

عن عمل CEE "ةومجمل ماظن ةرادا" نيوكتب مق دقعل رصم صارقأل ةلمالكلا ةلحال

تاوتحمل

[ةمدقمل](#)

[ةفلخل](#)

[ةلكشملا](#)

[لئلحت](#)

[لحل](#)

ةمدقمل

ةكبش يف ةدقعل رصم صرق اهظحال يتل ةلمالكلا ةلكشملا دن تسمل اذه فصى
مدختسمل.

ةفلخل

ةجيتن ريشت، (CEE) ةومجمل ماظن ريءمل كرتشملا ذيفنتلا ةئيبلا ةعجارم ءارء دن
دقعل رصم صرق ءالتما لىل قيقدتلا.

ةلكشملا

ةعاس 24 لىل ف لمالكلااب صرقلا ةلاح ثودح عقوتمل نم هنأل ةجرح ةروطخ هيبنت ةلاح دجوت
CEE لىل هيبنتلا اذه ةظحال م مت دقو، ةيلتلا

"ةيلتلا ةعاس 24 لىل لال خ /dev/sda3 زاوجل لم تكى نأ عقوتمل نم"
4dd4a4dd4a

لئلحت

موقت يتل (CEE) ةومجمل ءنسحمل تنرثي ةكبش يف هنع مالءال مت يذل هيبنتلا دجوي
يف ثدحتس يتل لمالكلااب صرقلا ةلاح زربتو لمالحلااب ةصاخلا ءزهجال لكاشم بقعتب
ةيلتلا نيرشعل او عربال تاعاسلا.

```
cisco@deployer-cm-primary:~$ kubectl get pods -A -o wide | grep node  
cee03 node-exporter-4dd4a4dd4a 1/1 Running 1 111d 10.10.1.1 deployer-cm-primary <none> <none>
```

```
root@deployer-cm-primary:/# df -h  
Filesystem Size Used Avail Use% Mounted on  
overlay 568G 171G 368G 32% /  
tmpfs 64M 0 64M 0% /dev  
tmpfs 189G 0 189G 0% /sys/fs/cgroup  
tmpfs 189G 0 189G 0% /host/sys/fs/cgroup  
/dev/sda1 9.8G 3.5G 5.9G 37% /host/root  
udev 189G 0 189G 0% /host/root/dev
```

```
tmpfs 189G 0 189G 0% /host/root/dev/shm
tmpfs 38G 15M 38G 1% /host/root/run
tmpfs 5.0M 0 5.0M 0% /host/root/run/lock
/dev/sda3 71G 67G 435M 100% /host/root/var/log
علاج ثدحت نأ لم تحملا نم، كذلك عجات ونو تالجس لاب ظفتحي هنا قيقدت لل صحت رهظي
لم الكلاب ردصملا ةدقع صرقب ةصاخلا مداخل.
```

```
root@deployer-cm-primary:/host/root/var/log# du -h --max-depth=1
76M ./sysstat
16K ./lost+found
4.0K ./containers
4.0K ./landscape
9.3M ./calico
1.1G ./apiserver
808K ./pods
5.6G ./journal
60G ./audit
36K ./apt
67G .
```

علاج ثدحت نأ لم تحملا نم، كذلك عجات ونو تالجس لاب ظفتحي هنا قيقدت لل صحت رهظي
لم الكلاب ردصملا ةدقع صرقب ةصاخلا مداخل.

```
cisco@deployer-cm-primary:~$ sudo cat /etc/audit/auditd.conf
#
# This file controls the configuration of the audit daemon
#

local_events = yes
write_logs = yes
log_file = /var/log/audit/audit.log
log_group = adm
log_format = RAW
flush = INCREMENTAL_ASYNC
freq = 50
max_log_file = 8
num_logs = 5
priority_boost = 4
disp_qos = lossy
dispatcher = /sbin/audispd
name_format = NONE
##name = mydomain
max_log_file_action = keep_logs
space_left = 75
space_left_action = email
verify_email = yes
action_mail_acct = root
admin_space_left = 50
admin_space_left_action = halt
disk_full_action = SUSPEND
disk_error_action = SUSPEND
use_libwrap = yes
##tcp_listen_port = 60
tcp_listen_queue = 5
tcp_max_per_addr = 1
##tcp_client_ports = 1024-65535
tcp_client_max_idle = 0
enable_krb5 = no
krb5_principal = auditd
##krb5_key_file = /etc/audit/audit.key
distribute_network = no
cisco@deployer-cm-primary:~$
```

الحل

Deployment-cm جعل العمل لاساسا لرادصا لال نل لك لى ع ، دعب امي ف جردم لال رماو الال زمر دادع اب مق ةلمت حملا ةدق لال رصم لال صرق لال ةلم الك لال ةلحال احي صتل Deployment-cm يونال لال مداخل او

```
sudo vim /etc/audit/auditd.conf
```

ري و دتل لال keep_log نل لخال لال فل م لال ري ي غت را و ج ب دو ج و م لال زمر لال مدخت سا م ث

```
max_log_file_action = rotate
```

ةمدخال لال لي غشت ةدع اب مق ، زمر لال ري ي غت دعب

```
sudo systemctl restart auditd.service
```

م اهل ال ه ي ب ن ن ال ةلازا نل ق ق حت

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن ت س مل ا ذه Cisco ت مچرت
م ل اع ل اء ن ا ع مچ ي ف ن ي م دخت س مل ل م عد ي و ت ح م م ي دقت ل ة ي ر ش ب ل و
امك ة ق ي ق د ن و ك ت ن ل ة ي ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ال 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 مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ال ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م اء ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
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 دن ت س مل ا