安全的Astra数据存储

Astra Data Store

NetApp
June 16, 2022

目录

安全的Astra数据存储

管理安全证书

Astra数据存储在集群的软件组件之间使用相互传输层安全(MTLS)加密。每个Astra Data Store集群都有一个自签名根CA证书(`astrads-cert`)和一个中间CA证书(`astrads-cert -<cluster_name>`)。这些证书由Astra数据存储操作员管理；操作员会在每个证书到期日期前7天自动续订这些证书。您也可以手动撤消这些证书。

撤消证书

如果Astra数据存储控制器、节点或CA证书受到影响、您可以通过删除其MTLS密钥来撤消该证书。执行此操作时、Astra数据存储操作员会自动颁发一个新证书。您可以随时撤消Astra数据存储证书。

如果您撤消CA证书、则此操作将撤消由该CA签名的任何证书。

步骤

1. 登录到Astra Data Store集群中的控制器节点。
2. 列出系统上的现有证书。例如：

```
kubectl get secrets -n astrads-system | grep astrads-cert
```

输出应类似于以下内容：

```
astrads-cert-astrads-cluster-controller
kubernetes.io/tls     4      6d6h
astrads-cert-astrads-cluster-f23d158
kubernetes.io/tls     4      6d6h
astrads-cert-astrads-ds-dms-astrads-cluster-f23d158
kubernetes.io/tls     4      6d6h
astrads-cert-astrads-ds-support-astrads-cluster-f23d158
kubernetes.io/tls     4      6d6h
astrads-cert-astrads-support-astrads-cluster-f23d158
kubernetes.io/tls     4      6d6h
astrads-cert-root
kubernetes.io/tls     4      6d6h
astrads-cert-sti-net-com
kubernetes.io/tls     5      6d6h
```

3. 在输出中、记下需要撤消的证书的名称。
4. 使用`kubectl`实用程序撤消证书、并将`certificate_name`替换为证书的名称。例如：

```
kubectl delete secret CERTIFICATE_NAME -n astrads-system
```

现有证书将被撤消、并自动生成一个新证书。

管理外部密钥

您可以使用一个或多个外部密钥管理服务器来保护集群用于访问加密数据的密钥。外部密钥管理服务器是存储环境中的第三方系统，可使用密钥管理互操作性协议（ Key Management Interoperability Protocol ， KMIP ）为节点提供密钥。

默认情况下、在创建Astra Data Store集群时、Astra Data Store会通过内部密钥提供程序启用空闲软件加密(软件加密)。

管理密钥涉及以下自定义资源定义(CRD)：

- * AstraDSKeyProvider*：配置外部KMIP服务器、该服务器可以是服务器集群。
- * AstraDSSEARKeyrotate*：从密钥提供程序获取新的密钥加密密钥并将其提供给Astra数据存储。

您可以执行以下与外部密钥管理相关的任务：

- [Set up external key management]
- [Check the software encryption at rest status]
- [Change external to internal key management]
- [Rotate keys for security]

设置外部密钥管理

在Astra Data Store中设置外部密钥管理时、可以使用`kubectl astrad`命令。

您需要在集群或KMIP服务器上获得SSL证书、以便可以设置外部密钥、例如使用OpenSSL。

步骤

1. 为密钥提供程序客户端准备证书。包括客户端证书、客户端专用密钥和信任CA捆绑包。

   您需要在集群或KMIP服务器上准备SSL证书、以便设置外部密钥、例如、使用OpenSSL。

2. 登录到Astra Data Store集群中的一个节点。
3. 输入以下kubectl扩展命令、为Astra Data Store集群配置密钥提供程序：

```
kubectl-astrads key-provider certs --key key.pem
--client-cert client_cert.pem --ca-cert server_ca.pem
--hostnames=<kmip_server_ip> <key_provider_cr_name>
--namespace astrads-system --cluster <ads_cluster_name>
```

以下示例将为ADS集群"astrads-cluster-f23d158"配置一个名为"hashicorp"的外部密钥提供程序。

```
kubectl-astrads key-provider certs --key key.pem
--client-cert client_cert.pem --ca-cert server_ca.pem
--hostnames=10.235.nnn.nnn hashicorp
--namespace astrads-system --cluster astrads-cluster-f23d158
```

1. 将Astra数据存储集群配置为通过AstraDSCluster CR对sear使用外部密钥管理器。显示帮助。

   ```
   kubectl-astrads clusters sears -h
   ```

   响应：

```
Configure SEARS in AstraDS cluster

Usage:
  astrads clusters sears [flags]

Flags:
  -d, --duration string   Duration for key rotation (default "2160h")
  -h, --help              help for sears


Global Flags:
      --ads-cluster-name string        Name of the ADS Cluster
      --ads-cluster-namespace string   Namespace of the ADS Cluster
      ...
```

以下命令会将Astra Data Store集群配置为使用`AstraDSKeyProvider hashicorp`作为sear的密钥管理器。此命令还会使用密钥轮换时间、其默认值为90天(2160小时)。

```
kubectl-astrads clusters sears -d 500h hashicorp
--ads-cluster-name=astrads-cluster-f23d158
--ads-cluster-namespace=astrads-system
```

检查软件空闲加密状态

您可以检查空闲软件加密的配置。

步骤

1. 检查AstraDSCluster CR。

```
Name:         astrads-cluster-f23d158
Namespace:    astrads-system
Labels:       <none>
Annotations:  <none>
API Version:  astrads.netapp.io/v1beta1
Kind:         AstraDSCluster
...
Spec:
...
  Software Encryption At Rest:
    Ads Key Provider:     hashicorp
    Key Rotation Period:  500h0m0s
...
Status:
...
  Software Encryption At Rest Status:
    Key Active Time:       2022-05-16T15:53:47Z
    Key Provider Name:     hashicorp
    Key Provider UUID:     ccfc2b0b-dd98-5ca4-b778-99debef83550
    Key UUID:              nnnnnnnn-nnnn-nnnn-nnnn-nnnnnnnnnnnn
```

将外部密钥管理更改为内部密钥管理

如果您当前使用的是外部密钥管理器、则可以将其更改为内部密钥管理器。

步骤

1. 通过删除SoftwareEncryptionAtRest配置来更改AstraDSCluster CR。
2. (可选)删除先前的AstraDSKeyProvider及其关联密钥。

> 不会自动删除先前的密钥提供程序和密钥。

为安全起见、请轮换密钥

密钥轮换可增强安全性。默认情况下、Astra数据存储每90天自动轮换一次密钥。您可以更改默认设置。此外、您还可以根据需要轮换按键。

配置自动密钥轮换

1. 更新CRD中的AstraDSSEARKeyrotate参数。

```
kubectl patch astradscluster astrads-cluster-f23d158
-n astrads-system
--type=merge -p '{"spec": {"softwareEncryptionAtRest": {
"keyRotationPeriod": "3000h"}}}'
```

配置按需密钥轮换

1. 创建AstraDSSEARKeyrotateRequest CR以轮换密钥。

```
cat << EOF | kubectl apply -f  -
apiVersion: astrads.netapp.io/v1beta1
kind: AstraDSSEARKeyRotateRequest
metadata:
  name: manual
  namespace: astrads-system
spec:
  cluster: astrads-cluster-f23d158
EOF
```