

يُفلّخ لفرط الة ةيوس تال تاي لمع snort و Lina ل ةدحوم ةروص وه Cisco نم نم آل ةي امحل رادج Cisco ةي امحل رادج ىلع ةجل امعل طويخو تاي لمعل يوتحت Cisco نم نم آل ةي امحل رادج ماظنل ةدحو ةاونب طبارت رشؤم وأ ةي لمع طبر ىلع ةردقل ال ري شي ام وهو ،ةلص ىلع نم آل وأ انيل لثم ،تاي لمعل ضع ب .تاجال امعل زكارم نم ةعومجم وأ ةني عم (CPU) ةي زكرمل ةجل امعل تارشؤم وأ ىرخأ تاي لمع ال نكمي ال هنأ نني عم امم ،ةني عم يونب ةي رصح ةلص اهل ،تروش

ي.ونال هذه ىلع لمعت نأ طبارت

اهحالصإو ءاطخال فاشكتسا

يلالعال جلالعمال كللهتست يتال سكونيل ةيلمع ىلع فرعت

Cisco ةيامح رادج ىلع ةيلال (CPU) ةيزكرم ةجالعمال ءحو كللهتست يتال تايلمعمال ديءحتل
ةيالاتل تاءارءملا ىلأ عءرا، نملأا

ةجالعمال ءحو مظعم كللهتست يتال تايلمعمال ديءحت في فولعمال رملأا تاءارءم اندعاست
(CPU) ةيزكرملا.

```
top - 17:27:37 up 62 days, 22:52, 2 users, load average: 0.41, 0.55, 0.48
Tasks: 158 total, 1 running, 157 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.9 us, 1.1 sy, 0.7 ni, 93.4 id, 3.9 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem : 7981.8 total, 821.0 free, 3184.3 used, 3976.5 buff/cache
MiB Swap: 5378.2 total, 4361.2 free, 1017.0 used. 4563.9 avail Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
3394	root	25	5	425680	4860	4652	S	7.6	0.1	6494:36	loggerd
3685	root	0	-20	2958720	1.4g	130268	S	6.0	18.0	5062:29	lina
4494	root	1	-19	1339224	509956	44688	S	1.7	6.2	1659:12	snort3
3979	root	20	0	2270592	141480	16840	S	0.7	1.7	637:29.39	SFDataCorrelator

زكرم لكل (CPU) ةيزكرملا ةجالعمال ءحو مءاءءتسا نم ققءءءو 1 ىلع طغضا

```
top - 17:30:36 up 62 days, 22:55, 2 users, load average: 0.33, 0.47, 0.45
Tasks: 157 total, 1 running, 156 sleeping, 0 stopped, 0 zombie
%Cpu0 : 3.0 us, 0.0 sy, 0.0 ni, 97.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
%Cpu1 : 0.0 us, 0.0 sy, 0.0 ni, 100.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
%Cpu2 : 0.0 us, 0.3 sy, 0.0 ni, 99.7 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
%Cpu3 : 1.3 us, 5.3 sy, 2.7 ni, 90.7 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem : 7981.8 total, 831.5 free, 3173.6 used, 3976.7 buff/cache
MiB Swap: 5378.2 total, 4361.2 free, 1017.0 used. 4574.7 avail Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
3394	root	25	5	425680	4860	4652	S	7.6	0.1	6494:36	loggerd
3685	root	0	-20	2958720	1.4g	130268	S	6.0	18.0	5062:29	lina
4494	root	1	-19	1339224	509956	44688	S	1.7	6.2	1659:12	snort3
3979	root	20	0	2270592	141480	16840	S	0.7	1.7	637:29.39	SFDataCorrelator

ةيلمعمال لىصافء نم ققءءءلل C ىلع طغضا

```
top - 17:31:53 up 62 days, 22:56, 2 users, load average: 0.34, 0.45, 0.45
Tasks: 157 total, 1 running, 156 sleeping, 0 stopped, 0 zombie
%Cpu0 : 3.7 us, 1.0 sy, 0.0 ni, 95.3 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
%Cpu1 : 0.0 us, 0.3 sy, 0.0 ni, 99.7 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
```

```
%Cpu2 : 0.0 us, 0.0 sy, 0.0 ni,100.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
%Cpu3 : 2.0 us, 3.7 sy, 2.7 ni, 91.7 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem : 7981.8 total, 831.4 free, 3173.7 used, 3976.7 buff/cache
MiB Swap: 5378.2 total, 4361.2 free, 1017.0 used. 4574.5 avail Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
3394	root	25	5	425680	4860	4652	S	7.3	0.1	6494:55	/ngfw/usr/local/sf/bin/loggerd
3685	root	0	-20	2958720	1.4g	130268	S	6.0	18.0	5062:45	lina -p 3562 -t -l
4494	root	1	-19	1339224	509956	44688	S	2.3	6.2	1659:17	/ngfw/var/sf/detection_engines/ad5
3418	root	20	0	1640540	16824	13900	S	0.7	0.2	274:48.05	/ngfw/usr/local/sf/bin/adi
3979	root	20	0	2270592	141480	16840	S	0.7	1.7	637:31.13	/ngfw/usr/local/sf/bin/SFDataCorre
3380	root	20	0	3860	2852	2336	S	0.3	0.0	6:27.14	/bin/bash /ngfw/usr/local/sf/bin/p

دع ب ةيلاع (CPU) ةيتركرم ةجلالعام ةدحوكلهتست (MONETDB) ةيملعملالاثم رابتعالا ي ف عض ل.وؤسمال وه MoneyDB ربتعي يذال يولعلالرمأال نم ققحتال

ngfw/var/log/monetdb/merovingian.log ءاربخلالعضو تحت merovingian.log بقعت كنكمي

```
root@FirePower:/# cd /ngfw/var/log/#catmerovingian.log
```

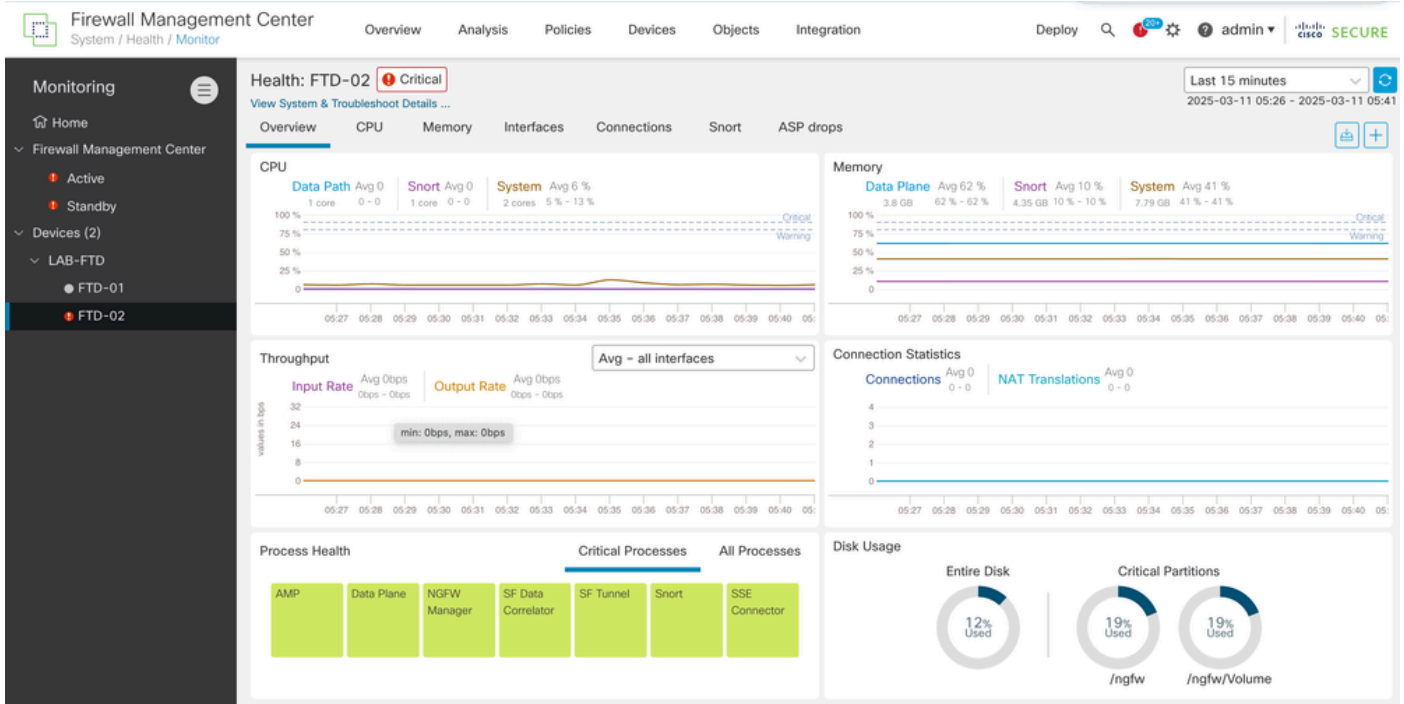
```
2025-03-06 23:24:11 ERR eventdb[26531]: #client12: createExceptionInternal:
!ERROR: SQLException:sql.drop_table:42000!DROP TABLE: unable to drop table connectionevent_1720808160_0
2025-03-06 23:24:11 ERR eventdb[26531]: #client12: createExceptionInternal:
!ERROR: SQLException:sql.drop_table:42000!DROP TABLE: unable to drop table
connectionevent_1720971900_0 (there are database objects which depend on it)
```

نمآال ةيالحال رادج ماظن زكارم ىلع (CPU) ةيتركرمال ةجلالعامال ةدحوول لالعامادختسإ نم Cisco

(CPU) ةيتركرمال ةجلالعامال ةدحو ةلاح ي ف اهلصإو ءاطخأال فاشكتسأ تاوطخ ي لي امي فو Cisco نم نمآال ةيالحال رادج ماظن زكارم ىلع ةيلاعال

1. FMC ةمالس ةبقارم ىلع ةيتركرمال ةجلالعامال ةدحو ماظنل يلاعال مادختسالال ديكتأ.

- ةدحوول عفترمالمادختسالال نم ققحتلل FMC ىلع دوجومالمالعالإال دومع نم ققحت ةيتركرمال ةجلالعامال
- اهتبقارمو ةرثأتمال زكارمالمال ةبقارم>ةيالح>ماظنلالإال لقتنا



2. ل (CLI) رم او ال رطس هه جاو ىل ع ةرثأت الم (CPU) ةي زك ر الم ةج ل اع م ال ةحو و زك ارم نم ققحت ال FTD.

- زك ر م يه ةرثأت الم زك ارم ال نأ نم دكأت و (CPU) ةي زك ر الم ةج ل اع م ال ةحو و ل ص نم ققحت م اظن ال.

```
> pmtool show affinity
```

Received status (0):

Affinity Status

System CPU Affinity: 3,9 (desired 3,9)

..

```
<#root>
```

```
admin@firepower:~$
```

```
sudo mpstat -P 3,9 1
```

```
Linux 4.18.45-yocto-standard (firepower)      03/03/25      _x86_64_      (64 CPU)
```

