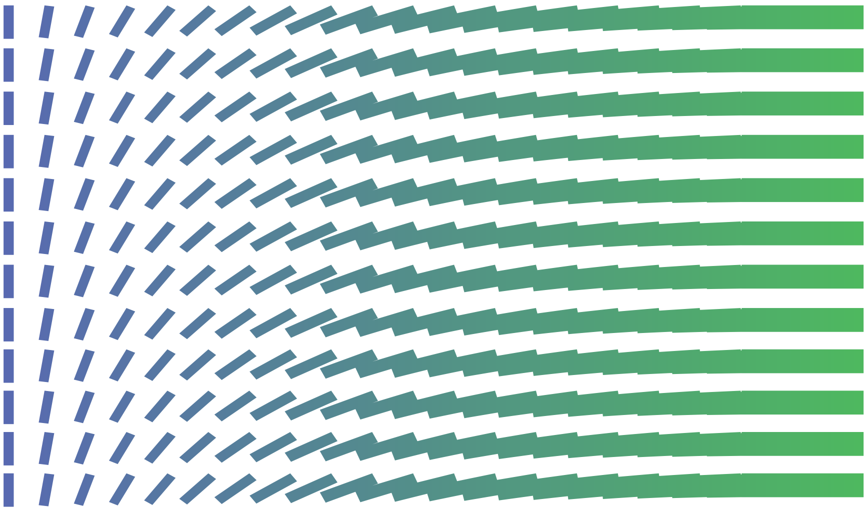
Hillrom™

Welch Allyn® Connex® Device Integration Suite (CDIS) Network Connectivity Engine (NCE) software



Best practices guide

Legal Statement Welch Allyn, Inc. ("Welch Allyn”) assumes no responsibility for any injury to anyone that may result from (i) failure to properly use the product in accordance with the instructions, cautions, and warnings published in this manual or the statement of intended use published in the *Instructions for use*, or (ii) any illegal or improper use of the product.

Welch Allyn, Connex, CSM, and CVSM are registered trademarks of Welch Allyn.

Microsoft Windows is a trademark of the Microsoft group of companies.

Software in this product is Copyright 2021 Welch Allyn or its vendors. All rights are reserved. The software is protected by United States of America copyright laws and international treaty provisions applicable worldwide. Under such laws, the licensee is entitled to use the copy of the software incorporated with this instrument as intended in the operation of the product in which it is embedded. The software may not be copied, decompiled, reverse-engineered, disassembled, or otherwise reduced to human-perceivable form. This is not a sale of the software or any copy of the software; all right, title, and ownership of the software remain with Welch Allyn or its vendors.

This product may contain software known as “free” or “open source” software (FOSS). Hill-Rom uses and supports the use of FOSS. We believe that FOSS makes our products more robust and secure, and gives us and our customers greater flexibility. To learn more about FOSS that may be used in this product, please visit our FOSS website at hillrom.com/opensource. Where required, a copy of FOSS source code is available on our FOSS website.

PATENTS / PATENT hillrom.com/patents.

May be covered by one or more patents. See above Internet address. The Hill-Rom companies are the proprietors of European, US, and other patents and pending patent applications.

For information about any product, contact Hillrom Technical Support: hillrom.com/en-us/about-us/locations/.

DIR 80020208 Ver. D

Revision date: 2021-11

Welch Allyn, Inc.
4341 State Street Road
Skaneateles Falls, NY 13153 USA

hillrom.com

Welch Allyn, Inc. is a subsidiary of Hill-Rom Holdings, Inc.

Hillrom™

Contents

Overview

Introduction

The intent of this document is to describe the usage and integration of best practices for the CDIS-NCE connectivity software.

The Welch Allyn® CDIS-NCE software is intended to provide bi-directional connectivity between Welch Allyn medical devices and various Welch Allyn and non-Welch Allyn data management systems.

The CDIS-NCE software supports the device initiated network workflow where the device is sending data to a server. The device initiated network workflow occurs when the device initiates communication with the server (for example verifying a patient ID, clinician ID, or sending vitals data).

The CDIS-NCE software does not honor requests for data from the server.

Intended audience

The intended audiences of this document include:

- Customer site IT professionals
- Integrators
- Welch Allyn Field Engineers
- Welch Allyn Technical Support personnel

Personnel providing integration of devices into EMR systems need to know the components included in the software solution (e.g. NCE and DCP).

- Site IT professionals need to understand the TCP/IP Ports used in the solution.
- Site IT professionals may need to know basic troubleshooting.
- Welch Allyn service personnel need to know basic and advanced troubleshooting.

References

- See the appropriate EMR summary for solution context.
- 60072721 CDIS-NCE Deployment Instructions
- 60059617 IDS-CFG CDIS-NCE HL7 EMR Interface
- 60072805 IDS-CFG MatrixCare-WA - CDIS-NCE EMR Interface

Definitions

Term	Definition
WACP	Welch Allyn Communication Protocol
CDIS	Connex Device Integration Suite – A suite of software to enable connecting medical devices to host systems (e.g. EMR software)
CSM	Welch Allyn Connex® Spot Monitor
CVSM	Welch Allyn Connex® Vital Signs Monitor
DCP	Device Connectivity Protocol – Used as an address/port resolution service to help devices find where servers for specific services are located
HL7	Health Level Seven (HL7) is a standard for exchanging information between medical applications. This standard defines a format for the transmission of health-related information.
NCE	Network Connectivity Engine – Part of CDIS to support device-initiated network connectivity workflow
NRS	Network Rendezvous Service – Used to assist devices in finding the server(s) for specific device functions (e.g. sending vitals, remote service, etc.). NRS is the communications protocol used by the DCP service.

Technical specifications

Computer requirements (per NCE instance)

Computer	Requirement
Operating System	Windows® Server 2012 R2, Windows Server 2016, Windows Server 2019 **NOTE** NCE will not run if the Windows Server is configured as a Domain Controller. Do not install NCE on a PDC or BDC.
CPU	4 cores
RAM	Minimum 8 GB
Storage	2 GB for solution software 100 GB available after install

NOTE NCE software is capable of operating on a virtual machine as long as each virtual machine runs one instance of NCE and meets the specifications.

Network connection

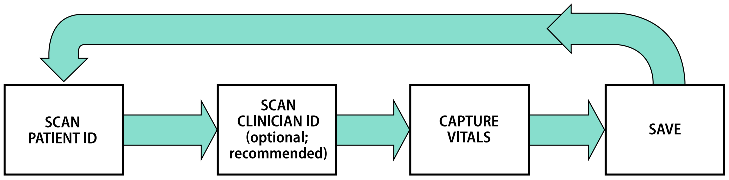
Network connection	Requirement
NIC	1 GB or higher recommended
Internet connection	An Internet connection is required for installation and first-time use

Device support

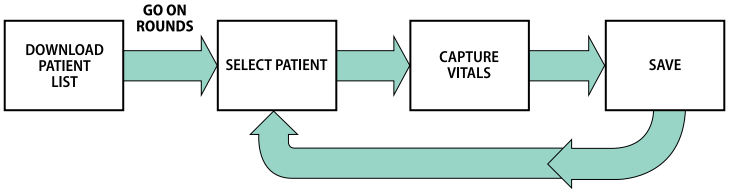
Device	Supported
Models	Connex Vital Signs Monitor (CVSM), Connex Integrated Wall System (CIWS), Connex Spot Monitor (CSM)
Capacity	Episodic: Up to 400 spot check vitals devices per instance of NCE. Continuous: Up to 48 continuous devices per instance of NCE. **NOTE** A single instance of NCE software can handle up to 400 episodic devices and 48 continuous devices. **NOTE** Only one instance of NCE can be installed to run on a server.

Workflows

Device Initiated Vitals Workflow



Device Initiated Patient List Vitals Workflow



Custom data/modifiers/scores

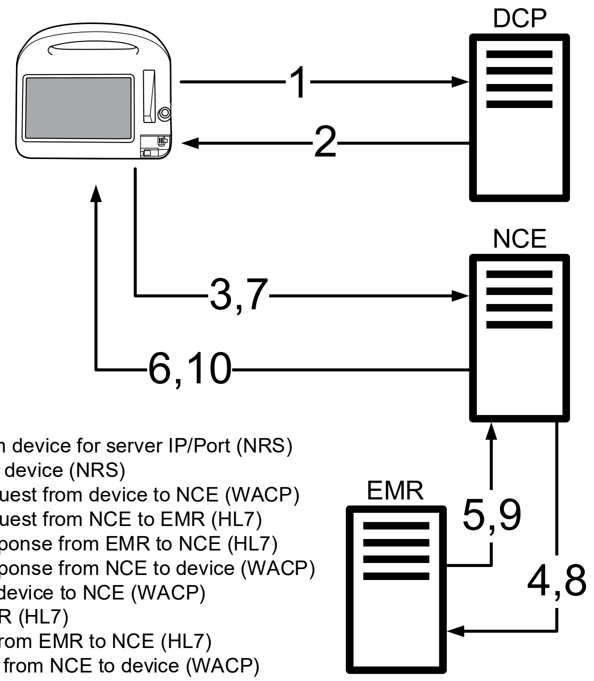
For information on custom data modifiers and custom scores, contact your sales representative, or see the web-based Welch Allyn configuration tool https://config.welchallyn.com/configurator/.

Data flow diagrams

Vitals device workflow (using NRS IP)

Configuring the device to use NRS IP is the best practice so that the device can take advantage of sending vital data and it also supports the remote service features. The diagram shows the sequence of data transactions.

Dataflow



1. DCP request from device for server IP/Port (NRS)
2. DCP response to device (NRS)
3. Patient query request from device to NCE (WACP)
4. Patient query request from NCE to EMR (HL7)
5. Patient query response from EMR to NCE (HL7)
6. Patient query response from NCE to device (WACP)
7. Vitals send from device to NCE (WACP)
8. Vitals data to EMR (HL7)
9. Vitals data ACK from EMR to NCE (HL7)
10. Vitals data ACK from NCE to device (WACP)

Performance and capacity guidelines

Depending on network performance, a given installation may be able to handle up to the specified number of devices on a single instance of CDIS-NCE. When the installation requires more devices to be connected (or the solution is not performing as needed due to network bandwidth, network, or server performance) it is a best practice to scale up the solution by using a load balance solution between the devices and the CDIS-NCE servers.

Please consider the following when configuring the system as it will have some impact on performance based on the type and number of devices used in the environment.

For applications that are made up of only episodic devices (e.g. spot check), one CDIS- NCE server can be used for up to the specified number of devices per the technical specifications for a non-high availability configuration.

For applications that combine episodic and continuous devices, the following actions are recommended:

1. The technical specifications are followed for deterministic performance and high data reliability.
2. The NCE software is connected to a host capable of receiving and processing concurrent messages on the same IP/port.
3. Devices typically use DHCP for acquiring their IP address. When using continuous devices in the solution it is required to reserve all IP Addresses < X.Y.Z.26 to not be allocated by DHCP to the vitals devices.
4. Configure the NCE's continuous and alarms host index's maximum concurrent connections setting to 0 or the number of continuous devices connected to the instance of NCE.
5. Configure the HL7 integration engine to have one connection per continuous device plus one additional connection for every 10 episodic devices.

   For example: If the environment has 250 devices connected to the same IP/Port of the HL7 integration engine and 30 are continuous and 220 episodic, then the HL7 integration engine's max connections should be set to 52 = (30 + 220 / 10).
6. If the environment has 288 devices and all may be used as a continuous device, based on the technical specifications, six NCE servers are required to support the six sets of 48 continuous devices plus one additional NCE server to cover the load if one of the other 6 goes down. Virtual servers can be used, but each virtual server needs to meet the technical specifications, so the server hardware needs to scale to support the virtual machines.
7. Configuring the Vitals CDIS-NCE solution for high-availability as shown in the architecture diagram is intended to provide a few additional benefits:
   a. High availability: If any one server goes down the other servers will take on the load
   b. Less costly deployment: Using virtual servers saves money over individual hardware for each server

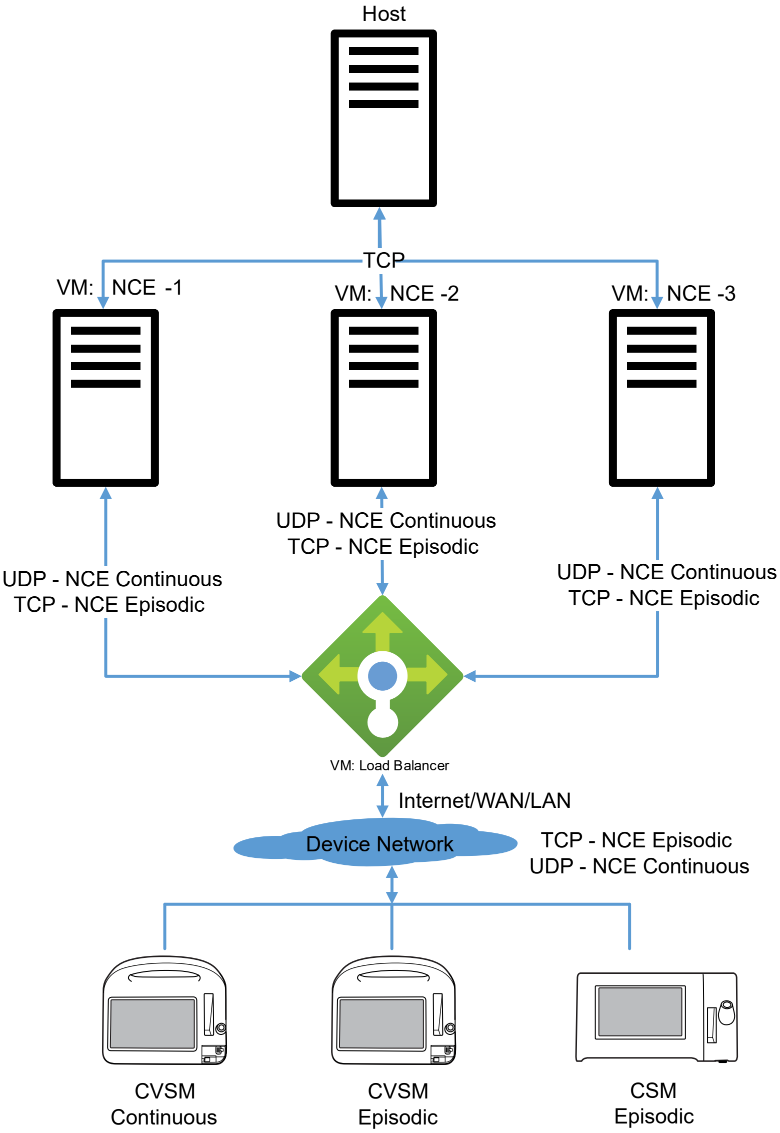
c. Easier deployments: Once one server is set up, that virtual server can be cloned

Architecture for scaling the system

The system is comprised of the following components:

- Vitals Devices: e.g. Welch Allyn Connex Vital Signs Monitors (CVSM)
- Load Balance solution
- Device Gateway: Welch Allyn Network Connectivity Engine (NCE)
- Host Application

NOTE See the Appendix for a reference configuration for the high availability scaled solution.


Host
TCP
VM: NCE -1
VM: NCE -2
VM: NCE -3
UDP - NCE Continuous
TCP - NCE Episodic
UDP - NCE Continuous
TCP - NCE Episodic
UDP - NCE Continuous
TCP - NCE Episodic
VM: Load Balancer
Internet/WAN/LAN
Device Network
TCP - NCE Episodic
UDP - NCE Continuous
CVSM
Continuous
CVSM
Episodic
CSM
Episodic

Site maintenance activities

The following actions may be needed to maintain the system.

NCE Server address changed

The NCE Server address change can happen for a few reasons:

- Moving from a test environment to a production environment. The facility may have NCE on a test server and the facility does not want to use that same server for production.
- The failure of a server and the resulting need to put in place a new server with a new IP address.
- Server software has been split across multiple servers.

To change the NCE Server address:

- Reconfigure the DCP ordinal settings to point to the correct server(s). Open the management console by opening C:\Program Files\Welch Allyn\DCP\Management\DCP.msc and configure the server address/ports as appropriate.

EMR Server address changed

The EMR Server address change can happen for a few reasons:

- Moving from a test environment to a production environment, where the NCE configuration needs to be updated to point to the EMR's production server.
- EMR server failure and the resulting need to put in place a new server with a new IP address.
- EMR server software has been split across multiple servers.

To change the EMR Server address:

1. Open the NCE Configuration Interface. See the ✓ icon in the system tray.
2. Select "*Information Network*" in the Settings menu on the left column (for each appropriate Host Index, typically 1,2,3,6 and 7):
   a. Select Host Index representing the outbound connection.
   b. Update the Host Address to the proper IP address.
   c. Press the "Save Settings" button on the bottom right of the configuration interface.
   d. Repeat for each additional Host Index where the IP address changed.
3. Close the NCE configuration interface.

Troubleshooting

To investigate an issue:

- Set Log level to 9
- Enable SavedCopies files and set to at least 7 days and at least 5000 files

After investigating the issue, return the logs back to:

- Set Log level to 3
- Disable SavedCopies files (leave 7 days and at least 5000 files)

Collecting log files and saved or failed files

Whenever you contact techincal support and a support ticket needs investigation, have the following files available:

- NCE log files
- Transaction files (SavedCopies and FailedCopies)
- Device log files
- TransformSheets folder

NCE log files can be found in the folder c:\ProgramData\Welch Allyn\NCE. There may be many log files named NCEDebugLog-YYYY.MM.DD-HH.MM.SS.txt. These files are critical to determine the root causes of issues. These files will need to be collected when issues arise.

NCE message transactions can be found in the SavedCopies folder within the path c:\ProgramData \Welch Allyn\NCE\SavedCopies. When the Local Data Cache: feature is enabled in the NCE Configuration, it will save data coming in from the device (DeviceToNCE); messages going to the host (NCEToHost) containing the message that NCE sent to the host; and responses received from the host (HostToNCE) containing the message the host sent back to the NCE engine. This data is very helpful to diagnose formatting or other application issues.

NCE failed message transactions can be found in the FailedCopies folder within the path c: \ProgramData\Welch Allyn\NCE\SavedCopies. When the Failed Data Cache feature is enabled in the NCE Configuration, it will save data coming in from the device when a failure happens. This is helpful to see what data was sent from the device that may have caused a failure to happen.

NCE troubleshooting

Item	Conditions	Causes	Actions
1	Device indicates that it is not connected to the wireless network	Outside range of all wireless networks	Move within the wireless network.
		There are no wireless networks available	Verify that the wireless network router(s) are powered up and properly configured.
		Device configuration	Check the device's network settings. Verify that these settings match the access point settings.
		The device cannot connect to the network	Wireless: Check wireless settings and ensure that they match the access point settings. Ethernet: 1. Connect the network cable. 2. Wait a few seconds. 3. Navigate to the network.setting screen and verify that the device has a valid IP address. **NOTE** If you are still having trouble connecting the device to a wireless network, try connecting the device via Ethernet to determine whether the wireless network is the issue.
2	"Test network connection" failed	Connectivity software not installed on a computer on the network	Reinstall CDIS-NCE per 60072721 CDIS-NCE Deployment Instructions on a server where the devices have a path to connect to the server.
		DCP improperly installed or DCP configuration is incorrect	1. Reinstall DCP per 60072721 CDIS-NCE Deployment Instructions section 7.3. 2. Verify (and correct) DCP configuration per 60072721L CDIS-NCE Deployment Instructions section 7.3.1.
		NCE improperly installed or NCE configuration is incorrect	1. Reinstall NCE per 60072721 CDIS-NCE Deployment Instructions section 8. 2. Verify, and if necessary, correct NCE configuration per 60072721L CDIS-NCE Deployment Instructions section 8.1.
		DCP service is not running	Check the services to verify that the "Welch Allyn DCP" service is running, restart if needed.
		NCE service is not running	Check the services to verify that the "Welch Allyn NCE" service is running, restart if needed.
		Firewall settings are blocking the required ports	Check firewall to ensure that exceptions are set per 60072721 CDIS-NCE Deployment Instructions.
		Device configuration	Check the device network settings and connectivity mode and verify these settings match the access point settings.

Item	Conditions	Causes	Actions
		The server IP address has changed or is incorrectly configured in the device	1. Verify the device has the correct server IP configured. 2. Check that the DCP Server's IP address matches the IP address setting on the device's "Host address" setting.
		DCP configuration is incorrect	Check the DCP configuration to make sure it is pointing to the correct NCE Server IP address and port at Ordinal 8 (non-encrypted episodic/spot vitals data); Ordinal 5 (Continuous vitals data) and Ordinal 14 (encrypted episodic/spot vitals data). DCP configuration can be found in the registry at: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Welch Allyn DCP\Parameters.
3	Test send or patient query or patient list query failed (wireless or ethernet)	Patient search contained no results	Server does not contain any patients that match the search criteria.
		The NCE configuration is pointing to the incorrect EMR server	
		Device's location is incorrectly configured	Verify the device's location ID is set to the proper facility [;unit[;floor]], where unit and floor are optional.
		NCE is not receiving files	Verify that the C:\ProgramData\Welch Allyn\NCE\SavedCopies folder has new files with a date/time stamp about when you sent it and that the folder updates as you send more tests. • If yes, NCE is getting files • If no, check steps in #2 Follow steps in #2 for NCE Service is not running and/or NCE improperly installed or NCE configuration is incorrect.
		1. Device could not connect to the NCE server e.g. timeout between the device and NCE. 2. NCE server could not connect to the host system (EMR) e.g. timeout between NCE and the EMR 3. EMR rejected the patient list query / patient query / vitals message.	Follow the step-by-step instructions below to determine why the failure happened. The reason for failed transactions can be identified by using the NCE log files and the saved transaction files. **NOTE** Default log file location: C:\ProgramData\Welch Allyn\NCE. 1. Select the log file containing date around the time of the failure. 2. In Notepad++ search for "Response Type = NACK". 3. Press "Find All in Current Document". This will display all the failures in this log file. 4. Note the MessageContext number next to the line containing "Response Type = NACK". Look in the file and find where the log file shows "Attempting to transform XML data using provided.xsl sheet" and matches the same MessageContext number.

Item	Conditions	Causes	Actions
			If the next line shows “Connecting to information host” and matches the same MessageContext number then this NACK was a failure from a message sent to the host system (e.g. EMR). 5. Around this area in the log there will be 3 lines that say “XML formatted device data saved locally to file”. These lines point to the saved transaction files: • DeviceToNCE.xml Data sent from device to NCE in the WACP XML format . Patient List: Contains data that the device sent for the query; e.g. facility; unit. Patient ID: Contains data that the device sent for the query; e.g. patient ID . Vitals Send: Contains patient data; serial number; location; software version; clinical data. • NCEToHost.txt Data sent from NCE to host in the host format (e.g. HL7) Patient List: Contains data that is sent to the host for the query; e.g. facility; unit Patient ID: Contains data that is sent to the host for the query; e.g. patient ID Vitals Send: Contains patient data; clinical data • HostToNCE.txt Response data sent from host to NCE in the host format (e.g. HL7) May tell specifically what is wrong based on the error data
		The NCE application stopped listening to incoming messages from devices.	Execute a telnet session to see if the NCE listener is still running. If garbage is returned the port is still listening. If nothing is returned or a timeout happens, restart NCE service. Example: telnet 10.20.30.40 281".
		The host system is being unresponsive (host system timeouts)	A customer may indicate there are failures at the device. That statement does not clarify if the failures are network-related or if the failures are data-related. If timeouts occur between NCE and one or more hosts, the host was not available when the problem occurred at the device. 1. Select the log file containing data around the time statistics would like to be captured. Typically the latest log file is sufficient.

Item	Conditions	Causes	Actions
			2. Determine if there are timeouts reported between NCE and the hosts. • In Notepad++ enter “timeout” into the Find dialog • Press “Find All in Current Document” • The number reported at the bottom of the display is how many messages were sent from NCE to all hosts that timed out
4	Vitals sent but date-time stamp is wrong	Device configuration	1. Ensure that the device’s “Time zone” is set to the correct time zone. 2. Verify the correct setting for automatically adjust for daylight settings. 3. Ensure that “Emulate Spot Vital Signs LXi” is disabled.
5	NCE configuration page is inaccessible or showing blank values	The configuration web-interface has been disabled	1. Open NCEConfig.xml (located in the NCE installation directory) with a text editor. 2. Search for “InterfaceEnabled.” On the line following this term, find the section that reads: “<![CDATA[0]]>". 3. Edit the file and replace the 0 with a 1, so the entry reads: “<![CDATA[1]]>". **NOTE** If the entry already reads “<![CDATA[1]]>", then the web-interface is enabled and something else is causing the issue.
		The configuration interface port is being used by another application	1. Restart the service and try interface again. 2. If problem persists, then for some reason the application may be crashing and restarting on its own and when the configuration interface is called up it may be when the application is not running. Check the setting for "Heartbeat interval" (found in "Device Network Settings"). If this is zero, set it to 10 and then press "Save Settings" button. Wait 20 seconds then set it to 600 and then press "Save Settings" button. 3. Reinstall or reconfigure NCE application. • Reinstall NCE per 60072721 CDIS-NCE Deployment Instructions section 8. • Verify (and correct) NCE configuration per 60072721L CDIS-NCE Deployment Instructions section 8.1.

Limitations

- CDIS-NCE cannot push a file to a remote server.

  If file output is desired, the files must be stored locally on the server NCE is running within the NCE folder.
- CDIS-NCE is supported only on Windows OS platforms.
- Thin client (Citrix or RDP) is not supported. The CDIS-NCE solution is intended to be a server software solution where the device(s) will connect to CDIS-NCE via a network connection.

- CDIS-NCE does not support a Bluetooth connection.
- CDIS-NCE does not support ADT. CDIS-NCE only supports query-response of patient or clinician information.
- Sending of data (e.g. HL7 ORU) is initiated by the device only. A host system cannot query for data from the CDIS-NCE software or directly from the device.
- Batch workflow is not a preferred workflow since not all EMR systems can properly handle sending a bulk set of data.
- When a test send fails, the test data is saved on the device. The device will attempt to resend the test data from a failed send when the device sends another (new) test. If there is something wrong with the test data (as opposed to a wireless connectivity issue) that caused it to fail a send on the first attempt, it will also fail on the second attempt. To avoid an abundance of errors in the EMR, remove records from the device that failed to send.
- Modifications of the solution configuration (transforms or EMR data mapping) need to be done by Welch Allyn personnel.

Appendix

Vitals Connectivity Using CDIS-NCE With High Availability

The following section describes a reference high availability CDIS-NCE system configuration with vital signs continuous and episodic workflows.

Networking

The physical LAN is configured as a 172.18.0.0/24 network with a default gateway of 172.18.0.1. Four IP addresses are reserved on the external network:

IP Address	Use
172.18.0.238	F5 External Self IP (non-floating)
172.18.0.239	F5 External Self IP (floating)
172.18.0.240	NCE Service IP Address
172.18.0.245	DCP Service IP Address

Virtual Machine Host/Hypervisor

Hypervisor	VMware ESXI
Version	6.7.0
Build	8169922
Manufacturer	Dell Inc.
Model	PowerEdge R530
CPU	28 CPUs x Intel(R) Xeon(R) CPU E5-2660 v4 @ 2.00GHz
Memory	191.78 GB
Data stores	8 data stores, 7450 GB total capacity

The hypervisor has multiple LANs configured. Two virtual LANs were configured: management and internal. The hypervisor has a connection to the physical LAN within the reference network.

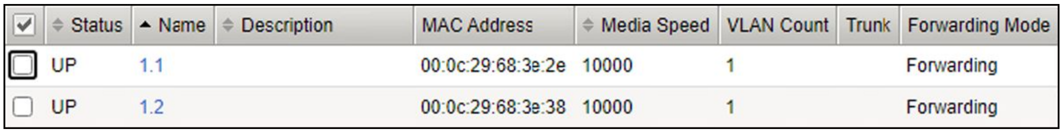
F5 Virtual Machine

Product	BIG-IP Local Traffic Manager Virtual Edition
License	Lab (10 Mbps, v12.1.x - v18.x)
Version	15.1.3
CPU	2 cores
Memory	12 GB
Data store	Datastore #5, 76 GB (Thin provisioned)

By default, the F5 virtual machine is configured with four network adapters: management, internal, external, and high availability (HA). The HA adapter is not used and is disabled.

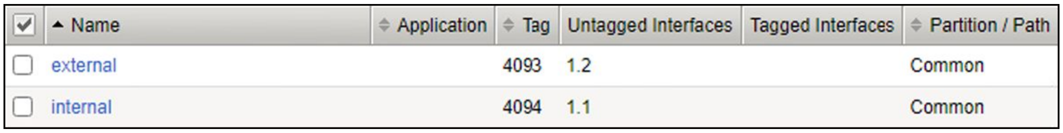
Both the management and internal network adapters are connected to virtual LANs configured within the hypervisor. The external network adapter is connected to a physical LAN within the reference network.

Figure 1 - F5 Interfaces (management interface not shown)



☑	Status	▲ Name	Description	MAC Address	Media Speed	VLAN Count	Trunk	Forwarding Mode
□	UP	1.1		00:0c:29:68:3e:2e	10000	1		Forwarding
□	UP	1.2		00:0c:29:68:3e:38	10000	1		Forwarding

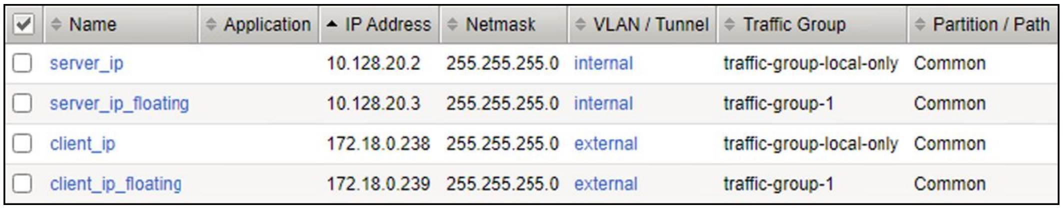
Figure 2 - F5 VLANs (management VLAN not shown)



☑	▲ Name	Application	Tag	Untagged Interfaces	Tagged Interfaces	Partition / Path
□	external		4093	1.2		Common
□	internal		4094	1.1		Common

Floating and non-floating self IP addresses are configured for both internal and external networks. The internal self IP addresses are configured to the reserved IP addresses on the internal network. The external self IP addresses are configured to the reserved IP addresses on the external network.

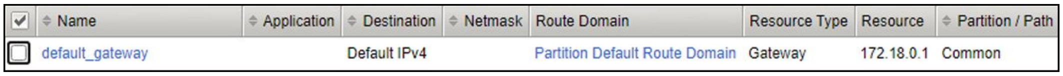
Figure 3 - F5 Self IPs



☑	Name	Application	▲ IP Address	Netmask	VLAN / Tunnel	Traffic Group	Partition / Path
□	server_ip		10.128.20.2	255.255.255.0	internal	traffic-group-local-only	Common
□	server_ip_floating		10.128.20.3	255.255.255.0	internal	traffic-group-1	Common
□	client_ip		172.18.0.238	255.255.255.0	external	traffic-group-local-only	Common
□	client_ip_floating		172.18.0.239	255.255.255.0	external	traffic-group-1	Common

A default gateway route to the Internet was created. This route was created to allow resources on the internal network to access the Internet. The resource is the reference network default gateway.

Figure 4 - F5 Routes



☑	Name	Application	Destination	Netmask	Route Domain	Resource Type	Resource	Partition / Path
□	default_gateway		Default IPv4		Partition Default Route Domain	Gateway	172.18.0.1	Common

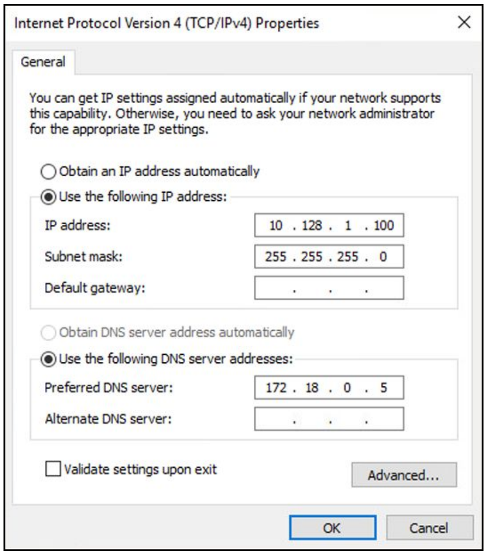
Mirth Server Virtual Machine

Operating System	Microsoft Windows Server 2016 Standard
Version	1607
Build	14393.4467
CPU	4 cores
Memory	16 GB
Data store	Datastore #3, 120GB (Preallocated)
Primary service	Mirth Connect
Additional Services	None

The Mirth server / application serves multiple roles within the system. It acts as the management computer for the F5 environment and the HL7 EMR system.

The Mirth Server has two network adapters. One network adapter is connected to the internal virtual LAN configured within the hypervisor. This network card is configured to use a unique static IP address on the internal network and use the F5 internal self IP address as the default gateway.

Figure 5 - Mirth Server Internal IP Configuration



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 10 . 128 . 1 . 100
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

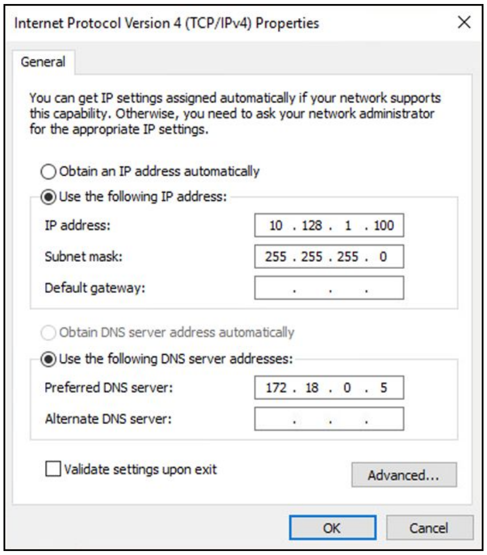
○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: 172 . 18 . 0 . 5
Alternate DNS server: . . .

□ Validate settings upon exit

The second adapter is connected to the management virtual LAN configured within the hypervisor. This network card is configured to use a unique static IP address on the management network and does not have a default gateway configured.

Figure 6 - Mirth Server Management IP Configuration



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 128 . 1 . 100

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 172 . 18 . 0 . 5

Alternate DNS server: . . .

□ Validate settings upon exit

Ping/ICMP echo request is enabled on this server.

NCE Server #1 Virtual Machine

Operating System	Microsoft Windows Server 2016 Standard
Version	1607
Build	14393.4467
CPU	4 cores
Memory	8 GB
Data store	Datastore #4, 60GB (Preallocated)
Primary service	NCE
Additional Services	DCP

NCE Server #2 Virtual Machine

Operating System	Microsoft Windows Server 2016 Standard
Version	1607
Build	14393.4467
CPU	4 cores
Memory	8 GB
Data store	Datastore #6, 60GB (Preallocated)
Primary service	NCE

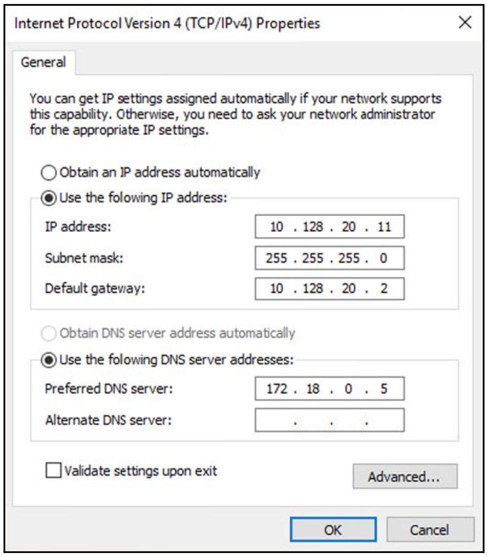
Additional Services	DCP

NCE Server #3 Virtual Machine

Operating System	Microsoft Windows Server 2016 Standard
Version	1607
Build	14393.4467
CPU	4 cores
Memory	8 GB
Data store	Datastore #2, 60GB (Preallocated)
Primary service	NCE
Additional Services	DCP

Each NCE server has a single network adapter connected to the internal virtual LAN configured within the hypervisor. The network card on each server is configured to use a unique static IP address on the internal network and use the F5 internal self IP address as the default gateway.

Figure 7 - NCE Server 1 IP Configuration



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 128 . 20 . 11

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 10 . 128 . 20 . 2

○ Obtain DNS server address automatically

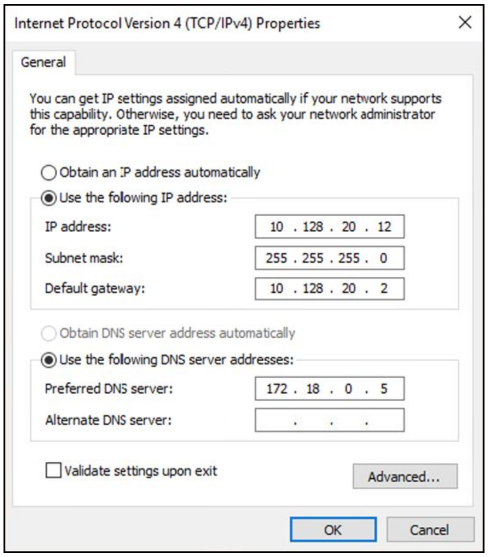
● Use the following DNS server addresses:

Preferred DNS server: 172 . 18 . 0 . 5

Alternate DNS server: . . .

□ Validate settings upon exit

Figure 8 - NCE Server 2 IP Configuration



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	10 . 128 . 20 . 12
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	10 . 128 . 20 . 2

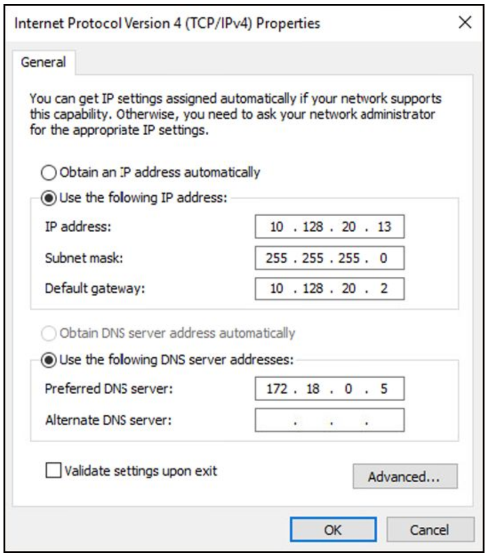
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:	172 . 18 . 0 . 5
Alternate DNS server:	. . .

□ Validate settings upon exit

Figure 9 - NCE Server 3 IP Configuration



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	10 . 128 . 20 . 13
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	10 . 128 . 20 . 2

○ Obtain DNS server address automatically

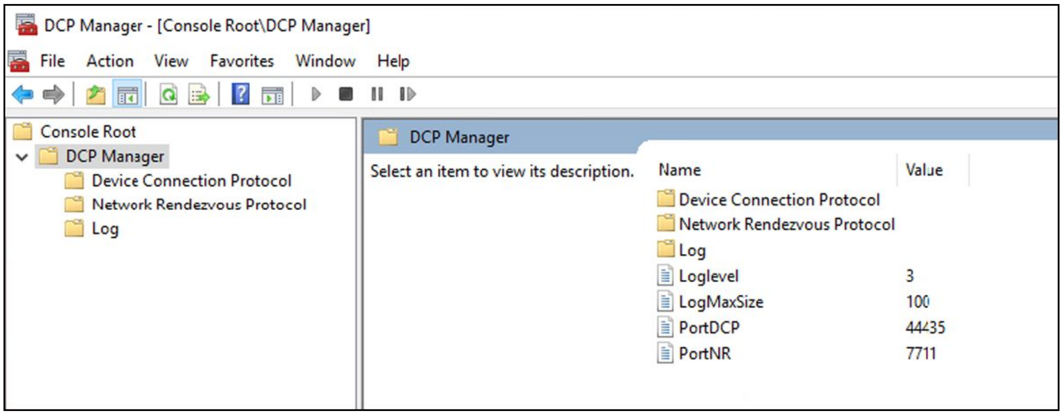
● Use the following DNS server addresses:

Preferred DNS server:	172 . 18 . 0 . 5
Alternate DNS server:	. . .

□ Validate settings upon exit

The DCP service is installed on each of the NCE servers using the default settings for log level and ports, and the log maximum size is set to 100.

Figure 10 - DCP Manager Configuration

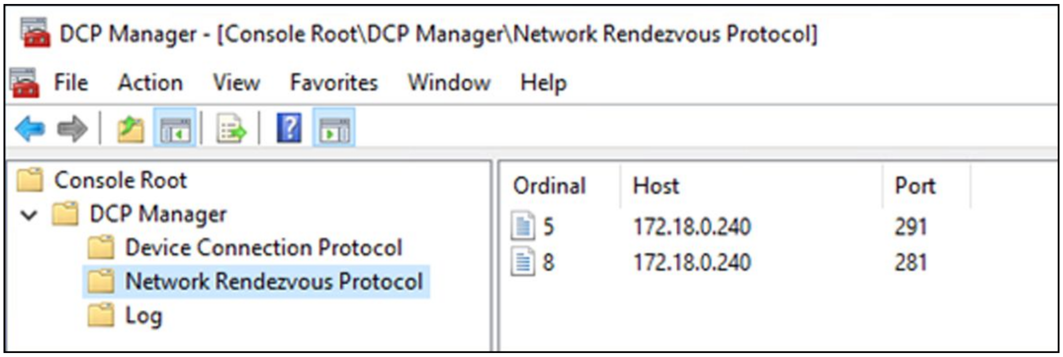

DCP Manager - [Console Root\DCP Manager]
File
Action
View
Favorites
Window
Help
Console Root
DCP Manager
Device Connection Protocol
Network Rendezvous Protocol
Log
DCP Manager

Select an item to view its description.

Name	Value
Device Connection Protocol	
Network Rendezvous Protocol	
Log	
Loglevel	3
LogMaxSize	100
PortDCP	44435
PortNR	7711

The DCP service is configured with ordinals 5 and 8 (or 14). The host addresses used are the IP addresses reserved for these services on the external network. The standard port for NCE is used.

Figure 11 - DCP Network Rendezvous Protocol Configuration


DCP Manager - [Console Root\DCP Manager\Network Rendezvous Protocol]
File
Action
View
Favorites
Window
Help
Console Root
DCP Manager
Device Connection Protocol
Network Rendezvous Protocol
Log

Ordinal	Host	Port
5	172.18.0.240	291
8	172.18.0.240	281

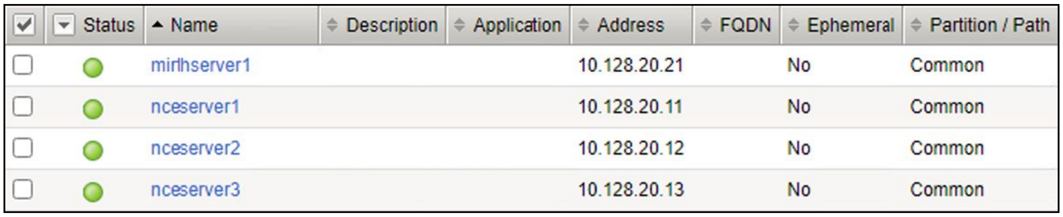
All NCE servers are configured using the HL7 TCP/IP installation instructions. The NCE information network is configured to use the IP address and ports of the Mirth server on the internal network.

Ping/ICMP echo request is enabled on these servers.

Nodes

In F5, a separate node was created for each of the NCE servers as well as the Mirth server. For ease of identification, the node name used for each node is the computer names of the target server. The nodes are configured with the internal network static IP address for the server. The default node health monitor is used to track the health of the servers. “gateway_icmp” is the default node health monitor.

Figure 12 - F5 Nodes

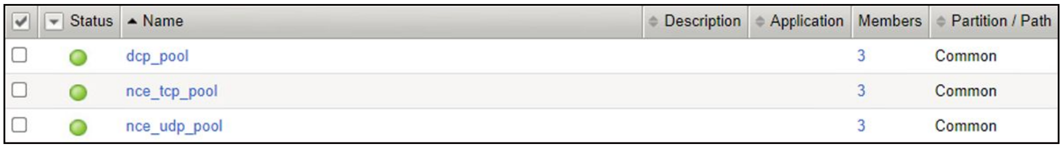


☑	Status	▲ Name	Description	Application	Address	FQDN	Ephemeral	Partition / Path
☐	●	mirlhserver1			10.128.20.21		No	Common
☐	●	nceserver1			10.128.20.11		No	Common
☐	●	nceserver2			10.128.20.12		No	Common
☐	●	nceserver3			10.128.20.13		No	Common

Pools

F5 uses pools - a logical set of computers - to receive and process traffic. In F5, three pools were created:

Figure 13 - F5 Pools

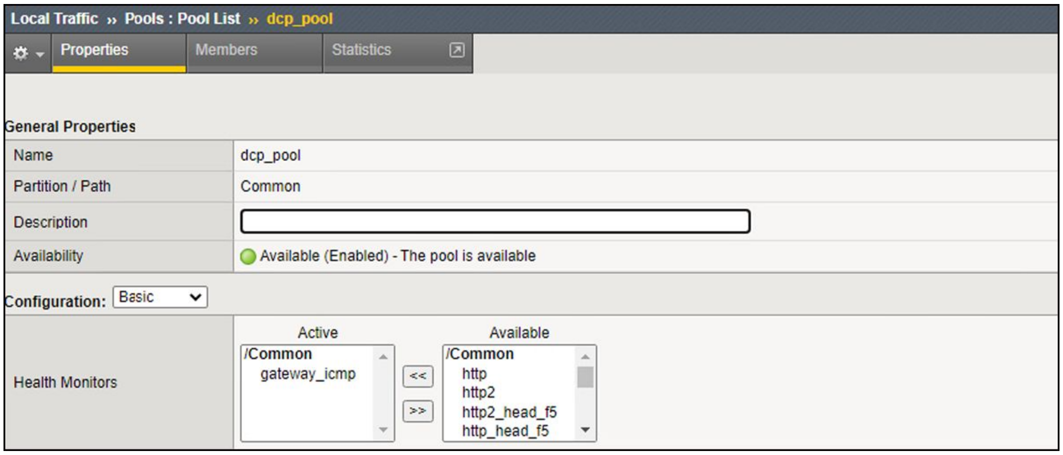


☑	Status	Name	Description	Application	Members	Partition / Path
□	●	dcp_pool			3	Common
□	●	nce_tcp_pool			3	Common
□	●	nce_udp_pool			3	Common

DCP Pool

The DCP pool was created to identify the nodes used for the DCP service. The NCE servers have DCP installed and configured, and each server is included in the pool. The health monitor for the pool is “gateway_icmp”.

Figure 14 - DCP Pool Properties



General Properties

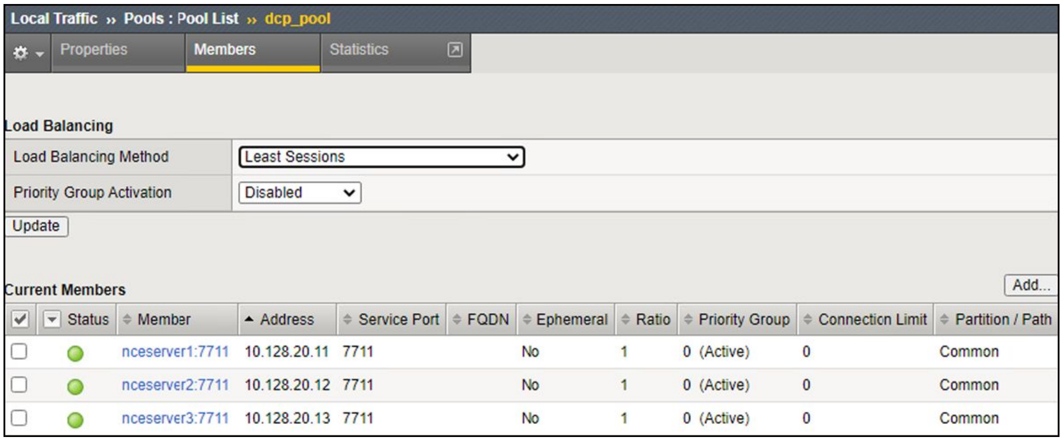
Name	dcp_pool
Partition / Path	Common
Description	
Availability	● Available (Enabled) - The pool is available

Configuration: Basic

	Active		Available
Health Monitors	/Common gateway_icmp	<< >>	/Common http http2 http2_head_f5 http_head_f5

The load balancing method is “Least Sessions”, and the service port is configured to the DCP Network Rendezvous port.

Figure 15 - DCP Pool Members



Load Balancing

Load Balancing Method	Least Sessions
Priority Group Activation	Disabled

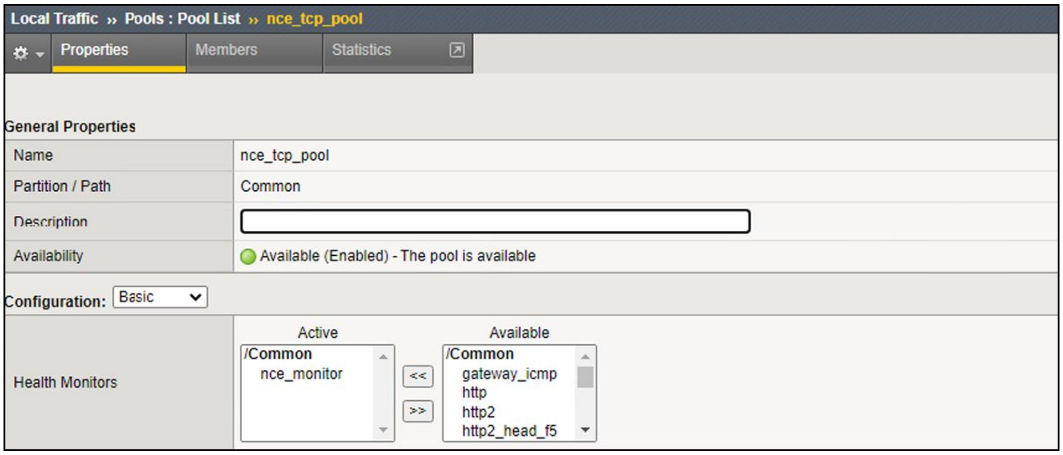
Current Members

☑	Status	Member	Address	Service Port	FQDN	Ephemeral	Ratio	Priority Group	Connection Limit	Partition / Path
□	●	nceserver1:7711	10.128.20.11	7711		No	1	0 (Active)	0	Common
□	●	nceserver2:7711	10.128.20.12	7711		No	1	0 (Active)	0	Common
□	●	nceserver3:7711	10.128.20.13	7711		No	1	0 (Active)	0	Common

NCE TCP Pool

The NCE TCP pool was created to identify the nodes used for the NCE service over TCP. There are three servers that have NCE installed and configured. All three servers have a node included in the pool. The health monitor for the pool is “nce_monitor”, which is an HTTP monitor designed to listen to the NCE web browser connection port.

Figure 16 - NCE TCP Pool Properties



General Properties

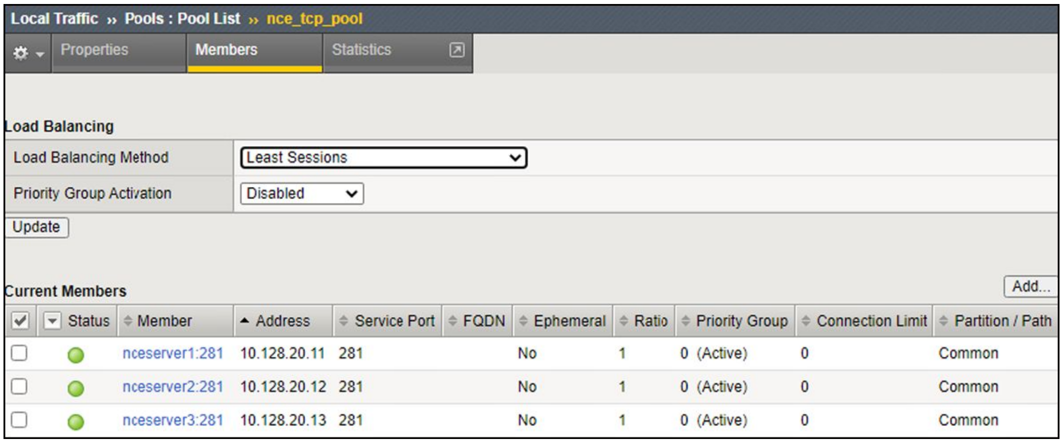
Name	nce_tcp_pool
Partition / Path	Common
Description	
Availability	● Available (Enabled) - The pool is available

Configuration: Basic

	Active		Available
Health Monitors	/Common nce_monitor	<< >>	/Common gateway_icmp http http2 http2_head_f5

The load balancing method is “Least Sessions”, and the service port is configured to the NCE TCP port configured in the DCP Network Rendezvous protocol configuration settings.

Figure 17 - NCE TCP Pool Members



Load Balancing

Load Balancing Method	Least Sessions
Priority Group Activation	Disabled

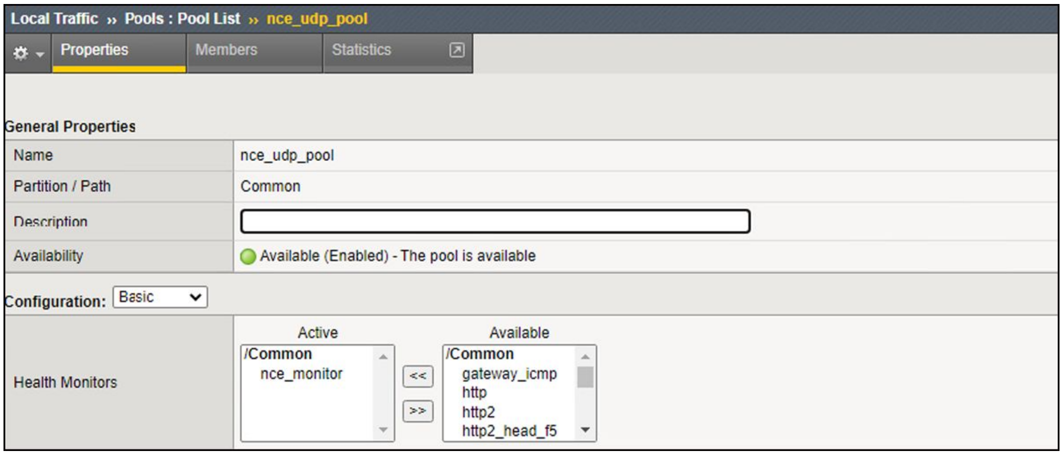
Current Members

☑	Status	Member	Address	Service Port	FQDN	Ephemeral	Ratio	Priority Group	Connection Limit	Partition / Path
□	●	nceserver1:281	10.128.20.11	281		No	1	0 (Active)	0	Common
□	●	nceserver2:281	10.128.20.12	281		No	1	0 (Active)	0	Common
□	●	nceserver3:281	10.128.20.13	281		No	1	0 (Active)	0	Common

NCE UDP Pool

The NCE UDP pool was created to identify the nodes used for the NCE service over UDP. There are three servers that have NCE installed and configured. All three servers have a node included in the pool. The health monitor for the pool is “nce_monitor”, which is an HTTP monitor designed to listen to the NCE web browser connection port.

Figure 18 - NCE UDP Pool Properties



General Properties

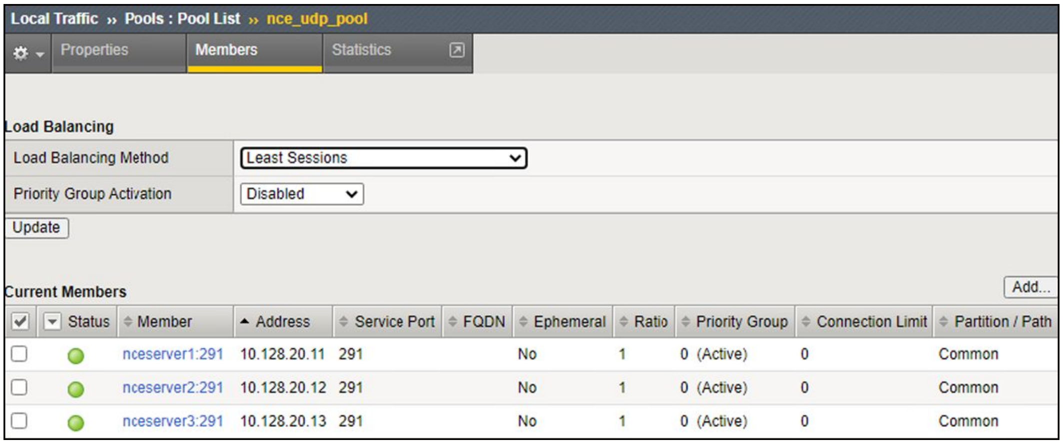
Name	nce_udp_pool
Partition / Path	Common
Description	
Availability	● Available (Enabled) - The pool is available

Configuration: Basic

	Active	Available
Health Monitors	/Common nce_monitor	/Common gateway_icmp http http2 http2_head_f5

The load balancing method is "Least Sessions", and the service port is configured to the NCE UDP port configured in the DCP Network Rendezvous protocol configuration settings.

Figure 19 - NCE UDP Pool Members



Load Balancing

Load Balancing Method	Least Sessions
Priority Group Activation	Disabled

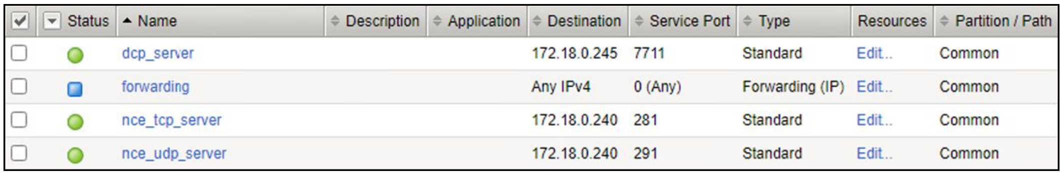
Current Members

☑	Status	Member	Address	Service Port	FQDN	Ephemeral	Ratio	Priority Group	Connection Limit	Partition / Path
□	●	nceserver1:291	10.128.20.11	291		No	1	0 (Active)	0	Common
□	●	nceserver2:291	10.128.20.12	291		No	1	0 (Active)	0	Common
□	●	nceserver3:291	10.128.20.13	291		No	1	0 (Active)	0	Common

Virtual Servers

As a "default deny" device, F5 requires a specific configuration to support traffic flow. This configuration comes in the form of virtual servers. Four virtual servers were created:

Figure 20 - F5 Virtual Servers

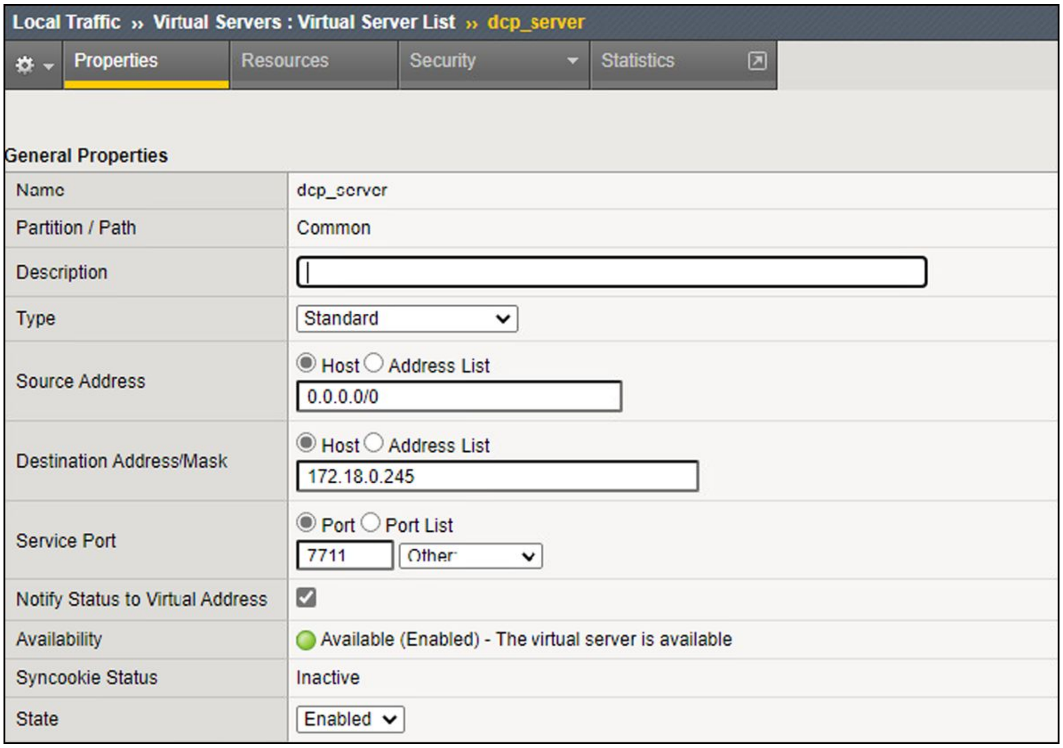


☑	Status	Name	Description	Application	Destination	Service Port	Type	Resources	Partition / Path
□	●	dcp_server			172.18.0.245	7711	Standard	Edit...	Common
□	■	forwarding			Any IPv4	0 (Any)	Forwarding (IP)	Edit...	Common
□	●	nce_tcp_server			172.18.0.240	281	Standard	Edit...	Common
□	●	nce_udp_server			172.18.0.240	291	Standard	Edit...	Common

DCP Virtual Server

The DCP virtual server provides the virtual IP address for the devices connected to the external network to communicate with the DCP service hosted on the internal network. The type of virtual server is "Standard". Its source address is 0.0.0.0/0, and the destination address is the virtual IP address reserved on the external network for DCP. Its service port is configured to the DCP Network Rendezvous port.

Figure 21 - DCP Virtual Server Properties

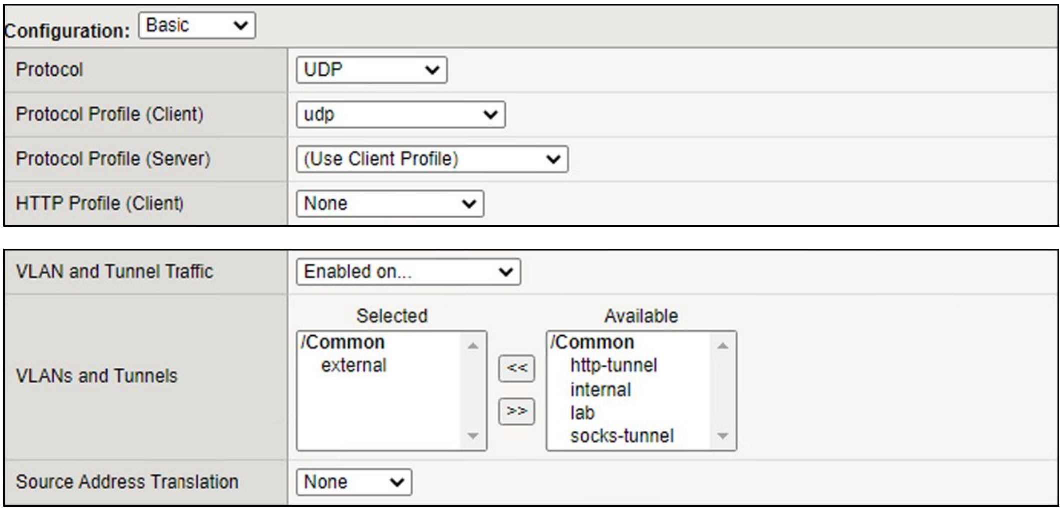

Local Traffic » Virtual Servers : Virtual Server List » dcp_server
Properties
Resources
Security
Statistics

General Properties

Name	dcp_server
Partition / Path	Common
Description	
Type	Standard
Source Address	● Host ○ Address List 0.0.0.0/0
Destination Address/Mask	● Host ○ Address List 172.18.0.245
Service Port	● Port ○ Port List 7711 Other:
Notify Status to Virtual Address	☑
Availability	● Available (Enabled) - The virtual server is available
Syncookie Status	Inactive
State	Enabled

Configuration is "Basic" for this virtual server. The UDP protocol is configured for this virtual server. It is enabled on the external VLAN only. Source address translation is "none".

Figure 22 - DCP Virtual Server Configuration



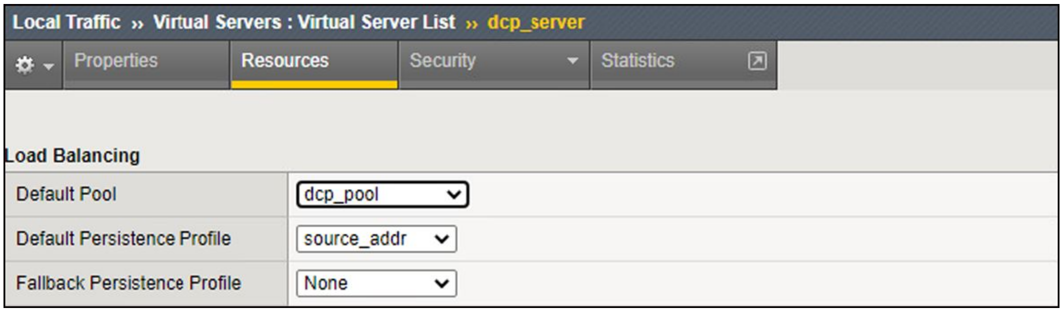
Configuration: Basic

Protocol	UDP
Protocol Profile (Client)	udp
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile (Client)	None

VLAN and Tunnel Traffic	Enabled on...
VLANs and Tunnels	Selected: /Common external Available: /Common http-tunnel internal lab socks-tunnel
Source Address Translation	None

Default pool for the DCP virtual server is the DCP pool, and the default persistence profile is "source_addr".

Figure 23 - DCP Virtual Server Resources


Local Traffic » Virtual Servers : Virtual Server List » dcp_server
Properties
Resources
Security
Statistics

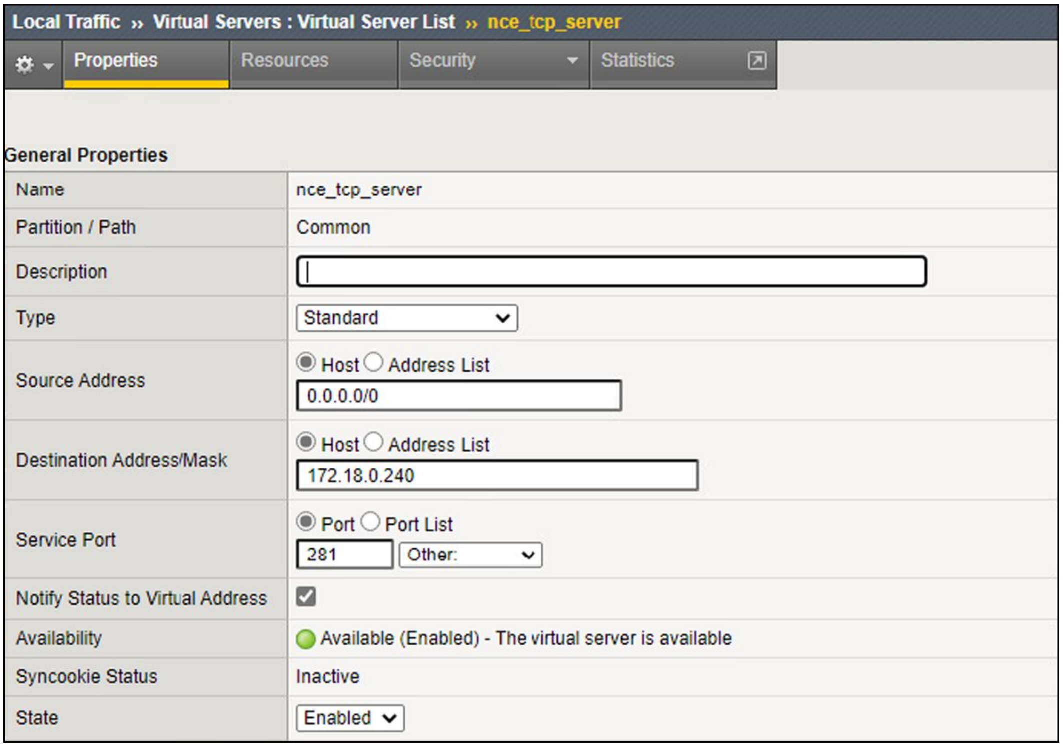
Load Balancing

Default Pool	dcp_pool
Default Persistence Profile	source_addr
Fallback Persistence Profile	None

NCE TCP Virtual Server

The NCE TCP virtual server provides the virtual IP address for the devices connected to the external network to communicate with the NCE TCP service hosted on the internal network. The type of virtual server is "Standard". Its source address is 0.0.0.0/0, and the destination address is the virtual IP address reserved on the external network for NCE. Its service port is configured to the NCE TCP port configured in the DCP Network Rendezvous protocol settings.

Figure 24 - NCE TCP Virtual Server Properties

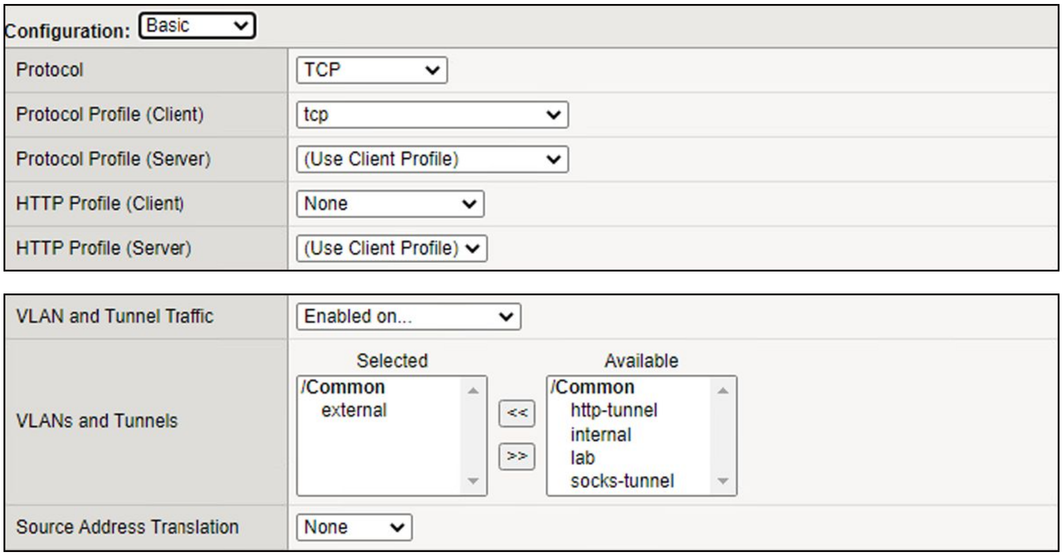

Local Traffic » Virtual Servers : Virtual Server List » nce_tcp_server
Properties
Resources
Security
Statistics

General Properties

Name	nce_tcp_server
Partition / Path	Common
Description	
Type	Standard
Source Address	● Host ○ Address List 0.0.0.0/0
Destination Address/Mask	● Host ○ Address List 172.18.0.240
Service Port	● Port ○ Port List 281 Other:
Notify Status to Virtual Address	☑
Availability	🟢 Available (Enabled) - The virtual server is available
Syncookie Status	Inactive
State	Enabled

Configuration is "Basic" for this virtual server. The TCP protocol is configured for this virtual server. It is enabled on the external VLAN only. Source address translation is "none".

Figure 25 - NCE TCP Virtual Server Configuration



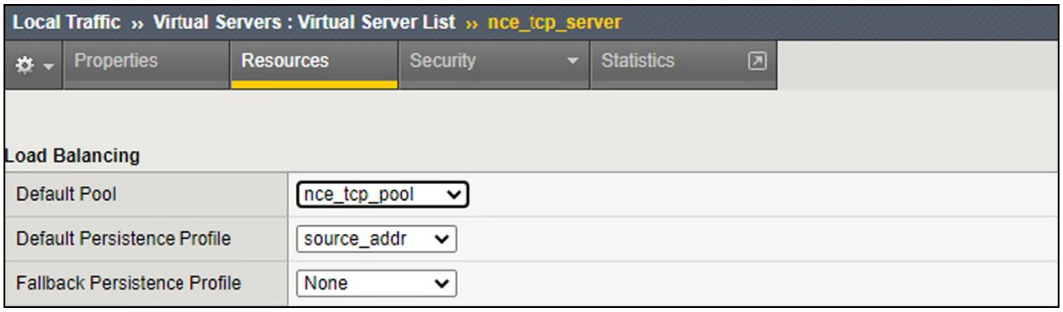
Configuration: Basic

Protocol	TCP
Protocol Profile (Client)	tcp
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile (Client)	None
HTTP Profile (Server)	(Use Client Profile)

VLAN and Tunnel Traffic	Enabled on...
VLANs and Tunnels	Selected: /Common external Available: /Common http-tunnel internal lab socks-tunnel
Source Address Translation	None

Default pool for the NCE TCP virtual server is the NCE TCP pool, and the default persistence profile is “source_addr”.

Figure 26 - NCE TCP Virtual Server Resources



Local Traffic » Virtual Servers : Virtual Server List » nce_tcp_server

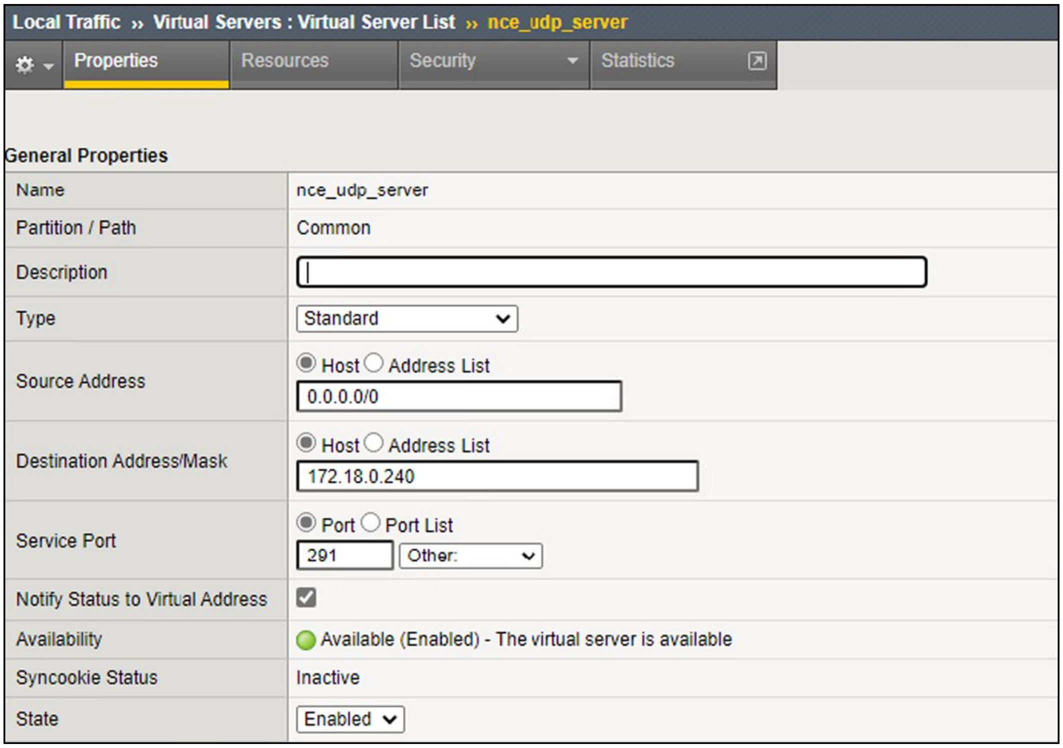
Load Balancing

Default Pool	nce_tcp_pool
Default Persistence Profile	source_addr
Fallback Persistence Profile	None

NCE UDP Virtual Server

The NCE UDP virtual server provides the virtual IP address for the devices connected to the external network to communicate with the NCE UDP service hosted on the internal network. The type of virtual server is “Standard”. Its source address is 0.0.0.0/0, and the destination address is the virtual IP address reserved on the external network for NCE. Its service port is configured to the NCE UDP port configured in the DCP Network Rendezvous protocol configuration settings.

