文章

Michael Lei · 六月 23, 2021 阅读大约需 3 分钟

加密一个数据库需要多久?

一位客户请求估计使用 cvencrypt 实用工具加密一个数据库需要多久。

这个问题有点像问一根绳子有多长 — 视情况而定。 但这是一个有趣的问题。 答案主要取决于客户使用的目标平台上的 CPU 和存储的性能,因此答案更关乎的是提出一个简单方法,可以在运行 cvencrypt 时使用该方法对 CPU 和存储进行基准测试。

方法

- 1. 将一个有代表性的大文件 CACHE.DAT 复制到目标存储
- 2. 通过系统管理门户创建密钥文件(包括密钥)
- 3. 对 CACHE.DAT 示例文件运行 cvencrypt (如下所示)

下面显示了测试文件到位后的过程:

输出:

```
Fri Oct 27 10:36:53 AEDT 2017
```

Cache for UNIX (Red Hat Enterprise Linux for x86-64) 2016.2.1 (Build 803) Wed Oct 26 2016 12:30:49 EDT

Stand-alone encryption utility for Cache databases and journal files

Database has 6870912 blocks. Encrypting. Processed: 6870912 blocks (done!) Fri Oct 27 10:43:25 AEDT 2017

根据上面的信息可以得出:

字节数/秒= 56.286.511.104 字节/392 秒 = 156.351.420 字节/秒 = 156 MB/秒

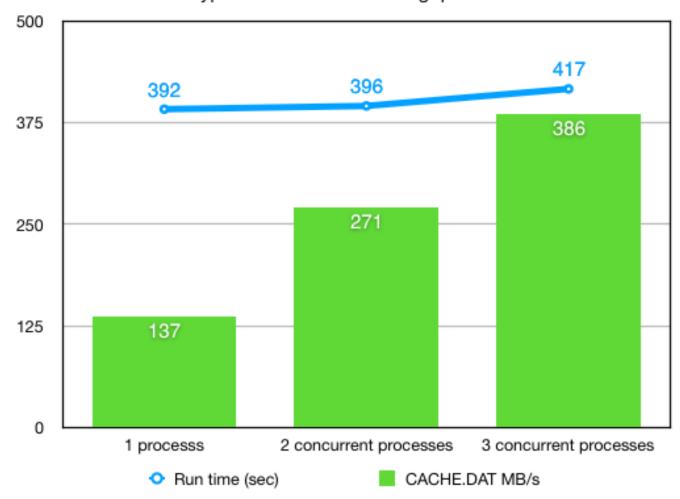
此测试在我们的悉尼实验室系统上进行。 但请记住,**您的情况将有所不同**,您必须**在您自己的系统上测试**。 我在帖子末尾附上了我使用的设置的详细信息。

并行运行多个加密

在转换期间,停机时间必须保持在最低限度,所以我对并行运行多个 cvencrypt 进程是否可扩展很感兴趣。 是否可以并行运行多个 cvencrypt 进程取决于存储和 CPU 的 IO 限制。 因此,通过精心计划,您应该能够在最短的时间内边玩俄罗斯方块边加密多个数据库。

下图显示了当并行运行多个线程时漂亮的扩展模式(并不十分线性)。

cvencrypt time to run and throughput - E5-2680 V3



并行测试脚本

以下是我运行并行测试的方式。 在子目录中建立多个 CACHE.DAT 文件 — 我使用了同一个文件的副本,但您需要测试您的数据库副本。

为进行测试, 我将这些文件布置成简单的树状结构:

ls -l *
-rw-r--r- 1 root root 56286511104 Oct 26 21:57 CACHE.DAT

加密一个数据库需要多久?

Published on InterSystems Developer Community (https://community.intersystems.com)

```
-rwxr-xr-x 1 root root
                               189 Oct 26 22:29 enc_p.sh
-rw-r--r-- 1 root root
                               241 Oct 26 19:56 syd_enc_key
db1:
total 54967296
-rw-r--r-- 1 root root 56286511104 Oct 26 22:33 CACHE.DAT
db2:
total 54967296
-rw-r--r- 1 root root 56286511104 Oct 26 22:46 CACHE.DAT
total 54967296
-rw-r--r-- 1 root root 56286511104 Oct 26 22:54 CACHE.DAT
简单脚本 encp.sh 运行 cvencrypt:
# cat ./enc_p.sh
#!/bin/sh
echo "Start " ${1} " " `date`
/hs/h20162/bin/cvencrypt -dbfile ./db${1}/CACHE.DAT -outkeyfile ./syd_enc_key -outuse
r xxx -outpass xxx
echo "End " ${1} " " `date`
对子目录进行迭代:
```

```
# for i in 1 2 3; do ( ./enc_p.sh $i & ) ; done
```

测试系统配置

Red Hat 7.4,使用 LVM2 上的 xfs 磁盘。 运行 VMWare 6.5。

Dell PowerEdge R730 服务器

- 2 个英特尔至强 E5-2680 v3 2.5GHz, 30M 高速缓存, 9.60GT/s QPI, 睿频, 超线程, 12C/24T (120W)

Dell PowerVault MD3420 存储

- 24 个 960GB 固态硬盘 SAS 读取密集型 MLC 12Gbps 2.5 英寸热拔插驱动器
- 双 8GB 缓存控制器(总共 16GB 缓存,每个控制器包含 8GB

缓存,与另一个控制器的缓存互为镜像,以实现高可用性。)

- 一个 24 磁盘 RAID6 磁盘组。

#InterSystems 业务解决方案和架构 #加密 #其他

源

URL:

https://cn.community.intersystems.com/post/%E5%8A%A0%E5%AF%86%E4%B8%80%E4%B8%AA%E6%95%B0%E6%8D%AE%E5%BA%93%E9%9C%80%E8%A6%81%E5%A4%9A%E4%B9%85%EF%BC%9F