

ىل ل و خ د ل ل لئاسر ل لاسر ل ةزه ج أ ل ن ي و ك ت ا ه ح ال ص و ا ط خ أ ل ف ا ش ك ت س ا ب ة ص ا خ ل م ا ظ ن ل FMC ل ل ع ا ه ض ر ع و

ت ا ي و ت ح م ل ا

[ة م د ق م ل ا](#)

[ة ي س ا س أ ل ا ت ا ب ل ط ت م ل ا](#)

[ت ا ب ل ط ت م ل ا](#)

[ة م د خ ت س م ل ا ت ا ن و ك م ل ا](#)

[ة ز ي م ل ا ل ل ع ة م ا ع ة ر ظ ن](#)

[ن ي و ك ت ل ا](#)

[ن ي و ك ت ل ا ن م ق ق ح ت ل ا](#)

ة م د ق م ل ا

ىل ة ي ص ي خ ش ت ل a syslog لئاسر ل لاسر ل ة ر ا د م ل ا ة ز ه ج أ ل ن ي و ك ت ة ي ف ي ك د ن ت س م ل ا ا ذ ه ح ض و ي
د ح و م ل ا ث ا د ح أ ل ا ض ر ا ع ي ف ا ه ض ر ع و FMC.

ة ي س ا س أ ل ا ت ا ب ل ط ت م ل ا

ت ا ب ل ط ت م ل ا

ة ي ل ل ا ت ل ا ع ي ض ا و م ل ا ب ة ف ر ع م ك ي د ل ن و ك ت ن ا ب Cisco ي ص و ت:

- Syslog لئاسر
- Firepower (FMC) ة ر ا د ا ز ك ر م
- Firepower Threat Defense (FTD)

ة م د خ ت س م ل ا ت ا ن و ك م ل ا

ة ي ل ل ا ت ل ا ة ي د ا م ل ا ت ا ن و ك م ل ا و ج م ا ر ب ل ا ت ا ر ا د ص ل ا ل ا د ن ت س م ل ا ا ذ ه ي ف ة د ر ا و ل ا ت ا م و ل ع م ل ا د ن ت س ت

- Firepower. ة ي س ا س أ ل ا ة م ظ ن أ ل ا ع ي م ج ل ل ع د ن ت س م ل ا ا ذ ه ق ب ط ن ي
- ر ا د ص ل ا ج م ا ن ر ب ب ل م ع ي ي ذ ل ا (FTD) ن م أ ل ا ة ي ا م ح ل ا ر ا د ج ت ا د ي د ه ت د ض ي ر ه ا ط ل ا ع ا ف د ل ل و ك و ت و ر ب 7.6.0

• ن م 7.6.0 ر ا د ص ل ا ل ل غ ش ي ي ذ ل ا (FMC) Secure Firewall Management Center Virtual ق ي ب ط ت
ج م ا ن ر ب ل ا

ة ص ا خ ة ي ل م ع م ة ئ ي ب ي ف ة د و ج و م ل ا ة ز ه ج أ ل ا ن م د ن ت س م ل ا ا ذ ه ي ف ة د ر ا و ل ا ت ا م و ل ع م ل ا ا ش ن ا م ت

ت ن ا ك ا ذ ا (ي ض ا ر ت ف ا). ح و س م م ن ي و ك ت ب د ن ت س م ل ا ا ذ ه ي ف ة م د خ ت س م ل ا ة ز ه ج أ ل ا ع ي م ج ت ا د ب
ر م ا ي أ ل ل م ت ح م ل ا ر ي ث ا ت ل ل ك م ه ف ن م د ك ا ت ف ، ل ي غ ش ت ل ا د ي ق ك ت ك ب ش

ة ز ي م ل ا ل ل ع ة م ا ع ة ر ظ ن

لودج ي ف "اهحالصإو ءاطخألأ فاشككتسأل دي دج ثدح عون ة فاضإ متت ، "نمألأ ءي امحل رادج" ي ف لاسرا م عدي وهو يساسألأ ماظنلأ تادادعإ ليجست نيوكت عيسوت مت . "ةدحوملأ ثادحلأ ضراع" VPN تالجس نم ال دب FMC ل لINA ءطساوب اهؤاشنإ مت ي تلأ ءي صيخش تلأ syslog لئاسر ال FMC 7.6.0 عم قفاوتم جم انرب رادصإ لغشي FTD ي أ ل ع ءزيملأ هذه نيوكت نكمي . طقف تاليلحت تاودأ ل ع يوتحي ال Cdfmc نأل Cdfmc م ع م ي .

- ءرحل تالجس لآ تا يوتسمو ه ي بن تلأ وئراوطلأ ل ع تالجس لآ عيمج رايخ رصتقي ثدحلأ م ج ب بسب .
- FMC ل ل زاهلأ نم هل اسرا م تي syslog ي أ هذه اهحالصإو ءاطخألأ فاشككتسأ تالجس رهظت (رخأ و VPN).
- (FMC) ءكبشلأ ءرادإ ي ف مكحتلأ ءدحو ل ل اهحالصإو ءاطخألأ فاشككتسأ تالجس قفدتت > اهحالصإو ءاطخألأ فاشككتسأ > ءزهجألأ تحتو دحوملأ ثدحلأ ضرع ي ف ءيئرم نوكتو > اهحالصإو ءاطخألأ فاشككتسأ تالجس .

نيوكتلأ

يولعل نكرلأ ي ف ريرحت ءنوقي أ قوف رقن او يساسألأ ماظنلأ تادادعإ > FMC ءزهجألأ ل ل قتنا ءسايسلأ نم نم يألأ .

The screenshot shows the Cisco Firewall Management Center (FMC) interface. The top navigation bar includes the Cisco logo, "Firewall Management Center", "Devices / Platform Settings", a search bar, a "Deploy" button, and user information "admin". The main content area displays a table with the following data:

Platform Settings	Device Type	Status
FTD1_platform_settings	Threat Defense	Targeting 1 device(s) Up-to-date on all targeted devices

There are icons for edit and delete in the status column of the first row.

يساسألأ ماظنلأ تادادعإ جهن

ل ل ليجستلأ لفسأ تاراخي ءثال ءدهاشم كنكمي . ليجستلأ دادعإ > Syslog ل ل قتنا نمألأ ءي امحل رادج ءرادإ زكرم .

The screenshot shows the configuration page for 'FTD1_platform_settings'. The left sidebar contains navigation options: Home, Overview, Analysis, Policies, Devices (selected), Objects, and Integration. The main content area is divided into several sections: 'Logging Setup' (selected), 'Logging Destinations', 'Email Setup', 'Event Lists', 'Rate Limit', 'Syslog Settings', and 'Syslog Servers'. The 'Logging Setup' section includes 'Basic Logging Settings' with options like 'Enable logging' (checked), 'Enable logging on the failover standby unit', 'Send syslogs in EMBLEM format', and 'Send debug messages as syslogs'. It also shows 'Memory Size of the Internal Buffer (bytes)' set to 4096. The 'Logging to Secure Firewall Management Center' section has radio buttons for 'Off', 'All Logs' (selected), and 'VPN Logs'. Below this, the 'Logging Level' is set to '2 - critical'. The 'FTP Server Information' section has an unchecked option for 'FTP server buffer wrap'.

ليجستل تاراخي ةثالث

ةثالث ليجستل تايوتسم نم ي ديحت كنكم في ،تالجس لاي م راي تخاب تمق اذا
 ام ب) FMC الى اهل اسراو ةيصي خش لال syslog لئاسرر تاهي بنتل او ئراوطلال تالاج :ةرفوتم لال
 في لذي VPN).

This screenshot is similar to the first one but shows the 'Logging Level' dropdown menu expanded. The menu lists three options: '0 - emergencies', '1 - alerts', and '2 - critical'. The '2 - critical' option is currently selected. The rest of the page configuration remains the same as in the first screenshot.

ةحاتم لاليجستل تايوتسم

تايوتسم عي م رفوتم سف ،VPN) ةيره اطلال ةصاخلال ةكبشلال تالجس راي تخاب تمق اذا
 تايوتسم لال هذ دحأ ديحت كنكم يولي ليجستل لال.

