Configure Cluster Serviceability Improvements in Firewall Management Center 7.4

Contents

Introduction

What's New

Prerequisites, Supported Platforms, Licensing

Minimum Software & Hardware Platforms

Components Used

CCL Link Diagnostics

Cluster Control Link Interface MTU Warning in the Cluster Summary Page
Problem
MTU Size Recommendations Per Platform
Solution

CCL Ping Test in Cluster Live Status

Check CCL Connectivity

Solution

Added CCL MTU Sizes for Public Cloud

CLIs Available in FMC

Device Lina CLI Prompt Available in Device/Cluster Tab

Run Cluster Lina CLIs from FMC

Commonly Used CLIs Shown by Default

Predefined Cluster CLIs

Manual Entry of Commands Available

Generation of Troubleshoots

Automatic Troubleshoot Generation on Node Join Failure

Troubleshoot Trigger and Download Button Available inDevice and Cluster Tabs

Easier Generation of Cluster Troubleshoots

Cluster Troubleshoot Generation

Node (Device) Troubleshoot Generation

Notification of Cluster Troubleshoot Generation Complete

<u>Q & A</u>

Revision History

Introduction

This document describes how you can use serviceability improvements in FMC 7.4

What's New

- Cluster Control Link (CCL) link diagnostics and assistance with ensuring settings are correct.
- Cluster Lina CLIs can now be seen in Firewall Management Center (FMC).

- Troubleshoot Generation
 - Can now be generated all at once for all devices in a cluster.
 - Troubleshoot generation is automatic if a node fails to join a cluster.
 - Troubleshoot generation and navigation from the Devices > Cluster/Device tab.

Prerequisites, Supported Platforms, Licensing

Minimum Software & Hardware Platforms

Application and Minimum Version	Managed Devices	Min Supported Managed Device Version Required	Notes
Secure Firewall 7.4	All which support clustering on FTD Only "Generation of Troubleshoots" enhancement requires FTD version to be 7.4 and higher	 FMC On-Prem + FMC REST API cloud-delivered FMC 	This is an FMC feature, so configuration can be applied to any device that FMC 7.4 can manage.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Firewall Management Center (FMC) running 7.4
- Cisco Firepower Threat Defense (FTD) running 7.4 or higher.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

CCL Link Diagnostics

Cluster Control Link Interface MTU Warning in the Cluster Summary Page

Problem

- Clustering requires a higher MTU for the cluster control link than data interfaces.
- You often do not set the MTU to a high enough value, which causes reliability issues.
- Recommendation is CCL MTU must be 100 or 154 bytes more than the maximum data interface MTU, based on the platform, to sync the cluster state across the nodes.

CCL MTU = (Maximum Data Interface MTU) + 100 /154

For example, for an FTDv device, if 1700 bytes is the maximum data interface MTU, then the value of CCL interface MTU would be set as 1854: 1854 = 1700 + 154

MTU Size Recommendations Per Platform

Platform	Sample maximum Data Interface MTU	Add	Total Recommended Setting for MTU for CCL Link
Sec FW 3100 Series	1700	100	1800
FTDv	1700	154	1854

Solution

- When a cluster is created, the MTU value for the CCL link is automatically set to the recommended value on the interface.
 - Make the switch side configuration to match this value.
- Sample warning message: Clustering requires a higher MTU for the cluster control link. The maximum current data interface MTU is 1500 bytes; the recommended cluster control link MTU is 1654 bytes or higher. Before proceeding, make sure connected switches match the MTUs for data interfaces and the cluster control link, otherwise the cluster formation would fail.
- If the switch side configuration for CCL interface does not match this value, the device fails to join the cluster.

1500, you need to manually rebo	for the cluster control link. If you did ot each node after the cluster is form	i not enable jumbo frames at o ned and healthy. Use the 'show	teployment or have not previously v jumbo-frame reservation' comm	enabled jumbo frames by settin and on the device to check jumb	g the MTU of an interface ab oo frame status.			
 Clustering requires a higher MTU proceeding, make sure connecte 	for the cluster control link. The maxi d switches match the MTUs for data	mum current data interface M interfaces and the cluster con	TU is 1600 bytes; the recommend trol link, otherwise the cluster form	ed cluster control link MTU is 17 nation will fail. More info *	54 bytes or higher. Before			
Cluster Name: testCluster								
Cluster Key:				1				
Control Node								
Name	Priority	VNI Network	VTEP IPv4 Address	Cluster Control Link	VTEP Network			
10.10.43.24	1	10.2.2.0/27	10.102.3.1	GigabitEthernet0/0	10.102.3.0/27			
Name 10.10.43.25	Priority 2	VTEP IPv4 Addres 10.102.3.2	15					
10.10.43.25	2	10.102.3.2						
uarning honner has	been added in the	Summany tab. du	ring aluator areatic	n or Add Nodo	with the			
varning banner nas	been added in the s	summary tao du. viteb eide	ring cluster creatic	on, or Add Node,	with the			
culated IVITO values	to be set on the sw	nich side.						
	shown before the s	vetom procoods	to create the clus	ter or add a node	a. If there is a			
ie warning ie alwave	Shown before the 3	"bint" to the user	that the issue mic	aht he with the C(Cl interface			
is warning is always de join failure the m	essage provides a "	mint to the user	that the issue mig					

CCL Ping Test in Cluster Live Status

Check CCL Connectivity

• Need for user provision to verify the CCL connectivity with CCL MTU packet size

Solution

luster Status				0	
Dverall Status: 🗃 Clus Nodes details (3)	tering is disabled for 1 node(s)	Refresh	Reconcile All Q Enter	node name	
Status V In Sync.	Device Name 10.10.43.21 Control	Unit Name 10.10.43.21	Chassis URL	1	Navigate to Cluster Live Status
Summary Histor	y OCL Ping				->
ping 10.10.3.2 size 1 Sending 5, 1654-byte 77777	654 e ICMP Echos to 10.10.3.2, timeout is	2 seconds:			CCL Ping option -> Executes
-tes to to a state is o per	cent (0/5)				ping
Clustering is disable	led 10.10.43.22	10.10.43.22	NA	E	command on all devices.
.ted: 18:38:41 01 Ma	r 2023			Close	

Added CCL MTU Sizes for Public Cloud

AWS and Azure Cluster MTU Values

There are new recommended CCL and data interface MTU values for 7.4 public cloud FTDv clusters.

	Recommended CCL MTU in 7.3	Recommended CCL MTU in 7.4	Recommended Data interface MTU in 7.3	Recommended Data interface MTU in 7.4
Azure NLB cluster	1554	1454	1400	1300
Azure GWLB cluster	1554	1454	1454	1374
AWS GWLB cluster	1960	1980	1806	1826

FMC updates the CCL and data interface MTU to recommended values after upgrade of a cluster to 7.4 version.

CLIs Available in FMC

Device Lina CLI Prompt Available in Device/Cluster Tab

Run Cluster Lina CLIs from FMC

• It is now possible to execute cluster LINA troubleshoot CLIs from FMC.

Image: Security Light Image: Security Light Lienter PTD-00 A CLI Rank: Security Light Security Light Security Light PTD-00 Buttom is newly added in the General Security Intersection Security Intersection Security Physics Security Light Secur	Firewall Ma Control (Sector Cluster/VFTD Close Report Times	nagement Center Downlaw Cheve Institute Defense for Viteore Route Defense for Viteore	Analysis Policies De	adoss Objects	Inegation		Deploy 0, 🌮 O D when Y 🏦 SECURE	
Rame @ duter/ID Pateraroo Tir: FTDo0 DUttion Is newly Tareb Press: No Exores: N1 added in the Server: 0 Exores: N1 added in the General Exore: No General Cheer Lie float: No Section Source Creek Annee: NA Section Source Creek Na Device Source Creek Tabbs Tabbs		General		/		License	/	A CLI
Twent Pacitizi No Borrows No No added in the Searce 0 Development No added in the General No Searce No General General No Searce No Searce General No Searce No Searce General No Searce No Searce Toteleners No Searce No Searce Toteleners No Searce Searce No Searce Tree Assess No Searce Searce On both the Searce Tree Assess No Searce Device Searce Tree Searce No No Device Searce Searce No Tabbs Tabbs		Name: 0		clusterV/10		Parlormance Tier :	FTDv60	button is newly
Sank Image: Sank Deprive Detroised Free/min Yes Addred In the General Maren befree Maren befree Maren befree Maren befree General Maren befree Maren befree Maren befree Maren befree Touser Jack with Carlier Maren befree Maren befree Maren befree Touser Jack with Carlier Maren befree Maren befree Maren befree Touser Jack with Carlier Maren befree Maren befree Maren befree Security Engine Baser 3.0 Maren befree Cluster and Reader Jack with Carlier Maren befree Devicee Interview Stater Baser 3.0 Maren befree Tabbs		Tranafus Paciata:		No		Essentials	Y0.5	a shaha ah ta sha a
Guessi National basis National basis National basis National basis National basis National basis General Triveservoir View Dimensional basis National basis National basis Security and the security for the security		Status		۰		Export-Controlled Feellures:	Yos	added in the
Charactive fistorie Yes Yes Yes General TrideWorkWC: Weillingtone Base Base Security Lingtone Security Lingtone System N/A Security Lingtone Security Lingtone System N/A Cluster and Device Image: Security Lingtone System New Cluster and Device Image: Security Lingtone Based State New Device		Certrol		10.10.43.21		Malwore Defense	No	2 /
Notestative Definition Definition Source Over Parket No. Security Control Con		Clubar Uve Status		Wares.		P5.	Yes	General
Lite: No Section Source Creater NA Section Source Creater Annualization Source Creater Annualizatio Source Creater Annualization Source Creater Annualization Sou		Troublashoot	Logo [CLE Drumbook		Center:	No	
Security Engine Bourd Start June 2000 Cited Juni City 2000 Cited Juni Ci						URL:	No	section
Security Engine Bourd 2014 UNI One State Device UNI						Source Creek Prieman	104	
Security Engine System Cluster and Cluster and Device Health Tables Pour Pour Pour Pour Pour Pour Pour Pour						Solure Cleve, VIN Owx	104	on both the
Security Legine System Cluster and Cluster and Device A								Olyatar and
None Device Devi		Security Engine				System		Cluster and
(new back proce Tabs		Intrusion Presention Engine:		Sepri 3.0		Policy	fare	Daviaa
Health Tabs		Terret to Sect 2						Device
						Health	mail Presity (Policy	Tabs

Commonly Used CLIs Shown by Default

CLI Troubleshoot × >Command: → Execute >Command: → Execute > show remainsg-coofig cluster cluster group clusterVTD local-unit 10:10.43.21 > > show remainsg-coofig cluster cluster group clusterVTD local-unit 10:10.43.21 > > show remainsg-coofig cluster cluster group clustervite clustervit > <	 Executes a set of predefined CLIs for cluster troubleshooting on the device that is selected in the Device selection dropdown.
<pre>> show cluster info Cluster of UniterVPD: CD Interfore mode: individual Cluster Member Link: 16 This is '10.10.43:21' in state CONTROL_NOODE 10</pre>	 The refresh button re-runs the commands. Copy button can be used to copy the CLI output

Predefined Cluster CLIs

• The CLIs which are run by default are:

show running-config cluster

show cluster info

show cluster info health

show cluster info transport cp

show version

show asp drop

show counters

show arp
show int ip brief
show blocks
show cpu detailed
show interface <ccl_interface>
ping <ccl_ip> size <ccl_mtu> repeat 2

Manual Entry of Commands Available



Generation of Troubleshoots

Automatic Troubleshoot Generation on Node Join Failure

- When a node fails to join the cluster, a device Troubleshoot is automatically generated.
- A notification is shown in Task Manager.

Concord of Image: I	Firewall Management Center Own-Vev Andreas View By Grasp • • All(0) Emer (2) • Warning (1) • Offices (0) • Named (2)	Policies Devices Deployment Pending (0)	Objects Upgret	Integration de (0) Snort 3 (6)	Deploy Q Q admin v ddd SECURE Deployments Liggrades @Hoath @Tools & (Show Notifications (Admin downing downi	Ta sl	ask manager hows
• 10.18.43.27 box 3 10.10.43.27 box 3 • 0.40.43.3V[Correl] bind • 0.10.43.27 box 3 • 0.10.43.3V[Correl] bind • 0.10.43.27 box 3 • 0.10.43.3V[Correl] bind • 0.10.43.27 box 3 • 0.10.43.27 box	Collector All Name variation	Hadal	Version	Diseals	Contract Touchendrating Files Generative translater housing Files Generative translater housing files for 10.10.43.25 Formats amounts Dereveling traditional files Outsite Goster Indicater - Colorer configuration for all or color soft 10.10.43.25, berit fielded to denote Males serve the color configuration and an orthogenetic field and and an orthogenetic field and and and and and and and and and an	•	Cluster node join failure That a
Image: Note of the Stable St	Childram Constant Constan	FTD v for VMissore	7.4.0	NUA	Pridry Diployeese Policy Diployeese Policy Diployeese Policy Diployeese Counter Counter	1.	Troubleshoo
	10.10.43.21(Control Section 3 10.10.43.22(1) - fixe.101 10.10.43.22 - fixe.101 10.10.43.22 - fixe.10	PTD+ for VMwere	7.4.0	NIA NIA	10.10.01.34 k now the consult roads in cluster tradicator: 405 × .		t nas been generated.

Troubleshoot Trigger and Download Button Available in Device and Cluster Tabs

Easier Generation of Cluster Troubleshoots

Cluster Devi	e Routing Interfaces Inline Sets DHCP VTEP	
 A "Logs" button has been added to the cluster device page and to the main cluster page. 	General	
 The button opens a Generate Troubleshoot Files dialog. 	Transfer Packets: Yes Status:	
 Once the Troubleshoot generation has completed, a new "Download" button allows for downloading the Troubleshoot(s). 	Control: 10.10.43.21 Cluster Live Status: View Troubleshoot:	

Cluster Troubleshoot Generation

Outrie Triad Datase Triad based Outrie Triad Datase Triad based Outrie Triad Datase Triad Datase Outrie Triad Datase	10.10.43.21	Concern readons routes 1996.8 Solition Hilly 1997	Learning the Grant Solution	Generate Troubleshoot Files - clusterVFTD ×
available devices in the cluster	Close Response Thread Derivers for Vikiaan Cluster Derive Reacting Interfaces General Name © Tandon Record Cluster Law Stand Cluster Law Stand Taubitsmoot Security Engine Encares Preventes tog Security Engine	rine Sec P V19 	When generated from the Cluster Tab, note that the Generate Troubleshoot Files dialog gives the cluster name to show Troubleshoots will be generated for all nodes. The user can pick All Devices or a single device from the Devices dropdown in the dialog. The dropdown lists all available devices in the cluster	 This operation may take several minutes to complete, the status can be tracked in Message Center Tasks. Devices All Devices All Data Snort Performance and Configuration Hardware Performance and Logs System Configuration, Policy, and Logs Interface and Network Related Data Detection Configuration, Policy, and Logs Interface and Network Related Data Discovery, Anvenees, VDB Data, and Logs All Database Data All Database Data All Database Data Network Map Information Deployment Logs Cluster Logs

Node (Device) Troubleshoot Generation

Firewall Management Center Overview Analysis Device I Secure Howar Device Summary	Policies Devices Objects	integration		Deploy 🔍 🌮 O 🕢 Hamma 🗸 💷 Secure		
ClusterVFTD Cisio Ropewar Thrust Distriction for VMHvaen Diator Division Rocking Incentrations Inlike Sets DHCP VTD					•	Click on the new
				10.10.43.21 +		Logs button to
General X±3	System	0 G	Health			trianan a daviaa
Name: 10.10.43.21	Model	Cisco Firepower Threat Defense for Valuese	Status	•		trigger a device
Mode: Boulad	Serial	\$7M0P680P23	Policy:	Intol_Hoults_Policy 2023-02-08 17:07543		
Camplance Made: None	TIM	2028-08-02 12:47:99	Exclusion	N 890	-	troubleshoot
TLS Crypto Acceleration: Disabled	Time Zenet	UTC (UTC+0.00)				00000000000
Device Sonlywater:	Version: Time Zane setting for Time based Rules:	7.4.0 UTC AUTC+ATRA			•	Once completed,
Management	Inventory Details	¢				the Troubleshoot is
Remote Host Address: 10.10.40.21	CPU Tepe	CPU Xeon E5 series 2100 MHz				
Secondary Address:	CPU Cores:	1 GPU (4 conta)				available for
Striker 0	Namory:	8152 MB FAM				avallable 101
	Storage	N/A.				
	Chaosis URL:	N/M.				aownioaa using the
	Chassis Seriel Number	N/A.				
	Chaosis Madule Number	N/A.				Download button

Notification of Cluster Troubleshoot Generation Complete

The Task manager shows the progress of the troubleshoot generation for each node in the cluster. Wait for that before clicking **Download**.

Deploy Q 🔮 🌣 🔞	admin ~ divide SECURE
Deployments Upgrades Health Tasks	Show Notifications
20+ total 0 waiting 1 running 0 retrying 20+ success 6 failures	२ Filter
 Generate Troubleshooting Files Create bundle tar troubleshooting files for cluster with name testCluster Click to retrieve generated bundle tar file. 	<u>5s</u> ×
 Generate Troubleshooting Files Generate troubleshooting files for 10.10.43.23 Click to retrieve generated files. 	6m 8s 🗙
 Generate Troubleshooting Files Generate troubleshooting files for 10.10.43.21 Click to retrieve generated files. 	$_{\rm 6m~4s}$ $ imes$
 Generate Troubleshooting Files Generate troubleshooting files for 10.10.43.23 Click to retrieve generated files. 	6m 27s 🗙

Q & A

Q: In Azure it reduced but increased in AWS for MTU?

A: For the new MTU values in public clouds, in Azure the recommended MTU is reduced, but it is

increased in AWS.

Q: During Upgrade if MTU is changed automatically - is there a Syslog entry?

A: No, there is no Syslog entry made at this time. We can relook at it if this is needed.

Q: Where is the MTU value of each node shown?

A: Show the MTU value as a column on the device management > interfaces page, on the cluster tab.

Q: Is this failure showing because Switch is not set, or the other node is not set?

A: No, it is a warning message as precaution which is displayed all the time to user.

Q: Which command - show cluster - shows the MTU size?

A: CCL ping is in the default and shows in the CLI defaults.

Q: In case of AWS, can we document the steps on how to increase the MTU on switch?

A: For tech pubs to check.

Q: For HW - you only listed 3100 series -what about 4K/9K/2K/1K?

A: Clustering on 9300, 4100, 3100 and virtual only. 3100 can be done from FMC, but 4100 and 9300 clusters are done in the chassis manager, not FMC.

Q: Do you have to deploy from the FMC for the changes to take effect, post-device upgrade?

A: Yes, need to deploy after upgrade. You must use the recommended MTU values.

Q: Are we providing any warning message to user that MTU is changed, as if FTD is middle of path where GRE tunnel build, would user see the tunnel flapping or went down?

A: It is in the documentation. Can work on warning message. Nodes would adjust to control node. Switch would have to be adjusted to the new values. Value is changed after control node is upgraded. MTU value is sent by control.

Q: Are we going to reboot the FTD device if post upgrade we are changing the MTU?

A: No explicit reboot is triggered on FTD on upgrade when MTU values are changed.

Revision History

Revision	Publish Date	Comments
2.0	17-Jul-2024	Added Alt Text. Updated Formatting.
1.0	17-Jul-2024	Initial Release