Cisco UCS M5 C220 1UR Server

Quick Start Guide

08/20/2020

Summary:

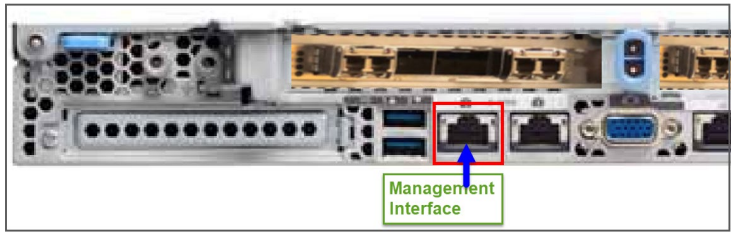
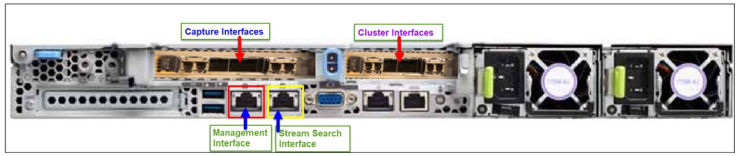
The Cisco UCS M5 C220 1UR Server can be reconfigured based on the connection process in this document to run the NextComputing Packet Continuum to provide enhanced packet capture and forensics analysis tools that help you investigate security events and anomalous network activity. It works in conjunction with Cisco Stealthwatch and Cisco Firepower to speed incident response and network forensics. Other supporting documents include the Cisco UCS M5 C220 1UR Server BIOS settings and CentOS7.6 installation document as well all standard Packet Continuum, Packet Continuum Federation Manager, REST API and associated user documentation.

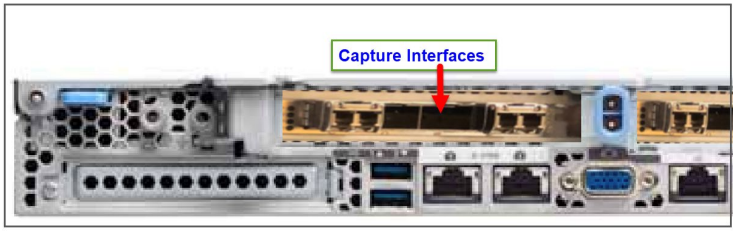
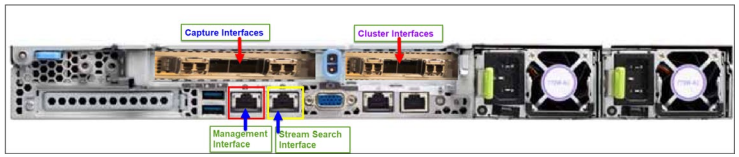
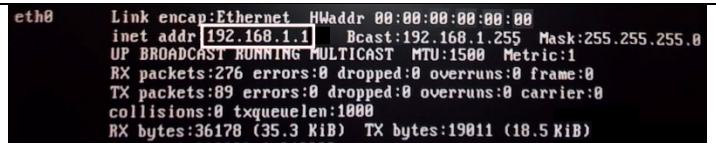
1 Network Configuration

Before capturing packets, some initial configuration is required.

A VGA display and USB keyboard are necessary at first for locally configuring the network. An Ethernet connection to an onboard gigabit interface is also required.

Note: By default, the management Ethernet port is pre-configured for DHCP. If a static IP is needed, you will need to set this during the quick start process.

1. Provide a network connection for remote access to server	Provide an Ethernet connection to Management Port as shown in figure (a).	 figure (a) Management Port  Back Panel for reference
2. Provide network connection(s) for network capture.	Provide 10G network connection **to Capture Port** as shown in figure (b). **Note**: Make sure there is traffic being generated over the connections.	

		 figure (b)Capture Interfaces  Back Panel for reference
3. Log in	After booting the system to the OS, login with the following user information: User: *continuum* Password: Contact Support for password	
4. Record the IP Address	Once logged in, open a terminal and enter: #ifconfig This will provide the IP address of the Ethernet port currently connected. Record the IP address. (Note: to set a static IP address, please review the Packet Continuum User Guide.)	
5. Test connection	To test the connection, ping your internal network or login remotely via SSH on port 22. If there is a successful connection, please go to part 2 of this guide. If not please contact support.	

2 Start Recording

Now that there is a successful network and/or cluster connection to the system, it's time to begin recording network packets to disk. Using the web interface, the user can begin recording and view statistics about traffic on a network.

1. Start the web interface	**Remote Access**: On any remote system connected to the network, open a web browser (firefox) and enter the IP address of the system followed by the port# 41390 in the form: https://<IP Address>:41390 **Local Access:** On the VM, click on the Application tab and select internet. Open a web browser (firefox) and enter https://<localhost>:41390	
2. Log in:	Now you should see the Packet Continuum login screen. By default, a "continuum" account has already been created. Enter "continuum" for the UserName, and *contact support* for the Password.