# ES 数据库备份快照

作者：xialei0755
原文链接：https://ld246.com/article/1674016140926
来源网站：链滴

# 背景：

某客户UCSS-HA+DB高可用环境，由于事件和日志量非常大，预估20G+，考虑到导出事件和日志备有一定风险导出失败，故考虑该手工备份ES数据库相关表

下述操作部署，为3.10 db高可用环境操作，参考文档：ElasticSearch手工归档

---

1.

## 登录db-master服务器，启用并配置nfs挂载信息

说明：为什么要启用nfs挂载备份路径：

es备份时，需要所有节点都可以访问同一个路径，默认是本地路径，相当于每个节点访问的这个备份径都是不同的，备份就会失败

```
vi /opt/skyguard/elasticsearch/es-all.yaml  #取消下述列的注释
108       #- name: backups
109       #  mountPath: /backups

121       #- name: backups
122       #  nfs:
123       #    path: /mnt/nfs_shared   #修改为nfs挂载路径
124       #    server: 172.22.111.11   #修改为nfs服务器ip
```

安装nfs客户端组件

ubuntu环境

```
dpkg -l |grep nfs-common  #查询是否有安装包
ii  nfs-common      1:1.2.8-9ubuntu12.3         amd64        NFS support files common to client a
d server
apt install nfs-common  #执行安装
```

redhat/centos/oraclelinux环境

```
yum list |grep nfs-utils  #查询是否有安装包
nfs-utils.x86_64                    1:1.3.0-0.68.0.1.el7.2      @ol7_latest
yum install nfs-utils  #执行安装
```

2.

## 启用仓库地址

配置备份后的快照文件存放地址（此地址为es容器内的地址)

```
root@k8s-master2 ~]# vi /opt/skyguard/elasticsearch/es-cm.yaml
# path.repo: "/backups"  #取消注释，生效备份快照的路径
```

3.

## 生效配置：

```
kubectl apply -f  /opt/skyguard/elasticsearch/es-all.yaml
```

```
kubectl apply -f  /opt/skyguard/elasticsearch/es-cm.yaml
```

停掉当前的es

kubectl delete statefulset es

之后使用kubectl get pods | grep es命令查看es pod的情况，直到检索不到结果为止，说明es的po都已经删除掉了。

4.

## 删掉ES集群界节点容器

查看ES容器节点

```
kubectl get pods | grep es
es-0                            1/1     Running   0          16h
es-1                            1/1     Running   0          16h
es-2                            1/1     Running   0          16h
```

删掉ES容器节点

```
kubectl delete pod es-0 es-1 es-2
pod "es-0" deleted
pod "es-1" deleted
pod "es-2" deleted
```

确认看K8S已经已经创建好新的容器节点（看Runling的运行时间判断是否是新创建）

```
kubectl get pods | grep es
es-0                            1/1     Running   0          2m37s
es-1                            1/1     Running   0          2m6s
es-2                            1/1     Running   0          2m36s
```

5.

## 生成仓库地址

生成仓库地址的过程，就是指定ES的备份文件存放路径的过程

注意：此命令及下述命令，均需要在ucss服务器的sps容器上执行

原因：db高可用环境，只授信了ucss ip

```
curl -H "Content-Type: application/json"  -XPUT http://172.22.2.179:9200/_snapshot/backup_archive -d '{"type":"fs","settings":{"location":"/backups"}}' -u skyguard:Elastic@SkyGuard     #表仓库地址为/backups
响应信息：{"acknowledged":true}  #表示执行成功
```

6. 查看需要生成快照的表信息

```
curl http://172.22.2.179:9200/_cat/indices -u skyguard:Elastic@SkyGuard
green open swg-20221119-01              460ytmRqRuK85gtLy1aOsw 5 1 1206 3   2.5mb   1.2b
green open ucwi-20221119-01             KFqxV4LUTxWsbeBL-SxzUg 5 1    0 0     2kb     1kb
green open dlp-mobile-20221119-01       A4mn4ef0QoK4-x6qcgEEAg 5 1    0 0     2kb     1k

green open connect-log-20221119-01      q1WtputiQxq6R0oJwtbWlA 5 1   39 0 436.7kb 218
```

```
3kb
green open dlp-discovery-20221119-01       tKtXvhw8STS5m-38aKCMCg 5 1     0 0      2kb      1
b
green open email-message-20221119-01       QPCnoOWZQPm5ZwnmUpd69A 5 1    38 0    1.2
b 649.7kb
green open dlp-endpoint-20221119-01        W_obj8ExSKia5v7rQJTNRw 5 1     0 0      2kb      1kb
green open dlp-network-20221119-01         oKqBLAfJSIitTFjJL1cW2Q 5 1    35 3    3.8mb    1.9m

green open dlp-watermark-20221119-01       sqQpxwz8T82hgomfcX_uxw 5 1     0 0      2kb      1
b
green open mobile-app-incident-20221119-01 drzGKMroQsKULGDaKC2zYA 5 1     0 0      2kb
 1kb
green open mobile-mag-log-20221119-01      yJQSxhKPS4OhElVydO0-mQ 5 1     0 0      2kb
1kb
green open itm-scores-20221119-01          Z0G6pV01SWiyDT3JFIIADA 5 1     0 0      2kb      1kb
```

7. 生成快照（会自动导出到nas目录）

```
curl -X PUT -H "Content-Type:application/json" http://172.22.2.179:9200/_snapshot/backup_a
chive/dlp-20230118 -d '{"indices":"swg-20221119-01,connect-log-20221119-01"}' -u skyguard
Elastic@SkyGuard
```

## 完成上诉操作后，进入nas目录，便可以看到备份的快照信息了，如图所示：

```
[root@k8s-master1 backups]# pwd
/var/lib/kubelet/pods/fa0aaf80-5c04-4676-a52a-7cfdc40bd113/volumes/kubernetes.io~nfs/b
ckups
[root@k8s-master1 backups]# ls -lh
total 36K
drwxrwxr-x 4 skyguard root 4.0K Jan 17 23:21 indices
-rw-rw-r-- 1 skyguard root  27K Jan 17 23:21 meta--9kdlqjSSlWSeIP7ZD_svQ.dat
-rw-rw-r-- 1 skyguard root 2.2K Jan 17 23:21 snap--9kdlqjSSlWSeIP7ZD_svQ.dat
```

拷贝完后，请其实copy走数据，防止被后续的备份冲掉。