```
1:06:15      CPU
```

```
%usr      %nice      %sys
```

```
%iowait      %irq      %soft      %steal      %guest      %gnice
```

```
%idle
```

1:06:15 3

4

.00	54.00	24.00				
0.00	0.00	0.00	0.00	0.00	0.00	0.00

14.00

1:06:15 9

0.00	74.00	25.00				
0.00	0.00	0.00	0.00	0.00	0.00	0.00

0.00

1:06:15 CPU

%usr	%nice	%sys				
%iowait	%irq	%soft	%steal	%guest	%gnice	%idle

1:06:16 3

6

.00	44.00	34.00				
0.00	0.00	0.00	0.00	0.00	0.00	0.00

4

.00

1:06:16 9

2.00	74.00	22.00				
0.00	0.00	0.00	0.00	0.00	0.00	0.00

0.00

1:06:16 CPU

%usr	%nice	%sys				
%iowait	%irq	%soft	%steal	%guest	%gnice	%idle

1:06:16 3

6

.00	34.00	24.00				
0.00	0.00	0.00	0.00	0.00	0.00	0.00

34.00

1:06:16 9

0.00	74.00	24.00				
0.00	0.00	0.00	0.00	0.00	0.00	0.00

0.00

...

Average: 9 3.71 67.43 22.14 0.00 0.00 0.00 0.00 0.00 0.00 9.71

- Runmpstatorsarto اذه في. ماطنلا زكارم ىلع ةيزكرملا ةجلاعمل ةدحو مادختسا بقاري ةيناث/1 نم ةبقارملا ةرتف ىلا ريشي 1، لاثملا

% لئامجا - 100 يواسي هنال idle ل نندال دحلا، وه ةيزكرملا ةجلاعمل ةدحو لىلعال مادختسالال رخآ دومع.

<#root>

admin@firepower:~\$

sudo

sar -P 3,9 1

Linux 4.18.45-yocto-standard (firepower) 03/03/24 _x86_64_ (64 CPU)

1:06:17 CPU

%user %nice %system

%iowait %steal

%idle

1:06:18 3

5

.00 54.00 28.00

0.00 0.00

14.00

1:06:18 9

1.00 80.00 19.00

0.00 0.00

0.00

1:06:18 CPU

%user %nice %system

%iowait %steal

%idle

1:06:19 3

5

.00 41.00 22.00

0.00 0.00

24.00

1:06:19 9

2.00 84.00 12.00

0.00 0.00

0.00

1:06:19 CPU

%user %nice %system

%iowait %steal

%idle

1:06:20 3

1.00 67.00 15.00

0.00 0.00

4

.00

1:06:20 9

5

.00 68.00 24.00

0.00 0.00

0.00

1:06:20 CPU

%user %nice %system

%iowait %steal

%idle

1:09:21 3

6.00 26.00 27.00

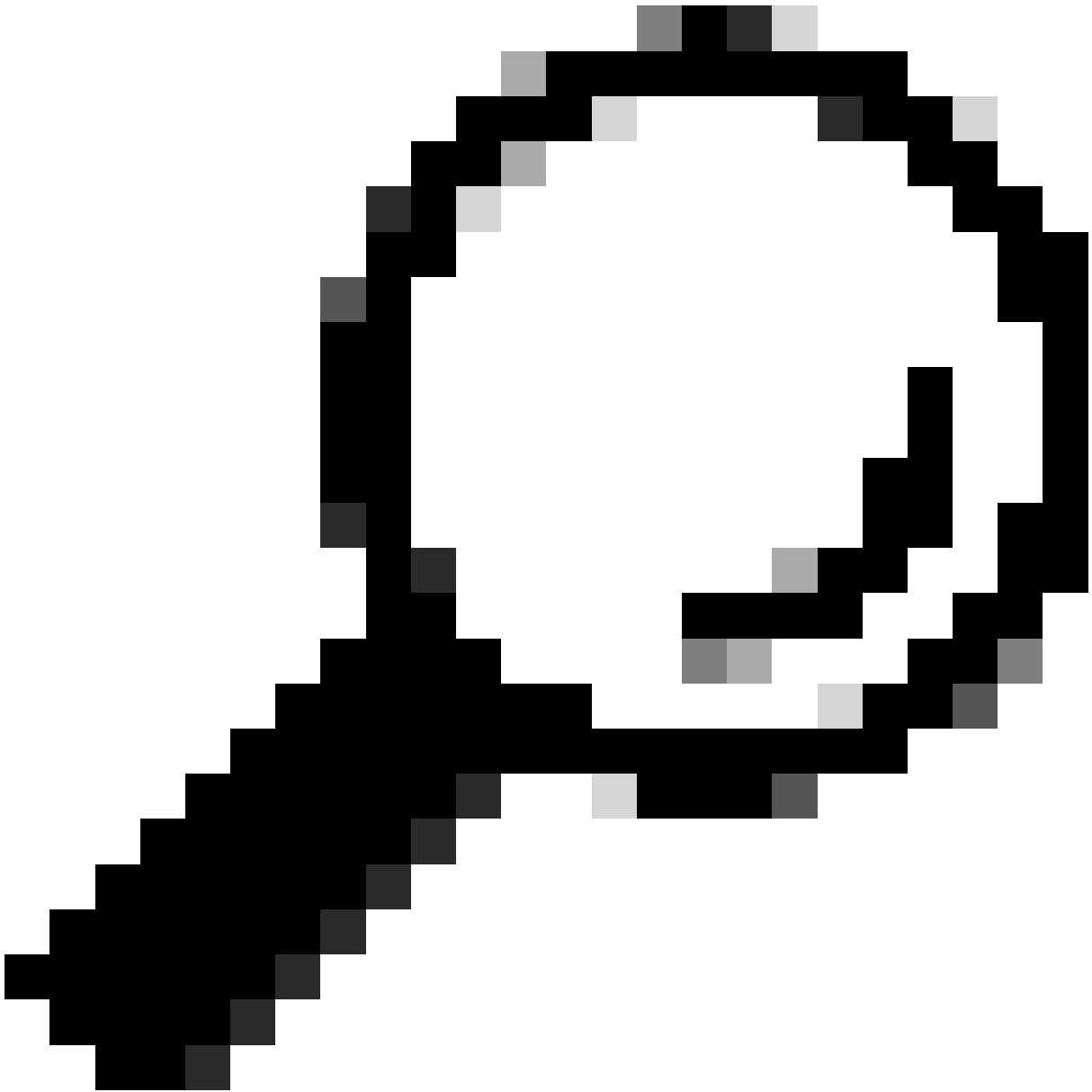
0.00 0.00

41.00

1:09:21	9	
0.00	86.00	14.00
	0.00	0.00
0.00		

ييلي امك دومعلا ناونع صيخلت متي:

- (قبيطتلال زمر) مدختسملا ءحاسم في (CPU) ءيزكرملا ءجالعملل ءءوماءءءسلا - %user ءيضااءءفالا ءءيالا ءميقلال عم.
- (قبيطتلال زمر) مدختسملا ءحاسم في (CPU) ءيزكرملا ءجالعملل ءءوماءءءسلا - فيطل% ءءيالا ءبيءااءي ءميقلال.
- صقان 100% - لماء% kernel ءحاسم في (CPU) ءيزكرملا ءجالعملل ءءوماءءءسلا - %system لوقءال يقاب



ىلع لمعت يتي طبارتال تارشؤم ةمئاق ىلع روثلل رمال اذه ليغشتب مق :خملت
نةم يون.

```
pidstat -h -t -p all 1 | awk '($10="%CPU") || ($10==xx || $10==YY) و{$9+0 > 10.00}
```

متي يتي تاي لمعال ةمئاق ىلع روثلل ريبلخال عضو في top رمال ليغشتب مق
نةم زكارم ىلع اهليغشت.

3. تاراسمال ةددعتم ةيلمعال تناك اذا امم ققحت.

<#root>

admin@firepower

:

~\$

sudo pidstat -h -t -p \$(pidof snort3) 1

Linux 4.18.45-yocto-standard (firepower)				03/03/25		_x86_64_		(64 CPU)		
# Time	UID	TGID	TID	%usr	%system	%guest	%wait	%CPU	CPU	Command
4:20:05	0	4162	-	279.08	17.17	0.00	0.99	285.15	3	snort3 <-
4:20:05	0	-	4162	3.96	0.99	0.00	0.99	4.95	3	__
snort3										
4:20:05	0	-	4165	0.00	0.00	0.00	0.00	0.00	7	__
snort3										
4:20:05	0	-	4167	0.00	0.00	0.00	0.00	0.00	9	__
snort3										
4:20:05	0	-	4168	0.00	0.00	0.00	0.00	0.00	9	__
snort3										
4:20:05	0	-	4169	0.00	0.00	0.00	0.00	0.00	9	__snort3
4:20:05	0	-	4172	0.00	0.00	0.00	0.00	0.00	9	__snort3
4:20:05	0	-	4175	0.00	0.00	0.00	0.00	0.00	9	__snort3
4:20:05	0	-	4177	0.00	0.00	0.00	0.00	0.00	3	__snort3

<#root>

admin@firepower

:

~\$

sudo

pidstat -h -t -p \$(pidof rsyslog) 1

Linux 4.18.45-yocto-standard (firepower)				03/03/25		_x86_64_		(64 CPU)		
# Time	UID	TGID	TID	%usr	%system	%guest	%wait	%CPU	CPU	Command
4:22:47	0	1	-	0.00	0.00	0.00	0.00	0.00	32	init
4:22:47	0	-	1	0.00	0.00	0.00	0.00	0.00	32	__init <---- single

م.ماظنل زكأرم ىلع لمعت ةي لمعلل طبأرت تارشؤم ةيأ تناك اذإ امم ققحت 4.

<#root>

05:13:30	0	-	327457	74.24	15.83	0.00	7.92	94.18	3	Even
----------	---	---	--------	-------	-------	------	------	-------	---	------

<---- Thread on system cores with highest CPU usage

05:13:30	0	-	327458	0.00	0.00	0.00	0.00	0.00	3	__Even
05:13:30	0	-	327459	0.00	0.00	0.00	0.00	0.00	9	__zmqi
05:13:30	0	-	327465	0.00	0.00	0.00	0.00	0.00	9	__zmqi
05:13:30	0	-	327466	0.00	0.99	0.00	0.00	0.99	3	__Even
05:13:30	0	-	327468	1.98	2.97	0.00	5.94	4.85	9	__Even
05:13:30	0	-	327470	0.00	0.00	0.00	0.99	0.00	3	__Even
05:13:30	0	-	327475	0.00	0.00	0.00	0.00	0.00	9	__Even
05:13:30	0	-	327476	0.00	0.00	0.00	0.00	0.00	9	__Even
05:13:30	0	-	327477	0.00	0.00	0.00	0.00	0.00	9	__Even
05:13:30	0	-	327478	0.00	0.00	0.00	0.00	0.00	3	__zmqi
05:13:30	0	-	327479	0.00	0.00	0.00	0.00	0.00	9	__zmqi

- زكّارم ىل ع لمعت ةي ب عشتل تاطا برال ةددعت م ةي زكّرم ةجل اع م ةحو EventHandler دعي م اظنل
- ةي زكّرم ل ةجل اع م ل ةحو ل م ادختس اىل ع ا هيدل TID=327457 و TID=327456 طبارت ل رشؤم
- ةي زكّرم ل ةجل اع م ل ةحو م ادختس ا عومج م يواسي ةي زكّرم ل ةجل اع م ل ةحو م ادختس ا ةجل اع م طبارت ل تارشؤم ةفاكل

ةلص تاذا تامول عم

[7.6 رادصلال Cisco نم نملآل ةي امحلل رادج ةرادا زكّرم ةرادا ليلد](#)

[7.6 رادصلال Cisco نم نملآل ةي امحلل رادج ةرادا زكّرم زاهج نيوك ت ليلد](#)

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا