Aggiorna FTD HA gestito da FDM

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Panoramica
Premesse
Configurazione
Passaggio 1. Caricare il pacchetto di aggiornamento
Passaggio 2. Verifica della fattibilità
Passaggio 3. Aggiornare FTD in HA
Passaggio 4. Cambiare il peer attivo (facoltativo)
Passaggio 5. Distribuzione finale
Convalida

Introduzione

In questo documento viene descritto il processo di aggiornamento di Cisco Secure Firewall Threat Defense in High Availability gestito da un gestore dispositivi Firepower.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Concetti e configurazione dell'alta disponibilità (HA, High Availability)
- Configurazione di Cisco Secure Firepower Device Manager (FDM)
- Configurazione Cisco Secure Firewall Threat Defense (FTD)

Componenti usati

Il riferimento delle informazioni contenute in questo documento è il Virtual Cisco FTD versione 7.2.8.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica

Il funzionamento di FDM prevede l'aggiornamento di un peer alla volta. Prima lo standby, quindi lo stato Attivo, che esegue un failover prima dell'avvio dell'aggiornamento Attivo.

Premesse

Prima di eseguire l'aggiornamento, il pacchetto di aggiornamento deve essere scaricato dal sito software.cisco.com.

Al termine della CLI, eseguire il comando show high-availability configcommand nell'FTD attivo per controllare lo stato dell'HA.

> show high-availability config Failover On Failover unit Primary Failover LAN Interface: failover-link GigabitEthernet0/2 (up) Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 3 of 311 maximum MAC Address Move Notification Interval not set failover replication http Version: Ours 9.18(3)53, Mate 9.18(3)53 Serial Number: Ours 9A10UNFWPK1. Mate 9A45VNEHB5C Last Failover at: 11:57:26 UTC Oct 8 2024 This host: Primary - Active Active time: 507441 (sec) slot 0: ASAv hw/sw rev (/9.18(3)53) status (Up Sys) Interface diagnostic (0.0.0.0): Normal (Waiting) Interface inside (192.168.45.1): Normal (Waiting) Interface outside (192.168.1.10): Normal (Waiting) slot 1: snort rev (1.0) status (up) slot 2: diskstatus rev (1.0) status (up)

```
Other host: Secondary - Standby Ready
Active time: 8 (sec)
Interface diagnostic (0.0.0.0): Normal (Waiting)
Interface inside (0.0.0.0): Normal (Waiting)
Interface outside (0.0.0.0): Normal (Waiting)
slot 1: snort rev (1.0) status (up)
slot 2: diskstatus rev (1.0) status (up)
```

Se non sono visibili errori, procedere con l'aggiornamento.

Configurazione

Passaggio 1. Caricare il pacchetto di aggiornamento

• Caricare il pacchetto di aggiornamento FTD su FDM utilizzando la GUI.

Questa versione deve essere scaricata in precedenza dal sito del software Cisco in base al modello FTD e alla versione desiderata. Selezionare Periferica > Aggiornamenti > Aggiornamento sistema.



Aggiornamenti

• Cercare l'immagine scaricata in precedenza, quindi scegliere Carica.



Nota: Caricare l'immagine sui nodi attivi e in standby.

0	Important
	This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see link ⊘
77	
Ine	re are no software upgrades available on the system.

Esegui verifica preparazione

Passaggio 2. Verifica della fattibilità

I controlli di idoneità confermano che gli accessori sono pronti per l'aggiornamento.

• Scegliere Esegui verifica preparazione aggiornamento.

System Upgrade Current version 7.2.5-3	208			
i Important This device is a p precise order. Fo	eer in a high availability configuration. You must install upgrades in a r details, see link 🖸			
File Cisco_FTD_Upgrade-7.2.8-25.sh.REL Replace file 14 Oct 2024 05:06 PM				
Upgrade to	7.2.8-25			
Readiness Check	Not Performed Yet Run Upgrade Readiness Check			
UPGRADE NOW	Reboot required			

Important	
This device is a precise order. F	peer in a high availability configuration. You must install upgrades in a or details, see link 🖸
File	Cisco_FTD_Upgrade-7.2.8-25.sh.REL a Replace file
Upgrade to	7.2.8-25
Readiness Check	Not Performed Yet Run. Upgrade. Readiness Check

Esegui verifica preparazione

 Important This device is a peer in a high availability configuration. You must install upgrades in a precise order. For details, see link 					
File	Cisco_FTD_Upgrade-7.2.8-25.sh.REL The second s				
Upgrade to	7.2.8-25				
Readiness Check	ululu Please Wait				
UPGRADE NOW	i Reboot required				

Esegui verifica preparazione

Per controllare lo stato di avanzamento, selezionare Sistema > Aggiorna.

Precheck Success Run Upgrade Readiness Check
7.2.8-25
Cisco_FTD_Upgrade-7.2.8-25.sh.REL a Replace file
peer in a high availability configuration. You must install upgrades in a or details, see link 🗷

Esegui verifica preparazione

L'aggiornamento può essere eseguito quando il controllo di fattibilità viene completato sia in FTD che in caso di esito positivo.

Passaggio 3. Aggiornare FTD in HA

• Scegliere Standby FDM e fare clic su Aggiorna ora.

Important This device is a precise order. F	peer in a high availability co or details, see link C	onfiguration. You must install upgrades in a
File	Cisco_FTD_Upgrade-7 14 Oct 2024 05:06 PM	2.2.8-25.sh.REL 💼 Replace file
Upgrade to	7.2.8-25	
Readiness Check	Precheck Success 14 Oct 2024 05:51 PM	Run Upgrade Readiness Check
UPGRADE NOW	Reboot required	

Aggiorna

Prima di avviare l'aggiornamento:

- 1. Non avviare un ripristino di sistema contemporaneamente a un aggiornamento del sistema.
- 2. Non riavviare il sistema durante l'aggiornamento. Se necessario, il sistema si riavvia automaticamente al momento opportuno durante l'aggiornamento.
- 3. Non spegnere la periferica durante l'aggiornamento. L'interruzione dell'aggiornamento può rendere inutilizzabile il sistema.

Al momento dell'avvio dell'aggiornamento si è disconnessi dal sistema. Al termine dell'installazione, il dispositivo viene riavviato.

Confirm System Upgrade					
 Before starting the upgrade: 1. Do not start a system restore at the same time as a system upgrade. 2. Do not reboot the system during the upgrade. The system automatically reboots at the appropriate time during upgrade if a reboot is necessary. 3. Do not power off the device during the upgrade. Interrupting the upgrade can leave the system in an unusable state. You will be logged out of the system when the upgrade begins. After the installation completes, the device will be rebooted. UPGRADE OPTIONS Automatically cancel on upgrade failure and roll back to the previous version 					
CANCEL					

Continua



Nota: L'aggiornamento richiede circa 20 minuti per FTD.

Dalla CLI, lo stato può essere verificato nella cartella di aggiornamento /ngfw/var/log/sf; passare alla modalità expert e all'accesso alla directory principale dell'azienda.

> expert admin@firepower:~\$ sudo su

Password:

root@firepower:/home/admin# cd /ngfw/var/log/sf

root@firepower:/ngfw/var/log/sf# ls

Cisco_FTD_Upgrade-7.2.8.

root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.8# ls -lrt

root@firepower:/ngfw/var/log/sf/Cisco_FTD_Upgrade-7.2.8# tail -f status.log

ui: Upgrade in progress: (8% done.22 mins to reboot). Preparing to upgrade... (200_pre/011_check_self. ui: Upgrade in progress: (8% done.22 mins to reboot). Preparing to upgrade... (200_pre/015_verify_rpm. ui: Upgrade in progress: (8% done.22 mins to reboot). Preparing to upgrade... (200_pre/100_check_dashb ui: Upgrade in progress: (8% done.22 mins to reboot). Preparing to upgrade... (200_pre/100_get_snort_f ui: Upgrade in progress: (12% done.21 mins to reboot). Preparing to upgrade... (200_pre/110_setup_upgra ui: Upgrade in progress: (12% done.21 mins to reboot). Preparing to upgrade... (200_pre/120_generate_au ui: Upgrade in progress: (12% done.21 mins to reboot). Preparing to upgrade... (200_pre/120_generate_au

ui: Upgrade in progress: (79% done. 5 mins to reboot). Finishing the upgrade... (999_finish/999_zz_inst ui: Upgrade in progress: (83% done. 4 mins to reboot). Finishing the upgrade... (999_finish/999_zzz_com ui: Upgrade complete

ui: The system will now reboot.

ui: System will now reboot.

Broadcast message from root@firepower (Mon Oct 14 12:01:26 2024): System will reboot in 5 seconds due to system upgrade.

Broadcast message from root@firepower (Mon Oct 14 12:01:31 2024): System will reboot now due to system upgrade.

Broadcast message from root@firepower (Mon Oct 14 12:01:39 2024): The system is going down for reboot NOW! Aggiornare la seconda unità.

Cambia ruoli per rendere attivo il dispositivo: Scegliete Periferica> Alta disponibilità, quindi Cambia modalità dal menu Ingranaggi. Attendere lo stato dell'unità per passare allo stato attivo e verificare che il traffico scorra normalmente. Quindi, disconnettersi.

Aggiornamento: Ripetere i passaggi precedenti per accedere al nuovo standby, caricare il pacchetto, aggiornare il dispositivo, monitorare lo stato e verificare il successo.



Alta disponibilità

Dalla CLI, passare a LINA (system support diagnostic-cli) e controllare lo stato di failover sull'FTD in standby utilizzando il comando show failover state.

> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

primary_ha> enable

Password:

primary_ha# show failover state

State Last Failure Reason Date/Time

This host - Primary

Standby Ready None Other host - Secondary Active None

====Configuration State===

Sync Skipped - STANDBY

====Communication State===

Mac set

primary_ha#

Passaggio 4. Cambiare il peer attivo (facoltativo)



Nota: Se il dispositivo secondario è attivo, non ha alcun impatto operativo.

L'attivazione del dispositivo primario e la messa in standby del dispositivo secondario è una procedura ottimale che consente di tenere traccia di eventuali failover.

In questo caso, l'FTD attivo è ora Standby e può essere utilizzato un failover manuale per reimpostarlo su Attivo.

• Selezionare Dispositivi > Alta disponibilità.

Φ	Firewall Device Mana	ger Monitorin	9 Policies	前回 Objects	Device: firepower	(0 🚑	۲	?	admin Administ	ator ~	cuce SECURE
	Mod Cise	ol o Firepower Threat I	efense for VMwa	Software 7.2.8-25	VD8 Intrusion Rule Update 353.0 20220511-1540	Cloud Services Not Register	red Registe	Prim	Availability sary Device	Blandby 2	Peer: Active	
										Ξ.		
				Cisco Firepowe	er Threat Defense for VMware 🕲	MONT				NS Server		
		6	side Network				ISP/WAN	Kateway	© **	TP Server		
					609							

Alta disponibilità

Scegliere Cambia modalità.

Firewall Device Manager Monitoring Policies Objects Device: firepower	(5.) 🚑 🎯 🕐 🗄 admin Administrator	· dealer SECURE
Device Summary High Availability		
Primary Device Current Device Mode: Standby 2 Peer: Active Failover History Deployment History		Resume HA
High Availability Configuration	Fallover Criteria	Suspend HA Break HA
Select and configure the peer device based on the following characteristics.	Failure Oriteria	- Switch Mode
GENERAL DEVICE INFORMATION	Number of failed interfaces exceeds	1
Model Cisco Firepower Threat Defense for VMware		1411

Cambia modalità

• Per confermare il failover, scegliere OK.

Make This Device the Active Peer 🛛 😨						
Please check whether the active unit is currently switch modes while a deployment job is in progre lose your configuration changes. Are you sure you want to switch modes to make t	running a deployme ess, the job will fail his device the activ	ent job. If you and you will ve unit?				
	CANCEL	ОК				

Convalida dello stato HA al termine dell'aggiornamento e del failover eseguiti.

Firewall Device Manager Monitoring Policies	Device: firepower	🕗 🚑 🞯 🕐 🗄 admin Administrator 🗸 🐝 SECURE
Model Cisco Firepower Threat Defense for VMwa	Software VDB Intrusion Rule Update 7.2.8-25 353.0 20220511-1540	Cloud Services High Availability © Not Registered Register Primary Device: Active 2 Peer: Standby
	Cisco Firepower Thread Defense for Wilware	Enternet
C Inside Network		Shystaal Sateway
	80	

Dispositivi

Passaggio 5. Distribuzione finale

• Distribuire il criterio ai dispositivi facendo clic su DISTRIBUISCI ADESSO nella scheda Distribuzione.



Pend	ina	Char	naes
1 0110		e num	.900

0	\times
•	\sim

	Last Deployment Completed Successfully 14 Oct 2024 06:26 PM. See Deployment History		
	Deployed Version (14 Oct 2024 06:26 PM)	Pending Version	EGEND
Ø	Rule Update Version Edited: 20220511-1540		
	lastSuccessSRUDate: 2024-10-08 06:15:04Z -	2024-10-14 12:53:26Z lspVersions[1]: 20220511-1540	
Ø	VDB Version Edited: 353		
0	Snort Version Added: 3.1.21.800-2		- 1
	-	snortVersion: 3.1.21.800-2	
	-	<pre>snortPackage: /ngfw/var/sf/snort-3.1.21.800-2/snor name: 3.1.21.800-2</pre>	
			_
0	Data SSL Cipher Setting Edited: DefaultDataSSLCipherSetting		
Ø	SSL Cipher Edited: DefaultSSLCipher		
	-	<pre>protocolVersions[0]: TLSV1</pre>	
	-	protocolVersions[1]: DTLSV1 protocolVersions[2]: TLSV1 1	
0	Intrusion Policy Edited: Security Over Connectivity - Cisco Talos		
0	Intrusion Policy Edited: Maximum Detection - Cisco Talos		
М	IORE ACTIONS V	CANCEL DEPLOY NOW	~

Distribuzione criteri

Convalida

Per verificare che lo stato HA e l'aggiornamento siano stati completati, è necessario confermare lo stato:

Primario: Active Secondario: Pronto per lo standby

Entrambi si trovano nella versione modificata di recente (7.2.8 in questo esempio).

Firewall Device Manager Monitoring Policies	Device: firepower	(administrator
Model Cisco Prepower Threat Defense for VMws	Software VDB Intrusion Rule Update 7.2.8-25 353.0 20220511-1540	Cloud Services O Not Registered Register Primary Device: Active
	Cisco Firepower Threat Defense for Vidware	E Child Server
C Inside Network		CONTRACTOR

Failover

• Al di sopra della CLI, controllare lo stato del failover utilizzando i comandi show failover status e show failover per informazioni più dettagliate.

Cisco Firepower Extensible Operating System (FX-OS) v2.12.1 (build 73) Cisco Firepower Threat Defense per VMware v7.2.8 (build 25)

> show failover state				
	State	Last Failure Reason	Date/Time	
This host -	Primary			
	Active	None		
Other host -	Secondary			
	Standby Ready	None		
====Configurat	ion State===			
Sync S	kipped			
====Communicat	ion State===			
Mac se	t			
> show failove	r			
Failover On				
Failover unit Primary				
Failover LAN Interface: failover-link GigabitEthernet0/2 (up)				

Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 3 of 311 maximum MAC Address Move Notification Interval not set failover replication http Version: Ours 9.18(4)210, Mate 9.18(4)210 Serial Number: Ours 9A1QUNFWPK1, Mate 9A45VNEHB5C Last Failover at: 14:13:56 UTC Oct 15 2024 This host: Primary - Active Active time: 580 (sec) slot 0: ASAv hw/sw rev (/9.18(4)210) status (Up Sys) Interface diagnostic (0.0.0.0): Normal (Waiting) Interface inside (192.168.45.1): Normal (Waiting) Interface outside (192.168.1.10): Normal (Waiting) slot 1: snort rev (1.0) status (up) slot 2: diskstatus rev (1.0) status (up) Other host: Secondary - Standby Ready Active time: 91512 (sec) Interface diagnostic (0.0.0.0): Normal (Waiting) Interface inside (0.0.0.0): Normal (Waiting) Interface outside (0.0.0.0): Normal (Waiting) slot 1: snort rev (1.0) status (up) slot 2: diskstatus rev (1.0) status (up)

Stateful Failover Logical Update Statistics

Link : failover-link GigabitEthernet0/2 (up)				
Stateful Obj	xmit	xerr	rcv	rerr
General	11797	0	76877	0

sys cmd	11574	0	11484	0
up time	0	0	0	0
RPC services	0	0	0	0
TCP conn	0	0	0	0
UDP conn	176	0	60506	0
ARP tbl	45	0	4561	0
Xlate_Timeout	0	0	0	0
IPv6 ND tbl	0	0	0	0
VPN IKEv1 SA	0	0	0	0
VPN IKEv1 P2	0	0	0	0
VPN IKEv2 SA	0	0	0	0
VPN IKEv2 P2	0	0	0	0
VPN CTCP upd	0	0	0	0
VPN SDI upd	0	0	0	0
VPN DHCP upd	0	0	0	0
SIP Session	0	0	0	0
SIP Tx 0	0	0	0	
SIP Pinhole	0	0	0	0
Route Session	1	0	0	0
Router ID	0	0	0	0
User-Identity	0	0	30	0
CTS SGTNAME	0	0	0	0
CTS PAC	0	0	0	0
TrustSec-SXP	0	0	0	0
IPv6 Route	0	0	0	0
STS Table	0	0	0	0
Umbrella Device	-ID 0	0	0	
Rule DB B-Sync	0	0	30	0
Rule DB P-Sync	1	0	266	0
Rule DB Delete	0	0	0	0

Logical Update Queue Information

	Cur	Max	Total
Recv Q:	0	31	123591
Xmit Q:	0	1	12100

Se entrambi gli FTD si trovano nella stessa versione e lo stato HA è integro, l'aggiornamento è completato.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).