

صيخرتال

يهر اظلال باسحل راودأ

يكلذل باسحل طبر زايتم اب يكلذل باسحل لوؤسم وأ يهر اظلال باسحل لوؤسم طقف عتم تي باسحل SSE.

عمئاق تحتو software.cisco.com لى لقتنا، يكلذل باسحل رود ءحص نم ققحتلل 1. ووطخل يكلذل باسحل ءرادإ دح، ءرادإل

The screenshot displays the Cisco Software Central dashboard with several service tiles:

- Download & Upgrade:** Includes links for Software Download, eDelivery, Product Upgrade Tool (PUT), and Upgradeable Products.
- Network Plug and Play:** Includes links for Plug and Play Connect and Learn about Network Plug and Play.
- License:** Includes links for Traditional Licensing, Smart Software Licensing, Enterprise Agreements, and View My Consumption.
- Order:** Includes links for Buy Directly from Cisco and End User License and SAAS Terms.
- Administration:** Includes links for All Users, Request a Smart Account, Request Access to an Existing Smart Account, Manage Smart Account (highlighted with a red box), and Learn about Smart Accounts.

تحت هنا نم ققحتو، نيمدختسمل لى لقتنا، مدختسمل رود ءحص نم ققحتلل 2. ووطخل ءروصل ي فحضم وه امك، يهر اظلال باسحل لوؤسم لى تاباسحل نيي عتم تي راودأل

Users

User	Email	Organization	Account Access	Role	User Group	Actions
<input type="checkbox"/>	<input type="text" value="danieben"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	
<input type="checkbox"/>	Daniel Benitez danieben	Cisco Systems, Inc.	All Virtual Accounts Mex-AMP TAC	Smart Account Administrator Virtual Account Administrator	-	Remove...

ةزهجأل صيخرت يلع يوتحي SSE ب طابتراللدحملا "يرهاظلا باسحلا" نأ نم دكأت 3. ةوطخلا
 ال ثدحلاو نامأل ةزهجأو SSE ب نامأل صيخرت يلع يوتحي ال باسح طابترال ةلاحي في نامأل
 SSE ةباوب يلع رهظي.

Cisco Software Central > Smart Software Licensing TAC Cisco Systems, Inc. ▾

Smart Software Licensing

[Feedback](#) [Support](#) [Help](#)

[Alerts](#) | [Inventory](#) | [Convert to Smart Licensing](#) | [Reports](#) | [Preferences](#) | [On-Prem Accounts](#) | [Activity](#)

Virtual Account: **Mex-AMP TAC** ▾ 13 Minor | Hide Alerts

General | **Licenses** | Product Instances | Event Log

Available Actions ▾ | Manage License Tags | License Reservation... |

By Name | By Tag


Search by License





<input type="checkbox"/>	License	Billing	Purchased	In Use	Balance	Alerts	Actions
<input type="checkbox"/>	FPR1010 URL Filtering	Prepaid	10	0	+ 10		Actions ▾
<input type="checkbox"/>	FPR4110 Threat Defense Malware Protection	Prepaid	1	0	+ 1		Actions ▾
<input type="checkbox"/>	FPR4110 Threat Defense Threat Protection	Prepaid	1	0	+ 1		Actions ▾
<input type="checkbox"/>	FPR4110 Threat Defense URL Filtering	Prepaid	1	0	+ 1		Actions ▾
<input type="checkbox"/>	HyperFlex Data Platform Enterprise Edition Subscription	Prepaid	2	0	+ 2		Actions ▾
<input type="checkbox"/>	ISE Apex Session Licenses	Prepaid	1	0	+ 1		Actions ▾
<input type="checkbox"/>	ISE Base Session Licenses	Prepaid	10	0	+ 10		Actions ▾
<input type="checkbox"/>	ISE Plus License	Prepaid	10	0	+ 10		Actions ▾
<input type="checkbox"/>	Threat Defense Virtual Malware Protection	Prepaid	10	1	+ 9		Actions ▾
<input type="checkbox"/>	Threat Defense Virtual Threat Protection	Prepaid	10	1	+ 9		Actions ▾

10 ▾ Showing Page 5 of 7 (85 Records) |◀◀▶▶|











صيخارت يل لقتنا، حيصلال يرهاظلا باسحلا في FMC ليچست نم ققحتلل 4. ةوطخلا
 ي: كذل صيخرتال اظنلا

Smart License Status

Cisco Smart Software Manager 

Usage Authorization:	 Authorized (Last Synchronized On Jun 10 2020)
Product Registration:	 Registered (Last Renewed On Jun 10 2020)
Assigned Virtual Account:	Mex-AMP TAC
Export-Controlled Features:	Enabled
Cisco Success Network:	Enabled 
Cisco Support Diagnostics:	Disabled 

Smart Licenses

License Type/Device Name	License Status
>  Firepower Management Center Virtual (1)	
>  Base (1)	
>  Malware (1)	
>  Threat (1)	
>  URL Filtering (1)	
>  AnyConnect Apex (1)	
>  AnyConnect Plus (1)	
AnyConnect VPN Only (0)	

Note: Container Instances of same blade share feature licenses

ةزهجال لچسو SSE ب كت اباسح طبرأ

SSE اباسح ب ي كذل ك اباسح طبر ك ل ع ب چي SSE اباسح ي ل لوخذل ل چست دن ع 1 ةوطخل
تاباسحل طبر ديحتو "تاودأ" زمر قوف رقنل ل ل چاتحت ك لذل



Daniel Benitez 

Link Smart/Virtual Accounts

Link CDO Account

Downloads

ةيره اظلالا تاباسحلا ةفاك ىلع يوتحي يذلا بكذلا باسحلا ىرتس ،باسحلا طبر درجم ب هيلع ةدوجوملا

SSE في ةزهجالا ليحست

كئيب في اهب حومسم هذه URL نيوانع نا نم دكأت 1. ةوطخلا

ةيكيرمالا ةقطنملا

- api-sse.cisco.com
- eventing-ingest.sse.itd.cisco.com

يبوروالا داخالا ةقطنم

- api.eu.sse.itd.cisco.com
- eventing-ingest.eu.sse.itd.cisco.com

نابايلو اءاهلاو ايسآ ةقطنم

- api.apj.sse.itd.cisco.com
- eventing-ingest.apj.sse.itd.cisco.com

اذه URL ناونع مادختساب SSE ةباوب ىل لوخدلا ليحستب مق 2. ةوطخلا

حيحصت نييرايلالا الك نيكم تو ،ةباحسلا تامدخ ىل اءافصتو <https://admin.sse.itd.cisco.com>. ةيلاللا ةروصلل في حضوم وه امك ، Cisco SecureX ديدهت ةباحسلاو

Cloud Services for Sourcefire Support

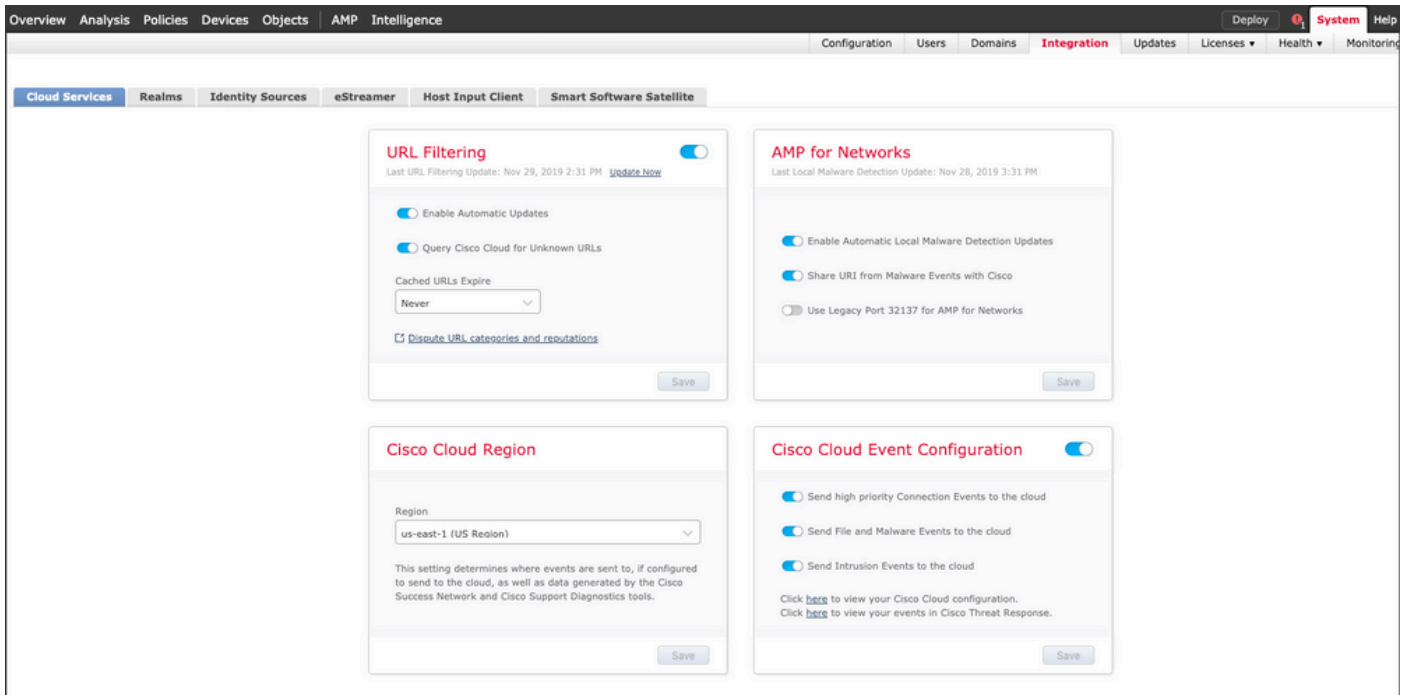
Cisco SecureX threat response

Cisco SecureX threat response enablement allows you to utilize supported devices in the course of a cybersecurity investigation. It also allows this platform to send high fidelity security events and observations to Threat Response.

Eventing

Eventing allows you to collect and view events in the cloud.

تامدخ >Integration> System ىل لقتناو Firepower ةرادك زكرم ىل لوخدلا لىحس 3. ةوطخلا
ىل اءاسرا ديرت يئلا ءادجالا ددحو Cisco Cloud ءدح نيوكت نيكم تب مقو ،ةباحسلا
ةباحسلا:



ةلجسملل ةزهجالا ةيؤر نالال كنكمي هنا نم ققحتلاو SSE ةبابو يلا عوجرلا كنكمي 4. ةوطخلال SSE:

Name	Type	Version	Status	Description
Firepower	Cisco Firepower Threat Defense for VMware	6.5.0	Registered	17 Firepower (FMC managed)
MEX-AMP-FMC	Cisco Firepower Management Center for VMware	6.5.0	Registered	24 MEX-AMP-FMC

ققحتلل SSE ةبابو يلا ةدوجوملا شادجالا يلا لقتنا، FTD ةزهجالا ةطساوب شادجالا لاسرا متي ةروصلال يلا حضورم وه امك، SSE يلا ةزهجالا ةطساوب اهلا لاسرا متي شادجالا نم:

Talos Disposition	Incident	Destination IP	Event Time	Ingest Time	Message	Protocol	Reporting Device ID	Source IP
Neutral	No	252	2020-08-05 18:48:50 UTC	2020-08-05 18:48:51 UTC		tcp	09d441eedce5	100
Neutral	No	145	2020-08-05 18:47:38 UTC	2020-08-05 18:47:38 UTC		tcp	09d441eedce5	100
Unknown	No	100	2020-08-05 18:47:30 UTC	2020-08-05 18:47:30 UTC		tcp	09d441eedce5	100
Neutral	No	252	2020-08-05 18:46:50 UTC	2020-08-05 18:46:50 UTC		tcp	09d441eedce5	100

SecureX يلا ةصصخملا تامولعملال تاحول نيوكت

دح، ةديج تامولعملال ةحول + ةنوقي يلا رقنا ك ةصاخلا تامولعملال ةحول عاشنال 1. ةوطخلال ةروصلال يلا حضورم وه امك، تامولعملال ةحولل امه مداخلتسا ديرت بناجتو مسا:

Create Dashboard



Dashboard Name

Test Dashboard

Available Tiles

- > AMP Global Intelligence
- > AMP for Endpoints-mshukur (RD)
- > Email Security Appliance
- > Email Security Appliance esa03
- > FMC 6.5.0
- > Firepower
- > Firepower - Mosterbe
- > Firepower CSSP
- ✓ Firepower dasieben

Event Summary

A set of metrics summarizing Firepower event activity in your organization



Incident Promotion Reason

A set of metrics summarizing Firepower incident activity in your organization



Talos IP Reputation

A set of metrics summarizing Talos disposition activity in your organization



Intrusion Top Attackers

List of top attackers for intrusion events in your organization



Intrusion Top Targets

List of top targets for intrusion events in your organization



ليجست مسق نم 4 ةوطخال يف روكذم وه امك SSE ةبواب ىلع شادخال ليجست نم ققحت SSE ىلع ةزهجال

ىتح API تالجس نم ققحت و SecureX تامولعم ةحول ىلع تامولعمل ضرع ةحص نم ققحت لىلحم ل API لشف ببس ىلع عالطال كنكمي

اهحالص او ءاطخال فاشكتسا

لاصتالا لكاشم فاشتك

لشفال تالاج يف action_queue.log فلم نم ةماعلا لاصتالا لكاشم نع فشكل كنكمي فللمل يف ةدووملا تالجسلا هذه ةيؤر كنكمي:

```
ActionQueueScrape.pl[19094]: [SF::SSE::Enrollment] canConnect: System (/usr/bin/curl -s --connect-timeo
```

لاصتالا نم ققحتلا بجيو ةيولمعال ةلهم ءاهتنا 28 جورخال زمر ينعي، ةلجال هذه يف DNS ةقد يف لكاشم ينعي امم 6 جورخال زمر اضيا ىرت دق. تنرتنللاب

DNS ةقد ببسب لاصتالا تالكشم

جحص لكشب لمعي لاصتالا نأ نم ققحت 1. ةوطخال

```
root@ftd01:~# curl -v -k https://api-sse.cisco.com
* Rebuilt URL to: https://api-sse.cisco.com/
* getaddrinfo(3) failed for api-sse.cisco.com:443
* Couldn't resolve host 'api-sse.cisco.com'
* Closing connection 0
curl: (6) Couldn't resolve host 'api-sse.cisco.com'
```

هذه يفو، <https://api-sse.cisco.com> URL ناو نع لىل رداق ريغ زاجال نأ هالعأ جارخال حضوي هتحص نم ققحتلا كنكمي و، ببسانملا DNS مداخ نيوكت نم ققحتلا ىل جاتحن، ةلجال ريبلال (CLI) رماوالا رطس ةهجاو نم NSLOOKUP مادختساب

```
root@ftd01:~# nslookup api-sse.cisco.com
;; connection timed out; no servers could be reached
```

DNS، تاداعل ديكأتل، هنيوكت مت يذلا DNS ىل لوصولا متي مل هنأ هالعأ جارخال رهظي show network رمالا مدختسا


```

> show network
===== [ System Information ] =====
Hostname           : ftd01
DNS Servers        : x.x.x.10
Management port    : 8305
IPv4 Default route
Gateway            : x.x.x.1

===== [ eth0 ] =====
State              : Enabled
Link               : Up
Channels           : Management & Events
Mode               : Non-Autonegotiation
MDI/MDIX           : Auto/MDIX
MTU                : 1500
MAC Address        : x:x:x:x:9D:A5
----- [ IPv4 ] -----
Configuration      : Manual
Address            : x.x.x.27
Netmask            : 255.255.255.0
Broadcast          : x.x.x.255
----- [ IPv6 ] -----
Configuration      : Disabled

===== [ Proxy Information ] =====
State              : Disabled
Authentication     : Disabled

```

رمألا اذه مادختساب DNS تادادعإ رييغت كنكمي، أطخلال DNS مداخل مادختسا مت، لاثملا اذه ي:

```
> configure network dns x.x.x.11
```

اجحان لاصتال نوكي، ةرملا هذه ىرخأ ةرم لاصتالا اذه رابتخإ دعب.

```

root@ftd01:~# curl -v -k https://api-sse.cisco.com
* Rebuilt URL to: https://api-sse.cisco.com/
* Trying x.x.x.66...
* Connected to api-sse.cisco.com (x.x.x.66) port 443 (#0)
* ALPN, offering http/1.1
* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH
* successfully set certificate verify locations:
* CAfile: none
CPath: /etc/ssl/certs
* TLSv1.2 (OUT), TLS header, Certificate Status (22):
* TLSv1.2 (OUT), TLS handshake, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (IN), TLS handshake, Server key exchange (12):
* TLSv1.2 (IN), TLS handshake, Request CERT (13):
* TLSv1.2 (IN), TLS handshake, Server finished (14):
* TLSv1.2 (OUT), TLS handshake, Certificate (11):
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):

```

```

* TLSv1.2 (OUT), TLS change cipher, Client hello (1):
* TLSv1.2 (OUT), TLS handshake, Finished (20):
* TLSv1.2 (IN), TLS change cipher, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.2 / ECDHE-RSA-AES128-GCM-SHA256
* ALPN, server accepted to use http/1.1
* Server certificate:
* subject: C=US; ST=California; L=San Jose; O=Cisco Systems, Inc.; CN=api -sse.cisco.com
* start date: 2019-12-03 20:57:56 GMT
* expire date: 2021-12-03 21:07:00 GMT
* issuer: C=US; O=HydrantID (Avalanche Cloud Corporation); CN=HydrantID S SL ICA G2
* SSL certificate verify result: self signed certificate in certificate chain (19), continuing anyway.
> GET / HTTP/1.1
> Host: api-sse.cisco.com
> User-Agent: curl/7.44.0
> Accept: */*
>
< HTTP/1.1 403 Forbidden
< Date: Wed, 08 Apr 2020 01:27:55 GMT
< Content-Type: text/plain; charset=utf-8
< Content-Length: 9
< Connection: keep-alive
< Keep-Alive: timeout=5
< ETag: "5e17b3f8-9"
< Cache-Control: no-store
< Pragma: no-cache
< Content-Security-Policy: default-src 'self'
< X-Content-Type-Options: nosniff
< X-XSS-Protection: 1; mode=block
< Strict-Transport-Security: max-age=31536000; includeSubdomains;

```

SSE ةب اوب ىلإ لىجستلا لكاشم

امهبة صاخلا ةرادالاه جاولى لس SSE URLs ناو نعب لاصتلا ىلإ FTD و FMC نم لك جاتحي
رذجلال لوصولاه عم Firepower CLI ىلع رماوأللاه هذه لخدأ، لاصتالارابتخال

<#root>

```
curl -v https://api-sse.cisco.com/providers/sse/services/registration/api/v2/clients --cacert /ngfw/etc/
```


```
curl -v https://est.sco.cisco.com --cacert /ngfw/etc/ssl/connectorCA.pem
```

```
curl -v https://eventing-ingest.sse.itd.cisco.com --cacert /ngfw/etc/ssl/connectorCA.pem
```

```
curl -v https://mx01.sse.itd.cisco.com --cacert /ngfw/etc/ssl/connectorCA.pem
```

رمأللاه اذهب ةداهشلال نم ققحتلال زواجت نكمي

```
root@ftd01:~# curl -v -k https://api-sse.cisco.com
* Rebuilt URL to: https://api-sse.cisco.com/
* Trying x.x.x.66...
* Connected to api-sse.cisco.com (x.x.x.66) port 443 (#0)
* ALPN, offering http/1.1
* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH
* successfully set certificate verify locations:
* CAfile: none
CPath: /etc/ssl/certs
* TLSv1.2 (OUT), TLS header, Certificate Status (22):
* TLSv1.2 (OUT), TLS handshake, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (IN), TLS handshake, Server key exchange (12):
* TLSv1.2 (IN), TLS handshake, Request CERT (13):
* TLSv1.2 (IN), TLS handshake, Server finished (14):
* TLSv1.2 (OUT), TLS handshake, Certificate (11):
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.2 (OUT), TLS change cipher, Client hello (1):
* TLSv1.2 (OUT), TLS handshake, Finished (20):
* TLSv1.2 (IN), TLS change cipher, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.2 / ECDHE-RSA-AES128-GCM-SHA256
* ALPN, server accepted to use http/1.1
* Server certificate:
* subject: C=US; ST=California; L=San Jose; O=Cisco Systems, Inc.; CN=api -sse.cisco.com
* start date: 2019-12-03 20:57:56 GMT
* expire date: 2021-12-03 21:07:00 GMT
* issuer: C=US; O=HydrantID (Avalanche Cloud Corporation); CN=HydrantID S SL ICA G2
* SSL certificate verify result: self signed certificate in certificate chain (19), continuing anyway.
> GET / HTTP/1.1
> Host: api-sse.cisco.com
> User-Agent: curl/7.44.0
> Accept: */*
>
< HTTP/1.1 403 Forbidden
< Date: Wed, 08 Apr 2020 01:27:55 GMT
< Content-Type: text/plain; charset=utf-8
< Content-Length: 9
< Connection: keep-alive
< Keep-Alive: timeout=5
< ETag: "5e17b3f8-9"
< Cache-Control: no-store
< Pragma: no-cache
< Content-Security-Policy: default-src 'self'
< X-Content-Type-Options: nosniff
< X-XSS-Protection: 1; mode=block
< Strict-Transport-Security: max-age=31536000; includeSubdomains;
```

 نم اهل اسرار مت ي التا تام ل عمل نأل ة روظح م لا 403 ة ل اسررلا لى لى ل و ص ح ل ك ن ك م ي : ة ظ ح الم
ل اص ت ال ا نم ق ق ح ت ل ل ي ف ك ي ام ب ت ب ث ي ا ذ ه ن ك ل و SSE ه ع ق و ت ي ام ت س ي ل ر اب ت خ ال ا

ل ا ح ن م ق ق ح ت ال SsecConnector ة ل ا ح ن م ق ق ح ت ال

ح ض و م و ه ام ك ل ص و م ل ا ص ئ ا ص خ ن م ق ق ح ت ال ك ن ك م ي

```
# more /ngfw/etc/sf/connector.properties
registration_interval=180
connector_port=8989
connector_fqdn=api-sse.cisco.com
```

لا ثم اذه، رمال اذه مادختس | كنكمي يذال EventHandler و SScontor ني بل لاصتال نم ققحتل ل
ئيس لاصتا يلع:

```
root@firepower:/etc/sf# netstat -anlp | grep EventHandler_SSEConnector.sock
unix 2 [ ACC ] STREAM LISTENING 3022791165 11204/EventHandler /ngfw/var/sf/run/EventHandler_SSEConnecto
```

ةلصتم قفدللا لاج نأ ىرت نأ كنكمي، تبات لاصتا يلع لاثم ي ف:

```
root@firepower:/etc/sf# netstat -anlp | grep EventHandler_SSEConnector.sock
unix 2 [ ACC ] STREAM LISTENING 382276 7741/EventHandler /ngfw/var/sf/run/EventHandler_SSEConnector.sock
unix 3 [ ] STREAM CONNECTED 378537 7741/EventHandler /ngfw/var/sf/run/EventHandler_SSEConnector.sock
```


CTR و SSE ةبابو يلإ ةلسرمل تانايبلا نم ققحتل

ع <https://eventing-ingest.sse.itd.cisco.com> عم TCP لاصتا عاشن | ةجاج يلع عالطالل FTD زا هج نم شادح لاسرل
و FTD لخدم ني ب هؤاشن | متي مل لاصتا يلع لاثم اذه <https://eventing-ingest.sse.itd.cisco.com>

```
root@firepower:/ngfw/var/log/connector# lsof -i | grep conn
connector 60815 www 10u IPv4 3022789647 0t0 TCP localhost:8989 (LISTEN)
connector 60815 www 12u IPv4 110237499 0t0 TCP firepower.cisco.com:53426->ec2-100-25-93-234.compute-1.a
```

تالجلسلا لصولم ي ف:

```
time="2020-04-13T14:34:02.88472046-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:co
time="2020-04-13T14:38:18.244707779-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:c
time="2020-04-13T14:42:42.564695622-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:c
time="2020-04-13T14:47:48.484762429-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:c
time="2020-04-13T14:52:38.404700083-05:00" level=error msg="[firepower.cisco.com][events.go:90 events:c
```

 <https://eventing-ingest.sse.itd.cisco.com> يلإ يمتنت 1x.x.x.246 و x.x.x.246 ةضورعمل IP نيوانع نأ طحال: ةظالم
ةكرحب حامسلا يه ةيصوتل نأ ي ف ببسلا وه اذهو، ريغتت دقو <https://eventing-ingest.sse.itd.cisco.com>
IP نيوانع نم الدب URL يلإ ادانتسا SSE ةبابو يلإ رورمل

لاصتا ىلع لاثم اذه SSE ةباوب ىل ائادحألا لاسرا متي نلف ،لاصتالا اذه عاشنإ متي مل اذإ
SSE ةباوبو FTD نيب تباث

```
root@firepower:# lsof -i | grep conn
connector 13277  www  10u  IPv4 26077573  0t0  TCP localhost:8989 (LISTEN)
connector 13277  www  19u  IPv4 26077679  0t0  TCP x.x.x.200:56495->ec2-35-172-147-246.compute-1.
```

ويديفلا

ةمچرتل هذه لوح

ةللأل تاي نقتلل نم ةومچم مادختساب دن تسمل اذه Cisco تمچرت
ملاعلاء انء عيچ ي ف ني مدختسمل معد ىوتحم مي دقتل ةيرشبلاو
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاخلا مهتغب
Cisco يلخت. فرتم مچرت مامدقي يتل ةيفارتهال ةمچرتل عم لاعلا وه
ىلإ أمئاد عوچرلاب ي صؤتو تامچرتل هذه ةقدنع اهتيلوئسم Cisco
Systems (رفوتم طبارلا) ي لصلأل يزي لچنإل دن تسمل