Policy Assignments (1)

Logging Setup | Logging Destinations | Email Setup | Event Lists | Rate Limit | Syslog Settings | Syslog Servers

Basic Logging Settings

- Enable logging
- Enable logging on the failover standby unit
- Send syslogs in EMBLEM format
- Send debug messages as syslogs

Memory Size of the Internal Buffer (bytes)
4096
(4096-52428800)

Logging to Secure Firewall Management Center

Off | All Logs | VPN Logs

Logging Level: 3 - errors

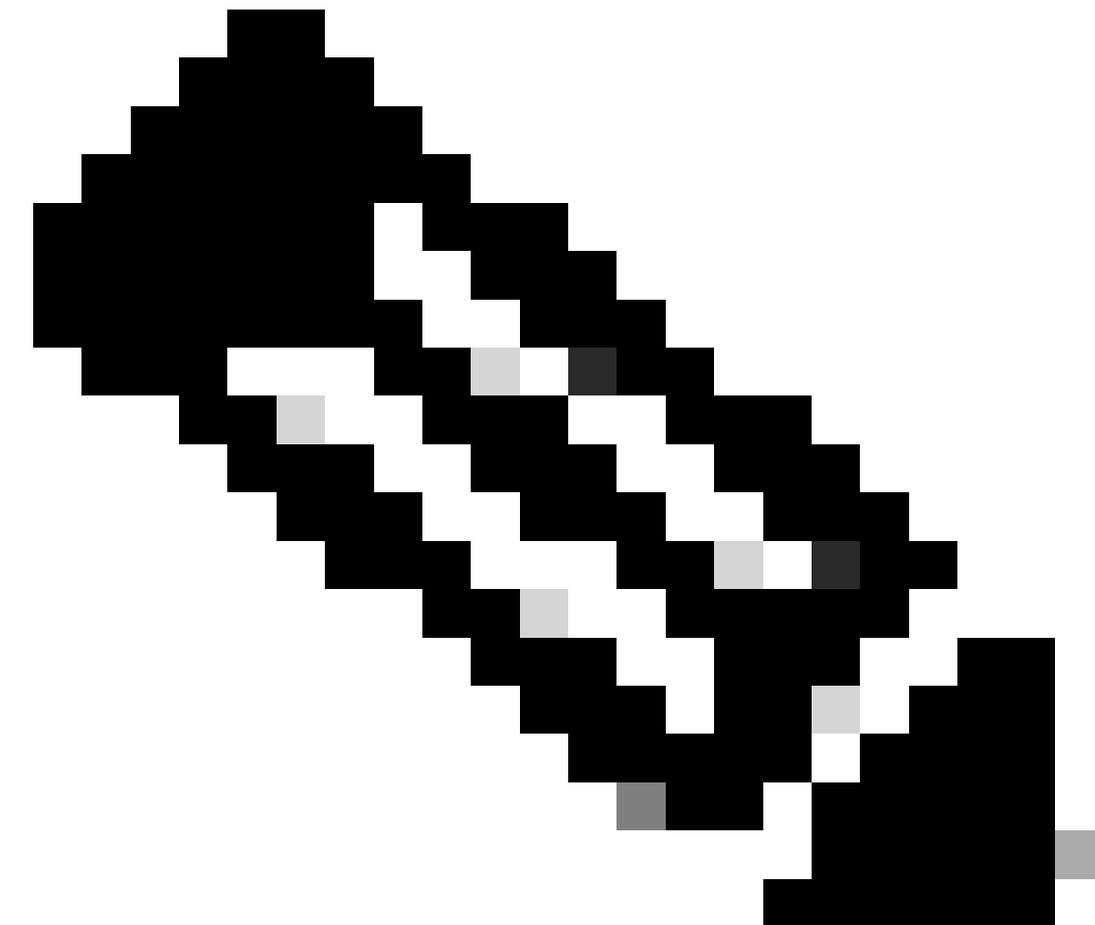
- 0 - emergencies
- 1 - alerts
- 2 - critical
- 3 - errors
- 4 - warnings
- 5 - notifications
- 6 - informational
- 7 - debugging

Available Interface Groups: Search

Selected Interface Groups

Add

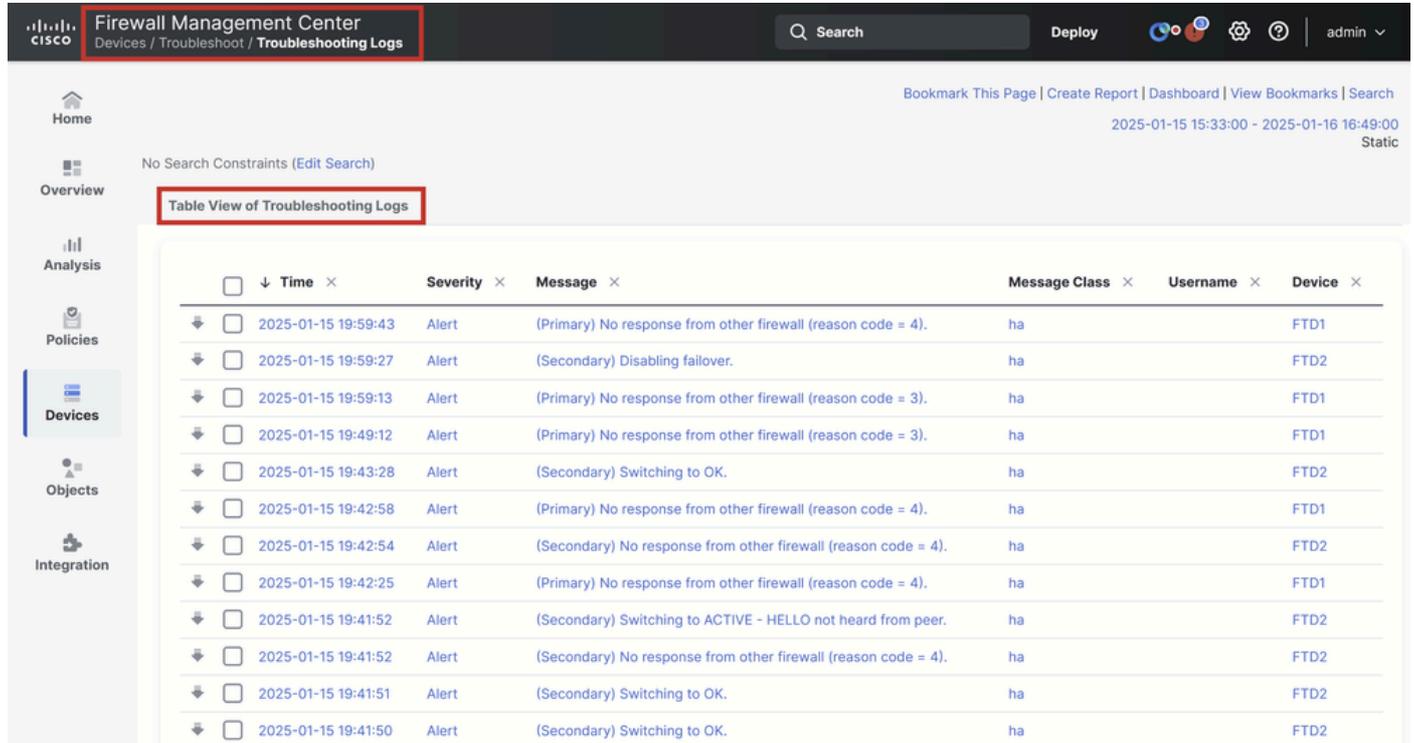
ةحاتم ل ليجست ل تاوتسم



ىل ا عقوم ىل ا لوصول ل VPN ةكبش مادختساب زاچ نيوكتب موقت ام دنع :ةطحال م

ةرادإلا زكرم ىلإ VPN مزح لاسررا نيكمتب ايئاقلت موقبي هنإف ،دعب نع لوصولأ عقوم
بناجب syslog لك لسري نأ لجس لك ىلإ وه تريغ عيطتسي تنأ .يضارتفا لكشب
VPN ىلإ لجس FMC.

تالجس > اءالصلإو اءاخالأ فاشكتسأ > ةزهجالأ نم تالجسلا هءه ىلإ لوصولأ نكمي
اءالصلإو اءاخالأ فاشكتسأ.



<input type="checkbox"/>	↓ Time ×	Severity ×	Message ×	Message Class ×	Username ×	Device ×
⌵	2025-01-15 19:59:43	Alert	(Primary) No response from other firewall (reason code = 4).	ha		FTD1
⌵	2025-01-15 19:59:27	Alert	(Secondary) Disabling failover.	ha		FTD2
⌵	2025-01-15 19:59:13	Alert	(Primary) No response from other firewall (reason code = 3).	ha		FTD1
⌵	2025-01-15 19:49:12	Alert	(Primary) No response from other firewall (reason code = 3).	ha		FTD1
⌵	2025-01-15 19:43:28	Alert	(Secondary) Switching to OK.	ha		FTD2
⌵	2025-01-15 19:42:58	Alert	(Primary) No response from other firewall (reason code = 4).	ha		FTD1
⌵	2025-01-15 19:42:54	Alert	(Secondary) No response from other firewall (reason code = 4).	ha		FTD2
⌵	2025-01-15 19:42:25	Alert	(Primary) No response from other firewall (reason code = 4).	ha		FTD1
⌵	2025-01-15 19:41:52	Alert	(Secondary) Switching to ACTIVE - HELLO not heard from peer.	ha		FTD2
⌵	2025-01-15 19:41:52	Alert	(Secondary) No response from other firewall (reason code = 4).	ha		FTD2
⌵	2025-01-15 19:41:51	Alert	(Secondary) Switching to OK.	ha		FTD2
⌵	2025-01-15 19:41:50	Alert	(Secondary) Switching to OK.	ha		FTD2

اءالصلإو اءاخالأ فاشكتسأ تالجسل لودجلا ضرع

ضراع ةءفص ي ف اءالصلإو اءاخالأ فاشكتسالا ةءءءج ضرع بيوبت ةمالع نألا رفوتت
(ةءءوم ءاءء) Unified Events > (لئلءء) Analysis ىلإ لءءنا ،ءاءءال هءه ضرعل .ةءءوملا ءاءءال
> Troubleshooting (اءالصلإو اءاخالأ فاشكتسأ).

Firewall Management Center Analysis / Unified Events

Search Deploy admin

Events Troubleshooting

Search... Refresh

14 0 0 0 14 events 2025-01-16 15:33:44 IST 1h 16m Go Live

Time	Event Type	Action	Reason	Source IP	Destination IP	Source Po	ICMP Type
2025-01-16 16:49:27	Connection	Block		198.51.100.178	192.0.2.171	2906 / tcp	
2025-01-16 16:48:37	Connection	Block		198.51.100.134	192.0.2.171	9025 / tcp	
2025-01-16 16:47:17	Connection	Allow		203.0.113.234	192.0.2.51	8902 / tcp	
2025-01-16 16:46:17	Connection	Allow		203.0.113.149	198.51.100.27	6789 / tcp	
2025-01-16 16:43:58	Connection	Block		192.0.2.214	203.0.113.139	8080 / tcp	
2025-01-16 16:43:25	Connection	Block		192.0.2.214	198.51.100.71	8080 / tcp	
2025-01-16 16:40:48	Connection	Allow		198.51.100.111	203.0.113.66	8 (Echo Re	
2025-01-16 16:39:32	Connection	Allow		198.51.100.145	203.0.113.186	8 (Echo Re	
2025-01-16 16:37:38	Connection	Block		198.51.100.39	192.0.2.176	7413 / tcp	
2025-01-16 16:36:28	Connection	Block		203.0.113.75	198.51.100.112	8421 / tcp	
2025-01-16 16:35:22	Connection	Allow		203.0.113.153	192.0.2.132	9876 / tcp	
2025-01-16 16:33:10	Connection	Block		198.51.100.49	192.0.2.63	3692 / tcp	
2025-01-16 16:32:10	Connection	Allow		198.51.100.95	203.0.113.99	8 (Echo Re	
2025-01-16 16:31:15	Connection	Allow		192.0.2.25	203.0.113.249	1234 / tcp	

اهحل الصا و اءاطخ ال فاشك تسأ ضرع ة قيرط

نكمي ال .هذه بيوبتلا ةمالع ىل لى دببتلا درجم لودجلا لخاد ايئرم ديدج شح عون نوكي
 ضرع ة قيرطلا ةيساسا اهنال ىرخال اعاونال لثم ضرعلا ةقيرط نم اهتلازا و اهتفاضلا
 اءاطخ ال فاشك تسأ

Firewall Management Center Analysis / Unified Events

Search Deploy admin

Events Troubleshooting

Event Type Troubleshooting + Refresh

399 399 events 2025-01-15 15:33:44 IST 1d 1h Go Live

Time	Event Type	Source IP	Device	Domain	Message	Message Class
2025-01-15 19:59:43	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
2025-01-15 19:59:27	Troubleshooting		FTD2	Global	(Secondary) Disabling f...	ha
2025-01-15 19:59:13	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
2025-01-15 19:49:12	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
2025-01-15 19:43:28	Troubleshooting		FTD2	Global	(Secondary) Switching t...	ha
2025-01-15 19:42:58	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
2025-01-15 19:42:54	Troubleshooting		FTD2	Global	(Secondary) No respon...	ha
2025-01-15 19:42:25	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
2025-01-15 19:41:52	Troubleshooting		FTD2	Global	(Secondary) No respon...	ha
2025-01-15 19:41:52	Troubleshooting		FTD2	Global	(Secondary) Switching t...	ha
2025-01-15 19:41:51	Troubleshooting		FTD2	Global	(Secondary) Switching t...	ha
2025-01-15 19:41:50	Troubleshooting		FTD2	Global	(Secondary) Switching t...	ha
2025-01-15 19:41:50	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
2025-01-15 19:41:49	Troubleshooting		FTD2	Global	(Secondary) Switching t...	ha
2025-01-15 19:41:48	Troubleshooting		FTD2	Global	(Secondary) Switching t...	ha

اهحل الصا و اءاطخ ال فاشك تسأ شح عون

ءاطخ ال فاشك تسأ" ضرع ة قيرط نم اهتلازا و ىرخال اءاطخ ال فاشك تسأ شح عون
 ىرخال اءاطخ ال فاشك تسأ" ضرع ة قيرط نم اهتلازا و ىرخال اءاطخ ال فاشك تسأ شح عون

Firewall Management Center
Analysis / Unified Events

Search Deploy admin

Events Troubleshooting

Event Type Troubleshooting Connection Intrusion +

399 14 0 413 events

2025-01-15 15:33:44 IST 2025-01-16 16:49:44 IST 1d 1h Go Live

Time	Event Type	Source IP	Device	Domain	Message	Message Class
2025-01-16 16:40:48	Connection	198.51.100.111	FTD1	Global		
2025-01-16 16:39:32	Connection	198.51.100.145	FTD1	Global		
2025-01-16 16:37:38	Connection	198.51.100.39	FTD1	Global		
2025-01-16 16:36:28	Connection	203.0.113.75	FTD1	Global		
2025-01-16 16:35:22	Connection	203.0.113.153	FTD1	Global		
2025-01-16 16:33:10	Connection	198.51.100.49	FTD1	Global		
2025-01-16 16:32:10	Connection	198.51.100.95	FTD1	Global		
2025-01-16 16:31:15	Connection	192.0.2.25	FTD1	Global		
2025-01-15 19:59:43	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
2025-01-15 19:59:27	Troubleshooting		FTD2	Global	(Secondary) Disabling f...	ha
2025-01-15 19:59:13	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
2025-01-15 19:49:12	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
2025-01-15 19:43:28	Troubleshooting		FTD2	Global	(Secondary) Switching t...	ha
2025-01-15 19:42:58	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
2025-01-15 19:42:54	Troubleshooting		FTD2	Global	(Secondary) No response f...	ha

درخأ شادجأ عاونأ

نيوكتال نم ققحتلا

نم ققحتلا نمك مي FMC، (GUI) ةيموسرلا مدختسم لة هجاو نم نيوكتال ذيفنت درجب
 show running-config logging رماوأل لايغشت لالخ نم FTD ل (CLI) رماوأل رطس هجاو نم هتحص
 و show logging و CLISH و LINA ءضوي ف

```
FTD1# show running-config logging
logging enable
logging timestamp
logging list MANAGER_ALL_SYSLOG_EVENT_LIST level critical
logging buffered errors
logging FMC MANAGER_ALL_SYSLOG_EVENT_LIST
logging device-id hostname
logging permit-hostdown
no logging message 106015
no logging message 313001
no logging message 313008
no logging message 106023
no logging message 710003
no logging message 302015
no logging message 302014
no logging message 302013
no logging message 302018
no logging message 302017
no logging message 302016
no logging message 302021
no logging message 302020
```

أمر CLI J FTD

```
FTD1# show logging
Syslog logging: enabled
  Facility: 20
  Timestamp logging: enabled
  Timezone: disabled
  Logging Format: disabled
  Hide Username logging: enabled
  Standby logging: disabled
  Debug-trace logging: disabled
  Console logging: disabled
  Monitor logging: disabled
  Buffer logging: level errors, 45 messages logged
  Trap logging: disabled
  Permit-hostdown logging: enabled
  History logging: disabled
  Device ID: hostname "FTD1"
  Mail logging: disabled
  ASDM logging: disabled
  FMC logging: list MANAGER ALL SYSLOG EVENT LIST, 45 messages logged
```

أمر CLI J FTD

