

FTD ل لش فلل زواجت ةلح لئاسر مهف

تاوت حمل

[ةمدقم](#)

[ةيساس الابل طت مل](#)

[تابل طت مل](#)

[ةمدخت سمل تانوك مل](#)

[ةيساس ا تامول عم](#)

[لش فلل زواجت ةلح لئاسر](#)

[لش فلل زواجت نود تاناي بلابل طت را دادس نا - مادخت س ال ةلح](#)

[ةمجاو ال ةي امح لش ف - ةلح ال مادخت س](#)

[صق بلبل يل ال مادخت س ال - مادخت س ال ةلح](#)

[Lina traceback - مادخت س ال ةلح](#)

[ل فس ال Snort لي ثم - ةلح ال مادخت س](#)

[ةق اطل ال و ةزه ال لش ف - مادخت س ال ةلح](#)

[\(ةزه ال\) MIO حل عمل بلق بل تاق دل لش ف - مادخت س ال ةلح](#)

[ةلص تا ذ تامول عم](#)

ةمدقم

ديدهت دض ةنم ال ةي امح ال يلع لش فلل زواجت ةلح لئاسر مهف ةي فيك دنت سمل اذه حضوي (FTD) ةي امح ال راجد.

ةيساس الابل طت مل

تابل طت مل

ةيل ال عيضاوم لابل ةفر عم كي دل نوك ت ناب Cisco ي صوت:

- Cisco Secure FTD ل (HA) يل ال رفوت ال دادع |
- Cisco نم (FMC) ةي امح ال راجد ةراد | زك رمل يساس ال مادخت س ال

ةمدخت سمل تانوك مل

ةيل ال ةي دام ال تانوك مل او جمار بل تارادصا ال دنت سمل اذه يف ةدراول تامول عم ال دنت ست:

- Cisco FMC v7.2.5
- Cisco Firepower 9300 Series v7.2.5

ةصاخ ةي لم عم ةئي ب يف ةدوجوم ال ةزه ال نم دنت سمل اذه يف ةدراول تامول عم ال عاشن ا مت تناك اذ | (يضا رت ف ا) حوس مم نيوك ت ب دنت سمل اذه يف ةمدخت سمل ةزه ال عي مج ت ادب رم ا ال لم تحت مل ري ثا تلل كم هف نم دك ات ف ، لي غش ت ال دي ق ك تك ب ش

سياسات اول عم

لإطلاع ألى على بلغتلل عمالسل عبقارم لىل عماع قرطن:

لإسزالل جم انرب لرىل. ةهأولل عمالسل و عمالل ءحصلل نامضل ءءو لك عبقارم ب FTD زاهل موقى ءءوولل عمالسل عبقارم لىل اءانلسا ءءو لك ءلاح ءىءءل ءارابءءل (FTD) ءعرسلل قىللف زواءء ءاءءل ءءءء HA، ءوز لىل ءءو لك ءلاح ءىءءل رابءءل لىل فى امءن عو. ةهأولل عبقارم و لىل فلل.

للىل زواءء ءلاح لىللسرر

للىل زواءء نوء ءانايبلل طابءلرل ءاءسلنا - ماءءءسلل ءلاح

مءى ال، ءانايبلل طابءلرل لىل ءلاح لىل فو FTD HA لىل ءهأولل عبقارم نىل كمء مءى ال امءن ع ءاهأولل عمالسل عبقارم ءارابءءل ءارءل مءعل ارطن لىل لىل زواءء ءءل لىل ءلءل.

للىل ءلءل ءانايبلل طابءلرل لىل ءلءل ءهأولل ءرولل هءه ءلءل لىل لىل زواءء ءهأولل لىل.

