Universal Compute Platform

Version 5.01.01

ExtremeCloud IQ Distributed

Deployment Guide

9037349-00 Rev AA
January 2022

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see: www.extremenetworks.com/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: https://www.extremenetworks.com/support/policies/open-source-declaration/

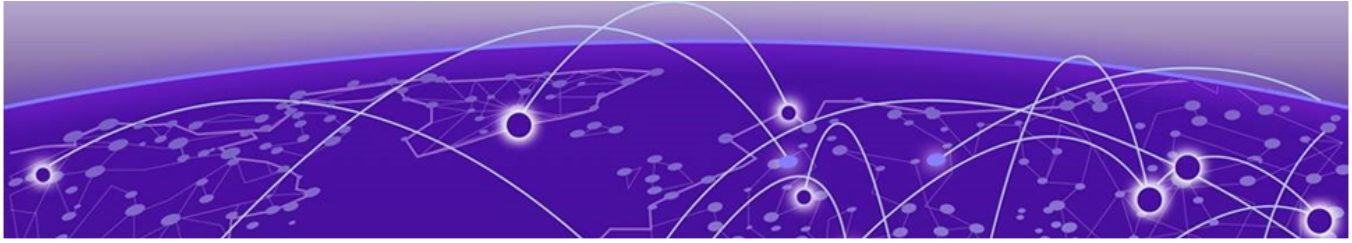


Table of Contents

Preface

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as ExtremeSwitching switches or SLX routers, the product is referred to as *the switch* or *the router*.

Table 1: Notes and warnings

Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product
	Note	Useful information or instructions
	Important	Important features or instructions
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

Table 2: Text

Convention	Description
`screen displays`	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words *enter* and *type*	When you see the word *enter* in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says *type*.
Key names	Key names are written in boldface, for example **Ctrl** or **Esc**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **Ctrl**+**Alt**+**Del**
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
italic text	Italic text indicates variable content.
`[ ]`	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
`{ x | y | z }`	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*`[`*member*`...]`.
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

Find Extreme Networks product information at the following locations:

- Current Product Documentation
- Release Notes
- Hardware and software compatibility for Extreme Networks products
- Extreme Optics Compatibility
- Other resources such as white papers, data sheets, and case studies

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit www.extremenetworks.com/education/.

Help and Support

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub

A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number, or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to The Hub.
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.

Send Feedback

The Information Development team at Extreme Networks has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.

- Improvements that would help you find relevant information.
- Broken links or usability issues.

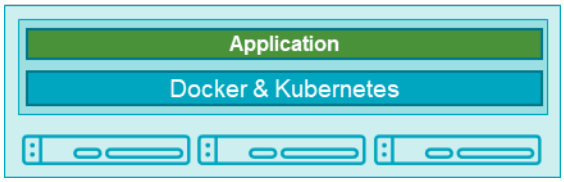
To send feedback, do either of the following:

- Access the feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

Provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Introduction and Prerequisites

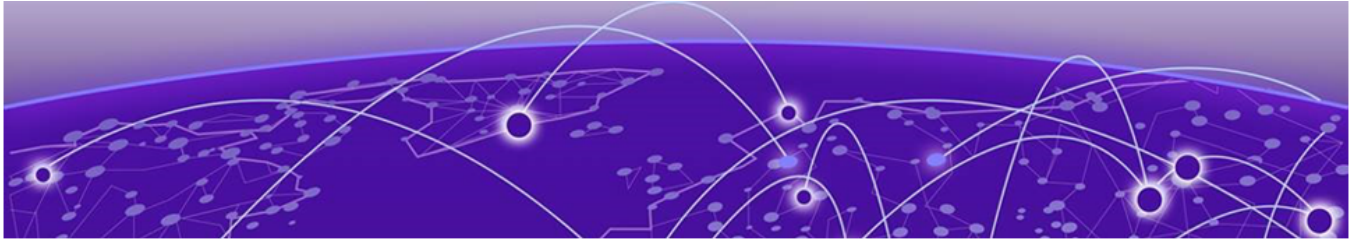
This guide provides the steps needed to bring a Universal Compute Platform cluster online. The Universal Compute Platform cluster requires three operational machines (referred to as nodes) that provide the computing power, storage, high availability, and load-balancing for the system. Universal Compute Platform leverages Kubernetes and Docker to deploy and manage the delivery of applications to the customer premises.



The system leverages VRRP (Virtual Router Redundancy Protocol) in order to provide support for both high-availability and load balancing, supported by an NGINX engine. All service operations to the cluster should be directed to the corresponding VRRP IP so that the load balancing logic can direct the request to the best node.

Deployment configuration requirements vary over different applications deployed into the Universal Compute Platform. One main requirement in the establishment and operation of the cluster is the Inter-Cluster Connection. This connection operates as the backplane between nodes in the cluster. This backplane carries all the synchronization data between nodes for both component and data states. It is a best practice to deploy the interface as a segregated 10 Gbps inter-connect (separate switch port), allowing for the best performance in synchronization between nodes.

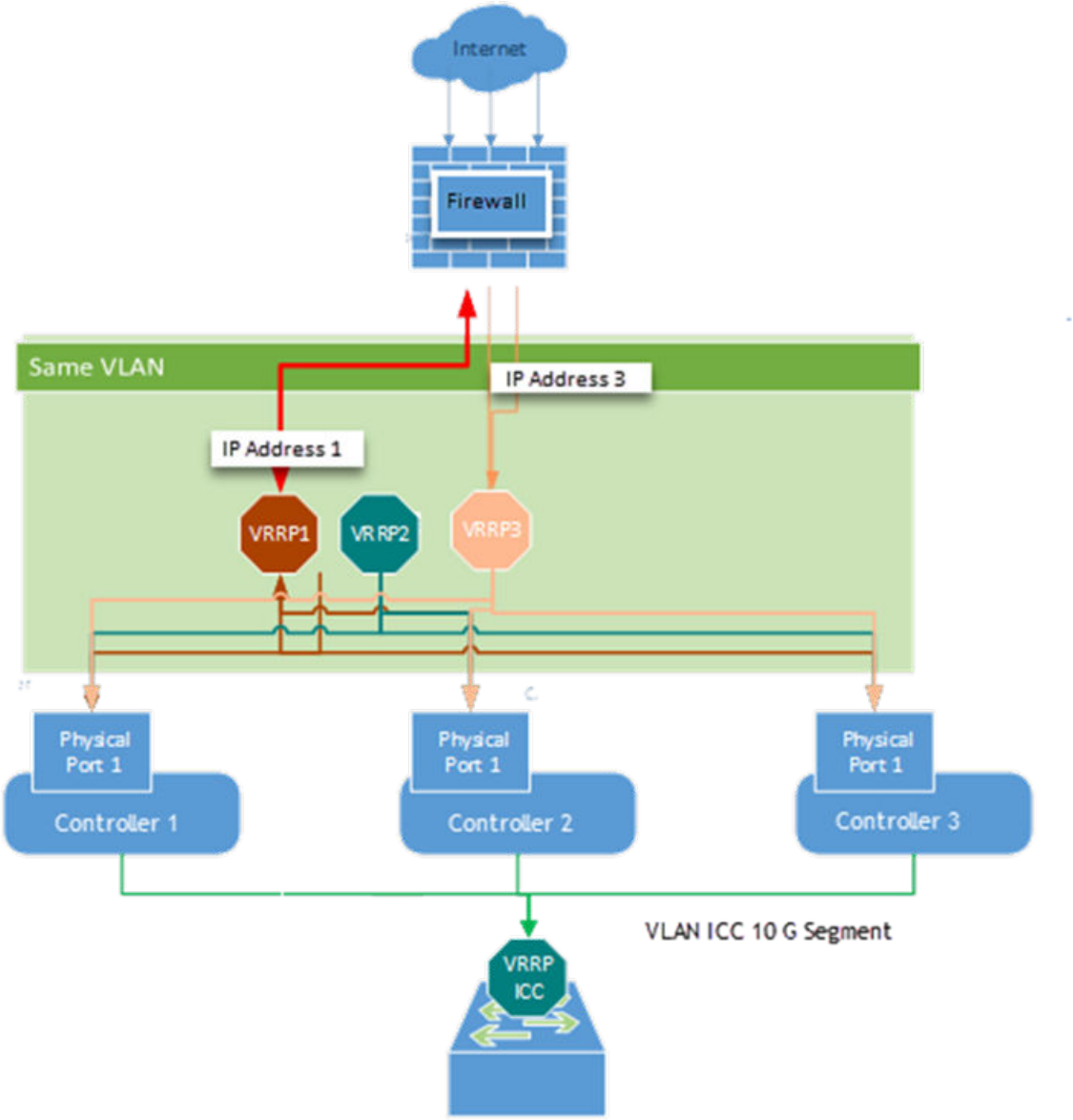
- Inter-Cluster Connection: Backend interaction and synchronization between all the members of a cluster. Minimum required connection requires 10 Gbps between nodes.
- The internal Kubernetes engine requires the reservation of two (2x) /16 subnets. Ensure that this IP address range does not conflict with any routable address space within the organization.



ExtremeCloud IQ

ExtremeCloud IQ is deployed as a Universal Compute Platform application. This deployment scenario includes the following application requirements for the cluster configuration:

- Three additional IP addresses representing the various services offered by the application to effectuate load balancing (Service Set 1 – 3).
- Each node in the cluster must map each of the services to a data interface, and all services can be mapped into the same interface. The same data interface can represent a direct point of reference for each of the front-end VRRP services.
- Three VRRP IP address are required to support port-overlap services for different services or a functional model (such as CAPWAP Master vs CAPWAP Server).



Service Set 1: Cluster Administration, Account Access (https), CAPWAP Master, Diagnostics

Table 4: Represented ports in Service Set 1

Protocol	Port	Service	Description
TCP	5825	Cluster Admin	Access to the cluster configuration user interface
TCP	443	NGINX	ExtremeCloud IQ Admin, software management
TCP	2083	IDM	IDM Auth
TCP	80	CAPWAP	CAPWAP Master

Table 4: Represented ports in Service Set 1 (continued)

Protocol	Port	Service	Description
TCP	12222	CAPWAP	CAPWAP Master
TCP	50054	XAPI	ExtremeCloud IQ API

Service Set 2: AP Registration/CAPWAP Load Balancing

Table 5: Represented ports in Service Set 2

Protocol	Port	Service	Description
TCP	80	CAPWAP	CAPWAP Master
TCP	12222	CAPWAP	CAPWAP Master
TCP	50054	XAPI	ExtremeCloud IQ API

Service Set 3: AP Registration/CAPWP Load Balancing

Table 6: Represented ports in Service Set 3

Protocol	Port	Service	Description
TCP	80	CAPWAP	CAPWAP Master
TCP	12222	CAPWAP	CAPWAP Master
TCP	50054	XAPI	ExtremeCloud IQ API

Firewall Setup

In a typical on-premise installation, the cluster is installed behind an access firewall, providing network address translations between the public and private address spaces. Always allow access for CloudOps management of the cluster. At a minimum, one IP address must be exposed to provide access. However, you can also choose to allow the managed APs and switches to connect to the private Remote Data Center (RDC). Two additional IP addresses are required for that. Therefore, for a typical installation, three public IP addresses must be provided. They are mapped to forward traffic into the three VRRP IP addresses of the service sets.

During system setup, the following configuration settings are critical to the deployment:

- Default Gateway: Each node in the cluster supports a single default gateway (0.0.0.0/0) definition. This gateway must be mapped to a next-hop attached on the data port interface.

  Note
  Do not configure the default gateway to map to the Inter-Cluster Connection (ICC) interface. The ICC is the Admin interface.

- DNS server: At least one reachable DNS server must be configurable, allowing the system to resolve several URLs during installation and interaction with ExtremeCloud IQ and CloudOps functions.

- Network Time Protocol (NTP) Servers: At least one reachable NTP, allowing the system to synchronize its time with a trusted time source. The same NTP must be configured, in the same order, on all nodes in the cluster.

  A best practice is to have two NTP definitions to support availability of the primary server. If there is an issue with the primary server, the system resorts to the alternate server.

Deployment Overview

This topic outlines the key deployment responsibilities for deploying ExtremeCloud IQ to Universal Compute Platform. Each of the following components have unique responsibilities:

- Customer On-Site Representative
- ExtremeCloud IQ CloudOPs
- System Administrator of Universal Compute Platform

Customer On-Site Representative

Customer On-Site Representatives are responsible for the following tasks:

- Set up a firewall that enables cluster access to the appropriate internet ports (for example, port 443) and enables CloudOps access. Follow the firewall configuration guidelines under Firewall Setup on page 11.
- Configure each node for service — Provide the necessary IP, DNS, and Host addresses, ICC Configure and form cluster (VRRP).
- Register the cluster with an ExtremeCloud IQ Public account.
- Register an ExtremeCloud IQ deployment request. The request requires a valid XIQ-CLOUDOPS-S in good standing. This SKU is a required component of a Distributed Cloud BOM quote.

For detailed information, see Prerequisites for ExtremeCloud IQ Installation on page 13.

ExtremeCloud IQ CloudOps

ExtremeCloud IQ CloudOps is responsible for the following tasks:

- Deploy ExtremeCloud IQ to the Universal Compute Platform cluster.
- Create monitoring and backup frameworks.
- Validate the state of all operational components.

Universal Compute Platform Administrator

Universal Compute Platform Administrators are responsible for the following tasks:

- Create ExtremeCloud IQ user accounts for end-device management.
- Onboard managed devices from the ExtremeCloud IQ local account.

Prerequisites for ExtremeCloud IQ Installation

Address planning is the fundamental step in successful deployment of the Universal Compute Platform in support of an ExtremeCloud IQ installation. It is important to understand the following:

- Decide how you will deploy and access the services offered by the cluster. Is the cluster going to serve applications that operate only within the on-premises installation? Or is application access going to require external access? Pre-determination of the IP address and connectivity structure are fundamental to a successful deployment. These deployment decisions drive the configuration choices.
- Consider the address plan of the installation, including how the cluster is going to be presented externally via a firewall. At least one address must be exposed via the firewall in order to support CloudOps access to the cluster to orchestrate the deployment, management and monitoring of the ExtremeCloud IQ software. If all of the managed devices are deployed within a campus (or campus connected infrastructure) the single externally available IP address will work. However, with ExtremeCloud IQ, which supports remote deployments outside a customer-controlled premises – like the Managed Service Provider (MSP) model of operations – three publicly accessed IP addresses are required.

  Each externally exposed address must be mapped to an internal VRRP of the cluster. You can either directly expose the VRRP IP addresses for the three service sets directly through a firewall, or in the case of NAT translation, ensure that the externally available IP addresses are mapped 1:1 to the internal services.

Important

Before you begin step-by-step configuration, make sure that you clearly understand and document all the elements of the network presence and topology related to the deployment.

The Inter-Cluster Connection (ICC) IP address is critical to the continuous operation of the system. If address definitions for ICC require re-addressing, the entire cluster will need to be rebuilt and the application re-deployed in order to re-established all the correct references of services within the cluster.

It is strongly recommended that the *entire* IP address structure for all services be defined once and not changed. Re-addressing may expose internal dependencies on references to mapped services and therefore affect the integrity and stability of the deployed installation.

IP Addresses

The most important point of definition is to record the IP address relationship between the cluster's direct interfaces (ICC, Service/Data ports), VRRP, and external access.

Table 7: IP address relationship between the cluster's direct interfaces and external access

Service Set	Node 1 (Data Interface IP)	Node 2 (Data Interface IP)	Node 3 (Data Interface IP)	VRRP IP	Public IP
Service Set 1 (cmudp, cmtcp, cmauth, https)	*Interface IP*	*Interface IP*	*Interface IP*	*VRRP IP 1*	*Public IP 1*
Service Set 2 (csupd1, cstcp1)				*VRRP IP 2*	*Public IP 2*
Service Set 3 (csudp2, cstcp2)				*VRRP IP 3*	*Public IP 3*
Inter-Cluster Connection					
Inter-Cluster Connection (ICC)	*Interface IP*	*Interface IP*	*Interface IP*	*ICC VRR-IP*	N/A

VRRP Configuration

In support of load balancing and high-availability functions, the Universal Compute Platform cluster relies on Virtual Router Redundancy Protocol (VRRP) to provide IP abstraction to several of its key functionality. VRRP is therefore another critical set of the configuration model.

For VRRP IP addressing details refer to Table 7 on page 14. Additionally, there are two critical operation settings that must be defined as part of the VRRP configuration of member nodes:

- **Priority**— VRRP uses priority settings as a mechanism to arbitrate mastery of the state of exchanges across members of the cluster. The node with the higher priority defaults to the master. However, in the case of failovers of the master node, VRRP algorithms assign mastery to the next higher priority member of the cluster. Therefore, it is important to properly assign corresponding priority settings to each node, so that their hierarchical priority in terms of VRRP state ownership is clear.

  As a best practice:

  - Designate node 1 as the highest priority, node 2 for second highest priority, and node 3 as the lowest priority.
  - The same priority should be used across all services (ICC, Services)
- **RouterID** — This setting allows segmentation of a routing domain, and it is important to separate from any other VRRP uses on the same network segment. The assigned value is arbitrary, but the value must not overlap when another VRRP usage is visible in the attached network segments.

Inter-Cluster VRRP Configuration

Note
Inter-Cluster Connection: Backend interaction and synchronization between all the members of a cluster. Minimum required connection requires 10 Gbps between nodes.

Table 8: Inter-Cluster Connection VRRP Configuration

	Node 1 (Port #)	Node 2 (Port 2)	Node 3 (Port #)
ICC	Node 1 ICC IP /CIDR	Node 2 ICC IP/CIDR	Node 3 ICC IP/CIDR
VLAN	VLAN Tagged/Untagged		
Port type	Physical		
VRRP			
VRRP IP addresses	ICC VRRP IP		
Priority	High (200)	Medium (100)	Low (50)
Router ID	ID (2)		

Services VRRP Configuration

Table 9: Services VRRP Configuration

	Node 1 (Port #)	Node 2 (Port 2)	Node 3 (Port #)
Data Port	Node 1 Port IP /CIDR	Node 2 Port IP/CIDR	Node 3 Port IP/CIDR
VLAN	VLAN Tagged/Untagged		
Port type	Physical		
VRRP			
VRRP IP addresses	VRRP 1, VRRP 2, VRRP 3		
Priority	High (200)	Medium (100)	Low (50)
Router ID	ID (1)		

Reserved IP Addressing

Container orchestration by Kubernetes within the cluster requires reservation of private network segments.

Note
Select two network segments (/16) that do not overlap or conflict with the deployed infrastructure network routing definitions.

Table 10: IP Address range for network segmentation

Restricted IP Range	IP Address /Range
POD Network IP Range	<reserved ip>/16
Service Network IP Range	<reserved ip>/16

VRRP operations require visual representation of where the IP addresses are allocated.

Node Default Credentials

Default factory settings for a Universal Compute Platform node:

Note
The values are case-sensitive.

- The default username is: admin
- The default password is: abc123

Port Information for Firewalls

Map the following service ports to the Service Set VRRP IP addresses listed in Table 7 on page 14.

- VLAN/VIP address for CAPWAP Master and API services (TCP 80/UDP 12222/TCP 2083/443)
- VLAN/VIP address for CAPWAP Server 1 service (TCP 80/UDP 12222)
- VLAN/VIP address for CAPWAP Server 2 (TCP 80/UDP 12222)

ExtremeCloud IQ on-premises installations require access to ExtremeCloud IQ core services. Make sure the firewall configuration allows for access to ExtremeCloud IQ core services.

Table 11 lists outbound ports for use when the firewall configuration requires rules that enable outbound traffic.

Table 11: Firewall Configuration Details

Domain Name	IPv4 Addresses	Protocol	Port
redirector.aerohive.com	54.172.0.252	HTTPS	TCP 443
		HTTP	TCP 80
		UDP	UDP 12222
hmupdates-ng.aerohive.com	54.86.95.132	HTTPS	TCP 443
extremecloudiq.com	34.253.190.192 ~ 34.253.190.255	HTTPS	TCP 443
	18.194.95.0 ~ 18.194.95.15		
	3.234.248.0 ~ 3.234.248.31		TCP 80
	44.234.22.92 ~ 44.234.22.95		
hac.extremecloudiq.com	34.253.190.192 ~ 34.253.190.255	HTTPS	TCP 443

Table 11: Firewall Configuration Details (continued)

Domain Name	IPv4 Addresses	Protocol	Port
Local Cloud	Load Balancer	HTTPS	TCP 443
		TCP	TCP 2083
	Capwap Master	HTTP	TCP 80
		UDP	UDP 12222
	Capwap Server 0	HTTP	TCP 80
		UDP	UDP 12222
	Capwap Server 1	HTTP	TCP 80
		UDP	UDP 12222
Rancher[PF1]	TBD	HTTPS	TCP 443
Universal Compute Platform — For lookup and download of Docker images.	Hosted area for Docker images	HTTPS	TCP 443
External DNS Server (Optional)	External DNS Server	HTTPS/UDP	TCP/UDP 53
Network Time Protocol (NTP) (Optional)	External NTP Server	UDP	UDP 123

Related Topics

Source Address Information on page 17

Source Address Information

For installations where APs are installed off-premises and connecting for service through a firewall, relax the access rules to specific service ports because source addresses are not always deterministic.

These settings are required to support remote diagnostics and to set up validation operations.

Table 12: Source address information

Source IP	Port	Description	Action	Mapped IP
0.0.0.0/0	TCP 80	AP CAPWAP registration	Allow	External IP1 -> Service Set 1 VRRP IP, External IP2 -> Service Set 2 VRRP IP, External IP3 -> Service Set 3
0.0.0.0/0	TCP 443	ExtremeCloud IQ login access and software updates	Allow	
0.0.0.0/0	TCP 2083	RADSEC	Allow	
0.0.0.0/0	UDP 12222	AP CAPWAP	Allow	

Table 12: Source address information (continued)

Source IP	Port	Description	Action	Mapped IP
Restricted IP list Extreme Bastion servers: • Raleigh Bastion Host 134.141.117.45/32 • Salem Bastion Host 134.141.4.8/32 Development assistance (BETA): • 3.64.95.0/29 • 99.254.120.40/32 • 99.234.167.169/32 • 69.165.217.208/32	TCP 22	Support SSH Access	Allow	External IP1-> Service Set 1 External IP1-> Service Set 1
	TCP 5825	Cluster Admin GUI. Remote diagnostics	Allow	

Install the Cluster

4120C Hardware Appliance

The 4120C hardware appliance is shipped with an existing license already installed. See Table 13 for appliance specifications.

Table 13: Hardware Specifications for 4120C Appliance

Platform	Description
CPU	Intel Xeon Silver 4114T (Skylake)
CPU Speed(GHz), L1 cache, L2 cache	2.20GHz/ L1I 32KB, L1D 32KB/ L2 1024KB/L3 14080 KB
Number of CPU	2
Cores per CPU	10
Number of Cores	20
Number of Virtual Cores	40
Memory Capacity (GB)	144 GB (12x8GB) DDR4 ECC
HDD (GB)	1 450 GB + 1 TB
Management Interface	1x 1/10 Gbps
Data Interface	2 X 1/10Gbps RJ45 (i40e) + 2 X 40Gbps QSPF28 (mlx5 core)

Basic Configuration Wizard

The Universal Compute Platform software provides a **Basic Configuration Wizard** that can help administrators configure the minimum settings necessary to deploy a fully functioning appliance on a network.

Administrators can use the wizard to quickly configure the appliances for deployment, and then after the installation is complete, continue to revise the configuration accordingly.

The wizard is automatically launched when an administrator logs on to the appliance for the first time, including after the system has been reset to the factory default settings.

The configuration wizard prompts with a set of **Yes** or **No** questions. The default value is indicated in parenthesis. To accept the default value, press **Enter**.

Related Topics

Use the Basic Configuration Wizard on page 20

Use the Basic Configuration Wizard

After logging into the appliance, the **Basic Configuration Wizard** displays. You are presented a set of **Yes** or **No** commands.

1. To begin the Admin password setup, press **Enter**. The **Admin Password Configuration** screen is displayed.
   a. To change the password for the admin account, press **Enter**.
   b. Enter the new password for the admin account.

      Note
      The password must be between 8-24 characters.

   c. Repeat the new password for the admin account and press **Enter**.

      If the passwords match, the password gets accepted.
   d. Press **Enter** to accept the changes.

      The AP access password screen is displayed.
2. To reset the AP access password, type a new password.

   Note
   The password must be between 5-30 alphanumeric characters and can include period, dash, underscore, and space.

   a. Retype the AP access password. Select **Enter**.

      Your AP access password is now reset and the **Current Data Port Settings** are displayed.
3. Walk through the ICC IP port (this is the Admin port) configuration wizard. Use the information gathered under ExtremeCloud IQ on page 9 and accept the changes.
4. Skip the data port configuration and go to Current Host Attributes on page 20.

Current Host Attributes

To set up the current host attributes:

1. Press **Enter** to change the Host Attributes.
2. Press **Enter** to enter the host name for the application.
3. Type **y** to set up a dedicated Admin port for out-of-band management. The default option is **n**.

   A note is displayed that the Admin port does not allow device registration.

4. Type the IP address to set up the IP address for the Admin port.
5. Press **Enter** to accept the default IP netmask for the Admin port.
6. Press **Enter** to accept the default domain name for the appliance. The default domain name is **`extremenetworks.com`**.

   Note
   The host name must be all lower case letters.

7. Press **Enter** to configure your Primary DNS server.
8. Type another IP address to set up the IP address of the primary DNS server and press **Enter**.
9. The default option to set up a secondary DNS server is **`no`**. Press **Enter** to accept the default option.

   The updated Host Attribute settings are displayed. To accept the changes you have made, press **Enter**.

Current Global Default Gateway Settings

The global default gateway can be on any Admin or data port topology/subnet. Enter the default gateway:

1. Type an IP address.
2. Press **Enter** to accept the changes.

   The **Current Time Settings** display.

Current Time Settings

The Current Time Settings option allows you to change the time zone as per your location.

1. Press **Enter** to change the Time settings.
2. Press **Enter** again if you would like to change the Time Zone. The Region number list is displayed.

   Important
   Ensure that Universal Compute Platform is configured with the correct Network Time Protocol (NTP) Server settings. Licensing management and several other system functions are dependent on an accurate timestamp.

3. Pick a number from those displayed on the screen that corresponds to the Continent. Then, enter a number that corresponds to the Region.

   You can enter **`n`** to move down the list, or **`p`** to move up the list. To go back to the Region selection, press **`c`**.

   The NTP servers used in this example are:

   server 0.ca.pool.ntp.org

   server 1.ca.pool.ntp.org

   For example, for Toronto select Americas (2) then New York (101).
4. Press **Enter** to run NTP as a client.
5. Provide the fully qualified domain name of the NTP server. Press **Enter**.
6. You are prompted to enter a second NTP server and the default option is **`y`**. Type **`n`** and press **Enter**.

   NTP Client is enabled.

7. Accept the changes you have made to the time zone and NTP server by pressing **Enter**.

   The **Controller Post Installation Configuration** menu displays.

8. If you want to revisit any of the previous screens or exit without applying the configuration changes, enter one of the corresponding numbers/alphabets displayed on screen.

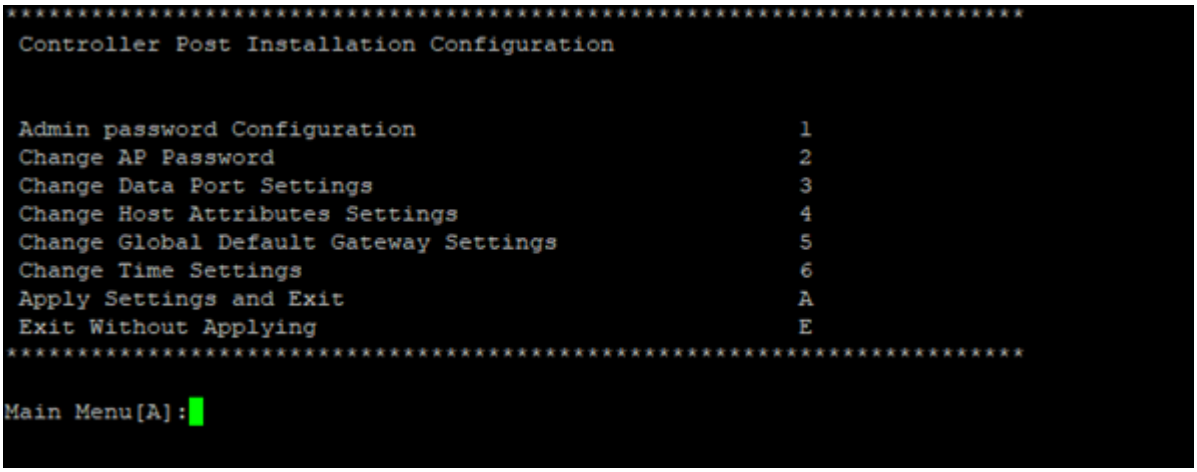


Figure 1: Controller Post Installation Configuration Menu Screen

Table 14: Controller Post Installation Configuration Menu

Menu Option	Command
Admin password Configuration	1
Change AP Password	2
Change Data Port Settings	3
Change Host Attribute Settings	4
Change Global Default Gateway Settings	5
Change Time Settings	6
Apply Settings and Exit	A
Exit Without Applying	E

When you revisit any other screen, you will have to reconfigure all subsequent area settings. For example, if you decide to reconfigure the Admin Password, which is at the beginning of the configuration wizard, you will have to reconfigure all the subsequent configuration wizard settings.

Press **Enter** to accept the settings. The default option for accepting the settings is **A**. Your settings are now applied successfully.

Next, repeat the basic configuration procedure for the remaining two appliances.

Test Connectivity

Test connectivity to the external services and each node in the cluster using the `ping` command.

1. To test connectivity to external services such as DNS, ping the IP address of the DNS server.
2. To test connectivity to the nodes in the cluster, ping the IP address of each node.

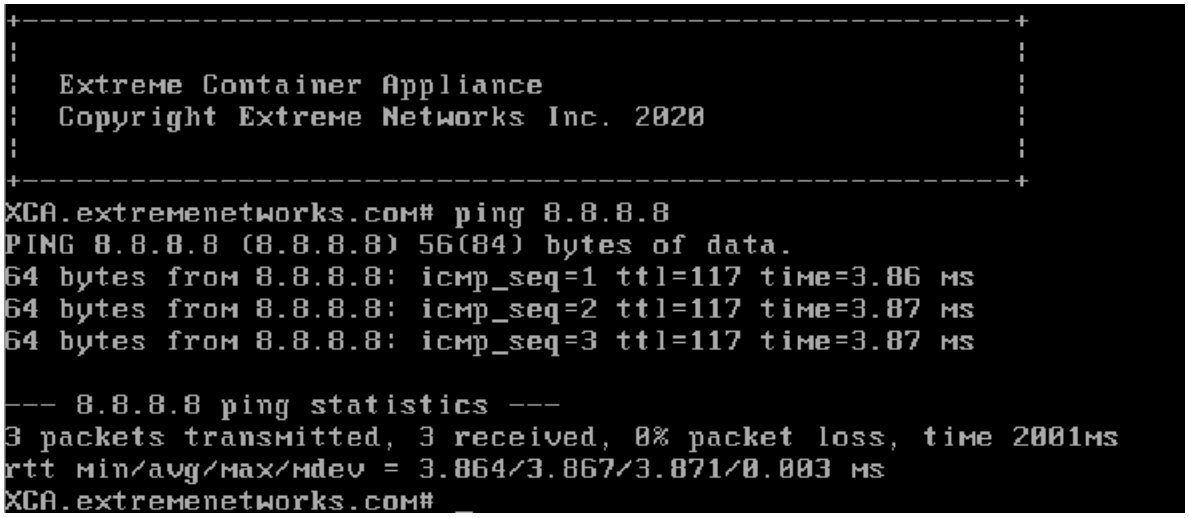


Figure 2: Example ping command

Upgrade the Cluster

Before configuring the cluster, perform an upgrade of each of the nodes using the Universal Compute Platform Admin user interface.

1. Log in to the controller Admin user interface: https://*node ip*:5825
2. Go to **Administration** > **System** > **Software Upgrade** > **Upload**.

3. Upload the desired revision of Universal Compute Platform.

Note
A best practice is to upgrade each of the nodes on a new cluster to the latest revision before proceeding with the cluster set up and configuration.

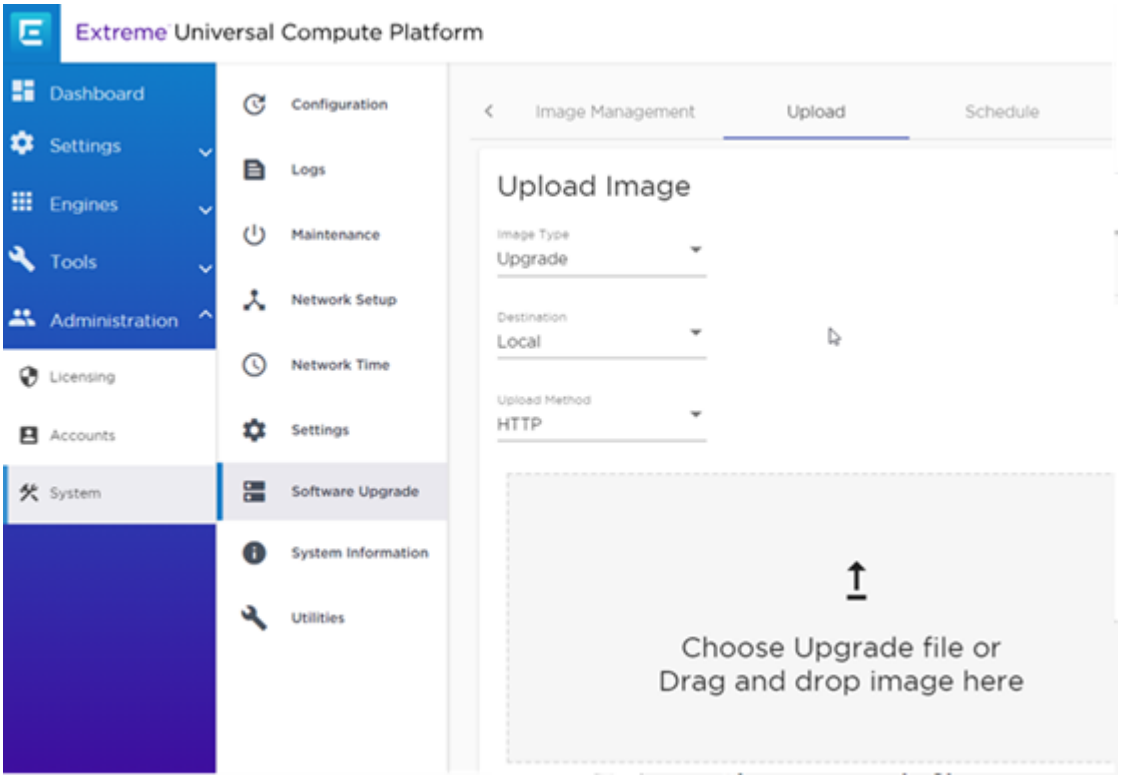


Figure 3: Select the upgrade image

4. From the **Image Management** Tab, select the Upgrade image, and select .

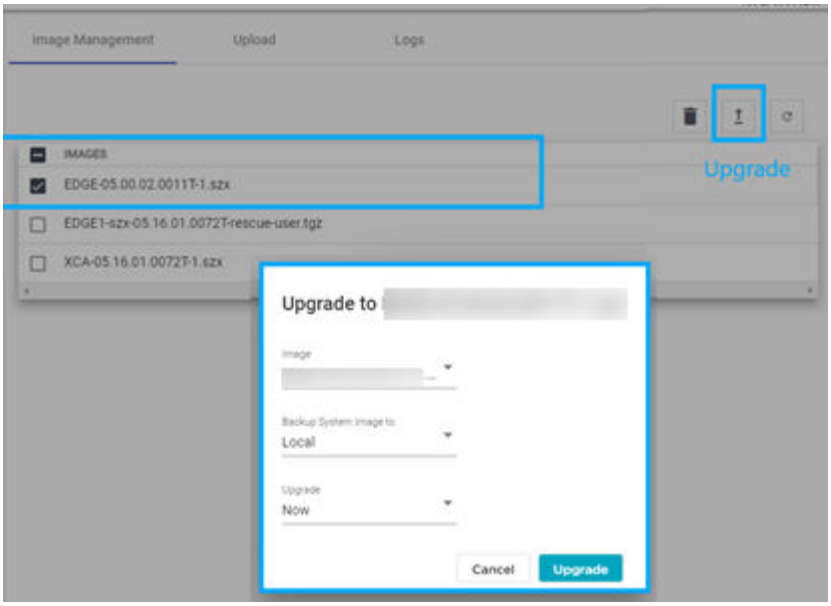


Figure 4: Upgrade the selected image

When all nodes in the cluster are upgraded to the latest revision, proceed to IP Address Configuration on page 25.

IP Address Configuration

Initialize nodes in a cluster to the pre-determined IP addresses.

Note
IP address configuration for interfaces on the cluster must be set only once. If IP addresses are changed after initial deployment (for example, due to a cluster relocation), it may be necessary to rebuild and re-deploy the cluster and then, re-install the application.

Table 15 displays example information that was gathered during the prerequisite stages. These IP addresses are listed as an example.

Table 15: Example of Prerequisite IP Addresses

	IP Address	Mask	Gateway	VRRP Precedence	ExtremeCloud IQ Services VLAN ID	Notes
Node1	192.227.109.81	/26 (255.255.255.192)	192.227.109.65	100 Router ID1	Provide a *VLAN ID*	Physical Host 1 (Cluster)
Node2	192.227.109.82	/26 (255.255.255.192)	192.227.109.65	75 Router ID1	Provide a *VLAN ID*	Physical Host 2 (Cluster)

Table 15: Example of Prerequisite IP Addresses (continued)

	IP Address	Mask	Gateway	VRRP Precedence	ExtremeCloud IQ Services VLAN ID	Notes
Node3	192.227.109.83	/26 (255.255.255.192)	192.227.109.65	50 Router ID1	Provide a *VLAN ID*	Physical Host 3 (Cluster)
ICC VRRP	192.227.109.72	/26 (255.255.255.192)	192.227.109.65		Provide a *VLAN ID*	Inter-Connect Cluster connection

Configure VRRP Setup

Take the following steps to configure the Virtual Router Redundancy Protocol (VRRP).

1. Navigate to **Administration** > **System** > **Network Setup**.
2. From the **Interfaces** list, select the data access interface that you configured from the **System Startup Wizard** for (Port 1).

   The **Port Configuration Settings** menu displays.
3. Provide a list of IP addresses that will be offered via VRRP.

4. Set the Router Priority and Router ID for each node.

   Each node must have the same list of IP addresses and the same Router ID, but have a unique Priority setting. The Priority setting determines which node in the cluster is the Primary node. The node with the higher priority is considered the default Primary node.

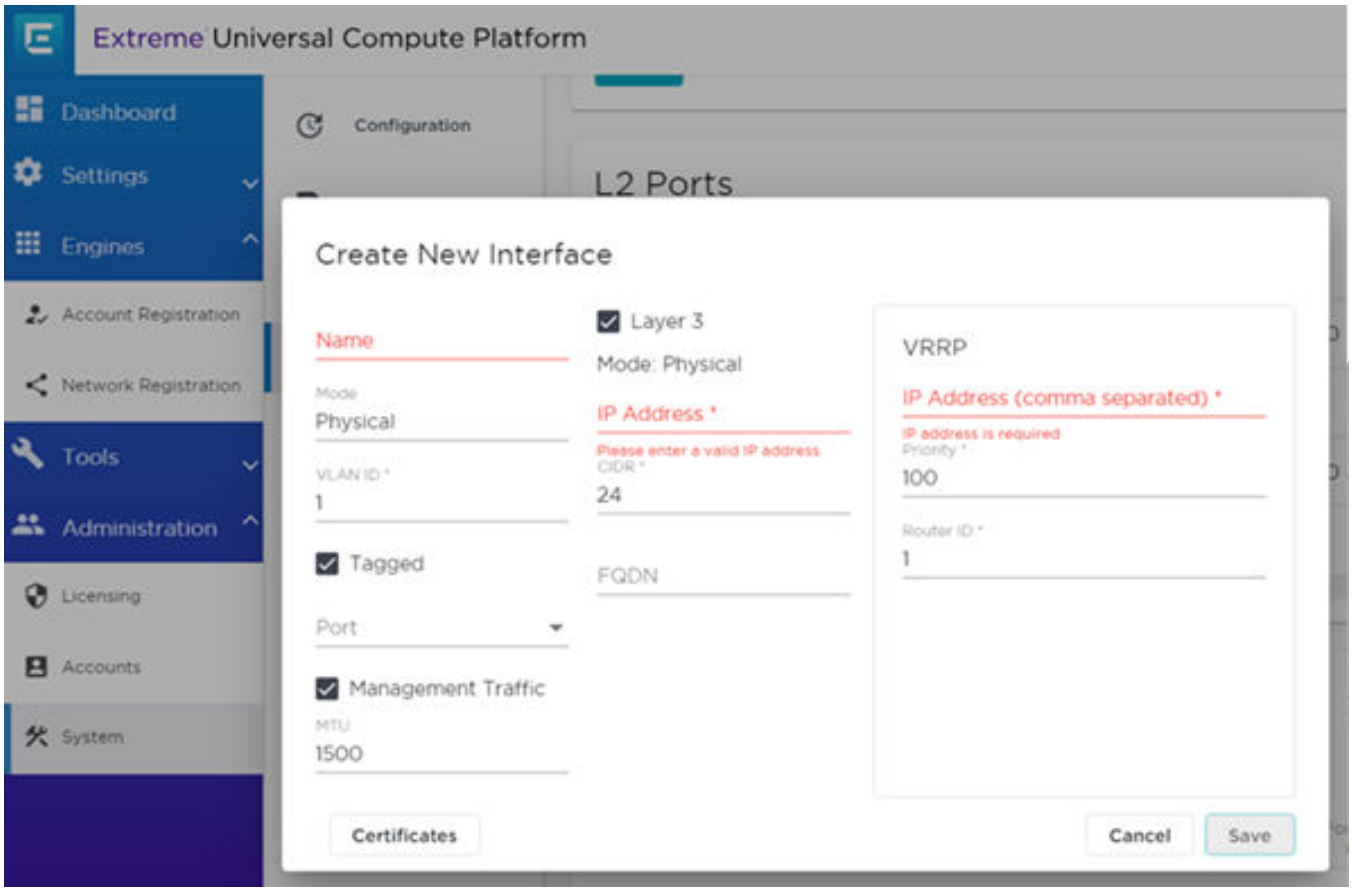


Figure 5: User Interface showing properties window for Port 1

5. Repeat this process in each of the nodes of the cluster.

Configure the Cluster

This topic steps you through the Cluster Configuration User Interface. From the management IP address of the primary node, log into the user interface using the node's credentials that you configured under Node Default Credentials on page 16.

1. Go to **Settings** > **Cluster Configuration** in the menu tree and complete the following sections:
   - Network Configuration
   - Cluster Node Information
   - Cluster Configuration
   - Finish

2. Provide the following Network Information and select **Next**.
   - Network topology name
   - IP address
   - CIDR (Classless Inter-Domain Routing)
   - VRRP (Virtual Router Redundancy Protocol)
     - IP addresses
     - Priority
     - Router ID

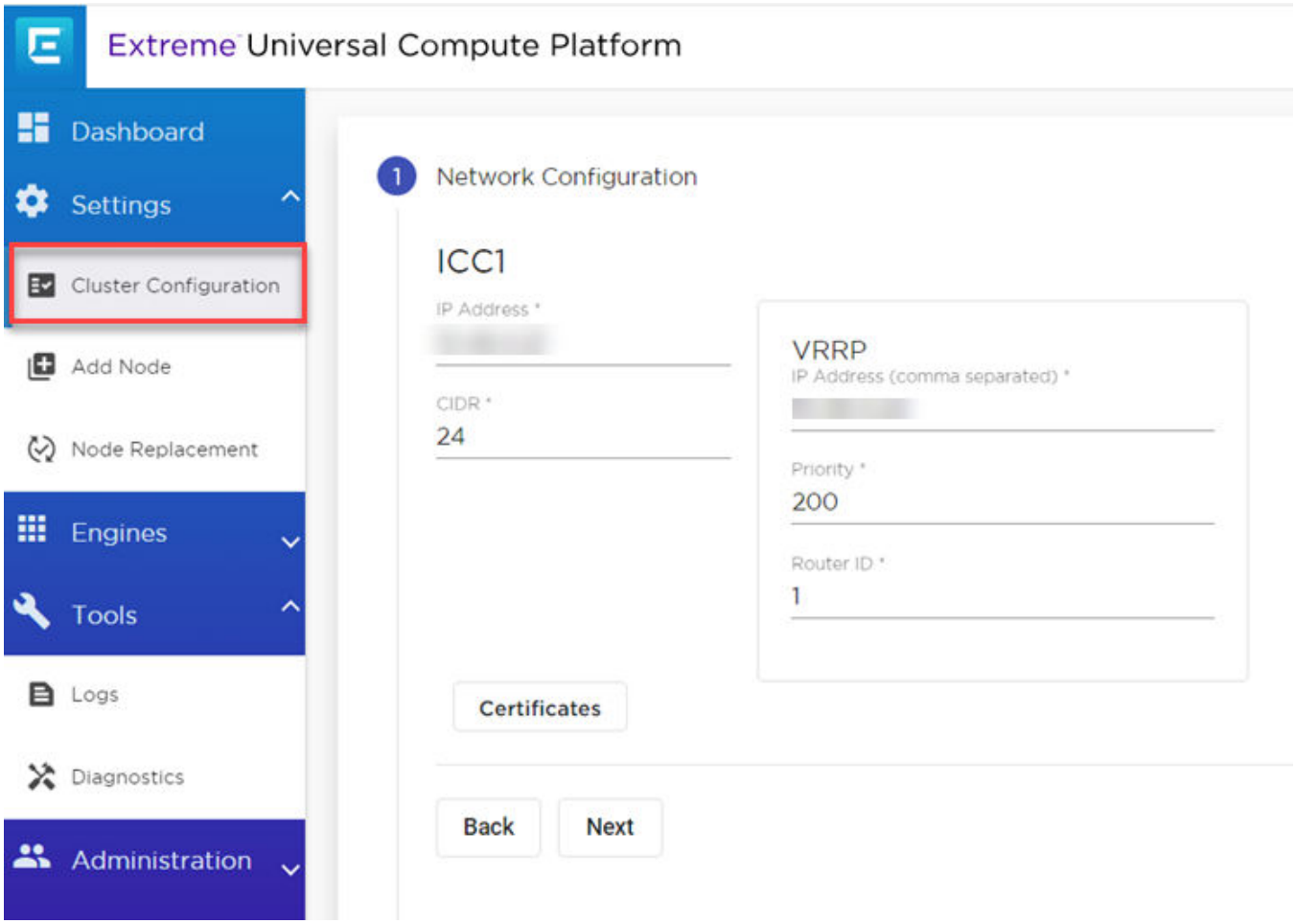


Figure 6: Cluster Configuration – Step 1

You are prompted to specify a list of IP address ranges for the Pod and Services for internal configuration.

3. Provide Cluster Node Information. View or modify the IP Address for each node in the cluster, and select **Next**.

4. Accept the default settings for the following Cluster Configuration settings:
   - Pod Network IP Address
   - Service Network IP Address
   - Pod Network CIDR
   - Service Network CIDR
5. Select **Create Cluster**.

   Note
   When creating the cluster for the first time, each node must download the required packages. This can take some time.

6. When cluster creation completes, configure the mapping of each core service set to the corresponding VRRP (front-end). From the **Assigned VRRP** field, select the IP address.

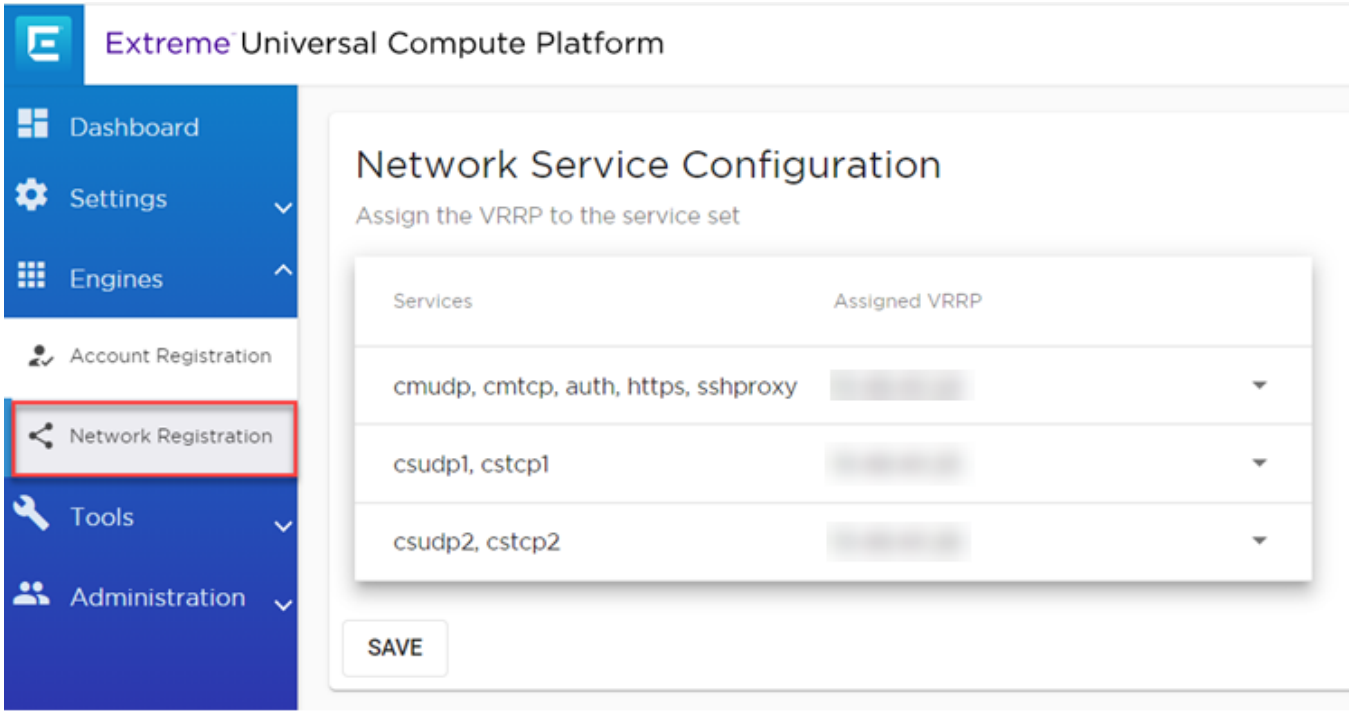


Figure 7: Network Service Configuration

Validate the Cluster

Use the Shell utility and take the following steps to validate the cluster:

1. Go to **Administration** > **System** > **Utilities**.

2. From the SSH Console, issue the following command:

   ```
   ip a |grep vrrp
   ```

   All nodes in the cluster should display as **Up**.

SSH Console

```
Username for localhost: admin
Password for admin@localhost:
Attempting connection...

                     +-----------------------------------------------------+
|                                                     |
|  Extreme Container Appliance                        |
|  Copyright Extreme Networks Inc. 2020               |
|                                                     |
+-----------------------------------------------------+
ExtremeCloud1.extremenetworks.com# shell
Password:
root@ExtremeCloud1:~# ip a |grep vrrp^C
root@ExtremeCloud1:~# ip a |grep vrrp
40: vrrp.1@eth0: <BROADCAST,MULTICAST,UP,LOWER_UP,80000000> mtu 1500 qdisc noqueue state UP group default qlen 1000
    inet 192.227.109.72/32 scope global vrrp.1
41: vrrp1.1@eth1.1: <BROADCAST,MULTICAST,UP,LOWER_UP,80000000> mtu 1500 qdisc noqueue state UP group default qlen 1000
    inet 10.1.0.21/32 scope global vrrp1.1
42: vrrp2.1@eth1.2: <BROADCAST,MULTICAST,UP,LOWER_UP,80000000> mtu 1500 qdisc noqueue state UP group default qlen 1000
    inet 10.2.0.21/32 scope global vrrp2.1
43: vrrp3.1@eth1.3: <BROADCAST,MULTICAST,UP,LOWER_UP,80000000> mtu 1500 qdisc noqueue state UP group default qlen 1000
    inet 10.3.0.21/32 scope global vrrp3.1
root@ExtremeCloud1:~#
```

Figure 8: SSH Console — grep command to display node status

3. To confirm the operation, issue the following command:

   ```
   Cat /etc/nginx/streams-enabled/stream.conf
   ```

SSH Console

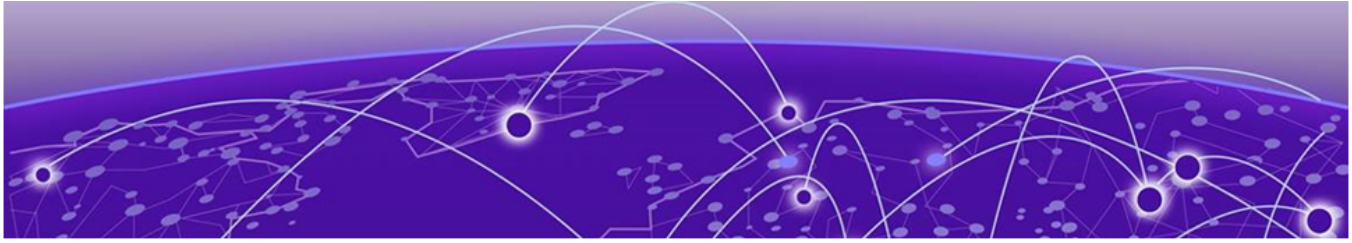
```
Username for localhost: admin
Password for admin@localhost:
Attempting connection...

                      +-----------------------------------------------------+
|                                                     |
|  Extreme Container Appliance                        |
|  Copyright Extreme Networks Inc. 2020               |
|                                                     |
+-----------------------------------------------------+
ExtremeCloud1.extremenetworks.com# shell
Password:
root@ExtremeCloud1:~# ip a |grep vrrp^C
root@ExtremeCloud1:~# ip a |grep vrrp
40: vrrp.1@eth0: <BROADCAST,MULTICAST,UP,LOWER_UP,80000000> mtu 1500 qdisc noqueue state UP group default qlen 1000
    inet 192.227.109.72/32 scope global vrrp.1
41: vrrp1.1@eth1.1: <BROADCAST,MULTICAST,UP,LOWER_UP,80000000> mtu 1500 qdisc noqueue state UP group default qlen 1000
    inet 10.1.0.21/32 scope global vrrp1.1
42: vrrp2.1@eth1.2: <BROADCAST,MULTICAST,UP,LOWER_UP,80000000> mtu 1500 qdisc noqueue state UP group default qlen 1000
    inet 10.2.0.21/32 scope global vrrp2.1
43: vrrp3.1@eth1.3: <BROADCAST,MULTICAST,UP,LOWER_UP,80000000> mtu 1500 qdisc noqueue state UP group default qlen 1000
    inet 10.3.0.21/32 scope global vrrp3.1
root@ExtremeCloud1:~# cat /etc/nginx/streams-enabled/stream.conf
```

Figure 9: SSH Console — Confirmation command

4. Scroll to find the VRRP address for each of the three configured services.

Figure 10: VRRP IP address for each of the configured services



Index