



Secure Astraデータストア Astra Data Store

NetApp
July 19, 2022

目次

Secure Astraデータストア	1
セキュリティ証明書を管理する	1
外部キーを管理します	2

Secure Astraデータストア

セキュリティ証明書を管理する

Astraデータストアでは、クラスタのソフトウェアコンポーネント間でMTLS（Mutual Transport Layer Security）暗号化を使用しています。各Astra Data Storeクラスタには、自己署名ルートCA証明書（「astrs-cert-root」）と中間CA証明書（「astrs-cert-<cluster_name>」）があります。この証明書はAstra Data Storeオペレータによって管理され、有効期限の7日前にオペレータが証明書を自動的に更新します。証明書を手動で取り消すこともできます。

証明書を取り消します

Astraデータストアコントローラ、ノード、またはCA証明書が侵害された場合、MTLSシークレットを削除することでCA証明書を取り消すことができます。これを行うと、Astra Data Storeオペレータは自動的に新しい証明書を発行します。Astraデータストア証明書はいつでも取り消すことができます。



CA証明書を取り消すと、そのCAによって署名された証明書がすべて取り消されます。

手順

1. Astra Data Storeクラスタのコントローラノードにログインします。
2. システム上の既存の証明書の一覧を表示します。例：

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

次のような出力が表示されます。

```
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. 出力には、取り消す必要がある証明書の名前が表示されます。
4. 'kubectl'ユーティリティを使用して証明書を削除しますこれは'certificate_name'を証明書の名前に置き換えます例：

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

既存の証明書が失効し、代わりに新しい証明書が自動的に生成されます。

外部キーを管理します

1 つ以上の外部キー管理サーバを使用して、暗号化されたデータにアクセスする際にクラスタで使用するキーを安全に保管できます。外部キー管理サーバはストレージ環境に配置されたサードパーティのシステムで、Key Management Interoperability Protocol (KMIP) を使用してノードにキーを提供します。



Astraデータストアでは、Astraデータストアクラスタを作成すると、デフォルトで内部キープロバイダを使用して保存データの暗号化 (sear) が有効になります。

キーの管理には、次のカスタムリソース定義 (CRD) が含まれます。

- *** AstraDSKeyProvider*** : 外部KMIPサーバを設定します。このサーバはサーバのクラスタの場合があります。
- *** AstraDSSEARKeyRotate *** : キープロバイダから新しいキー暗号化キーを取得し、Astraデータストアに提供します。

外部キー管理に関連して次のタスクを実行できます。

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

外部キー管理をセットアップする

Astra Data Storeで外部キー管理を設定するには'kubectl astrs'コマンドを使用します

クラスタまたはKMIPサーバにSSL証明書が必要です。これにより、OpenSSLなどを使用した外部キーの設定などが可能になります。

手順

1. キープロバイダクライアントの証明書を準備します。クライアント証明書、クライアント秘密鍵、および信頼CAバンドルが含まれます。



クラスタまたはKMIPサーバで、OpenSSLなどを使用した外部キーの設定を可能にするSSL証明書を準備します。

2. Astraデータストアクラスタのいずれかのノードにログインします。
3. 次のkubectl拡張コマンドを入力して、Astraデータストアクラスタのキープロバイダを設定します。

```
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>
```

次の例では、ADSクラスタ「astrs-cluster-f23d158」に対して「hashicorp」という名前の外部キープロバイダを設定します。

```
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. Astra Data StoreクラスタをAstraDSCluster CR経由で、外部キーマネージャを使用するように設定します。ヘルプを表示します。

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

対応：

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
...
```

次のコマンドは'Astra Data Storeクラスタを'AstraDSKeyProvider hashicorp'をsearのキー管理ツールとして使用するように設定しますまた、キーのローテーション時間も使用されます。この時間のデフォルト値は90日（2160時間）です。

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

ソフトウェアの保存データの暗号化ステータスを確認します

保存データのソフトウェア暗号化の設定を確認できます。

ステップ

1. AstraDSCluster CRを確認します。

```
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:     ccf2b0b-dd98-5ca4-b778-99debef83550
    Key UUID:              nnnnnnnnn-nnnn-nnnn-nnnn-nnnnnnnnnnnnnn
```

外部キー管理を内部キー管理に変更します

現在外部キー管理ツールを使用している場合は、内部キー管理ツールに変更できます。

手順

1. SoftwareEncryptionAtRest設定を削除してAstraDSCluster CRを変更します。
2. (オプション) 前のAstraeDSKeyProviderと関連付けられている秘密を削除します。



以前のキープロバイダとシークレットは自動的に削除されません。

キーをローテーションしてセキュリティを確保します

キーのローテーションにより、セキュリティが向上します。デフォルトでは、Astraデータストアはキーを90日ごとに自動的にローテーションします。デフォルト設定を変更できます。また、必要に応じてキーをオンデマンドでローテーションすることもできます。

自動キーローテーションを設定する

1. CRDのAstraeSSEARKeyRotateパラメータを更新します。

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

オンデマンドのキーローテーションを設定する

1. AstraatDSSEARKeyRotateRequest CRを作成してキーを回転します。

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

著作権情報

Copyright © 2022 NetApp, Inc. All rights reserved. 米国で印刷されていますこのドキュメントは著作権によって保護されています。画像媒体、電子媒体、および写真複写、記録媒体などの機械媒体など、いかなる形式および方法による複製も禁止します。テープ媒体、または電子検索システムへの保管-著作権所有者の書面による事前承諾なし。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、いかなる場合でも、間接的、偶発的、特別、懲罰的、またはまたは結果的損害（代替品または代替サービスの調達、使用の損失、データ、利益、またはこれらに限定されないものを含みますが、これらに限定されません。）ただし、契約、厳格責任、または本ソフトウェアの使用に起因する不法行為（過失やその他を含む）のいずれであっても、かかる損害の可能性について知らされていた場合でも、責任の理論に基づいて発生します。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、またはその他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1 つ以上の米国特許、その他の国の特許、および出願中の特許により特許、その他の国の特許、および出願中の特許。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7103（1988 年 10 月）および FAR 52-227-19（1987 年 6 月）の Rights in Technical Data and Computer Software（技術データおよびコンピュータソフトウェアに関する諸権利）条項の（c）（1）（ii）項、に規定された制限が適用されます。

商標情報

NetApp、NetAppのロゴ、に記載されているマーク <http://www.netapp.com/TM> は、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。