 : The Dell EMC PowerEdge R640, R740, and VEP4600 systems.

| <i>Specifications</i> | <i>VEP4600</i> | <i>PowerEdge R640</i> | <i>PowerEdge R740</i> |
|-----------------------------|---|---|---|
| Server Mounting Requirement | 1U rack server | 2U rack server | 2U rack server |
| RAM | 16GB Memory | 192GB Memory | 192GB Memory |
| TLS/SSL Acceleration | Built-in | 2x Security card (PCIe) | 2x Dual-chip security card (PCIe) |
| Network Interface | 4x 10GE(SFP+), 6x 1GE(BASE-T) | 6x 10GE(SFP+), 2x 1GE(BASE-T), | 10x 10GE(SFP+), 2x 1GE(BASE-T), |
| Power Supply | <ul style="list-style-type: none"> Single 230W Power Supply. Single AC power supply unit. | <ul style="list-style-type: none"> Dual 750W Power Supply Two AC redundant power supply units. | <ul style="list-style-type: none"> Dual 2000W Power Supply Two AC redundant power supply units. |
| System Capacity | L4/L7 Throughput: 10/7.5 Gbps | L4/L7 Throughput: 40 Gbps | L4/L7 Throughput: 75 Gbps |
| Processors | 1 x Intel Xeon 8-core | 2 x Intel Xeon 20-core | 2 x Intel Xeon 20-core |
| Hard Drives | 1 x 240GB SSD | 2 x 960GB SSD | 2 x 960GB SSD |
| Network Configuration | 2 x 1Gbe Base-T 6 x 10Gbe SFP+ | 10GE NIC Model: 2 x 1Gbe Base-T 10 x 10Gbe SFP+ 100GE NIC Model: 2 X 1 GE (BASE-T) 2 X 1/10 GE Fiber (SFP+) 2 X 100 GE Fiber (QSFP28) | 10GE NIC Model: 4 x 1Gbe Base-T 10x 10Gbw SFP+ 100GE NIC Model: 2 X 1 GE (BASE-T) 10 X 1/10 GE Fiber (SFP+) 4 X 100 GE Fiber (QSFP28) |
| SSL Acceleration | Yes | Yes | Yes (QAT) |

For more information, refer to the following data sheets available on the A10 Networks website:

- [A10 Thunder on Dell Technologies OEM Solution Bundle](#)
- [Thunder ADC Data Sheet](#)
- [Thunder SSLi Data Sheet](#)

Front View

[Figure 3](#) illustrates the front view of the PowerEdge R640 system.

FIGURE 3 : Front view of the PowerEdge R640 system

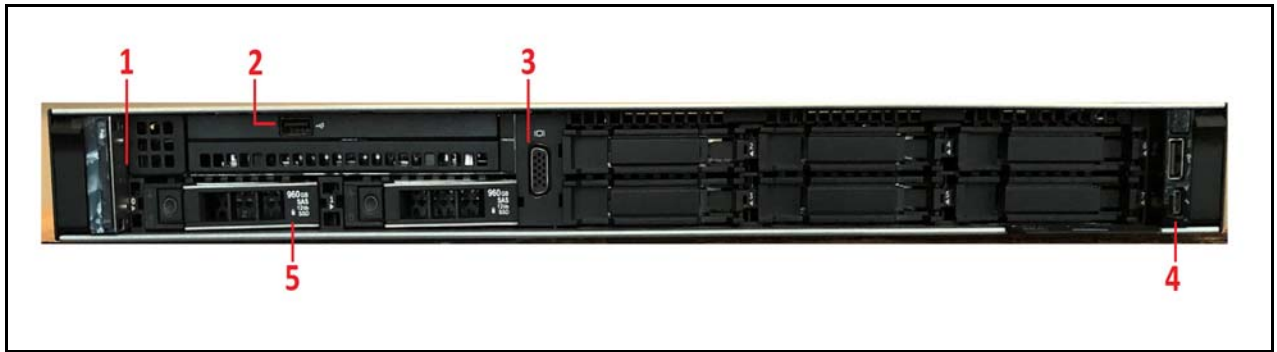


TABLE 2 : Features available on the front of the PowerEdge R640 system

| Item | Port, Panels, and Slots | Description |
|------|-------------------------|---|
| 1 | Left control panel | Contains the system health and system ID, status LED, and the iDRAC Quick Sync 2 wireless indicators. For more information, see the Rear View . |
| 2 | USB port | The USB ports are 9-pin, 3.0-compliant. These ports enable you to connect USB devices to the system. |
| 3 | VGA port | Allows you to connect a display device to the system. |
| 4 | Right control panel | Contains the power button, USB port, iDRAC Direct micro port, and the iDRAC Direct status LED. |
| 5 | Drive slots | Allows you to install drives that are supported on your system. |

FIGURE 4 : Features available on the front of the PowerEdge R740 system

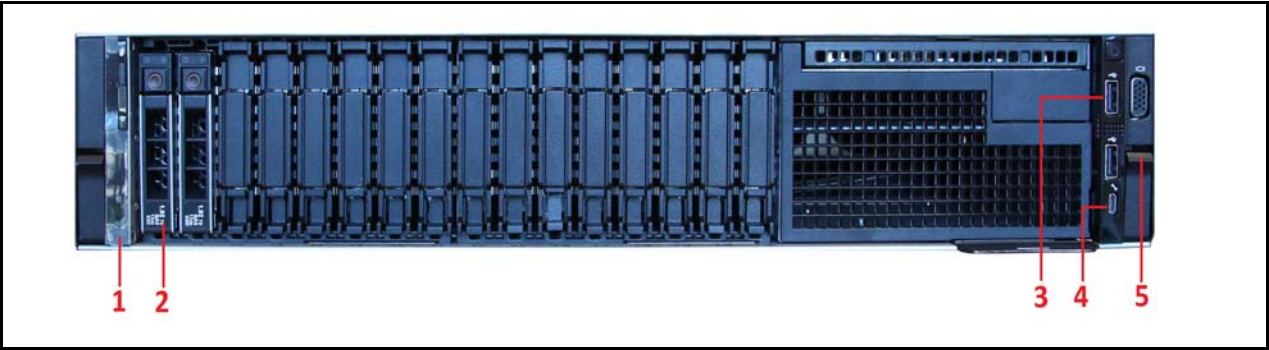


TABLE 3 : Features available on the front of the system

| Item | Port, Panels, and Slots | Description |
|------|-------------------------|--|
| 1 | Left control panel | Contains system health and system ID, status LED, and optional iDRAC Quick Sync 2 (wireless). |
| 2 | Drive slots | Allows you to install drives that are supported on your system. |
| 3 | USB 3.0 port | The USB ports are 9-pin, 3.0-compliant. These ports enable you to connect USB devices to the system. |
| 4 | Right control panel | Contains the power button, VGA port, iDRAC Direct micro USB port, and two USB 2.0 ports. |
| 5 | Information tag | The Information tag is a slide-out label panel that contains system information such as Service Tag, NIC, MAC address, and so on. If you have opted for the secure default access to iDRAC, the Information tag also contains the iDRAC secure default password. |

FIGURE 5 : Features available on the front of the VEP4600 system

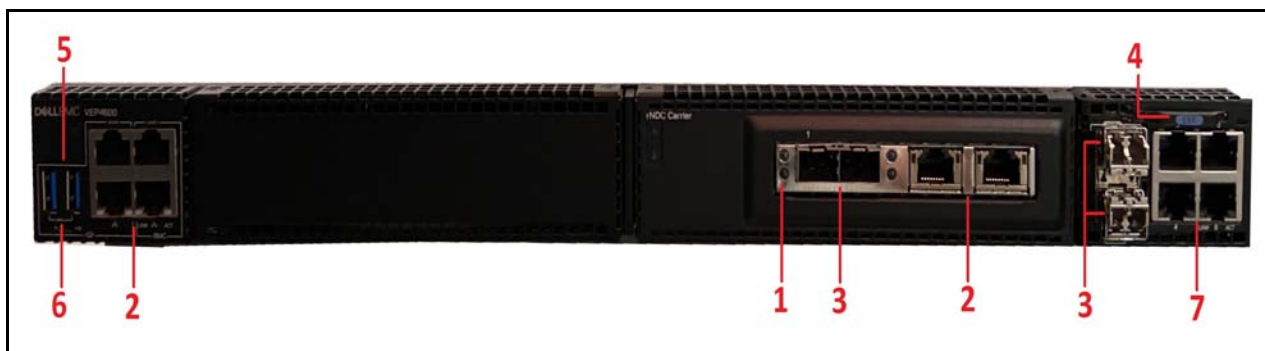


TABLE 4 : Features available on the front of the system

| Item | Port, Panels, and Slots | Description |
|------|--|---|
| 1 | Led Status Icon | Check the System Event Log or system messages for the specific issue. |
| 2 | RS-232 console ports (top) and 10/100/1000 Base-T ports (bottom) | It is the Top and 10/100/1000 Base-T ports (bottom) |
| 3 | SFP+ ports | An SFP port is a slot on a network device into which small form-factor pluggable (SFP) transceivers are inserted. |
| 4 | System luggage tag | The system luggage tag is a product identifier to access information about the device's specific tech specs and warranty so that we can provide personalized support options. |
| 5 | USB Type-A ports | USB "Type A" connections refer to the physical design of the USB port. Every USB connection is made of a port in the host device, a connecting cable, and a receptor device. |
| 6 | Micro USB-B ports | The micro B type connector holds 5 pins to support USB OTG, which permits smart-phones and similar mobile devices to read external drives or other peripherals as a computer might. |
| 7 | 10/100/1000 Base T ports | It is the Top and 10/100/1000 Base-T ports (far right) |

Rear View

This section displays the features available on the back of the R640, R740, and VEP4600 systems.

FIGURE 6 : Back view of the PowerEdge 10GE R640

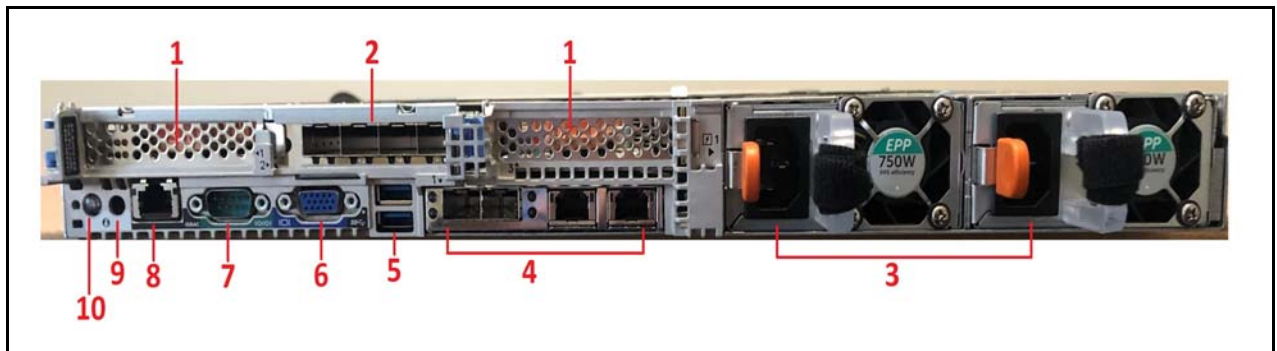


TABLE 5 : PowerEdge 10GE R640 drive system

| Item | Port, Panels, and Slots | Description |
|------|------------------------------------|---|
| 1 | SSL Acceleration Card | Hardware acceleration for encrypted technologies. |
| 2 | SFP+ Fiber ports | 10Gbps fiber ports. |
| 3 | Power supply unit (2) | Two AC redundant power supply units. |
| 4 | NIC port (4) | The NIC ports that are integrated on the network daughter card (NDC) provide network connectivity. |
| 5 | USB 3.0 port(2) | The USB ports are 9-pin and 3.0-compliant. These ports enable you to connect USB devices to the system |
| 6 | VGA Port | Allows you to connect a display device to the system. |
| 7 | Serial port | Allows you to connect a serial device to the system. |
| 8 | iDRAC9 dedicated network port | Allows you to securely access the embedded iDRAC on a separate management network, see the Integrated Dell Remote Access Controller User's Guide at www.dell.com/poweredge/manuals . |
| 9 | System status indicator cable port | Allows you to connect the status indicator cable and view system status when the CMA is installed. |
| 10 | System ID button | The System Identification (ID) button is available on the front and back of the systems. Press the button to identify a system in a rack by turning on the system ID button. You can also use the system ID button to reset iDRAC and to access BIOS using the step-through mode. |

FIGURE 7 : PowerEdge 100GE R640 drive system

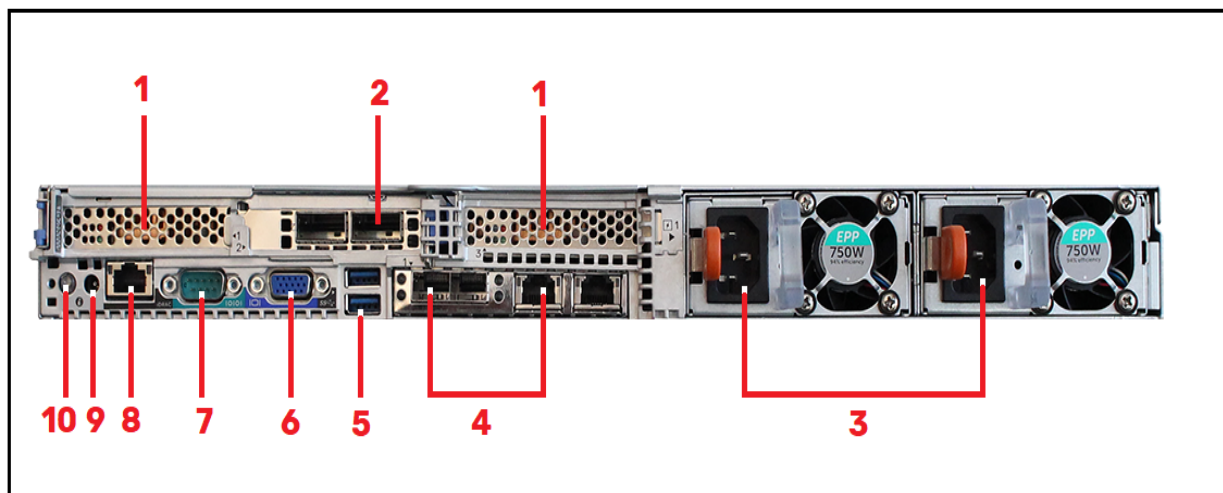


TABLE 6 : PowerEdge 100GE R640 drive system

| Item | Port, Panels, and Slots | Description |
|------|------------------------------------|---|
| 1 | SSL Acceleration Card | Hardware acceleration for encrypted technologies. |
| 2 | SFP+ Fiber ports | 10Gbps fiber ports. |
| 3 | Power supply unit (2) | Two AC redundant power supply units. |
| 4 | NIC port (4) | The NIC ports that are integrated on the network daughter card (NDC) provide network connectivity. |
| 5 | USB 3.0 port(2) | The USB ports are 9-pin and 3.0-compliant. These ports enable you to connect USB devices to the system |
| 6 | VGA Port | Allows you to connect a display device to the system. |
| 7 | Serial port | Allows you to connect a serial device to the system. |
| 8 | iDRAC9 dedicated network port | Allows you to securely access the embedded iDRAC on a separate management network, see the Integrated Dell Remote Access Controller User's Guide at www.dell.com/poweredge manuals . |
| 9 | System status indicator cable port | Allows you to connect the status indicator cable and view system status when the CMA is installed. |
| 10 | System ID button | The System Identification (ID) button is available on the front and back of the systems. Press the button to identify a system in a rack by turning on the system ID button. You can also use the system ID button to reset iDRAC and to access BIOS using the step-through mode. |

FIGURE 8 : Back view of the PowerEdge 10GE R740

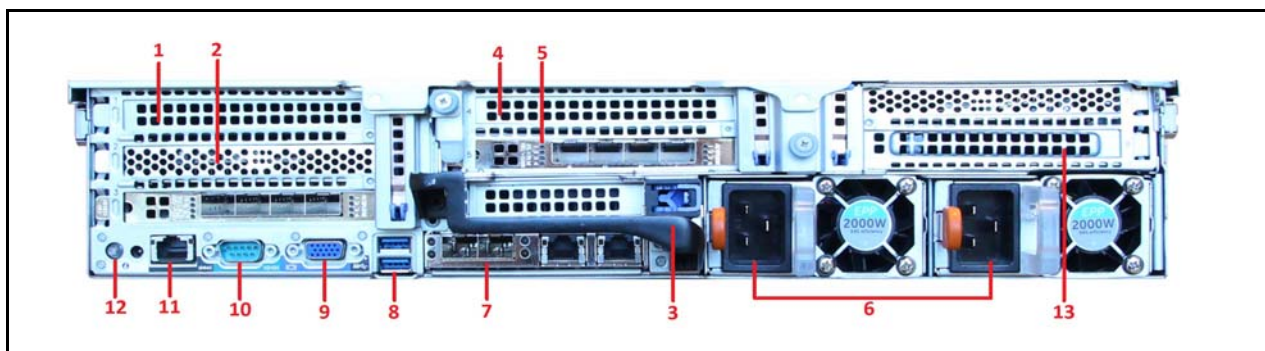


TABLE 7 : PowerEdge 10GE R740 drive system

| Item | Port, Panels, and Slots | Description |
|------|---|---|
| 1 | Full-height PCIe expansion card slot (blank slot) | The PCIe expansion card slot (riser 2) connects up to two full-height PCIe expansion cards to the system. |
| 2 | SSL Acceleration Card | Hardware acceleration for encrypted technologies. |
| 3 | Rear handle | The rear handle can be removed to enable any external cabling of PCIe cards that are installed in the PCIe expansion card slot 6. |
| 4 | Full-height PCIe expansion card slot (2) | The PCIe expansion card slot (riser 2) connects up to two full-height PCIe expansion cards to the system. |
| 5 | SFP+ Fiber ports | 10Gbps fiber ports. |
| 6 | Power supply unit (2) | Two AC 2000W PSUs. |
| 7 | NIC ports | The NIC ports that are integrated on the network daughter card (NDC) provide network connectivity. |
| 8 | USB port (2) | The USB ports are 9-pin and 3.0-compliant. These ports enable you to connect USB devices to the system. |
| 9 | VGA port | Allows you to connect a display device to the system. |
| 10 | Serial port | Allows you to connect a serial device to the system. |
| 11 | iDRAC9 dedicated port | Allows you to remotely access iDRAC. For more information, see the iDRAC User's Guide at www.dell.com/poweredgemanuals . |
| 12 | System identification button | The System Identification (ID) button is available on the front and back of the systems. Press the button to identify a system in a rack by turning on the system ID button. You can also use the system ID button to reset iDRAC and to access BIOS using the step-through mode. |
| 13 | Support Bracket | Support bracket for SSL card |

FIGURE 9 : Back view of PowerEdge 100GE R740 drive system

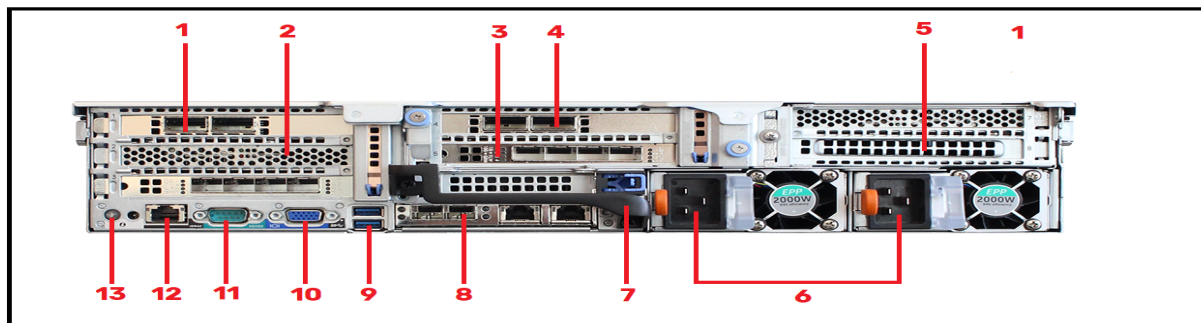


TABLE 8 : PowerEdge 100GE R740 drive system

| Item | Port, Panels, and Slots | Description |
|------|---|---|
| 1 | Full-height PCIe card slot. | The PCIe card slot (riser 2) connects two full-height PCIe cards to the system. |
| 2 | SSL Acceleration Card | Hardware acceleration for encrypted technologies. |
| 3 | Full-height PCIe cards slot (2 X 100Gbps) | The PCIe expansion card slot (riser 2) two 100 Gbps PCIe cards connected to the system. |
| 4 | SFP+ Fiber ports | 10Gbps fiber ports. |
| 5 | Support Bracket | Support bracket for SSL card |
| 6 | Power supply unit (2) | Two AC 2000W PSUs. |
| 7 | Rear handle | The rear handle can be removed to enable any external cabling of PCIe cards that are installed in the PCIe expansion card slot 6. |
| 8 | NIC ports | The NIC ports that are integrated on the network daughter card (NDC) provide network connectivity. |
| 9 | USB port (2) | The USB ports are 9-pin and 3.0-compliant. These ports enable you to connect USB devices to the system. |
| 10 | VGA port | Allows you to connect a display device to the system. |
| 11 | Serial port | Allows you to connect a serial device to the system. |
| 12 | iDRAC9 dedicated port | Allows you to remotely access iDRAC. For more information, see the iDRAC User's Guide at www.dell.com/poweredgemanuals . |
| 13 | System identification button | The System Identification (ID) button is available on the front and back of the systems. Press the button to identify a system in a rack by turning on the system ID button. You can also use the system ID button to reset iDRAC and to access BIOS using the step-through mode. |

FIGURE 10 : Rear view of VEP4600

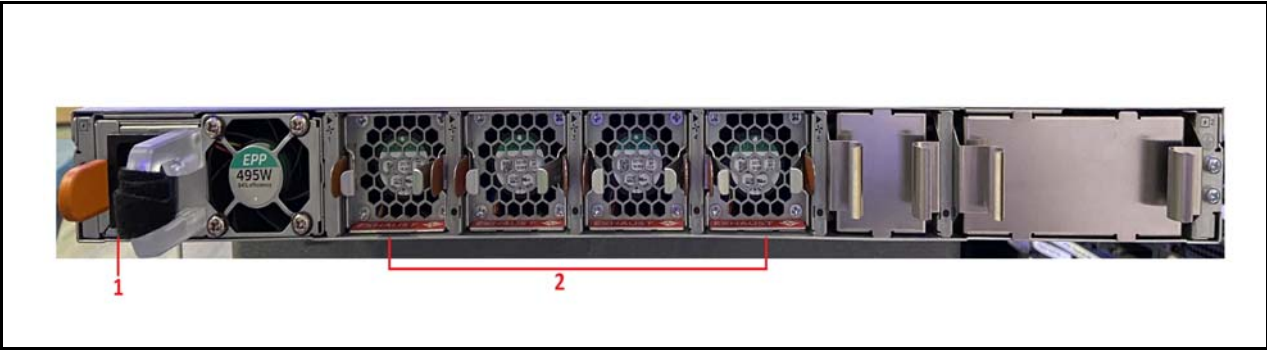


TABLE 9 : VEP4600drive system drive system

| Item | Port, Panels, and Slots | Description |
|------|-------------------------|--|
| 1 | PSUs | Enable to plug in the appropriate AC 3-prongs cord from the platform PSU to the external power source. |
| 2 | Fans | VEP 4600 supports an AC normal fan unit with fan airflow from the I/O to the PSU. The fan speed varies based on internal temperature monitoring. |

NOTE:

- The platform never intentionally turns off the fans.
- The hardware images in future are subject to updates and change.

Status LED indicators

Indicates the status of the system when an error occurs.

TABLE 10 : Status LED indicators and descriptions

| <i>Description</i> | <i>Condition</i> | <i>Action</i> |
|-----------------------|--|---|
| Drive indicator | The indicator turns solid amber if there is a drive error. | <ul style="list-style-type: none">• Check the System Event Log to determine if the drive has an error.• Run the appropriate Online Diagnostics test. Restart the system and run embedded diagnostics (ePSA).• If the drives are configured in a RAID array, restart the system, and enter the host adapter configuration utility program. |
| Temperature indicator | The indicator turns solid amber if the system experiences a thermal error (for example, the ambient temperature is out of range or there is a fan failure). | <p>Ensure that none of the following conditions exist:</p> <ul style="list-style-type: none">• A cooling fan has been removed or has failed.• System cover, air shroud, memory module blank, or back filler bracket is removed.• The ambient temperature is too high.• External airflow is obstructed. <p>If the problem persists, contact the support team.</p> |
| Electrical indicator | The indicator turns solid amber if the system experiences an electrical error (for example, voltage out of range, or a failed power supply unit (PSU) or voltage regulator). | <p>Check the System Event Log or system messages for the specific issue. If it is due to a problem with the PSU, check the LED on the PSU. Reset the PSU.</p> <p>If the problem persists, contact the support team.</p> |
| Memory indicator | The indicator turns solid amber if a memory error occurs. | <p>Check the System Event Log or system messages for the location of the failed memory. Reset the memory module.</p> <p>If the problem persists, contact the support team.</p> |
| PCIe indicator | The indicator turns solid amber if a PCIe card experiences an error | <p>Restart the system. Update any required drivers for the PCIe card. Reinstall the card.</p> <p>If the problem persists, contact the support team.</p> |

Service Tag Location

The unique Express Service Code and Service Tag help the user to identify the system. To view the Express Service Code and Service Tag pull out the information tag in front of the system. Alternatively, the information can be placed as a sticker on the chassis of the system. On the back of the system, a mini Enterprise Service Tag (EST) is found with the information of Dell EMC support center.

FIGURE 11 : Locating the Service Tag of your system



1. Information tag (front view)
2. Information tag (Rear view)
3. Open Manage Mobile (OMM) label
4. iDRAC MAC address and iDRAC secure password label
5. Service Tag

For more information on Dell, EMC Platform refer to:

- [Dell EMC PowerEdge R640](#)
- [Dell EMC PowerEdge R740](#)
- [VEP4600](#)

ASSIGNING MANAGEMENT IP TO DELL HOST

The Integrated Dell Remote Access Controller (iDRAC) is designed for system administrators to be more productive and improve the overall availability of Dell systems. iDRAC alerts administrators when there are system issues, helps them perform remote system management, and reduces the need for physical access to the system.

CAUTION: After configuring the iDRAC IP address, ensure that you change the default user name and password.

iDRAC IP Configuration

1. **Turn on** the management system.
2. Press **<F2>** during Power-On Self-Test (POST).



3. On the System Setup Main Menu page, click **iDRAC Settings**.
4. On the iDRAC Settings page, click **Network** to specify network settings.
5. Specify the network settings. Under Enable NIC, select **Enabled**.
 - Shared LOM (1, 2, 3 or 4) will share one of the NIC on the motherboard
 - Dedicated NIC uses the dedicated network interface
6. Set the IPv4 or IPv6 network settings, depending on the local configuration.
 - Initial network settings configuration includes setting up DHCP or the static IP for iDRAC. You can also set up the IP address or use the default iDRAC IP address 192.168.0.120. By default, the dedicated iDRAC network card is disabled.

- The iDRAC is sharing the network card on LOM 1 (LAN on Motherboard). In the case of blade servers, the iDRAC network interface is disabled by default.
7. Click **Back**.
 8. Click **Finish**.
 9. Click **Yes**. The network information is saved, and the system reboots.

NOTE: The iDRAC Web User Interface can be reached with any supported browser (IE, Firefox, Chrome, Safari).

ACOS UTILITIES COMMAND REFERENCE

This chapter provides the CLI utility command reference for Red Hat Enterprise Linux (RHEL) host system management. Use the CLI utilities for configuring automatic software updates, setting the management IP address, and restarting the UI.

For detailed information on setting up the virtual machines, attaching or detaching the VMs to the NIC VFs and SSL VFs, and importing images, host settings, and certificates, see MVP Manager.

The following are the commands provided by A10 Networks and must be run as 'sudo' command while logged in as the 'maintenance-admin'.

- The default password for the account is 'a10-networks-password'.
- It is recommended to change the password at initial login.
- In addition to the A10 utilities listed, 'reboot' and 'shutdown' commands are also available for usage.

Following topics are covered:

- [a10-config](#)
- [a10-show](#)
- [a10-update](#)
- [a10-gui](#)
- [a10-ifconfig](#)

a10-config

Syntax

```
sudo a10-config [--set | --get | --help] [options]
```

| Parameter | Description |
|------------|---------------------------|
| [no]--set | Will set the options |
| [no]--get | Will get the options |
| [no]--help | Will list the set options |

Example

To list the existing configuration, run the following command with no parameters:

```
[root@rhel7gui ~]# sudo a10-config
auto-install: true
auto-reboot: false
auto-time: * 0 * * *
```

To list the set options, pass --help to the --set command.

```
[root@rhel7gui ~]# sudo a10-config --set --help
auto-install: true|false
auto-reboot: true|false
auto-time: * * * * *
          | | | | |
          | | | | --- Day of week (0 - 7) (Sunday=0 or 7)
          | | | ----- Month (1 - 12)
          | | ----- Day of month (1 - 31)
          | ----- Hour (0 - 23)
          ----- Minute (0 - 59)
```

To enable automatic updates, use the --set auto-install true command.

```
[root@rhel7gui ~]# sudo a10-config --set auto-install true
Settings updated.
```

To set the time for executing auto updates, use --set auto-time. Make sure time set in quotes.

```
[root@rhel7gui ~]# sudo a10-config --set auto-time "*" 3 * * *"
Settings updated.
```

To allow system to automatically reboot when needed after auto updating setting use the --set --auto-reboot command.

```
[root@rhel7gui ~]# sudo a10-config --set auto-reboot true
Settings updated.
```

a10-show

Description

The command `a10-show` displays available updates and any pending reboot to be completed. It is not required to run in 'sudo'.

Syntax

```
a10-show[root@rhel7gui ~]# a10-show
No core libraries or services have been updated.
Reboot is probably not necessary.
Updates are available. You are on 0.0 and version 1.0 is the most recent.
```

System last updated on 2020-10-01 00:00:00

a10-update

Description

The command `a10-update` pulls the latest packages and install them on the server. If auto-reboot is set to true, and the update requires a reboot, the system will reboot upon completion.

- Use the `-n` flag parameter to suppress auto-reboot operation.
- Use the `-t` parameter to schedule the update for the future.
- The `-n` flag is ignored if `-t` is used.

Syntax

```
a10-update [-n | -t]
```

| Parameter | Description |
|-----------|----------------------------------|
| [no]-n | This parameters sets the options |
| [no]-t | This parameters gets the options |

Example

To schedule an update:

```
[root@rhtl7gui ~] # a10-update -n
```

The above command schedules an update for 3:30 AM (time is in a 24 hour clock) on Oct 21, 2021. If auto-reboot is true, then the system will reboot if necessary.

```
[root@rhtl7gui ~] # a10-update -t 0330 102121
```

a10-gui

Description

The command `a10-gui` can start, stop, and restart the GUI services from a terminal session.

Syntax

```
a10-gui [--restart | --stop | --start]
```

| Parameter | Description |
|----------------|---------------------------|
| [no] --restart | Restart the GUI services. |
| [no] --stop | Stop the GUI services. |
| [no] --start | Start the GUI services. |

Example

Restart the GUI services.

```
# sudo a10-gui --restart
```

Stop the GUI services.

```
# sudo a10-gui --stop
```

Start the GUI services.

```
# sudo a10-gui --start
```

a10-ifconfig

| | |
|--------------|--|
| Description | If the command <code>a10-ifconfig</code> sets the IPv4 configuration for the management port. The server is shipped DHCP enabled. |
| Syntax | <pre>a10-ifconfig management --dhcp (--ip4 x.x.x.x --prefix nn -- dns x.x.x.x --gateway x.x.x.x)</pre> |
| NOTE: | The parameter 'management' must be first. All others parameter the order after that is not stringent. |
| Example | <p>Configuring the management port for DHCP.</p> <pre># sudo a10-ifconfig management --dhcp</pre> <p>A static IP address passed in the configuration parameters.</p> <pre># sudo a10-ifconfig management --ip4 10.64.36.22 --prefix 24 -- dns 8.8.8.8 --gateway 10.64.36.1</pre> |

LICENSE MANAGEMENT

The hardware devices requires a license to operate. Without a license, the product cannot run production traffic, and the amount of bandwidth is only sufficient for testing network connectivity.

Global License Manager (GLM) is the primary portal for license management for A10 products. The GLM provides a GUI where you can view and manage advanced licensing functions. Creating a GLM account is optional. A GLM account enables you to perform advanced licensing functions and, where applicable, view, and monitor device usage. The GLM portal can be accessed at <https://glm.a10networks.com> and for new GLM account contact sales@a10networks.com.

The A10 Thunder Dell Appliances support the perpetual license. This licensing model is based on bandwidth. It is obtained by activation of key license for your A10 virtual appliance, URL Classification License installation, and GLM account management. All licenses are generated and installed manually.

NOTE: When a vThunder license expires, the functionality will continue at a reduced bandwidth.

For more information about license types and their activation procedure see Global License Manager guide available in the [Licensing User Guides](#) section.

For the A10 Thunder Dell Appliances, A10 networks provide a pre-licensed type of license. A pre-license is available per CPU per hour basis. For more information contact the A10 networks sales team at sales@a10networks.com.

vTHUNDER INITIAL CONFIGURATION

This section describes how to configure the device.

The following topics are covered:

- [Configuration Mode](#)
- [Management Interface Configuration](#)
- [Password Management](#)
- [Saving Changes](#)

Configuration Mode

To display commands in CLI, enter a question mark (?) and press Enter. The command list is displayed for each level. For syntax help, enter a command or keyword followed by a **space**, followed by pressing **Enter**. This works for commands with sub-commands also.

1. Log into vThunder with the default username **admin** and password **a10**.

```
login as: admin
Welcome to vThunder
Using keyboard-interactive authentication.
Password:***
[type ? for help]
```

2. Enable the Privileged EXEC level by typing **enable** and **Enter**.
There is no default password to enter Privileged EXEC mode.

```
vThunder>enable
Password:(just press Enter on a new system)
vThunder#
```

3. Enable the configuration mode by typing **config** and press **Enter**.

```
vThunder#config
vThunder(config)#
```

NOTE:

It is strongly recommended that a Privileged EXEC enable password is set up as: `vThunder(config)#enable-password [newpassword]`

Management Interface Configuration

Assign an IP to the management interface of the vThunder:

1. Configure the management interface IP address and default gateway. ACOS will obtain an IP for the management interface in the following order:
 - a. If there is a management port IP configuration (either a static IP address or DHCP) in the active startup-config file, then ACOS will either assign the static IP to the vThunder management interface or will attempt to get the IP address from the DHCP server.
 - b. If there is no management port IP configuration (neither a static IP address nor DHCP), then vThunder will attempt to get an IP address from an accessible DHCP server.
 - c. If vThunder cannot obtain an IP address from a DHCP server, then the default static IP address of "172.31.31.31/24" will be used.

NOTE: The management interface is an out-of-band interface and should not be on the same subnet as any of the data interfaces. If the management interface and the data interfaces are **not** kept in separate IP subnets, some operations such as pinging may not work as expected.

In the example below, the IP address for the management interface is 192.168.2.228. None of the data interfaces should have an IP address of 192.168.2.x.

```
vThunder(config)#interface management
vThunder(config-if:management)#ip address 192.168.2.228 /24
vThunder(config-if:management)#ip default-gateway 192.168.2.1
Verify the interface IP address change:
vThunder(config-if:management)#show interface management
GigabitEthernet 0 is up, line protocol is up.
Hardware is GigabitEthernet, Address is xxxx.yyyy.zzzz
Internet address is 192.168.2.228, Subnet mask is 255.255.255.0
```

2. Optionally, configure the ACOS device to use the management interface as the source interface for automated management traffic generated by the ACOS device:

```
ACOS(config-if:management)#ip control-apps-use-mgmt-port
```

```
vThunder(config-if:management)#exit
vThunder(config)#
```

Password Management

A10 recommends changing the administrator password immediately for security.

```
vThunder(config)#admin admin password newpassword
vThunder(config-admin:admin)#
```

The vThunder is now network accessible for configuration under the new IP address and admin password.

NOTE: By default, Telnet access is disabled on all interfaces, including the management interface. SSH, HTTP, HTTPS, and SNMP access are enabled by default on the management interface only and disabled by default on all data interfaces.

Saving Changes

Configuration changes must be saved to system memory to take effect the next time the vThunder device is powered on. Otherwise, the changes are lost when the vThunder virtual machine or its host machine is powered down.

To write the current configuration to system memory:

```
vThunder(config)#write memory
Building configuration...
[OK]
```

NOTE: For more information, see Command Line Interface Reference for SLB and SSL guides.

SLB CONFIGURATIONS

Server Load Balancing (SLB) allows you to share and distribute the load among multiple servers, thus improving throughput and performance beyond the capabilities of any single server. It also provides fault tolerance and redundancy. Distributing the load among multiple devices enables more network reliability in the event when one server becomes unavailable.

The primary goals of server load balancing are to:

- Share and distribute the load among multiple servers, thus improving throughput and performance beyond the capabilities of any single server.
- Provide fault tolerance and redundancy. Distributing the load among multiple devices enables more network reliability if one server becomes unavailable.

This section defines common load balancing terms that are used throughout this and another documents. Topics covered in this section include:

- [Real Server](#)
- [Service Group](#)
- [Virtual Server and Virtual IP \(VIP\)](#)
- [Wild-card VIPs, Ports, and Virtual Ports](#)

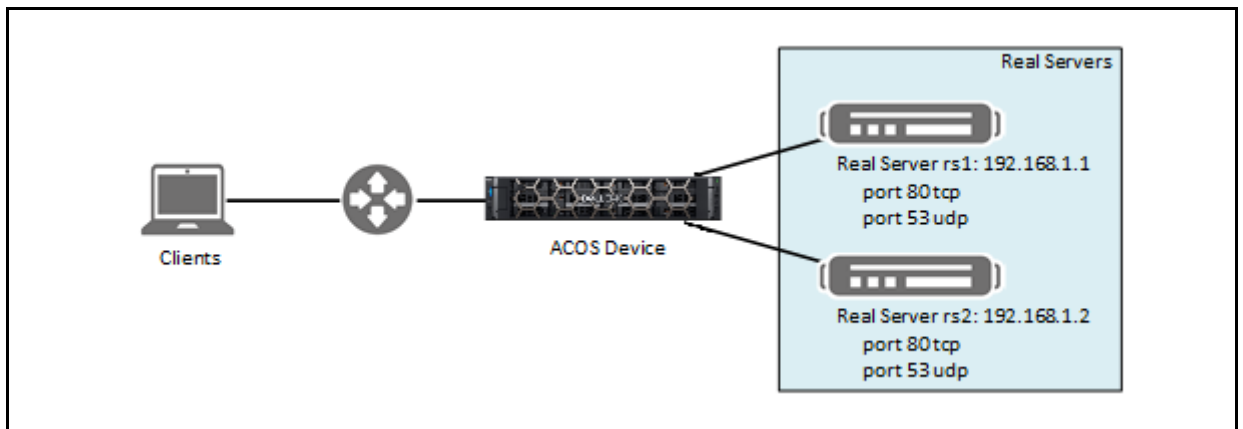
Real Server

A real server is a physical server (either individual servers or servers in a server farm) connected to the ACOS device, or another switch in the network. [Figure 12](#) displays real servers in a basic SLB deployment.

To configure a real server, use the **slb server** command from the CLI. The minimum configuration for a real server includes the following:

- Name (for example, rs1)
- IP address (for example, 192.168.1.1) or DNS name
- Ports (for example, port 80 for TCP)

FIGURE 12 : Real Servers



The following is an example of a real server configuration.

```
ACOS(config)# slb server rs1 192.168.1.1
ACOS(config-real server)# port 80 tcp
ACOS(config-real server-node port)#
```

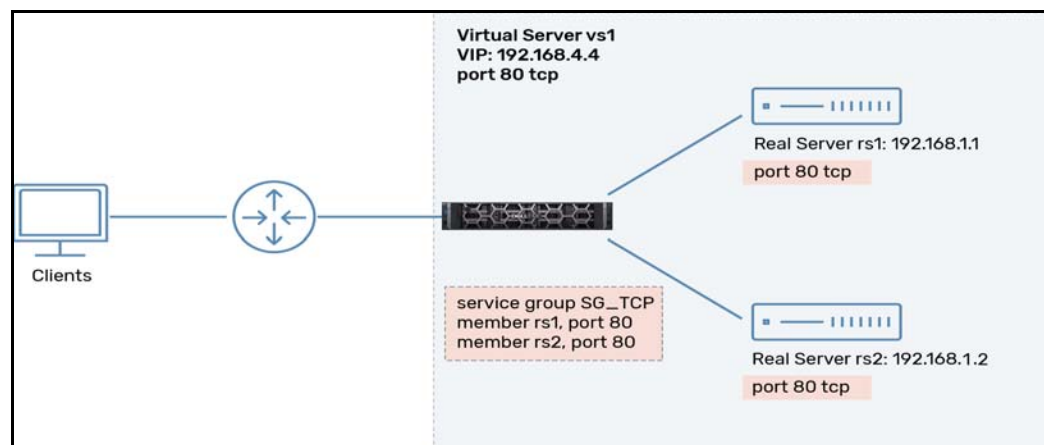
Service Group

A service group is a group of servers that fulfill a service. Service groups are where load balancing algorithms are applied. [Figure 13](#) displays a topology that utilizes two service groups.

Service groups are configured by using the **slb service-group** command from the CLI. The minimum configuration for a service group include the following:

- Name (for example, sg1)
- Type (for example, TCP)
- Load balancing algorithm (for example, round-robin)
- At least one member real server and port (for example, rs1 and port 80)

FIGURE 13 : Service Groups



Below is an example of this minimum configuration. First, configure two real servers “rs1” and “rs2”. The servers will use port 80 for TCP and port 53 for UDP:

```
ACOS(config)# slb server rs1 192.168.1.1
ACOS(config-real server)# port 80 tcp
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit
ACOS(config)# slb server rs2 192.168.1.2
ACOS(config-real server)# port 80 tcp
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit
```

Then, configure the service group “SG_TCP” and add the servers (port 80 only) as members of the group. Because round-robin load balancing is the default algorithm; the method command is not necessary.

```
ACOS(config)# slb service-group SG_TCP tcp
ACOS(config-slb svc group)# member rs1 80
ACOS(config-slb svc group-member:80)# exit
ACOS(config-slb svc group)# member rs2 80
ACOS(config-slb svc group-member:80)# exit
ACOS(config-slb svc group)# exit
```

Virtual Server and Virtual IP (VIP)

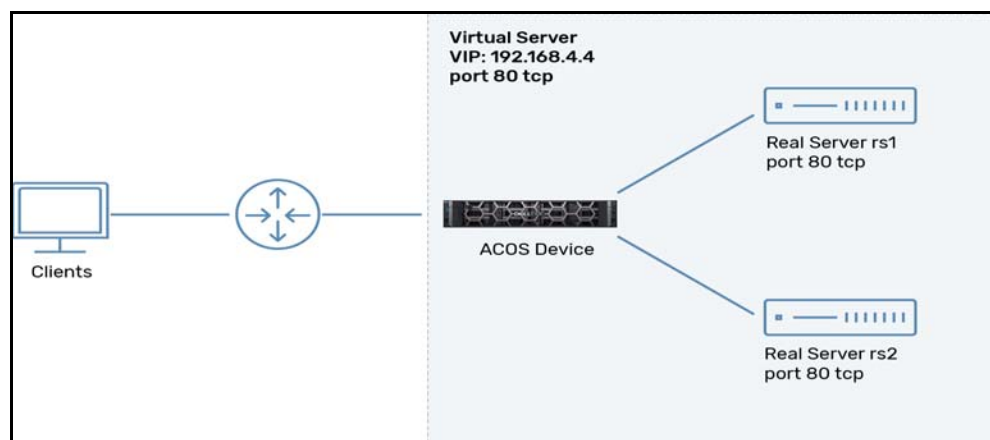
A virtual server is a combination of real servers and ACOS devices, which together appear as a single server to the client.

A virtual IP (VIP) is a virtual server IP address. Clients use this IP address to access the virtual server and are configured on the ACOS device. To a client, the VIP represents the individual real server or server farm.

Virtual servers and VIPs are configured by using the **slb virtual-server** command from the CLI. The minimum configuration for a virtual server include the following:

- Name (for example, vs1)
- IP address (for example, 192.168.4.4)
- Ports (for example, port 80 for TCP)

FIGURE 14 : Virtual Server and VIP



These commands are an example of this minimum configuration:

```
ACOS(config)# slb virtual-server vs1 192.168.4.4
ACOS(config-slb vserver)# port 80 tcp
ACOS(config-slb vserver-vport)#
```

Wild-card VIPs, Ports, and Virtual Ports

A wild-card VIP is a VIP that does not have a specific IP address. Instead, wild-card VIPs have IP address 0.0.0.0 (for IPv4) or 0000:0000:0000:0000:0000:0000:0000:0000 (for IPv6). Client requests sent to any IP address will be accepted when they are received at a wild-card VIP. Below is an example configuration for a wildcard VIP that will accept TCP requests on port 80:

```
ACOS(config)# slb virtual-server wildcard-vs1 0.0.0.0
ACOS(config-slb vserver)# port 80 tcp
ACOS(config-slb vserver)# slb virtual-server vs1 192.168.4.4
ACOS(config-slb vserver)# port 80 tcp
ACOS(config-slb vserver)# service-group SG_TCP
ACOS(config-slb vserver-vport)# exit
ACOS(config-slb vserver)# exit
```

Wild-card VIPs allows you to configure a feature that applies to multiple VIPs, without the need to re-configure the feature separately for each VIP. To specify the subset of VIP addresses and ports for which a feature applies, you can use an Access Control List (ACL). ACLs' also can specify the subset of clients allowed to access the VIPs, thus ensuring that only legitimate requests are allowed through to the real servers.

NOTE: Wild-card VIPs can be used for any type of load balancing. Port 0 is used as a wild-card port to match on any port number.

SSL CONFIGURATION

This section describes managing SSL certificates, private keys, and Certificate Revocation Lists (CRLs). An ACOS device can offload SSL processing from servers or, for some types of traffic, can be used as an SSL proxy.

The following topics are covered:

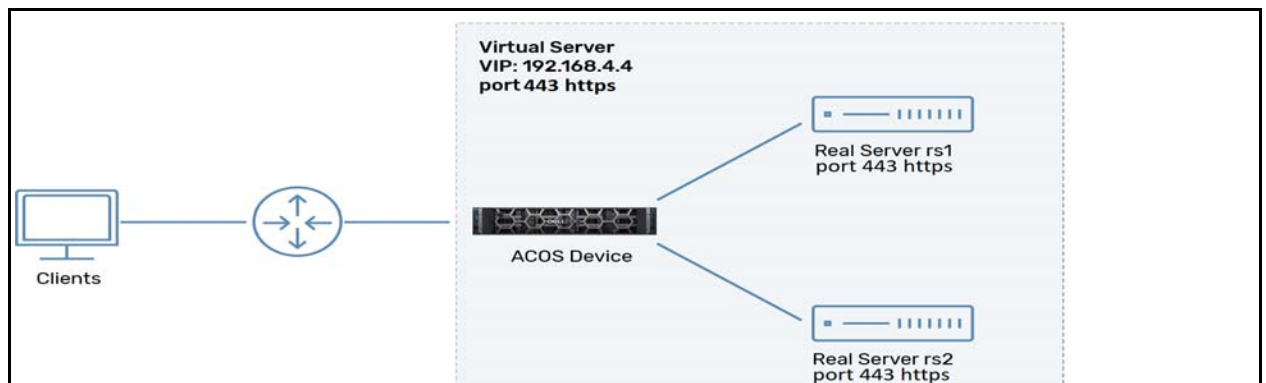
- [SSL Offload](#)
- [SSL Templates](#)
- [Managing CAs and CSRs](#)

SSL Offload

SSL offloading removes SSL based encryption from incoming traffic, which is received by a web server to clear it from decryption of data.

This in turn also configures the HTTPS virtual port type to enable the SSL handshake and optionally configures the HTTP template to enable packet inspection and header manipulation.

FIGURE 15 : SSL Offload (Load Balancing HTTPS Traffic)



CLI Configuration

- Configure a virtual server and add a virtual port that has the service type `https`. Bind the service-group to the virtual port and to the HTTP template (if configured) and client-SSL template.

The SSL offload feature is enabled by the `https` option of the `port` command.

```

ACOS(config)# slb virtual-server v1 192.168.4.4
ACOS(config-slb vsrver)# port 443 https
ACOS(config-slb vsrver-vport)# service-group SG_TCP
ACOS(config-slb vsrver-vport)# template client-ssl sslcert-tmpl
  
```

- In this example, traffic between the servers and ACOS is not encrypted.
 - If traffic between the servers and ACOS is also encrypted, you also need to configure a server-SSL template and bind it to the virtual port. In configurations that use both client-SSL and server-SSL, use the HTTPS/SSL port number in the real server configuration.
 - If only client-SSL is used, use the HTTP port number in the real server configuration. Use the HTTPS/SSL port number in the virtual server configuration.
 - If you configure server-SSL without client-SSL, the virtual port service type must be HTTP; not HTTPS.

GUI Configuration

- Configure client SSL template using [SSL Offload \(Load Balancing HTTPS Traffic\)](#)

- Configure a virtual server and add a virtual port that has the service type **HTTPS**. Bind the service-group to the virtual port and to the **Template HTTP** (if configured) and **Template Client-SSL**.
 - a. Select **ADC > SLB**.
 - b. Select the **Virtual Servers** tab from the menu bar.
 - c. Click **Create**.
 - d. In the **Name** field, enter a name for the virtual server.
 - e. Select the **Address Type** radio button (IPv4 or IPv6), and then enter the VIP address. This is the IP address to which client requests will be sent.
 - f. In the Virtual Port section, click **Create**.
 - g. From the page that appears, click the **Protocol** drop-down menu and select **HTTPS**.
The SSL offload feature is enabled by the **HTTPS** option.
 - h. In the **Port** field, enter the service port number.
 - i. Click the **Service Group** drop-down menu and select the service group.
 - j. Click **Templates** to expand the template configuration options.
 - k. Click the **Template HTTP** drop-down list and select the template you configured earlier.
 - l. Click the **Template Client-SSL** drop-down list and select the desired template.
 - m. Click **Create**. The port appears in the Port list for the virtual server.
 - n. Click **Update**. The virtual server appears in the virtual server table.
- In this example, traffic between the servers and ACOS is not encrypted.
 - If traffic between the servers and ACOS also is encrypted, you also need to configure a server-SSL template and bind it to the virtual port. In configurations that use both client-SSL and server-SSL, use the HTTPS/SSL port number in the real server configuration.
 - If only client-SSL is used, use the HTTP port number in the real server configuration. Use the HTTPS/SSL port number in the virtual server configuration.
- When configuring server-SSL without client-SSL, the virtual port service type must be HTTP, not HTTPS.

SSL Templates

You can install more than one key-certificate pair on the ACOS device. The ACOS device selects the certificate(s) to send a client or server based on the SSL template bound to the VIP. You can bind the following types of SSL templates to VIPs:

- Client-SSL template – Contains keys and certificates for SSL-encrypted traffic between clients and the ACOS device. A client-SSL template can also contain a certificate chain.
- Server-SSL template – Contains CA certificates for SSL-encrypted traffic between servers and ACOS device.

CLI Configuration

NOTE: The procedure of importing or creating certificates are the same whether they are used in an SSL proxy deployment or an SSL off-load deployment. Similarly, the procedure for configuring a client SSL template is the same for SSL proxy and SSL offload.

1. Import or create a certificate and its key to use for TLS sessions with clients. The configuration example in this chapter uses an imported SSL certificate and private key.

```
ACOS# import cert sslcert1.crt ftp:
Address or name of remote host []?1.1.1.2
User name []?Admin-15
Password []?*****
File name [/]?sslcert1.crt
ACOS# import key sslcertkey.pem ftp:
Address or name of remote host []?1.1.1.2
User name []?Admin-15
Password []?*****
File name [/]?sslcertkey.pem
```

2. Configure a client SSL template, bind the SSL certificate and private key to it.

ACOS uses SSL certificates with a private key to create proxied signed certificates for handshaking with SSL clients. SSL clients are configured to use a private CA that verifies the proxied certificate's validity.

```
ACOS(config)# slb template client-ssl sslcert-tmpl
ACOS(config-client ssl)# cert sslcert.crt
ACOS(config-client ssl)# key sslcertkey.pem
ACOS(config-client ssl)# exit
```

GUI Configuration

1. Import the SSL certificate:
 - a. Select **ADC > SSL Management > SSL Certificates > Import**
2. Enter the file name, the category of the import (Certificate), the location of the import (Local, Remote, or Text; if Remote or Text is selected the appropriate fields will pop up to indicate IP or text content), certificate format, and the certificate source for file search.
3. Click **Import**.
4. Import the SSL key:

- a. Select **ADC>SSL Management> SSL Certificates> Import**
 - b. Enter the file name, the category of the import (Key), the location of the import (Local, Remote, or Text), and the key source for file search.
 - c. Click **Import**.
5. Create the client SSL template using the imported certificate and key:
- a. Select **ADC> Templates> SSL**.
 - b. Select **Create** to pull the drop-down menu, and click **Client SSL**.
 - c. In the **Name** field, specify a name for the Client SSL template.
 - d. In the **Server Certificate** field, select an imported or configured SSL certificate, and in the **Server Private Key** field, select an imported or configured key. ACOS uses the SSL certificates with the private key to create proxied signed certificates for handshaking with SSL clients. The SSL clients are configured to use a private CA that verifies the proxied certificate's validity.
 - e. Click **OK** to finish.

Managing CAs and CSRs

Installing SSL resources on the ACOS device enables the device to provide SSL services on behalf of real servers. The following topics are covered in this section:

- [Certificate and Key](#)
- [Generating a SSL Certificate](#)
- [Generating a Certificate Signing Request \(CSR\)](#)
- [Generating a Self-Signed Certificate and Key](#)
- [Installing the Certificate](#)

Certificate and Key

To import certificate and key files, place them on the PC that is running the ACOS GUI or CLI session, or onto a PC or file server that ACOS can reach and fetch the files.

Importing Individual Files

To import an SSL certificate CA certificate, certificate chain, or private key, follow these instructions.

GUI Configuration

Import Certificates using GUI:

1. Navigate to **ADC > SSL Management > SSL Certificates**.
2. Click **Import** to import a certificate or certificate chain.
 - a. In the **File Name** field, enter a name for the certificate.
 - b. In the **Import** field, select the item you want to import
 - c. In the **Import Certificate from** field, select **Local** to import from a local drive on your management PC, **Remote** to import from a remote location, or **Text** to import from the text box that appears.
 - d. In the **SSL or CA Certificate** field, select either an **SSL Certificate** or **CA Certificate**.

NOTE: If you are importing a CA-signed certificate for which you used ACOS to generate the CSR, you do not need to import the key. The key is automatically generated by ACOS when you generate the CSR.

- e. In the **Certificate Format** field, select the file format of the certificate you are importing. Certificate and private keys in a single file use the PFX format, which is automatically chosen.
 - f. The **Certificate Source** field provides the location and other fields you need to import the selected item.
 - g. Decide whether to enable or disable the **Overwrite Existing File** option.
3. Click **Import**.

CLI Configuration

Import Certificates using CLI:

- Use the **import cert** command to import a certificate or certificate chain that you will be using with its private key to create proxy certificates for SSL handshaking with clients in the SSLi, SSL Proxy or SSL offload applications. If you import the cert and its key in a single file use the PFX format.
- Use the **import ca-cert** command to import a certificate or a certificate chain for certificates for verifying SSL servers and authenticating clients and other purposes. However the CA cert cannot be used for creating proxied signed certificates for handshaking with clients.

NOTE: If you are importing a CA-signed certificate for which you used ACOS to generate the CSR, you do not need to import the key. The key is automatically generated by ACOS when you generate the CSR.

- Use the `import cert-key` command to import a private key.

Generating a SSL Certificate

The following procedures generate an SSL self-signed certificate with a private key and also generates a CSR that you can send to a publicly recognized CA to register your self-signed SSL certificate.

This process also creates a public key - private key pair. The public key is sent in the CSR. The private key is used to encrypt the CSR and also to create the SSL proxied certificate used in the ACOS SSLi, SSL-Offload, and SSL-Proxy applications.

GUI Configuration

Generate a SSL Certificate - Private Key File with a CSR using GUI

1. Navigate to **ADC > SSL Management > SSL Certificates**.
2. Click **+Create**. The **Create SSL Certificates** dialog window appears.
 - a. In the **Create As** field, select **Certificate**.
 - b. In the **File Name** field, type the name you certificate that will be generated.
 - c. Click the **CSR Generate** box to enable the creation of a CSR.
 - d. In the **Cert Type** field, select **RSA** or **ECDSA** depending on which cryptography standard you want.
 - e. The **Common Name** field is required.

NOTE: If you need to create a request for a wild-card certificate, use an asterisk as the first part of the common name. For example, to request a wild-card certificate for domain example.com and it sub-domains, enter the following common name: *.example.com

- f. The **Division, Organization, Locality, State or Province**, and **Email** fields are optional.
- g. Enter a number the **Valid Days** (how many days the key will remain valid) and **Key Size**, or accept the defaults 730 days and 1024 bytes.

3. Click **OK**.
4. Verify the newly created SSL cert appears in the **ADC > SSL Management > SSL Certificates** page. Check the matching **Name** and **Common Name** fields. The **Type** should be **certificate/key**, and the expiration should match the number of days the cert remains valid. See RFC 6125 for help in reading the **Issuer** field. The GUI does not display the CSR separately.

Generating a Certificate Signing Request (CSR)

The following procedures generate a CSR that you can send to a server so that the server can send the CSR to a CA to request a new CA-signed certificate or renew an existing one.

This process also creates a public key and a private key pair. The public key is sent in the CSR. The private key used to encrypt the CSR.

Generating a CSR using GUI

1. Navigate to **ADC > SSL Management > SSL Certificates**.
2. Click **+Create**. The **Create SSL Certificates** dialog window appears.
 - a. In the **Create As** field, select **CSR**.
 - b. In the **File Name** field, type the name you certificate that will be provided by the CA.
 - c. In the **Digest** field, select the hashing algorithm used. The default is **sha1**.
 - d. In the **Certificate Type** field, select **RSA** or **ECDSA** depending on which cryptography standard you want.
 - e. The **Common Name** field is required.

NOTE: To create a wild-card certificate request, use an asterisk for the first part of the common name. For example, to request a wild-card certificate for domain example.com and its sub-domains, enter *.example.com as the common name.

- f. The **Division, Organization, Locality, State or Province**, and **Email** fields are optional.
 - g. Enter a number the **Valid Days** (how many days the key will remain valid) and **Key Size**, or accept the defaults 730 days and 1024 bytes.
3. Click **OK**.
4. Verify the newly created SSL cert appears in the **ADC > SSL Management > SSL Certificates** page. Check the matching **Name** and **Common Name** fields. The **Type**

should be **key**, and the expiration should match the number of days the cert remains valid. See RFC 6125 for help in reading the **Issuer** field.

Generating a Self-Signed Certificate and Key

In the following procedure, the certificate file also includes the corresponding private key.

See RFC 6125 for help in filling out some of the following fields.

Generating a Self-Signed Certificate and Key using GUI

1. Navigate to **ADC > SSL Management > SSL Certificates**.
2. Click **+Create**. The **Create SSL Certificates** dialog window appears.
 - a. In the **Create As** field, select **Certificate**.
 - b. In the **File Name** field, type the name you certificate that will be generated.
 - c. Keep **CSR Generate** check box unchecked. This check box enables the creation of a CSR.
 - d. In the **Cert Type** field, select **RSA** or **ECDSA** depending on which cryptography standard you want.
 - e. The **Common Name** field is required.

NOTE:

If you need to create a request for a wild-card certificate, use an asterisk as the first part of the common name. For example, to request a wild-card certificate for domain example.com and its sub-domains, enter the following common name: *.example.com

- f. The **Division, Organization, Locality, State or Province**, and **Email** fields are optional.
 - g. Enter a number the **Valid Days** (how many days the key will remain valid) and **Key Size**, or accept the defaults 730 days and 1024 bytes.
3. Click **OK**.
4. Verify the newly created SSL cert appears in the **ADC > SSL Management > SSL Certificates** page. Check matching **Name** and **Common Name** fields. The **Type** should be **certificate/key**, and the expiration should match the number of days the cert remains valid. See RFC 6125 for help in reading the **Issuer** field.

Installing the Certificate

To configure an ACOS device to perform SSL processing on behalf of real servers, you must install a certificate on the ACOS device. This certificate is the one that the ACOS device will present to clients during the SSL handshake. You also must configure a client-SSL template, add the key and certificate to the template, and bind the template to the VIP that will be requested by clients.

This section gives an overview of the process for each type of certificate and detailed procedures as:

- [Request and Install a CA-Signed Certificate](#)
- [Install a Self-Signed Certificate](#)

Request and Install a CA-Signed Certificate

To request and install a CA-signed certificate, use the following process. For detailed steps, refer to the [Certificate and Key](#) sections.

1. Create an encryption key.
2. Create a Certificate Signing Request (CSR).

The CSR includes the public portion of the key, as well as information you enter when creating the CSR. You can create the key and CSR on an ACOS device or a server running OpenSSL on a similar application.

3. Submit the CSR to the CA.

If the CSR was created on the ACOS device, do one of the following:

- Copy and paste the CSR from the ACOS CLI or GUI onto the CSR submission page of the CA server.
- Export the CSR to another device, such as the PC from which you access the ACOS CLI or GUI. Email the CSR to the CA, or copy-and-paste it onto the CSR submission page of the CA server.

If the CSR was created on another device, email the CSR to the CA, or copy-and-paste it onto the CSR submission page of the CA server.

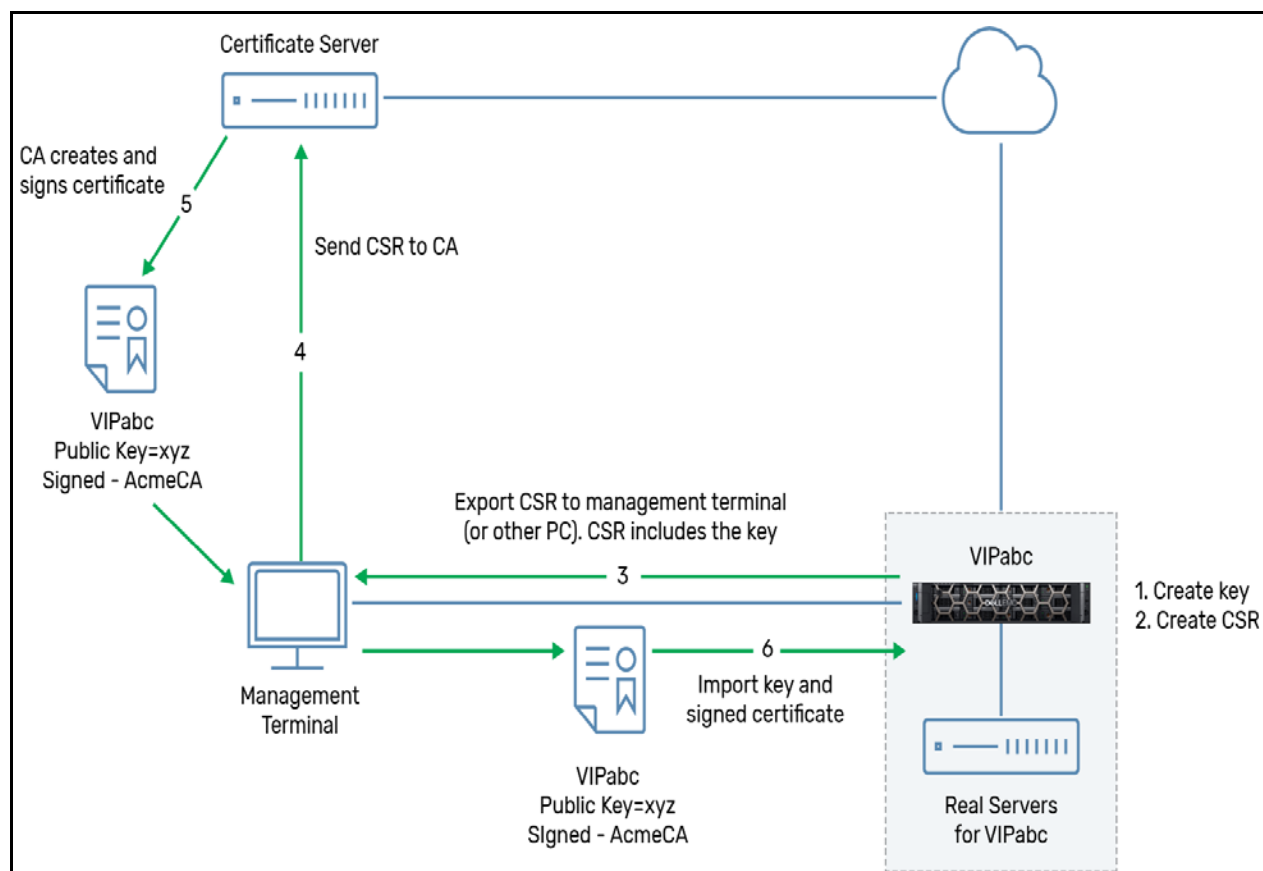
4. After receiving a signed certificate and the CA's public key from the CA, import them to the ACOS device.
 - If the key and certificate are provided by the CA in separate files (PKCS #7 format), import the certificate. The key does not need to be imported if the CSR was created on the ACOS device because the key is already on the ACOS device. If the certificate is not in PEM format, specify the certificate format (type) when importing it.

If the CSR was not created on the ACOS device, you do need to import the key also.

- If the key and certificate are provided by the CA in a single file (PKCS #12 format), specify the certificate format (type) when you import it. If the CSR was not created on the ACOS device, you need to import the key also.
- If applicable, import the certificate chain onto the ACOS device. The certificate chain must be a single text file, beginning with a root CA's certificate at the top, followed in order by each intermediate signing authority's certificate.

[Figure 16](#) shows the most common way to obtain and install a CA-signed certificate onto the ACOS device. You also may need to install a certificate chain file.

FIGURE 16 : Obtaining and Installing Signed Certificate from CA



NOTE:

As an alternative to using a CA, you can use an application such as **OpenSSL** to create a certificate, then use that certificate as a CA-signed certificate to sign another certificate. In this case, a client's browser is still likely to display a certificate warning to the end-user.

Install a Self-Signed Certificate

To install a self-signed certificate instead of a CA-signed certificate:

1. Create an encryption key.
2. Create a certificate.

For more information, refer to [Generating a Self-Signed Certificate and Key](#).

DEPLOYMENT MODE

The ACOS device can be deployed in different types of networking modes for server load balancing.

Different types of deployments are:

- Gateway Mode
- Transparent Mode
- Direct Server Return
- Route Health Injection

We have provided an example using Gateway mode below.

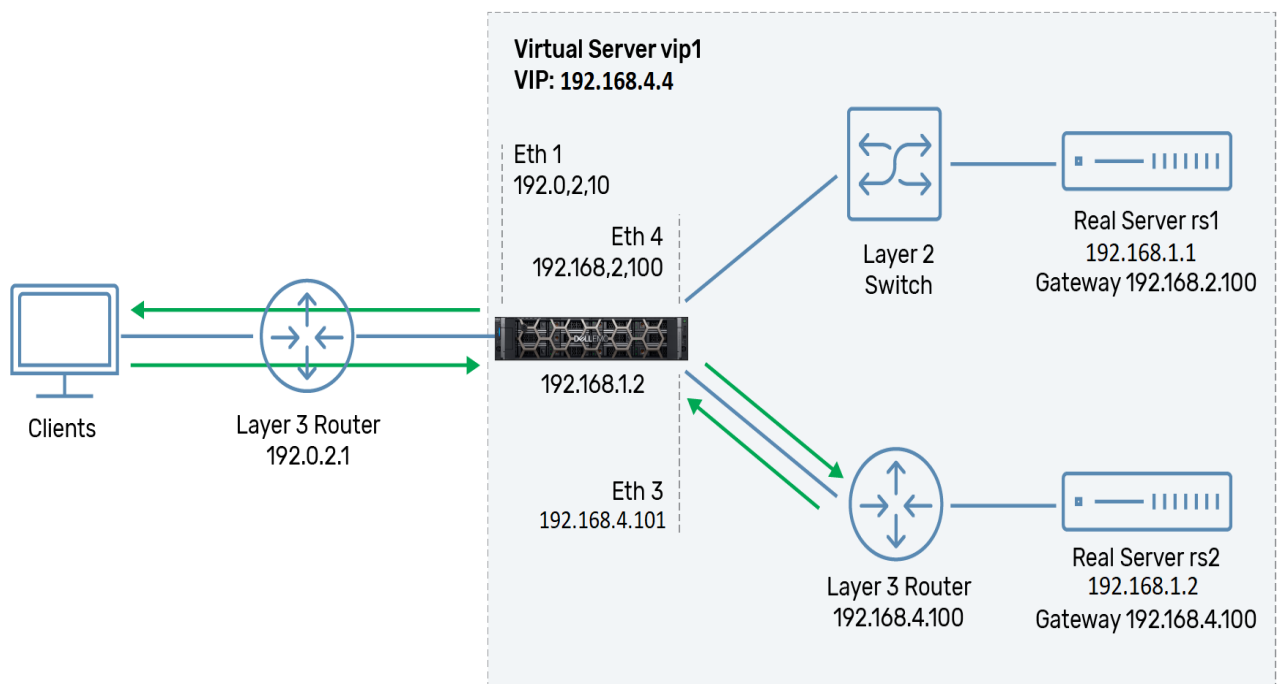
Gateway (Router) Mode

Gateway (router) mode provides the same Layer 2 functionality as transparent mode and performs Layer 3 features, such as IP NAT, Access-lists, static routes, RIP, OSPF, IS-IS, PBR, and BGP. Layer 3 features provide flexibility when integrating the ACOS device into the network. ACOS devices in route mode support separate IP addresses on each data interface.

Topology

[Figure 17](#) displays an ACOS device deployed in gateway mode.

FIGURE 17 : ACOS Deployment Example – Gateway Mode



The arrows display client-server traffic flow between clients and server 192.168.4.101. Real servers can reach the database server through the ACOS device just as they would through any other router. Replies to clients still travel from the real servers through the ACOS device back to the client.

In the above example, the ACOS device has separate IP interfaces in different subnets on each interface connected to the network. The ACOS device can be configured with static IP routes and enabled to run routing protocols such as OSPF and IS-IS. The example configures a static route as the default route through 192.0.2.1.

Although this example shows single physical links, you could use trunks as physical links. You also could use multiple VLANs. In this case, the IP addresses would be configured on Virtual Ethernet (VE) interfaces, one per VLAN, instead of being configured on individual Ethernet ports.

Since the ACOS device is a router in this deployment, downstream devices can use the ACOS device as their default gateway. The router connected to port 3 would use 192.168.1.111 as its default gateway, and the Layer 2 switch connected to 192.168.2.100 would use that address as its default gateway.

If a pair of ACOS devices in a VRRP-A configuration is used, the downstream devices would use a floating IP address shared by the two ACOS devices as their default gateway. (For more on VRRP-A, see the [Configuring VRRP-A High Availability](#) guide.) Source NAT is not required for this configuration. The ACOS device can send health checks to the real servers and receive the replies without NAT.

Configuration Example

Use the GUI to configure the topology shown in [Figure 17](#), perform the following tasks.

Interface Configuration

1. Navigate to Network > Interfaces > LAN.
2. Click Edit in the Actions column for interface e1.
3. Click Enable in the Status field.
4. Expand the IP pane.
5. Enter 192.0.2.10 in the "IPv4 Address" column of the table in the IP Address field.
6. Enter 255.255.255.0 in the "Netmask" column of the table in the IP Address field.
7. Click Update. (not shown in the figure).
8. Repeat the procedure to configure the other interfaces and IP addresses.

Update Ethernet

General Fields

| | |
|---------------------------------------|---|
| IF Num * | 1 |
| Name | |
| Status | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Trap Source | <input type="checkbox"/> |
| Duplexity | auto |
| Flow Control | <input type="checkbox"/> |
| MTU | 1500 |
| Speed | auto |
| Load Interval | 300 |
| ICMP Rate Limit | <input type="checkbox"/> |
| ICMPv6 Rate Limiting | <input type="checkbox"/> |
| L3 Vlan Fwd Disable | <input type="checkbox"/> |
| Configure LW-4over6 inside interface | <input type="checkbox"/> |
| Configure LW-4over6 outside interface | <input type="checkbox"/> |

IP

| Generate Membership Query | <input type="checkbox"/> | | | | | | |
|---------------------------|---|----------------------------------|---------|--|------------|---------------|----------------------------------|
| Allow Promiscuous VIP | <input type="checkbox"/> | | | | | | |
| Cache Spoofing Port | <input type="checkbox"/> | | | | | | |
| DHCP | <input type="checkbox"/> | | | | | | |
| IP Address | <input type="text"/> <input type="text"/> <input type="button" value="Add"/> | | | | | | |
| | <table><thead><tr><th>IPv4 Address</th><th>Netmask</th><th></th></tr></thead><tbody><tr><td>192.0.2.10</td><td>255.255.255.0</td><td><input type="button" value="✕"/></td></tr></tbody></table> | IPv4 Address | Netmask | | 192.0.2.10 | 255.255.255.0 | <input type="button" value="✕"/> |
| IPv4 Address | Netmask | | | | | | |
| 192.0.2.10 | 255.255.255.0 | <input type="button" value="✕"/> | | | | | |

Default Route Configuration

To configure the static route:

1. Navigate to Network > Routes > Static IPv4 Routes.
2. Click Create.
3. Enter 0.0.0.0 in the IP Dest Address field.
4. Enter /0 in the IP Mask field.
5. Enter 192.0.2.1 in the "Next Hop IP" column of the IP Next Hop field, and click Add.
6. Click Create Route.

SLB Configuration - Real Servers

Configure the real servers:

1. Navigate to ADC > SLB > Servers.
2. Click Create.
3. Enter rs1 in the Name field.
4. Enter 192.168.2.101 in the Host field.
5. In the Port section, click Create. In the Update Port page:
 - a. Enter 80 in the Port Number field.
 - b. Select TCP from the drop-down list in the Protocol field (should be the default value).
 - c. Click Create.
6. Click Update.
7. Repeat this procedure to create server rs2 with the IP address 192.168.4.101.

ADC >> SLB >> Servers >> Update Help

Update Server

| | |
|----------------------|---|
| Name * | s1 |
| Type | <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> FQDN |
| Host * | 192.0.2.50 |
| Action | Enable |
| Disable Health Check | <input type="checkbox"/> |
| Health Monitor | |
| Connection Limit | 8000000 |
| No Logging | <input type="checkbox"/> |

Advanced Fields +

Port

Delete Create

| | Port | Protocol | Weight | Conn Limit | Health Check | Range | Conn Resume | Actions |
|--------------------------|------|----------|--------|------------|--------------|-------|-------------|---------|
| <input type="checkbox"/> | 80 | tcp | 1 | 8000000 | Default | 0 | | Edit |

Cancel Update

SLB Configuration - Service Group

Configure the service groups.

1. Navigate to ADC > SLB > Service Groups.
2. Click Create.
3. Enter sg-web in the Name field.
4. Verify that TCP is the protocol shown in the Protocol field (should be the default value).
5. Click Create in the Member pane. On the Create Member page:
 - a. Select server rs1 from the drop-down list in the Server field.
 - b. Enter 80 in the port field.
 - c. Click Create.
 - d. Repeat to add server rs2 as a member to the group.
6. Click Update.

ADC >> SLB >> Service Groups >> Update Help

Update Service Group

Name *


Protocol

Algorithm





Health Check ☐

Disable ☐

Health Monitor

Advanced Fields 

Member

 Enable  Disable  Delete  Create

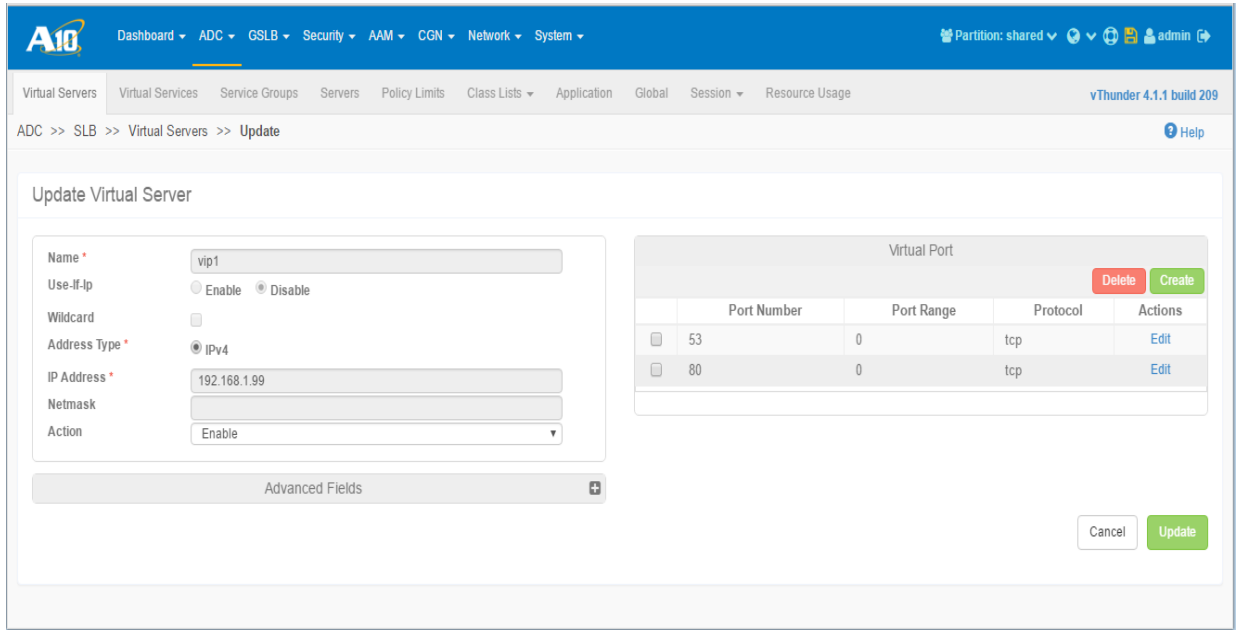
| <input type="checkbox"/> | Status | Name | Port | Actions |
|--------------------------|--------|------|------|----------------------|
| <input type="checkbox"/> | ✓ | rs1 | 80 | Edit |
| <input type="checkbox"/> | ✓ | rs2 | 80 | Edit |

SLB Configuration - Virtual Server

Configure the virtual servers.

1. Navigate to ADC > SLB > Virtual Servers.
2. Click Create.
3. Enter vip1 in the Name field.
4. Enter 192.0.2.99 in the IP Address field.
5. Click Create in the Virtual Port pane. On the next page:

- a. Verify TCP is selected in the Protocol field.
 - b. Enter 80 in the Port field.
 - c. Select sg-web from the drop-down list in the Service Group field.
 - d. Click Create.
6. Click Update.

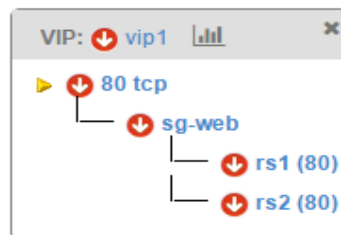


| Port Number | Port Range | Protocol | Actions |
|-------------|------------|----------|---------|
| 53 | 0 | tcp | Edit |
| 80 | 0 | tcp | Edit |

View Services Map

View the services map to verify that the configuration is correct.

1. Navigate to Dashboard > Services Map.
2. Select or search for vip1 in the left-side column.
3. Services map should look similar to the following:



Configure the Gateway Inline Deployment using CLI

To use the CLI to configure the topology shown in [Figure 17](#), perform the following tasks:

Interface Configuration

These commands enable the Ethernet interfaces used in the example and configure IP addresses on them:

```
ACOS(config)# interface ethernet 1
ACOS(config-if:ethernet:1)# enable
ACOS(config-if:ethernet:1)# ip address 192.0.2.10 /24
ACOS(config-if:ethernet:1)# exit
ACOS(config)# interface ethernet 3
ACOS(config-if:ethernet:3)# enable
ACOS(config-if:ethernet:3)# ip address 192.168.4.101 /24
ACOS(config-if:ethernet:3)# exit
ACOS(config)# interface ethernet 4
ACOS(config-if:ethernet:4)# enable
ACOS(config-if:ethernet:4)# ip address 192.168.2.100 /24
ACOS(config-if:ethernet:4)# exit
```

Default Route Configuration

The following command configures the default route through 192.0.2.1:

```
ACOS(config)# ip route 0.0.0.0 /0 192.0.2.1
```

SLB Configuration - Real Servers

```
ACOS(config)# slb server rs1 192.168.1.1
ACOS(config-real server)# port 80 tcp
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit
ACOS(config)# slb server rs2 192.168.1.2
ACOS(config-real server)# port 80 tcp
ACOS(config-real server-node port)# exit
ACOS(config-real server)# exit
```

SLB Configuration - Service Group

```
ACOS(config)# slb service-group sg-web tcp
ACOS(config-slb svc group)# member rs1 80
ACOS(config-slb svc group-member:80)# exit
ACOS(config-slb svc group)# member rs2 80
ACOS(config-slb svc group-member:80)# exit
ACOS(config-slb svc group)# exit
SLB Configuration - Virtual Server
ACOS(config)# slb virtual-server vip1 192.0.2.99
```

```
ACOS(config-slb vserver)# port 80 http
ACOS(config-slb vserver-vport)# service-group sg-web
ACOS(config-slb vserver-vport)# exit
ACOS(config-slb vserver)# exit
```

NOTE: For more information, see Command Line Interface Reference for SLB and SSL guides.

ADVANCED FEATURES

Following topics are covered in this chapter:

- [High Availability](#)
- [Cluster Configuration Management](#)

High Availability

VRRP-A is the ACOS implementation of high availability that is completely different from the industry-standard implementation of Virtual Router Redundancy Protocol (VRRP). In operation, VRRP-A is like VRRP since it borrows some concepts from VRRP; however, it is significantly different from VRRP. It does not inter-operate with VRRP-A. It also provides redundancy for the following IP resources:

- Virtual server IP addresses (VIPs)
- Floating IP addresses used as default gateways by downstream devices
- IPv6 NAT pools
- IPv4 NAT pools
- IPv4 static range lists and individual mappings for inside source NAT

Cluster Configuration Management

VCS is the ACOS implementation of cluster configuration management that enables you to manage a cluster of ACOS devices like a single, virtual chassis. One ACOS device in the virtual chassis is the virtual master (vMaster). The other ACOS devices are virtual blades (vBlades) within the virtual chassis, and are managed by the vMaster. As a controller for the vBlades, the vMaster provides centralized storage for the entire ACOS device configuration. Any configuration changes from the vMaster are automatically propagated to the vBlades.

