Sicherheit

Astra Trident

NetApp
March 19, 2023

Inhaltsverzeichnis

Sicherheit 1
Sicherheit 1
Linux Unified Key Setup (LUKS) 2

Sicherheit

Sicherheit

Stellen Sie mit den hier aufgeführten Empfehlungen sicher, dass Ihre Astra Trident Installation sicher ist.

Führen Sie Astra Trident in einem eigenen Namespace aus

Es ist wichtig, dass Applikationen, Applikationsadministratoren, Benutzer und Managementapplikationen auf die Objektdefinitionen von Astra Trident oder die Pods zugreifen können, um zuverlässigen Storage sicherzustellen und potenzielle schädliche Aktivitäten zu blockieren.

Zur Trennung der anderen Applikationen und Benutzer von Astra Trident muss immer Astra Trident in einem eigenen Kubernetes Namespace installiert werden (`trident`). Wenn Astra Trident in einem eigenen Namespace bereitgestellt wird, wird sichergestellt, dass nur die Administratoren von Kubernetes auf den Astra Trident Pod und die Artefakte (z. B. Backend und CHAP-Schlüssel, falls zutreffend) zugreifen können, die in den namenweisen CRD-Objekten gespeichert sind. Sie sollten sicherstellen, dass nur Administratoren Zugriff auf den Astra Trident Namespace und damit auf das haben `tridentctl` Applikation.

Verwenden Sie CHAP-Authentifizierung mit ONTAP SAN Back-Ends

Astra Trident unterstützt die CHAP-basierte Authentifizierung für ONTAP-SAN-Workloads (mithilfe von `ontap-san` Und `ontap-san-economy` Treiber). NetApp empfiehlt die Verwendung von bidirektionalem CHAP mit Astra Trident zur Authentifizierung zwischen einem Host und dem Storage-Backend.

Bei ONTAP-Back-Ends, die die SAN-Storage-Treiber verwenden, kann Astra Trident bidirektionales CHAP einrichten und CHAP-Benutzernamen und -Schlüssel über managen `tridentctl`. Siehe "Hier" Um zu erfahren, wie Astra Trident CHAP auf ONTAP Back-Ends konfiguriert.

CHAP-Unterstützung für ONTAP-Back-Ends ist mit Trident 20.04 und höher verfügbar.

Verwenden Sie CHAP-Authentifizierung mit NetApp HCI und SolidFire Back-Ends

NetApp empfiehlt die Implementierung von bidirektionalem CHAP, um die Authentifizierung zwischen einem Host und den NetApp HCI und SolidFire Back-Ends zu gewährleisten. Astra Trident verwendet ein geheimes Objekt mit zwei CHAP-Passwörtern pro Mandant. Wenn Trident als CSI-bereitstellung installiert wird, verwaltet es die CHAP-Geheimnisse und speichert sie in einem `tridentvolume` CR-Objekt für das jeweilige PV. Beim Erstellen eines PV verwendet CSI Astra Trident die CHAP-Schlüssel, um eine iSCSI-Sitzung zu initiieren und über CHAP mit dem NetApp HCI- und SolidFire-System zu kommunizieren.

Die von CSI Trident erstellten Volumes werden keiner Volume Access Group zugeordnet.

Im nicht-CSI-Frontend wird die Anbindung von Volumes als Geräte auf den Worker-Nodes durch Kubernetes übernommen. Nach der Volume-Erstellung ruft Astra Trident die API zum NetApp HCI/SolidFire System auf, um die Geheimnisse zu rufen, falls das Geheimnis für diesen Mandanten nicht bereits vorhanden ist. Astra Trident leitet die Geheimnisse an Kubernetes weiter. Das Kubelet, das sich auf jedem Node befindet, greift über die Kubernetes API auf die Geheimnisse zu und verwendet sie zum Ausführen/Aktivieren von CHAP zwischen jedem Node, der auf das Volume zugreift, und dem NetApp HCI/SolidFire System, in dem sich die Volumes befinden.

Nutzen Sie Astra Trident mit NVE und NAE

NetApp ONTAP bietet Verschlüsselung ruhender Daten zum Schutz sensibler Daten, wenn eine Festplatte gestohlen, zurückgegeben oder einer neuen Verwendung zugewiesen wird. Weitere Informationen finden Sie unter "NetApp Volume Encryption Übersicht konfigurieren".

- Wenn NAE auf dem Backend aktiviert ist, wird jedes im Astra Trident bereitgestellte Volume NAE-aktiviert.
- Wenn NAE im Backend nicht aktiviert ist, wird jedes in Astra Trident bereitgestellte Volume mit NVE aktiviert, es sei denn, Sie setzen das NVE-Verschlüsselungsflag auf `false` Bei der Back-End-Konfiguration:

> Volumes, die in Astra Trident auf einem NAE-fähigen Back-End erstellt werden, müssen NVE oder NAE-verschlüsselt sein.
>
> - Sie können das NVE-Verschlüsselungsflag auf einstellen `true` In der Trident-Back-End-Konfiguration können Sie die NAE-Verschlüsselung außer Kraft setzen und für jedes Volume einen bestimmten Verschlüsselungsschlüssel verwenden.
> - Setzen des NVE-Verschlüsselungsfahne auf `false` Auf einem NAE-fähigen Back-End wird ein NAE-fähiges Volume erstellt. Sie können die NAE-Verschlüsselung nicht deaktivieren, indem Sie das NVE-Verschlüsselungsfahne auf setzen `false`.

- Sie können in Astra Trident manuell ein NVE-Volume erstellen, indem Sie explizit das NVE-Verschlüsselungsflag auf festlegen `true`.

Weitere Informationen zu Back-End-Konfigurationsoptionen finden Sie unter:

- "ONTAP SAN-Konfigurationsoptionen"
- "NAS-Konfigurationsoptionen von ONTAP"

Linux Unified Key Setup (LUKS)

Sie können Linux Unified Key Setup (LUKS) aktivieren, um ONTAP SAN und ONTAP SAN ECONOMY Volumes auf Astra Trident zu verschlüsseln. Astra Trident unterstützt die Rotation von Passphrase und die Volume-Erweiterung für LUKS-verschlüsselte Volumes.

In Astra Trident verwenden LUKS-verschlüsselte Volumen den aes-xts-plain64 Zypher und den Modus, wie von empfohlen "NIST".

Bevor Sie beginnen

- Worker Nodes müssen cryptsetup 2.1 oder höher (aber unter 3.0) installiert sein. Weitere Informationen finden Sie unter "Gitlab: Cryptsetup".
- Aus Performance-Gründen wird empfohlen, dass Arbeiterknoten Advanced Encryption Standard New Instructions (AES-NI) unterstützen. Führen Sie den folgenden Befehl aus, um die Unterstützung von AES-NI zu überprüfen:

```
grep "aes" /proc/cpuinfo
```

Wenn nichts zurückgegeben wird, unterstützt Ihr Prozessor nicht AES-NI. Weitere Informationen zu AES-NI finden Sie unter: "Intel: Advanced Encryption Standard Instructions (AES-NI)".

Aktivieren Sie die LUKS-Verschlüsselung

Sie können die Verschlüsselung auf Host-Seite pro Volume mithilfe von Linux Unified Key Setup (LUKS) für ONTAP SAN und ONTAP SAN ECONOMY Volumes aktivieren.

Schritte

1. Definieren Sie LUKS-Verschlüsselungsattribute in der Backend-Konfiguration. Weitere Informationen zu den Back-End-Konfigurationsoptionen für ONTAP SAN finden Sie unter "ONTAP SAN-Konfigurationsoptionen".

```
"storage": [
    {
        "labels":{"luks": "true"},
        "zone":"us_east_1a",
        "defaults": {
            "luksEncryption": "true"
        }
    },
    {
        "labels":{"luks": "false"},
        "zone":"us_east_1a",
        "defaults": {
            "luksEncryption": "false"
        }
    },
]
```

2. Nutzung `parameters.selector` So definieren Sie die Speicherpools mit LUKS-Verschlüsselung. Beispiel:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: luks
provisioner: netapp.io/trident
parameters:
  selector: "luks=true"
  csi.storage.k8s.io/node-stage-secret-name: luks-${pvc.name}
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
```

3. Erstellen Sie ein Geheimnis, das die LUKS-Passphrase enthält. Beispiel:

```
kubectl -n trident create -f luks-pvc1.yaml
apiVersion: v1
kind: Secret
metadata:
  name: luks-pvc1
stringData:
  luks-passphrase-name: A
  luks-passphrase: secretA
```

Einschränkungen

LUKS-verschlüsselte Volumes können die ONTAP Deduplizierung und Komprimierung nicht nutzen.

Eine LUKS-Passphrase drehen

Sie können die LUKS-Passphrase drehen und die Drehung bestätigen.

> Vergessen Sie keine Passphrase, bis Sie überprüft haben, dass sie nicht mehr von einem Volume, einem Snapshot oder einem geheimen Schlüssel referenziert wird. Wenn eine referenzierte Passphrase verloren geht, können Sie das Volume möglicherweise nicht mounten und die Daten bleiben verschlüsselt und unzugänglich.

Über diese Aufgabe

DIE Drehung der LUKS-Passphrase erfolgt, wenn ein Pod, das das Volume bindet, nach der Angabe einer neuen LUKS-Passphrase erstellt wird. Bei der Erstellung eines neuen Pods vergleicht Astra Trident die LUKS-Passphrase auf dem Volume mit der aktiven Passphrase im Geheimnis.

- Wenn die Passphrase auf dem Volume nicht mit der aktiven Passphrase im Geheimnis übereinstimmt, erfolgt die Drehung.
- Wenn die Passphrase auf dem Volume mit der aktiven Passphrase im Geheimnis übereinstimmt, wird das angezeigt `previous-luks-passphrase` Parameter wird ignoriert.

Schritte

1. Fügen Sie die hinzu `node-publish-secret-name` Und `node-publish-secret-namespace` StorageClass-Parameter. Beispiel:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: csi-san
provisioner: csi.trident.netapp.io
parameters:
  trident.netapp.io/backendType: "ontap-san"
  csi.storage.k8s.io/node-stage-secret-name: luks
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
  csi.storage.k8s.io/node-publish-secret-name: luks
  csi.storage.k8s.io/node-publish-secret-namespace: ${pvc.namespace}
```

2. Identifizieren Sie vorhandene Passphrases auf dem Volume oder Snapshot.

Datenmenge

```
tridentctl -d get volume luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>

...luksPassphraseNames:["A"]
```

Snapshot

```
tridentctl -d get snapshot luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>/<snapshotID>

...luksPassphraseNames:["A"]
```

3. Aktualisieren Sie das LUKS-Geheimnis für das Volume, um die neuen und vorherigen Passphrases anzugeben. Unbedingt `previous-luke-passphrase-name` Und `previous-luks-passphrase` Übereinstimmung mit der vorherigen Passphrase.

```
apiVersion: v1
kind: Secret
metadata:
  name: luks-pvc1
stringData:
  luks-passphrase-name: B
  luks-passphrase: secretB
  previous-luks-passphrase-name: A
  previous-luks-passphrase: secretA
```

4. Erstellen Sie einen neuen Pod, der das Volume montiert. Dies ist erforderlich, um die Rotation zu initiieren.
5. Überprüfen Sie, ob die Passphrase gedreht wurde.

Datenmenge

```
tridentctl -d get volume luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>

...luksPassphraseNames:["B"]
```

Snapshot

```
tridentctl -d get snapshot luks-pvc1
GET http://127.0.0.1:8000/trident/v1/volume/<volumeID>/<snapshotID>

...luksPassphraseNames:["B"]
```

Ergebnisse

Die Passphrase wurde gedreht, wenn nur die neue Passphrase auf dem Volume und dem Snapshot zurückgegeben wird.

> Werden beispielsweise zwei Passphrases zurückgegeben `luksPassphraseNames: ["B", "A"]`, Die Rotation ist unvollständig. Sie können einen neuen Pod auslösen, um zu versuchen, die Rotation abzuschließen.

Aktivieren Sie die Volume-Erweiterung

Sie können Volume-Erweiterung auf einem LUKS-verschlüsselten Volume aktivieren.

Schritte

1. Aktivieren Sie die `CSINodeExpandSecret` Funktionstor (Beta 1.25+). Siehe "Kubernetes 1.25: Verwenden Sie Secrets zur Node-gesteuerten Erweiterung von CSI Volumes" Entsprechende Details.
2. Fügen Sie die hinzu `node-expand-secret-name` Und `node-expand-secret-namespace` StorageClass-Parameter. Beispiel:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: luks
provisioner: netapp.io/trident
parameters:
  selector: "luks=true"
  csi.storage.k8s.io/node-stage-secret-name: luks-${pvc.name}
  csi.storage.k8s.io/node-stage-secret-namespace: ${pvc.namespace}
  csi.storage.k8s.io/node-expand-secret-name: luks-${pvc.name}
  csi.storage.k8s.io/node-expand-secret-namespace: ${pvc.namespace}
allowVolumeExpansion: true
```

Ergebnisse

Wenn Sie die Online-Speichererweiterung initiieren, gibt das Kubelet die entsprechenden Zugangsdaten an den Treiber weiter.