The screenshot displays the Cisco Secure Manager interface. At the top, there are navigation tabs: Analysis, Policies, Devices (selected), Objects, and Integration. On the right, there are icons for Deploy, Search, Settings, and a user profile for 'admin'. Below the navigation, there is a summary bar showing 'Normal (2)', 'Deployment Pending (1)', and 'Upgrade (0)'. A notification box is overlaid on the right side, titled 'Dismiss all notifications', with a red 'X' icon and the text: 'Interface Status - 10.82.141.171', 'Interface 'Ethernet1/3' is not receiving any packets', and 'Interface 'Ethernet1/3' has no link'. Below the notification, there is a table with columns: Model, Version, Chassis, Licenses, Access Control Policy, and Auto RollBack. The table contains two rows of device information, both for 'Firepower 9300 with FTD' with version '7.2.5'. The first row has chassis 'F241-24-04-FPR9K-1.cisco.com:4' and license 'Security Module - 1'. The second row has chassis 'F241-F241-24-4-FPR9K-2.cisco.c' and license 'Security Module - 1'. Both rows have 'Essentials, IPS (2 more...)' under Licenses and 'FTD HA' under Access Control Policy. There are also icons for 'Auto RollBack' and a vertical ellipsis menu for each row.

للىل طابءلرل هىلءنء

رملل اءه مءءءسل، اهءلءل و ءانايبلل ءاطابءلرل ءلاح نم ققءءلل

- ءهأوو ءءو لك لىل لىل زواءء ءلاح لىل ءامول عمالل ضرعى - show failover

Monitored Interfaces 1 of 1291 maximum

...

This host: Primary - Active

Active time: 3998 (sec)

slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(3)53) status (Up Sys)

Interface DMZ (192.168.10.1): Normal (Waiting)


```
show failover history
```

```
=====
```

From State	To State	Reason
20:17:11 UTC Sep 26 2023 Active	Standby Ready	Other unit wants me Standby Inspection engine in other unit ha
20:17:11 UTC Sep 26 2023. Active	Standby Ready	Failed Detect Inspection engine fa due to disk failure

```
=====
```

- show failover - دحو لكل لش فال زواجت ةلاح لوح تامول عم لا ضرعي

```
<#root>
```

```
firepower#
```

```
show failover | include host|disk
```

```
This host: Primary - Failed  
slot 2: diskstatus rev (1.0) status (down)  
Other host: Secondary - Active  
slot 2: diskstatus rev (1.0) status (up)
```

- df -h - مخرج ل نمضت يت لا واهل ي محت مت يت لا تافل ملة مظن ان لك لوح تامول عم ضرعي
لي محت لا ةطقنو مادخت سالل ةي وئ ملة بس نلا وة مدخت سملا ةحاس م لا ويلي امجال

```
<#root>
```

```
admin@firepower:/ngfw/Volume/home$
```

```
df -h /ngfw
```

```
Filesystem Size Used Avail Use% Mounted on  
/dev/sda6 191G 186G 4.8G 98% /ngfw
```

Lina traceback - مادخت سالل ةلاح

لش فال زواجت ثدح لي غشت نكمي، traceback طاب ترا ةلاح ي

Lina traceback ةلاح ي فاه وشن ان مت يت لا تاهي بنت لا ةروصل هذه فرصت

Analysis Policies **Devices** Objects Integration Deploy 🔍 ⚙️ 👤 admin | SECURE

Normal (2) ● Deployment Pending (0) ● Upgrade (0)

Model	Version	Chassis	Licenses	Access Control
Firepower 9300 with FTD	7.2.5	F241-24-04-FPR9K-1.cisco.com:443 Security Module - 1	Essentials, IPS (2 more...)	FTD HA
Firepower 9300 with FTD	7.2.5	F241-F241-24-4-FPR9K-2.cisco.com:443 Security Module - 1	Essentials, IPS (2 more...)	FTD HA

Dismiss all notifications

- ⚠️ **Cluster/Failover Status - 10.82.141.171** ✕
PRIMARY (FLM19389LQR)
 FAILOVER_STATE_ACTIVE (HELLO not heard from peer)
- ✖️ **Interface Status - 10.82.141.171** ✕
Interface 'Ethernet1/1' is not receiving any packets
 Interface 'Ethernet1/2' is not receiving any packets
 Interface 'Ethernet1/3' is not receiving any packets
 Interface 'Ethernet1/4' is not receiving any packets
- ✖️ **Appliance Heartbeat - F241.24.04-FMC4600** ✕
Appliance 10.82.141.169 is not sending heartbeats.
- ⚠️ **Process Status - 10.82.141.169** ✕
lina exited 2 time(s).

traceback طخ مادختساب لشفال زواجت

رماً اذه، لشفال بلسال تقود in order to تلمعتسا

- show failover history - تاريخ لشفال زواجت تاظوفحم ضرعت. لشفال زواجت تاظوفحم ضرعت. لشفال زواجت تاظوفحم ضرعت. لشفال زواجت تاظوفحم ضرعت.

<#root>

firepower#

show failover history

```
=====
```

From State	To State	Reason
8:36:02 UTC Sep 27 2023 Standby Ready	Just Active	HELLO not heard from peer (failover link up, no response from peer)
18:36:02 UTC Sep 27 2023 Just Active	Active Drain	HELLO not heard from peer (failover link up, no response from peer)
18:36:02 UTC Sep 27 2023 Active Drain	Active Applying Config	HELLO not heard from peer (failover link up, no response from peer)
18:36:02 UTC Sep 27 2023 Active Applying Config	Active Config Applied	HELLO not heard from peer (failover link up, no response from peer)
18:36:02 UTC Sep 27 2023 Active Config Applied	Active	HELLO not heard from peer (failover link up, no response from peer)

ةيساسأل تاफलما ناكم ددحي نأ رماً اذه مدختسا، lina traceback ةلح يف

<#root>

```
root@firepower:/opt/cisco/csp/applications#
```

```
cd /var/data/cores
```

```
root@firepower:/var/data/cores#
```

```
ls -l
```

```
total 29016
```

```
-rw----- 1 root root 29656250 Sep 27 18:40 core.lina.11.13995.1695839747.gz
```

اهال صإو عاطخأل فاشكتسأ تافل م عي مجت ةدشب نسحتس مل نم ، Lina traceback ةلاحي في ، Cisco TAC ب لاصتال او ، ةيساسأل تافل مل ري دصتو .

ل فسأل Snort لي ثم - ةلاحي مادختسإ

لي غشت متي ، ةطشنل ةدحول ل ع لس فننل زاه تال ي ثم نم 50% نم رثكأ ضافخنا ةلاحي في لشل فال زواجت .

ل فطتل لشل ف دن ع اهؤاشنإ م تي تال تاهي بننل ةروصل هذه فصت

The screenshot shows the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'Devices' tab is active. Below the navigation bar, there are several status indicators: 'Normal (0)', 'Deployment Pending (0)', 'Upgrade (0)', and 'Snort 3 (2)'. A table lists the devices, with columns for 'Model', 'Version', 'Chassis', 'Licenses', and 'Access Control'. Two devices are listed: 'Firepower 9300 with FTD' with version 7.2.5. A notification window is open on the right, titled 'Dismiss all notifications'. It contains two notifications: 'Cluster/Failover Status - 10.82.141.169' and 'Process Status - 10.82.141.169'. The first notification indicates a failover event where the secondary unit wants to take over. The second notification indicates that the primary detection engine process terminated unexpectedly.

Snort traceback ةمدخ مادختسإ لشل فال زواجت

رمأ اذه تلمعتسا ، لشل فال ب بسال تققد لچأ نم

- show failover history - لشل فال زواجت تاطوفحم ضرع . لشل فال زواجت تاطوفحم ضرع . ةلاحي ري غت لشل فال زواجت تاطوفحم ضرع . ةلاحي ري غت ب بسو لشل فال زواجت ب ةصاخلا ةق ب اسال ةلاحي .

```
<#root>
```

```
firepower#
```

```
show failover history
```

```
=====
```


From State	To State	Reason
21:22:03 UTC Sep 26 2023 Standby Ready	Just Active	Inspection engine in other unit has failed due to snort failure
21:22:03 UTC Sep 26 2023	Just Active	Active Drain Inspection engine in other unit due to snort failure
21:22:03 UTC Sep 26 2023	Active Drain	Active Applying Config Inspection engine in o due to snort failure
21:22:03 UTC Sep 26 2023	Active	Applying Config Active Config Applied Inspect due to snort failure

- show failover - ةدحولل لشفلا زواجت ةلاح لوح تامولعملال ضرعي

<#root>

firepower#

show failover | include host|snort

```
This host: Secondart - Active
slot 1: snort rev (1.0) status (up)
Other host: Primary - Failed
slot 1: snort rev (1.0) status (down)
Firepower-module1#
```