Figure 27 - NCE UDP Virtual Server Properties



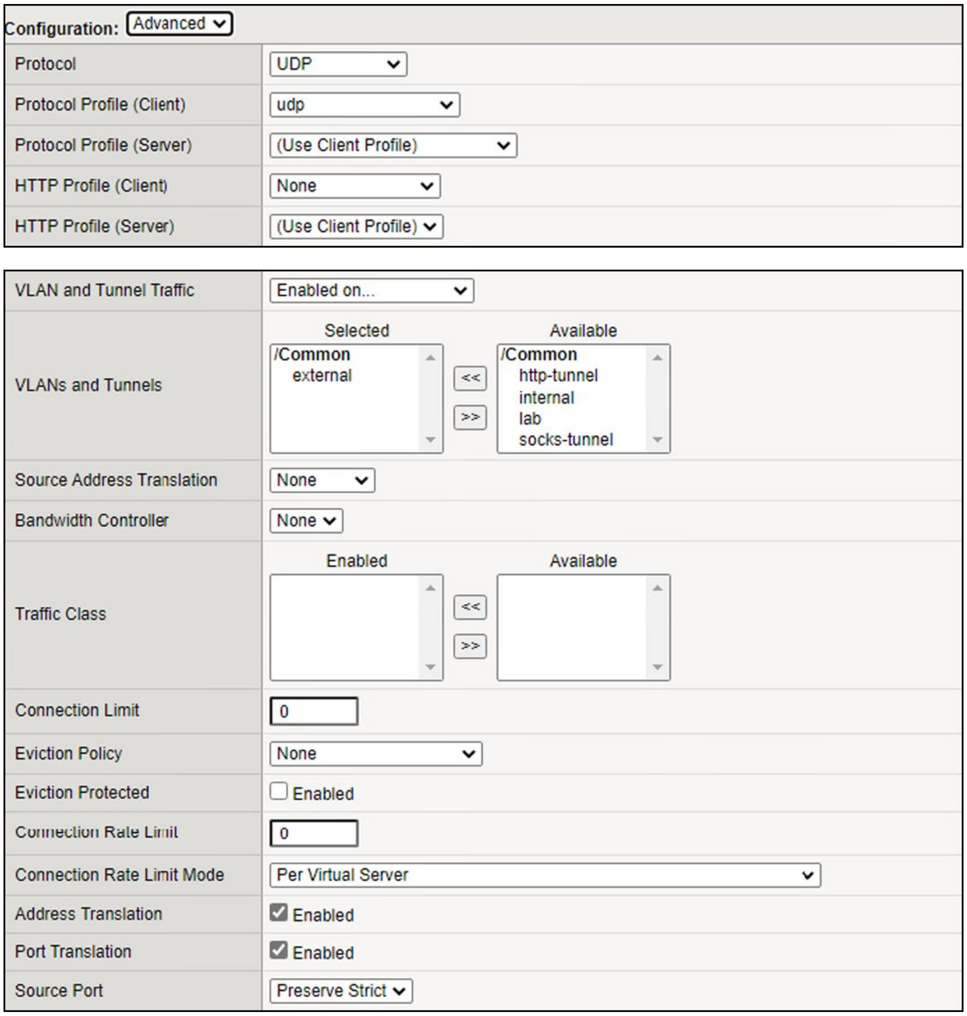
Local Traffic » Virtual Servers : Virtual Server List » nce_udp_server

General Properties

Name	nce_udp_server
Partition / Path	Common
Description	
Type	Standard
Source Address	● Host ○ Address List 0.0.0.0/0
Destination Address/Mask	● Host ○ Address List 172.18.0.240
Service Port	● Port ○ Port List 291 Other:
Notify Status to Virtual Address	☑
Availability	● Available (Enabled) - The virtual server is available
Syncookie Status	Inactive
State	Enabled

Configuration is “Advanced” for this virtual server. The UDP protocol is configured for this virtual server. It is enabled on the external VLAN only. Source address translation is “none” and the source port is configured to “Preserve Strict”.

Figure 28 - NCE UDP Virtual Server Configuration



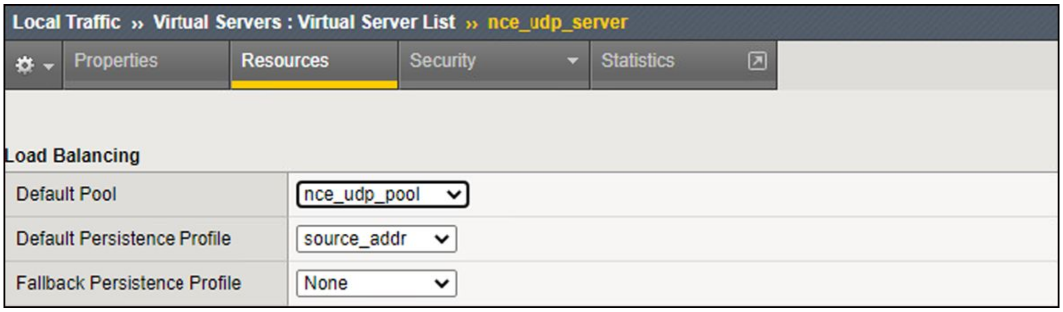
Configuration: Advanced

Protocol	UDP
Protocol Profile (Client)	udp
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile (Client)	None
HTTP Profile (Server)	(Use Client Profile)

VLAN and Tunnel Traffic	Enabled on...
VLANs and Tunnels	Selected: /Common external Available: /Common http-tunnel internal lab socks-tunnel
Source Address Translation	None
Bandwidth Controller	None
Traffic Class	Enabled: Available:
Connection Limit	0
Eviction Policy	None
Eviction Protected	☐ Enabled
Connection Rate Limit	0
Connection Rate Limit Mode	Per Virtual Server
Address Translation	☑ Enabled
Port Translation	☑ Enabled
Source Port	Preserve Strict

Default pool for the NCE UDP virtual server is the NCE UDP pool, and the default persistence profile is “source_addr”.

Figure 29 - NCE UDP Virtual Server Resources



Local Traffic » Virtual Servers : Virtual Server List » nce_udp_server

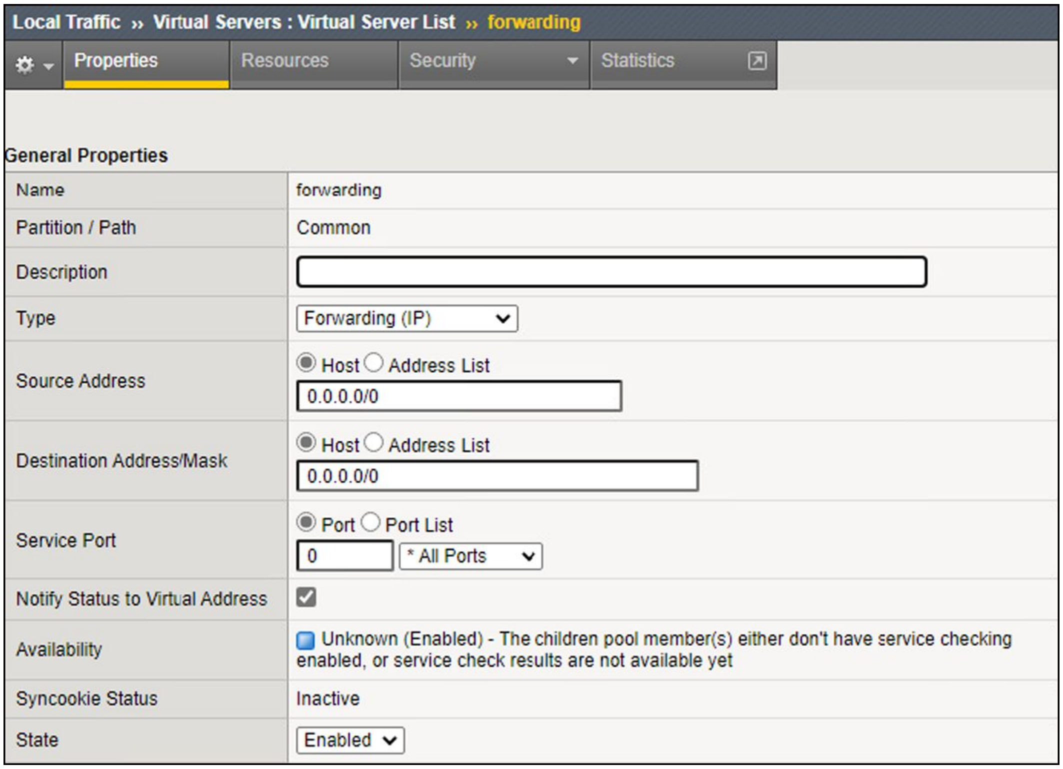
Load Balancing

Default Pool	nce_udp_pool
Default Persistence Profile	source_addr
Fallback Persistence Profile	None

Forwarding Virtual Server

The Forwarding virtual server was created to allow the servers on the internal network to access resources outside of the internal network (i.e. – Microsoft security patches). The type of virtual server is "Forwarding (IP)". Its source and destination address are 0.0.0.0/0 with a service port of 0.

Figure 30 - Forwarding Virtual Server Properties

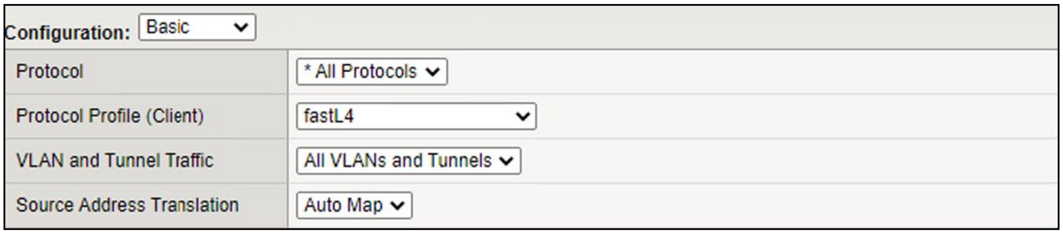

Local Traffic » Virtual Servers : Virtual Server List » forwarding
Properties
Resources
Security
Statistics

General Properties

Name	forwarding
Partition / Path	Common
Description	
Type	Forwarding (IP)
Source Address	● Host ○ Address List 0.0.0.0/0
Destination Address/Mask	● Host ○ Address List 0.0.0.0/0
Service Port	● Port ○ Port List 0 * All Ports
Notify Status to Virtual Address	☑
Availability	🟦 Unknown (Enabled) - The children pool member(s) either don't have service checking enabled, or service check results are not available yet
Syncookie Status	Inactive
State	Enabled

Configuration is "Basic" for this virtual server. All protocols are configured for this virtual server. It uses the "fastL4" protocol profile and it is open to all VLANs and tunnels. It uses "Auto Map" for source address translation.

Figure 31 - Forwarding Virtual Server Configuration



Configuration: Basic

Protocol	* All Protocols
Protocol Profile (Client)	fastL4
VLAN and Tunnel Traffic	All VLANs and Tunnels
Source Address Translation	Auto Map

Devices

In total, ninety-six devices were connected to the 172.18.10.0/24 network using Ethernet. This network is connected to the 172.18.0.0/24 network through a Cisco Layer-3 switch, which enabled routing between the physical networks. Once physically connected to the network, each device's NRS IP connectivity setting was set to the virtual IP address reserved on the external network for DCP. The NRS port was configured to the DCP Network Rendezvous port. The devices were placed into demo mode to provide continuous data to the system.