

ريغ ليغشتلا فاقيا دعب MongoDB حالصا فيظنلا

تايتوت حمللا

[عمدق مللا](#)

[ةيساسالا تابلطت مللا](#)

[تابلطت مللا](#)

[عمدختس مللا تانوك مللا](#)

[لجسلا تانايب عمجارم](#)

[أدبت مل اذا تانايبلا عمداق حالصا](#)

عمدق مللا

فورعمللا Secure Network Analytics زاهج يلع MongoDB حالصا ةيفيك دننتس مللا اذه حضوي حالص ريغ ليغشت فاقيا دعب Manager (Stealthwatch) مساب اقباس.

ةيساسالا تابلطت مللا

تابلطت مللا

دننتس مللا اذهل ةصاخ تابلطت مللا دجوت ال.

عمدختس مللا تانوك مللا

ةنعم ةيدام تانوك مللا وجمارب تارادصا يلع دننتس مللا اذه رصتقي ال.

ةصاخ ةيلمعم ةئيب في ةدوجوملا ةزهجالا نم دننتس مللا اذه في ةدراولا تامولعمللا عاشنإ مت تناك اذا. (يضا رتفا) حوسمم نيوكتب دننتس مللا اذه في عمدختس مللا ةزهجالا عيمج تادب رما يال لم تحملا ريثاتلل كمهف نم دكاتف، ةرشابم كتكباش.

لجسلا تانايب عمجارم

mongodb.log فلم عمجارم رمالا مدختسا

```
732smc:~# less /lancope/var/mongodb/log/mongodb.log
2021-06-21T14:54:43.029+0000 I CONTROL ***** SERVER RESTARTED *****
2021-06-21T14:54:43.033+0000 I CONTROL [initandlisten] MongoDB starting : pid=87057 port=27017
dbpath=/lancope/var/database/dbs/mdb/ 64-bit host=ussecrapstwsml
2021-06-21T14:54:43.033+0000 I CONTROL [initandlisten] db version v3.0.15
2021-06-21T14:54:43.033+0000 I CONTROL [initandlisten] git version:
b8ff507269c382bc100fc52f75f48d54cd42ec3b
2021-06-21T14:54:43.033+0000 I CONTROL [initandlisten] build info: Linux 3555b2234f08 4.9.0-2-
amd64 #1 SMP Debian 4.9.13-1 (2017-02-27) x86_64 BOOST_LIB_VERSION=1_49
2021-06-21T14:54:43.033+0000 I CONTROL [initandlisten] allocator: tcmalloc
2021-06-21T14:54:43.033+0000 I CONTROL [initandlisten] options: { config:
```

```

"/etc/mongodb/mongodb.conf", net: { port: 27017 }, processManagement: { fork: true }, storage: {
dbPath: "/lancope/var/database/dbs/mdb/" }, systemLog: { destination: "file", logAppend: true,
path: "/lancope/var/mongodb/log/mongodb.log" } }
2021-06-21T14:54:43.050+0000 W - [initandlisten] Detected unclean shutdown -
/lancope/var/database/dbs/mdb/mongod.lock is not empty.
2021-06-21T14:54:43.063+0000 I STORAGE [initandlisten] *****
old lock file: /lancope/var/database/dbs/mdb/mongod.lock. probably means unclean shutdown,
but there are no journal files to recover.
this is likely human error or filesystem corruption.
please make sure that your journal directory is mounted.
found 2 dbs.
see: http://dochub.mongodb.org/core/repair for more information
*****
2021-06-21T14:54:43.063+0000 I STORAGE [initandlisten] exception in initAndListen: 12596 old
lock file, terminating
2021-06-21T14:54:43.063+0000 I CONTROL [initandlisten] dbexit: rc: 100

```

أدبت مل اذا تانايا بل اةدعاق حالصا

وغنوم ةلاح نم ققحتلا 1. ةوطخلا

رمأل رادصا ب مق `systemCTL lc-mongodb` ةلاح نم ققحتلل

هباشتت فوس جئاتنل انا، ةطشن ةلاح يف وحنوم ناك اذا

```

732smc:/# systemctl is-active lc-mongodb
active
732smc:/#

```

هباشتت فوس جئاتنل انا، ةطشن ةلاح يف وحنوم نكي مل اذاو

```

732smc:/# systemctl is-active lc-mongodb
inactive
732smc:/#

```

وغنوم ةمدخ اوفقوا 2. ةوطخلا

رمأل مادختساب ةمدخل افاقيا ب مقف ، ةلاح يف LC-MONGODB ةمدخ ىلع روثعلا مت اذا
/bin/systemCTL stop lc-mongodb.service.

```

732smc:/# /bin/systemctl stop lc-mongodb.service
732smc:/# /bin/systemctl status lc-mongodb.service | grep Active
Active: inactive (dead) since Thu 2022-04-07 12:33:49 UTC; 1s ago7

```

ةلاح يف ةمدخل انا امضل ةجالحا بسح `status lc-mongodb.service` /bin/systemCTL رمأل مادختسا. فقوت ةلاح يف لازي ال وحنومل انا نم دكأتو قئاقد عضب رظتنا

عيميحتلا ةيلمع فرعم 3. ةوطخلا (PID)

cat رمأل رادصا ب مق PID ىلع يوتحي لازي ال نيماأتل فلم ناك اذا ام ةفرعمل ققحت
/lancope/var/database/dbs/mdb/mongod.lock.

نا بجي. ةيداحا ةمدخب صاخلا ةيلمعل فرعم ىلع يوتحي نيماأتل فلم نا جارخال اذه حضوي
ةطشن ةلاح يف ةمدخل انا ناك اذا طاقف تانايا ب ىلع فلمل اذه يوتحي.

4 ةوطخلا يف مدختسم وه امك، دحاو عاجرا مت اذا ةيلمعل فرعم طحال: ةطحال

```
732smc: /# cat /lancope/var/database/dbs/mdb/mongod.lock
14259
732smc: /#
```

إذا أغراف فلم الا اذه نوكي نأ بجي PID. فرعم يلع يوتحي ال ني مأتال فلم نأ جارخال اذه حضوي
7. ةوطخال ي ف رمتسا PID كانه نوكي مل اذا. ةطشن ةلاح ي ف ةيلمعال نكت مل

```
732smc: /# cat /lancope/var/database/dbs/mdb/mongod.lock
732smc: /#
```

PID ةلاح نم ققحتال. 4. ةوطخال

إذا `ps | grep` لي غشتب مق ف، PID يلع يوتحي 3 ةوطخال ي ف ددحمال MONGODB.Lock فلمال ناك اذا
مق م PID دوجو نم ققحتال (3 ةوطخال نم ك ب صاخال PID عم [1]4259 ري غشتب مق) رمأ [1] 4259
ه يلع روثل م اذا PID لتق ب كلذ دع ب

جارخال ي ف "grep" رمأل داعبتسا هنع جتن ي هنكلو بولطم ري غ سوقال ري بعت: ةطخال م

```
732smc: /# ps faux | grep [1]4259
mongodb 14259 0.3 0.4 516180 71520 ? S1 12:38 0:03 /lancope/mongodb/bin/mongod --fork --config
/etc/mongodb/mongodb.conf
732smc: /# kill -9 14259
732smc: /#
```

ني مأتال فلم تايوتحم حسم. 5. ةوطخال

ققحت `/lancope/var/database/dbs/mdb/mongod.lock` > رمأل مادختساب ل فقلال فلم يوتحم حسم
رمأ `cat /lancope/var/database/dbs/mdb/mongo.lock` مادختساب نأل اغراف فلمال نأ نم

```
732smc: /# > /lancope/var/database/dbs/mdb/mongod.lock
732smc: /# cat /lancope/var/database/dbs/mdb/mongod.lock
732smc: /#
```

MongoDB لي غشتب ةدب ةلواحم. 6. ةوطخال

درجم ب `/bin/systemctl start lc-mongodb.service` رمأل مادختساب LC-MONGODB ةمدخ ةدب لواح
`/bin/systemctl lc-mongodb.service` مادختساب ةيلمعال ةلاح نم ققحت، ك ب ةصاخال ةب لاطم ال اعرا
رمأ `grep` | `mongodb.service`

```
732smc: /# /bin/systemctl start lc-mongodb.service
732smc: /# /bin/systemctl status lc-mongodb.service | grep Active
Active: active (running) since Thu 2022-04-07 12:38:37 UTC; 27s ago
732smc: /#
```

نامضل ةل ل ق قئاقد نوضغ ي ف يرخأ ةرم ققحت ف، ةطشن ةلاح ي ف ةيلمعال تناك اذا
اذا. ل لمع ةلاح ي ف تلظ اذا تاناي ب ال ةدعاق حالصا يل جاتحت ال. ةطشن ةلاح ي ف اهئاقب
جالصا ةيلمع أ دباو 7 ةوطخال يل لقتنا، ةطشن ةلاقب ال ي ف ةيلمعال تلش ف

جالصال ةدب. 7. ةوطخال

رمأ `-u mongodb /lancope/mongodb/bin/mongod --dbpath /lancope/var/database/dbs/mdb` رادصا ب مق

```
732smc: /# sudo -u mongodb /lancope/mongodb/bin/mongod --dbpath /lancope/var/database/dbs/mdb/ --
```

repair

732smc:/#

هحالصإ مت يذلا MongoDB ليغشت ءدب ةلواحم 8. ةوطخلا

لظت نأ بجي .ةمدخلا ليغشت ءدب ل `/bin/systemctl start lc-mongodb.service` رمألا ليغشتب مق
رمألا مادختساب اهصحف نكميو ةطشن ةلاح يف ةي لمعلا
`/bin/systemctl status lc-mongodb.service`.

```
732smc:/# /bin/systemctl start lc-mongodb.service
```

```
732smc:/# /bin/systemctl status lc-mongodb.service | grep Active
```

```
Active: active (running) since Thu 2022-04-07 12:38:37 UTC; 27s ago
```

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نء مء دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةلخت. فرتمة مچرت مء مء دقء ةل ةل ةفارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزءل ءن إل دن تسمل