ةيساسالافلملا وأ crashinfo عقوم ديدحتل رماوالا هذه مدختسأ، snort traceback ةلاح يف

<#root>

For snort3:

root@firepower#

cd /ngfw/var/log/crashinfo/

root@firepower:/ngfw/var/log/crashinfo#

ls -l

total 4

```
-rw-r--r-- 1 root root 1052 Sep 27 17:37 snort3-crashinfo.1695836265.851283
```

For snort2:

root@firepower#

cd/var/data/cores


```

22:14:42 UTC Sep 26 2023
Standby Ready                Just Active                HELLO not heard from peer
                                                            (failover link down)

22:14:42 UTC Sep 26 2023
Just Active                   Active Drain               HELLO not heard from peer
                                                            (failover link down)

22:14:42 UTC Sep 26 2023
Active Drain                  Active Applying Config    HELLO not heard from peer
                                                            (failover link down)

22:14:42 UTC Sep 26 2023
Active Applying Config        Active Config Applied     HELLO not heard from peer
                                                            (failover link down)

22:14:42 UTC Sep 26 2023
Active Config Applied         Active                     HELLO not heard from peer
                                                            (failover link down)

```

- show failover state - غالباً ما يتبع رساؤنا فشل الزوجات أو تداخلها نم لك لشل فشل الزوجات أو رمأا اذه ضرعي لشل فشل الزوجات هنع.

<#root>

firepower#

show failover state

	State	Last Failure Reason	Date/Time
This host -	Primary		
	Active	None	
Other host -	Secondary		
	Failed	Comm Failure	22:14:42 UTC Sep 26 2023

مادختساال ةلاح (ةزهجال) MIO جلاعمل بلقلا تاقد لشف -

تاباجتساال يقلت مدع دنع. فرشمالا لبلق تابرض ايرود قيبتل لثم لسري لشل فشل الزوجات ثدح ليغشت نكمي، ةيروفلا.

رماً اذه تلمعتسا، لشلل بلسلا تققد لجا نم:

- show failover history - تاريخت لشل فشل الزوجات تاظوفحم ضرعت. لشل فشل الزوجات تاظوفحم ضرع ةلاحال ريغت بلسو لشل فشل الزوجات ةصاخال ةقباسال ةلاحال.

<#root>

firepower#

show failover history

```

=====
From State                To State                Reason
=====

```

02:35:08 UTC Sep 26 2023	Active	Failed	MIO-blade heartbeat failure
02:35:12 UTC Sep 26 2023	Failed	Negotiation	MIO-blade heartbeat recovered
.	.	.	.
02:37:02 UTC Sep 26 2023	Sync File	System Bulk Sync	Detected an Active mate
02:37:14 UTC Sep 26 2023	Bulk Sync	Standby Ready	Detected an Active mate

ءاطخألا فاشككسأ تافل م عيمجت ةدشب نسحتس مل نم ، MIO بلق تاق تاق د لش ف دن ع
 اءال ص او cisco TAC ب لاصتال او ، FXOS نم ةينقتال تال جس ضرعو ، اءال ص او

معدلا ةدحو ضرعو show tech-support ل كيه عيمجت ب مق ، Firepower 4100/9300 ل ةبس ن ل اب
 ين فل .

معدل ل show جذوم ن عيمجت ب مق ، 3100/4200 نم آلا ةي امحل رادحو و FPR1000/2100 ل ةبس ن ل اب
 ين فل .

ةلص تا ذ تام ول عم

- [FTD ل ةيلاع ل ةحات ل](#)
- [Firepower ةزهجأ ل ع رفاوت ل ل ةل اع FTD جم ان رب ن يوك ت](#)
- [اءال ص او FirePOWER فلم عاش ن اءار ج اءاطخأ فاشككسأ](#)
- [FXOS ل ع ين فل معدل تافل م ضرع عاش ن ةي في ك - وي دي فل](#)
- [Cisco Systems - تادن ت س مل او ينقتال معدل](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت
ملاعلاء ن أ عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ة ي رش ب ل و
امك ة ق ي قد ن و ك ت ن ل ة ي ل أ ة مچرت ل ض ف أ ن أ ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (رف و ت م ط بار ل ا) ي ل ص أ ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا