Methoden der Sicherheits-API

Element Software

NetApp
November 18, 2025

Inhalt

Methoden der Sicherheits-API

AddKeyServerToProviderKmip

Sie können die `AddKeyServerToProviderKmip` Methode zur Zuordnung eines KMIP-Schlüsselservers (Key Management Interoperability Protocol) zu dem angegebenen Schlüsselanbieter. Während der Zuweisung wird der Server kontaktiert, um die Funktionalität zu überprüfen. Wenn der angegebene Schlüsselserver bereits dem angegebenen Schlüsselanbieter zugewiesen ist, wird keine Aktion ausgeführt und es wird kein Fehler zurückgegeben. Sie können die Zuweisung mithilfe der folgenden Methode entfernen: `RemoveKeyServerFromProviderKmip` Verfahren.

Parameter

Diese Methode hat die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
keyProviderID	Die ID des Schlüsselanbieters, dem der Schlüsselserver zugewiesen werden soll.	ganze Zahl	Keine	Ja
SchlüsselServerID	Die ID des zuzuweisenden Schlüsselservers.	ganze Zahl	Keine	Ja

Rückgabewerte

Diese Methode hat keinen Rückgabewert. Die Aufgabe gilt als erfolgreich, solange kein Fehler zurückgegeben wird.

Anforderungsbeispiel

Anfragen für diese Methode ähneln dem folgenden Beispiel:

```
{
  "method": "AddKeyServerToProviderKmip",
  "params": {
    "keyProviderID": 1,
    "keyServerID": 15
    },
"id": 1
}
```

Antwortbeispiel

Diese Methode liefert eine Antwort, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result":
      {}
    }
}
```

Neu seit Version

11,7

CreateKeyProviderKmip

Sie können die `CreateKeyProviderKmip` Methode zum Erstellen eines KMIP-Schlüsselanbieters (Key Management Interoperability Protocol) mit dem angegebenen Namen. Ein Schlüsselanbieter definiert einen Mechanismus und einen Speicherort zum Abrufen von Authentifizierungsschlüsseln. Wenn Sie einen neuen KMIP-Schlüsselanbieter erstellen, sind diesem keine KMIP-Schlüsselserver zugewiesen. Um einen KMIP-Schlüsselserver zu erstellen, verwenden Sie den `CreateKeyServerKmip` Verfahren. Um es einem Anbieter zuzuordnen, siehe `AddKeyServerToProviderKmip` Die

Parameter

Diese Methode hat die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
keyProviderName	Der Name, der dem erstellten KMIP-Schlüsselanbieter zugeordnet werden soll. Dieser Name dient nur zu Darstellungszwecken und muss nicht eindeutig sein.	Schnur	Keine	Ja

Rückgabewerte

Diese Methode hat die folgenden Rückgabewerte:

Name	Beschreibung	Typ

kmipKeyProvider	Ein Objekt, das Details zum neu erstellten Schlüsselanbieter enthält.	"KeyProviderKmip"

Anforderungsbeispiel

Anfragen für diese Methode ähneln dem folgenden Beispiel:

```
{
  "method": "CreateKeyProviderKmip",
  "params": {
    "keyProviderName": "ProviderName",
    },
"id": 1
}
```

Antwortbeispiel

Diese Methode liefert eine Antwort, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result":
      {
    "kmipKeyProvider": {
        "keyProviderName": "ProviderName",
        "keyProviderIsActive": true,
        "kmipCapabilities": "SSL",
        "keyServerIDs": [
            15
        ],
        "keyProviderID": 1
    }
}
}
```

Neu seit Version

11,7

CreateKeyServerKmip

Sie können die `CreateKeyServerKmip` Methode zum Erstellen eines KMIP-Schlüsselservers (Key Management Interoperability Protocol) mit den angegebenen Attributen. Bei der Erstellung wird der Server nicht kontaktiert; er muss vor der

Anwendung dieser Methode nicht existieren. Bei Cluster-Key-Server-Konfigurationen müssen Sie die Hostnamen oder IP-Adressen aller Serverknoten im Parameter kmipKeyServerHostnames angeben. Sie können die `TestKeyServerKmip` Methode zum Testen eines Schlüsselservers.

Parameter

Diese Methode hat die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
kmipCaCertificate	Das öffentliche Schlüsselzertifikat der Stammzertifizierungsstelle des externen Schlüsselservers. Dies dient der Überprüfung des vom externen Schlüsselserver im Rahmen der TLS-Kommunikation vorgelegten Zertifikats. Für wichtige Servercluster, bei denen einzelne Server unterschiedliche Zertifizierungsstellen verwenden, geben Sie eine verkettete Zeichenkette an, die die Stammzertifikate aller Zertifizierungsstellen enthält.	Schnur	Keine	Ja
kmipClientCertificate	Ein im PEM-Format Base64-kodiertes PKCS#10 X.509-Zertifikat, das vom Solidfire KMIP-Client verwendet wird.	Schnur	Keine	Ja

Name	Beschreibung	Typ	Standardwert	Erforderlich
kmipKeyServerHostnames	Array der Hostnamen oder IP-Adressen, die diesem KMIP-Schlüsselserver zugeordnet sind. Mehrere Hostnamen oder IP-Adressen müssen nur dann angegeben werden, wenn sich die Schlüsselserver in einer Clusterkonfiguration befinden.	Zeichenketten-Array	Keine	Ja
kmipKeyServerName	Der Name des KMIP-Schlüsselservers. Dieser Name dient nur zu Darstellungszwecken und muss nicht eindeutig sein.	Schnur	Keine	Ja
kmipKeyServerPort	Die Portnummer, die diesem KMIP-Schlüsselserver zugeordnet ist (typischerweise 5696).	ganze Zahl	Keine	Nein

Rückgabewerte

Diese Methode hat die folgenden Rückgabewerte:

Name	Beschreibung	Typ
kmipKeyServer	Ein Objekt, das Details über den neu erstellten Schlüsselserver enthält.	"KeyServerKmip"

Anforderungsbeispiel

Anfragen für diese Methode ähneln dem folgenden Beispiel:

```
{
  "method": "CreateKeyServerKmip",
  "params": {
    "kmipCaCertificate": "MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/E...",
    "kmipClientCertificate": "dKkkirWmnWXbj9T/UWZYB2oK0z5...",
    "kmipKeyServerHostnames" : ["server1.hostname.com",
"server2.hostname.com"],
    "kmipKeyServerName" : "keyserverName",
    "kmipKeyServerPort" : 5696
  },
"id": 1
}
```

Antwortbeispiel

Diese Methode liefert eine Antwort, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result":
      {
        "kmipKeyServer": {
            "kmipCaCertificate":"MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/E...",
            "kmipKeyServerHostnames":[
                "server1.hostname.com", "server2.hostname.com"
            ],
            "keyProviderID":1,
            "kmipKeyServerName":"keyserverName",
            "keyServerID":1
            "kmipKeyServerPort":1,
            "kmipClientCertificate":"dKkkirWmnWXbj9T/UWZYB2oK0z5...",
            "kmipAssignedProviderIsActive":true
        }
    }
}
```

Neu seit Version

11,7

Öffentliches/Privates Schlüsselpaar erstellen

Sie können die `CreatePublicPrivateKeyPair` Methode zum Erstellen öffentlicher und privater SSL-Schlüssel. Sie können diese Schlüssel verwenden, um

Zertifikatsignierungsanforderungen zu generieren. Für jeden Speichercluster kann nur ein Schlüsselpaar verwendet werden. Bevor Sie diese Methode zum Ersetzen vorhandener Schlüssel anwenden, vergewissern Sie sich, dass die Schlüssel von keinem Anbieter mehr verwendet werden.

Parameter

Diese Methode hat die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
allgemeiner Name	Das X.509 Distinguished Name **Common Name** -Feld (CN).	Schnur	Keine	Nein
Land	Das X.509 Distinguished Name Feld **Country** ©.	Schnur	Keine	Nein
E-Mail-Adresse	Das X.509 Distinguished Name Feld **E-Mail-Adresse** (MAIL).	Schnur	Keine	Nein
Ort	Das X.509 Distinguished Name Feld **Locality Name** (L).	Schnur	Keine	Nein
Organisation	Das X.509 Distinguished Name Feld **Organisationsname** (O).	Schnur	Keine	Nein
Organisationseinheit	Das X.509 Distinguished Name Feld **Organisationseinheitsname** (OU).	Schnur	Keine	Nein
Zustand	Das X.509 Distinguished Name Feld **State** oder **Province Name** (ST oder SP oder S).	Schnur	Keine	Nein

Rückgabewerte

Diese Methode hat keinen Rückgabewert. Wenn kein Fehler auftritt, gilt die Schlüsselerstellung als erfolgreich.

Anforderungsbeispiel

Anfragen für diese Methode ähneln dem folgenden Beispiel:

```
{
  "method": "CreatePublicPrivateKeyPair",
  "params": {
    "commonName": "Name",
    "country": "US",
    "emailAddress" : "email@domain.com"
   },
"id": 1
}
```

Antwortbeispiel

Diese Methode liefert eine Antwort, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result":
      {}
}
```

Neu seit Version

11,7

DeleteKeyProviderKmip

Sie können die `DeleteKeyProviderKmip` Methode zum Löschen des angegebenen inaktiven KMIP-Schlüsselanbieters (Key Management Interoperability Protocol).

Parameter

Diese Methode hat die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
keyProviderID	Die ID des zu löschenden Schlüsselanbieters.	ganze Zahl	Keine	Ja

Rückgabewerte

Diese Methode hat keinen Rückgabewert. Der Löschvorgang gilt als erfolgreich, solange kein Fehler auftritt.

Anforderungsbeispiel

Anfragen für diese Methode ähneln dem folgenden Beispiel:

```
{
  "method": "DeleteKeyProviderKmip",
  "params": {
    "keyProviderID": "1"
    },
"id": 1
}
```

Antwortbeispiel

Diese Methode liefert eine Antwort, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result":
      {}
}
```

Neu seit Version

11,7

DeleteKeyServerKmip

Sie können die `DeleteKeyServerKmip` Methode zum Löschen eines vorhandenen KMIP-Schlüsselservers (Key Management Interoperability Protocol). Sie können einen Schlüsselserver löschen, es sei denn, es handelt sich um den letzten, der seinem Anbieter zugewiesen wurde, und dieser Anbieter stellt Schlüssel bereit, die derzeit in Gebrauch sind.

Parameter

Diese Methode hat die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SchlüsselServerID	Die ID des zu löschenden KMIP-Schlüsselservers.	ganze Zahl	Keine	Ja

Rückgabewerte

Diese Methode hat keinen Rückgabewert. Der Löschvorgang gilt als erfolgreich, wenn keine Fehler auftreten.

Anforderungsbeispiel

Anfragen für diese Methode ähneln dem folgenden Beispiel:

```
{
  "method": "DeleteKeyServerKmip",
  "params": {
     "keyServerID": 15
  },
"id": 1
}
```

Antwortbeispiel

Diese Methode liefert eine Antwort, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result":
      {}
}
```

Neu seit Version

11,7

DisableEncryptionAtRest

Sie können die `DisableEncryptionAtRest` Methode zum Entfernen der zuvor auf den Cluster angewendeten Verschlüsselung mithilfe der `EnableEncryptionAtRest` Verfahren. Diese Deaktivierungsmethode ist asynchron und gibt eine Antwort zurück, bevor die Verschlüsselung deaktiviert wird. Sie können die `GetClusterInfo` Methode, um das System abzufragen und festzustellen, wann der Prozess abgeschlossen ist.

- Mit dieser Methode lässt sich die Softwareverschlüsselung im Ruhezustand nicht deaktivieren. Um die Softwareverschlüsselung im Ruhezustand zu deaktivieren, müssen Sie"Einen neuen Cluster erstellen" mit deaktivierter Softwareverschlüsselung im Ruhezustand.
- Um den aktuellen Status der Verschlüsselung ruhender Daten, der Softwareverschlüsselung ruhender Daten oder beider im Cluster anzuzeigen, verwenden Sie die "Methode zum Abrufen von Clusterinformationen"Die Sie können die `GetSoftwareEncryptionAtRestInfo` "Methode zum Abrufen von Informationen, die der Cluster zur Verschlüsselung ruhender Daten verwendet"Die

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode hat keinen Rückgabewert.

Anforderungsbeispiel

Anfragen für diese Methode ähneln dem folgenden Beispiel:

```
{
   "method": "DisableEncryptionAtRest",
   "params": {},
   "id": 1
}
```

Antwortbeispiel

Diese Methode liefert eine Antwort, die dem folgenden Beispiel ähnelt:

```
{
   "id" : 1,
  "result" : {}
}
```

Neu seit Version

9,6

Weitere Informationen

- "GetClusterInfo"
- "SolidFire und Element-Softwaredokumentation"
- "Dokumentation für frühere Versionen der NetApp SolidFire und Element-Produkte"

EnableEncryptionAtRest

Sie können die `EnableEncryptionAtRest` Methode zur Aktivierung der Advanced Encryption Standard (AES) 256-Bit-Verschlüsselung ruhender Daten im Cluster, damit der Cluster den für die Laufwerke auf jedem Knoten verwendeten Verschlüsselungsschlüssel verwalten kann. Diese Funktion ist nicht standardmäßig aktiviert.

- Um den aktuellen Status der Verschlüsselung ruhender Daten und/oder der Softwareverschlüsselung ruhender Daten auf dem Cluster anzuzeigen, verwenden Sie die"Methode zum Abrufen von Clusterinformationen" Die Sie können die `GetSoftwareEncryptionAtRestInfo` "Methode zum Abrufen von Informationen, die der Cluster zur Verschlüsselung ruhender Daten verwendet"Die
- Diese Methode ermöglicht keine Softwareverschlüsselung im Ruhezustand. Dies kann nur mit Hilfe des/der"Methode zum Erstellen von Clustern" mit `enableSoftwareEncryptionAtRest` eingestellt auf `true` Die

Wenn Sie die Verschlüsselung ruhender Daten aktivieren, verwaltet der Cluster die Verschlüsselungsschlüssel für die Laufwerke auf jedem Knoten im Cluster automatisch intern.

Wenn eine keyProviderID angegeben wird, wird das Passwort entsprechend dem Typ des Schlüsselanbieters generiert und abgerufen. Dies geschieht üblicherweise mithilfe eines KMIP-Schlüsselservers (Key Management Interoperability Protocol), wenn ein KMIP-Schlüsselanbieter verwendet wird. Nach diesem Vorgang gilt der angegebene Provider als aktiv und kann erst gelöscht werden, wenn die Verschlüsselung ruhender Daten deaktiviert wird. `DisableEncryptionAtRest` Verfahren.

Wenn Sie einen Knotentyp mit einer Modellnummer haben, die auf "-NE" endet, `EnableEncryptionAtRest` Der Methodenaufruf schlägt mit der Antwort "Verschlüsselung nicht erlaubt" fehl. „Cluster hat einen nicht verschlüsselbaren Knoten erkannt.“

Die Verschlüsselung sollte nur dann aktiviert oder deaktiviert werden, wenn der Cluster läuft und sich in einem fehlerfreien Zustand befindet. Sie können die Verschlüsselung nach eigenem Ermessen und so oft wie nötig aktivieren oder deaktivieren.

Dieser Prozess ist asynchron und liefert eine Antwort, bevor die Verschlüsselung aktiviert wird. Sie können die `GetClusterInfo` Methode, um das System abzufragen und festzustellen, wann der Prozess abgeschlossen ist.

Parameter

Diese Methode hat die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
keyProviderID	Die ID eines zu verwendenden KMIP-Schlüsselanbieters.	ganze Zahl	Keine	Nein

Rückgabewerte

Diese Methode hat keinen Rückgabewert.

Anforderungsbeispiel

Anfragen für diese Methode ähneln dem folgenden Beispiel:

```
{
   "method": "EnableEncryptionAtRest",
   "params": {},
   "id": 1
}
```

Antwortbeispiele

Diese Methode liefert eine Antwort, die dem folgenden Beispiel der Methode EnableEncryptionAtRest ähnelt. Es gibt kein Ergebnis zu berichten.

```
{
   "id": 1,
   "result": {}
}
```

Während die Verschlüsselung ruhender Daten auf einem Cluster aktiviert wird, gibt GetClusterInfo ein Ergebnis zurück, das den Status der Verschlüsselung ruhender Daten ("encryptionAtRestState") als "aktiviert" beschreibt. Sobald die Verschlüsselung ruhender Daten vollständig aktiviert ist, ändert sich der zurückgegebene Status in „aktiviert“.

```
{
   "id": 1,
      "result": {
         "clusterInfo": {
            "attributes": { },
               "encryptionAtRestState": "enabling",
            "ensemble": [
               "10.10.5.94",
               "10.10.5.107",
               "10.10.5.108"
            ],
            "mvip": "192.168.138.209",
            "mvipNodeID": 1,
            "name": "Marshall",
            "repCount": 2,
            "svip": "10.10.7.209",
            "svipNodeID": 1,
            "uniqueID": "91dt"
      }
   }
}
```


Neu seit Version

9,6

Weitere Informationen

- "SecureEraseDrives"
- "GetClusterInfo"
- "SolidFire und Element-Softwaredokumentation"
- "Dokumentation für frühere Versionen der NetApp SolidFire und Element-Produkte"

GetClientCertificateSignRequest

Sie können die `GetClientCertificateSignRequest` Methode zur Generierung einer Zertifikatsignierungsanforderung, die von einer Zertifizierungsstelle signiert werden kann, um ein Clientzertifikat für den Cluster zu generieren. Signierte Zertifikate sind erforderlich, um eine Vertrauensbeziehung für die Interaktion mit externen Diensten herzustellen.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode hat die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Clientzertifikatsignierungsanfrage	Eine PEM-formatierte, Base64-kodierte PKCS#10 X.509 Clientzertifikatsignaturanforderung.	Schnur

Anforderungsbeispiel

Anfragen für diese Methode ähneln dem folgenden Beispiel:

```
{
  "method": "GetClientCertificateSignRequest",
  "params": {
  },
"id": 1
}
```

Antwortbeispiel

Diese Methode liefert eine Antwort, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result":
      {
        "clientCertificateSignRequest":
"MIIByjCCATMCAQAwgYkxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybm..."
   }
}
```

Neu seit Version

11,7

GetKeyProviderKmip

Sie können die `GetKeyProviderKmip` Methode zum Abrufen von Informationen über den angegebenen KMIP-Schlüsselanbieter (Key Management Interoperability Protocol).

Parameter

Diese Methode hat die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
keyProviderID	Die ID des zurückzugebenden KMIP-Schlüsselanbieterobjekts.	ganze Zahl	Keine	Ja

Rückgabewerte

Diese Methode hat die folgenden Rückgabewerte:

Name	Beschreibung	Typ
kmipKeyProvider	Ein Objekt, das Details zum angeforderten Schlüsselanbieter enthält.	"KeyProviderKmip"

Anforderungsbeispiel

Anfragen für diese Methode ähneln dem folgenden Beispiel:

```
{
  "method": "GetKeyProviderKmip",
  "params": {
    "keyProviderID": 15
    },
"id": 1
}
```

Antwortbeispiel

Diese Methode liefert eine Antwort, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result":
    {
    "kmipKeyProvider": {
        "keyProviderID": 15,
        "kmipCapabilities": "SSL",
        "keyProviderIsActive": true,
        "keyServerIDs": [
            1
        ],
        "keyProviderName": "ProviderName"
    }
   }
}
```

Neu seit Version

11,7

GetKeyServerKmip

Sie können die `GetKeyServerKmip` Methode zur Rückgabe von Informationen über den angegebenen KMIP-Schlüsselserver (Key Management Interoperability Protocol).

Parameter

Diese Methode hat die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SchlüsselServerID	Die ID des KMIP-Schlüsselservers, über den Informationen zurückgegeben werden sollen.	ganze Zahl	Keine	Ja

Rückgabewerte

Diese Methode hat die folgenden Rückgabewerte:

Name	Beschreibung	Typ
kmipKeyServer	Ein Objekt, das Details zum angeforderten Schlüsselserver enthält.	"KeyServerKmip"

Anforderungsbeispiel

Anfragen für diese Methode ähneln dem folgenden Beispiel:

```
{
  "method": "GetKeyServerKmip",
  "params": {
     "keyServerID": 15
  },
"id": 1
}
```

Antwortbeispiel

Diese Methode liefert eine Antwort, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result":
      {
        "kmipKeyServer": {
            "kmipCaCertificate":"MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/E...",
            "kmipKeyServerHostnames":[
                "server1.hostname.com", "server2.hostname.com"
            ],
            "keyProviderID":1,
            "kmipKeyServerName":"keyserverName",
            "keyServerID":15
            "kmipKeyServerPort":1,
            "kmipClientCertificate":"dKkkirWmnWXbj9T/UWZYB2oK0z5...",
            "kmipAssignedProviderIsActive":true
        }
    }
}
```

Neu seit Version

11,7

GetSoftwareEncryptionAtRestInfo

Sie können die `GetSoftwareEncryptionAtRestInfo` Methode zum Abrufen von Informationen über die Softwareverschlüsselung im Ruhezustand, die der Cluster zur Verschlüsselung ruhender Daten verwendet.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode hat die folgenden Rückgabewerte:

Parameter	Beschreibung	Typ	Optional
MasterkeyInfo	Informationen zum aktuellen Hauptschlüssel für die Softwareverschlüsselung im Ruhezustand.	EncryptionKeyInfo	WAHR
rekeyMasterKeyAsyncResultID	Die asynchrone Ergebnis-ID der aktuellen oder letzten Schlüsselaktualisierungsoperation (falls vorhanden), sofern diese noch nicht gelöscht wurde. `GetAsyncResult` Die Ausgabe wird Folgendes enthalten: `newKey` Feld, das Informationen über den neuen Hauptschlüssel und einen enthält `keyToDecommission` Feld, das Informationen über den alten Schlüssel enthält.	ganze Zahl	WAHR
Zustand	Der aktuelle Stand der Softwareverschlüsselung im Ruhezustand. Mögliche Werte sind `disabled` oder `enabled` Die	Schnur	FALSCH
Version	Eine Versionsnummer, die jedes Mal erhöht wird, wenn die Softwareverschlüsselung im Ruhezustand aktiviert wird.	ganze Zahl	FALSCH

Anforderungsbeispiel

Anfragen für diese Methode ähneln dem folgenden Beispiel:

```
{
 "method": "getsoftwareencryptionatrestinfo"
}
```

Antwortbeispiel

Diese Methode liefert eine Antwort, die dem folgenden Beispiel ähnelt:

```
{
    "id": 1,
    "result": {
        "masterKeyInfo": {
            "keyCreatedTime": "2021-09-20T23:15:56Z",
            "keyID": "4d80a629-a11b-40ab-8b30-d66dd5647cfd",
            "keyManagementType": "internal"
        },
        "state": "enabled",
        "version": 1
    }
}
```

Neu seit Version

12,3

Weitere Informationen

- "SolidFire und Element-Softwaredokumentation"
- "Dokumentation für frühere Versionen der NetApp SolidFire und Element-Produkte"

ListKeyProvidersKmip

Sie können die `ListKeyProvidersKmip` Methode zum Abrufen einer Liste aller vorhandenen Key Management Interoperability Protocol (KMIP)-Schlüsselanbieter. Sie können die Liste filtern, indem Sie zusätzliche Parameter angeben.

Parameter

Diese Methode hat die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
keyProviderIsActive	Die Filter gaben KMIP-Schlüsselserverobjekte basierend auf deren Aktivitätsstatus zurück. Mögliche Werte: • true: Gibt nur aktive KMIP-Schlüsselanbieter zurück (die Schlüssel bereitstellen, die aktuell verwendet werden). • false: Gibt nur KMIP-Schlüsselanbieter zurück, die inaktiv sind (keine Schlüssel bereitstellen und gelöscht werden können). Wenn die Angabe weggelassen wird, werden die zurückgegebenen KMIP-Schlüsselanbieter nicht danach gefiltert, ob sie aktiv sind.	boolescher Wert	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
kmipKeyProviderHasServerAssigned	Die Filter gaben KMIP-Schlüsselanbieter basierend darauf zurück, ob ihnen ein KMIP-Schlüsselserver zugewiesen ist. Mögliche Werte: • true: Gibt nur KMIP-Schlüsselanbieter zurück, denen ein KMIP-Schlüsselserver zugewiesen ist. • false: Gibt nur KMIP-Schlüsselanbieter zurück, denen kein KMIP-Schlüsselserver zugewiesen ist. Wird dieser Parameter weggelassen, werden die zurückgegebenen KMIP-Schlüsselanbieter nicht danach gefiltert, ob ihnen ein KMIP-Schlüsselserver zugewiesen ist.	boolescher Wert	Keine	Nein

Rückgabewerte

Diese Methode hat die folgenden Rückgabewerte:

Name	Beschreibung	Typ
kmipKeyProviders	Eine Liste der erstellten KMIP-Schlüsselanbieter.	"KeyProviderKmip"Array

Anforderungsbeispiel

Anfragen für diese Methode ähneln dem folgenden Beispiel:

```
{
  "method": "ListKeyProvidersKmip",
  "params": {},
"id": 1
}
```

Antwortbeispiel

Diese Methode liefert eine Antwort, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result":
    {
    "kmipKeyProviders": [
        {
            "keyProviderID": 15,
            "kmipCapabilities": "SSL",
            "keyProviderIsActive": true,
            "keyServerIDs": [
                1
            ],
            "keyProviderName": "KeyProvider1"
        }
    ]
}
}
```

Neu seit Version

11,7

ListKeyServersKmip

Sie können die `ListKeyServersKmip` Methode zum Auflisten aller erstellten Key Management Interoperability Protocol (KMIP)-Schlüsselserver. Sie können die Ergebnisse filtern, indem Sie zusätzliche Parameter angeben.

Parameter

Diese Methode hat die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
keyProviderID	Wenn angegeben, gibt die Methode nur KMIP-Schlüsselserver zurück, die dem angegebenen KMIP-Schlüsselanbieter zugeordnet sind. Wird dieser Parameter weggelassen, werden die zurückgegebenen KMIP-Schlüsselserver nicht danach gefiltert, ob sie dem angegebenen KMIP-Schlüsselanbieter zugeordnet sind.	ganze Zahl	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
kmipAssignedProviderIsActive	Die Filter gaben KMIP-Schlüsselserverobjekte basierend auf deren Aktivitätsstatus zurück. Mögliche Werte: • true: Gibt nur aktive KMIP-Schlüsselserver zurück (die Schlüssel bereitstellen, die aktuell verwendet werden). • false: Gibt nur KMIP-Schlüsselserver zurück, die inaktiv sind (keine Schlüssel bereitstellen und gelöscht werden können). Wenn die Angabe weggelassen wird, werden die zurückgegebenen KMIP-Schlüsselserver nicht danach gefiltert, ob sie aktiv sind.	boolescher Wert	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
kmipHasProviderAssigned	Die Filter gaben KMIP-Schlüsselserver basierend darauf zurück, ob ihnen ein KMIP-Schlüsselanbieter zugewiesen ist. Mögliche Werte: • true: Gibt nur KMIP-Schlüsselserver zurück, denen ein KMIP-Schlüsselanbieter zugewiesen ist. • false: Gibt nur KMIP-Schlüsselserver zurück, denen kein KMIP-Schlüsselanbieter zugewiesen ist. Wird dieser Parameter weggelassen, werden die zurückgegebenen KMIP-Schlüsselserver nicht danach gefiltert, ob ihnen ein KMIP-Schlüsselanbieter zugewiesen ist.	boolescher Wert	Keine	Nein

Rückgabewerte

Diese Methode hat die folgenden Rückgabewerte:

Name	Beschreibung	Typ
kmipKeyServers	Die vollständige Liste der erstellten KMIP-Schlüsselserver.	"KeyServerKmip"Array

Anforderungsbeispiel

Anfragen für diese Methode ähneln dem folgenden Beispiel:

```
{
  "method": "ListKeyServersKmip",
  "params": {},
"id": 1
}
```

Antwortbeispiel

Diese Methode liefert eine Antwort, die dem folgenden Beispiel ähnelt:

```
{
    "kmipKeyServers": [
        {
            "kmipKeyServerName": "keyserverName",
            "kmipClientCertificate": "dKkkirWmnWXbj9T/UWZYB2oK0z5...",
            "keyServerID": 15,
            "kmipAssignedProviderIsActive": true,
            "kmipKeyServerPort": 5696,
            "kmipCaCertificate": "MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/E...",
            "kmipKeyServerHostnames": [
                "server1.hostname.com", "server2.hostname.com"
            ],
            "keyProviderID": 1
        }
    ]
}
```

Neu seit Version

11,7

ModifyKeyServerKmip

Sie können die `ModifyKeyServerKmip` Methode zur Modifizierung eines bestehenden KMIP-Schlüsselservers (Key Management Interoperability Protocol) hinsichtlich der angegebenen Attribute. Obwohl der einzige erforderliche Parameter die keyServerID ist, wird eine Anfrage, die nur die keyServerID enthält, keine Aktion auslösen und es wird kein Fehler zurückgegeben. Alle anderen von Ihnen angegebenen Parameter ersetzen die vorhandenen Werte für den Schlüsselserver durch die angegebene keyServerID. Der Schlüsselserver wird während des Vorgangs kontaktiert, um sicherzustellen, dass er

funktionsfähig ist. Sie können mit dem Parameter kmipKeyServerHostnames mehrere Hostnamen oder IP-Adressen angeben, jedoch nur, wenn sich die Schlüsselserver in einer Clusterkonfiguration befinden.

Parameter

Diese Methode hat die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SchlüsselServerID	Die ID des zu ändernden KMIP-Schlüsselservers.	ganze Zahl	Keine	Ja
kmipCaCertificate	Das öffentliche Schlüsselzertifikat der Stammzertifizierungsstelle des externen Schlüsselservers. Dies dient der Überprüfung des vom externen Schlüsselserver im Rahmen der TLS-Kommunikation vorgelegten Zertifikats. Für wichtige Servercluster, bei denen einzelne Server unterschiedliche Zertifizierungsstellen verwenden, geben Sie eine verkettete Zeichenkette an, die die Stammzertifikate aller Zertifizierungsstellen enthält.	Schnur	Keine	Nein
kmipClientCertificate	Ein im PEM-Format Base64-kodiertes PKCS#10 X.509-Zertifikat, das vom Solidfire KMIP-Client verwendet wird.	Schnur	Keine	Nein

kmipKeyServerHostnames	Array der Hostnamen oder IP-Adressen, die diesem KMIP-Schlüsselserver zugeordnet sind. Mehrere Hostnamen oder IP-Adressen müssen nur dann angegeben werden, wenn sich die Schlüsselserver in einer Clusterkonfiguration befinden.	Zeichenketten-Array	Keine	Nein
kmipKeyServerName	Der Name des KMIP-Schlüsselservers. Dieser Name dient nur zu Darstellungszwecken und muss nicht eindeutig sein.	Schnur	Keine	Nein
kmipKeyServerPort	Die Portnummer, die diesem KMIP-Schlüsselserver zugeordnet ist (typischerweise 5696).	ganze Zahl	Keine	Nein

Rückgabewerte

Diese Methode hat die folgenden Rückgabewerte:

Name	Beschreibung	Typ
kmipKeyServer	Ein Objekt, das Details über den neu modifizierten Schlüsselserver enthält.	"KeyServerKmip"

Anforderungsbeispiel

Anfragen für diese Methode ähneln dem folgenden Beispiel:

```
{
  "method": "ModifyKeyServerKmip",
  "params": {
    "keyServerID": 15
    "kmipCaCertificate": "CPDCCAaUCEDyRMcsf9tAbDpq40ES/E...",
    "kmipClientCertificate": "kirWmnWXbj9T/UWZYB2oK0z5...",
    "kmipKeyServerHostnames" : ["server1.hostname.com",
"server2.hostname.com"],
    "kmipKeyServerName" : "keyserverName",
    "kmipKeyServerPort" : 5696
  },
"id": 1
}
```

Antwortbeispiel

Diese Methode liefert eine Antwort, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result":
      {
        "kmipKeyServer": {
            "kmipCaCertificate":"CPDCCAaUCEDyRMcsf9tAbDpq40ES/E...",
            "kmipKeyServerHostnames":[
                "server1.hostname.com", "server2.hostname.com"
            ],
            "keyProviderID":1,
            "kmipKeyServerName":"keyserverName",
            "keyServerID":1
            "kmipKeyServerPort":1,
            "kmipClientCertificate":"kirWmnWXbj9T/UWZYB2oK0z5...",
            "kmipAssignedProviderIsActive":true
        }
    }
}
```

Neu seit Version

11,7

RekeySoftwareEncryptionAtRestMasterKey

Sie können die `RekeySoftwareEncryptionAtRestMasterKey` Methode zur

Neukodierung des Software-Verschlüsselungs-im-Ruhezustand-Masterschlüssels, der zur Verschlüsselung von DEKs (Datenverschlüsselungsschlüsseln) verwendet wird. Bei der Clustererstellung wird die Softwareverschlüsselung im Ruhezustand so konfiguriert, dass sie Internal Key Management (IKM) verwendet. Diese Methode zur Schlüsselneuschlüsselung kann nach der Clustererstellung verwendet werden, um entweder IKM oder External Key Management (EKM) zu nutzen.

Parameter

Diese Methode hat die folgenden Eingabeparameter. Wenn die `keyManagementType` Wenn kein Parameter angegeben wird, wird die Neuschlüsselung unter Verwendung der bestehenden Schlüsselverwaltungskonfiguration durchgeführt. Wenn die `keyManagementType` ist angegeben und der Schlüsselanbieter ist extern, `keyProviderID` Der Parameter muss ebenfalls verwendet werden.

Parameter	Beschreibung	Typ	Optional
Schlüsselverwaltungstyp	Die Art des Schlüsselmanagements, die zur Verwaltung des Hauptschlüssels verwendet wird. Mögliche Werte sind: `Internal` : Neuverschlüsselung mittels interner Schlüsselverwaltung. `External` : Neuverschlüsselung mittels externer Schlüsselverwaltung. Wird dieser Parameter nicht angegeben, wird die Schlüsselerneuerung unter Verwendung der bestehenden Schlüsselverwaltungskonfiguration durchgeführt.	Schnur	WAHR
keyProviderID	Die ID des zu verwendenden Schlüsselanbieters. Dies ist ein eindeutiger Wert, der als Teil einer der folgenden Funktionen zurückgegeben wird: `CreateKeyProvider` Methoden. Die ID wird nur benötigt, wenn `keyManagementType` Ist `External` und ist andernfalls ungültig.	ganze Zahl	WAHR

Rückgabewerte

Diese Methode hat die folgenden Rückgabewerte:

Parameter	Beschreibung	Typ	Optional
asyncHandle	Ermitteln Sie mithilfe dieser Methode den Status des Schlüsselaustauschs. `asyncHandle` Wert mit `GetAsyncResult` Die `GetAsyncResult` Die Ausgabe wird Folgendes enthalten: `newKey` Feld, das Informationen über den neuen Hauptschlüssel und einen enthält `keyToDecommission` Feld, das Informationen über den alten Schlüssel enthält.	ganze Zahl	FALSCH

Anforderungsbeispiel

Anfragen für diese Methode ähneln dem folgenden Beispiel:

```
{
 "method": "rekeysoftwareencryptionatrestmasterkey",
 "params": {
   "keyManagementType": "external",
   "keyProviderID": "<ID number>"
 }
}
```

Antwortbeispiel

Diese Methode liefert eine Antwort, die dem folgenden Beispiel ähnelt:

```
{
    "asyncHandle": 1
}
```

Neu seit Version

12,3

Weitere Informationen

- "SolidFire und Element-Softwaredokumentation"
- "Dokumentation für frühere Versionen der NetApp SolidFire und Element-Produkte"

RemoveKeyServerFromProviderKmip

Sie können die `RemoveKeyServerFromProviderKmip` Methode zum Aufheben der Zuordnung des angegebenen KMIP-Schlüsselservers (Key Management Interoperability Protocol) zu dem Anbieter, dem er zugewiesen wurde. Sie können einen Schlüsselserver von seinem Anbieter trennen, es sei denn, es handelt sich um den letzten und sein Anbieter ist aktiv (d. h. er stellt Schlüssel bereit, die aktuell in Gebrauch sind). Wenn der angegebene Schlüsselserver keinem Anbieter zugewiesen ist, werden keine Maßnahmen ergriffen und es wird kein Fehler zurückgegeben.

Parameter

Diese Methode hat die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SchlüsselServerID	Die ID des KMIP-Schlüsselservers, dessen Zuweisung aufgehoben werden soll.	ganze Zahl	Keine	Ja

Rückgabewerte

Diese Methode hat keinen Rückgabewert. Die Entfernung gilt als erfolgreich, solange kein Fehler zurückgegeben wird.

Anforderungsbeispiel

Anfragen für diese Methode ähneln dem folgenden Beispiel:

```
{
  "method": "RemoveKeyServerFromProviderKmip",
  "params": {
    "keyServerID": 1
   },
"id": 1
}
```

Antwortbeispiel

Diese Methode liefert eine Antwort, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result":
      {}
    }
}
```

Neu seit Version

11,7

SignSshKeys

Nachdem SSH auf dem Cluster aktiviert wurde,"EnableSSH-Methode" Sie können die `SignSshKeys` Methode zum Erlangen von Zugriff auf eine Shell auf einem Knoten.

Beginnend mit Element 12.5, `sfreadonly` Ein neues Systemkonto ermöglicht die grundlegende Fehlerbehebung auf einem Knoten. Diese API ermöglicht den SSH-Zugriff über die `sfreadonly` Systemkonto auf allen Knoten im Cluster.

> Sofern Sie nicht vom NetApp Support dazu aufgefordert werden, sind jegliche Änderungen am System nicht unterstützt, führen zum Erlöschen Ihres Supportvertrags und können Instabilität oder den Verlust der Datenverfügbarkeit zur Folge haben.

Nachdem Sie die Methode angewendet haben, müssen Sie den Schlüsselbund aus der Antwort kopieren, ihn auf dem System speichern, von dem die SSH-Verbindung initiiert wird, und anschließend den folgenden Befehl ausführen:

```
ssh -i <identity_file> sfreadonly@<node_ip>
```

```
`identity_file`ist eine Datei, aus der die Identität (privater Schlüssel)
für die Public-Key-Authentifizierung gelesen wird und `node_ip` ist die
IP-Adresse des Knotens.  Weitere Informationen finden Sie unter
`identity_file` Siehe die SSH-Manpage.
```

Parameter

Diese Methode hat die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Dauer	Ganze Zahl von 1 bis 24, die die Anzahl der Stunden angibt, in denen der signierte Schlüssel gültig ist. Wird keine Dauer angegeben, wird der Standardwert verwendet.	ganze Zahl	1	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
öffentlicher Schlüssel	Falls dieser Parameter angegeben wird, wird lediglich der signierte öffentliche Schlüssel zurückgegeben, anstatt einen vollständigen Schlüsselbund für den Benutzer zu erstellen.  Öffentliche Schlüssel, die über die URL-Leiste in einem Browser übermittelt wurden, + werden als Zeichen mit Abständen und Unterbrechungen interpretiert.	Schnur	Null	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
sfadmin	Ermöglicht den Zugriff auf das sfadmin-Shell-Konto, wenn Sie den API-Aufruf mit supportAdmin-Clusterzugriff durchführen oder wenn sich der Knoten nicht in einem Cluster befindet.	boolescher Wert	FALSCH	Nein

Rückgabewerte

Diese Methode hat die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Keygen-Status	Enthält die Identität im signierten Schlüssel, die zulässigen Benutzer und die gültigen Start- und Enddaten für den Schlüssel.	Schnur
privater_key	Ein privater SSH-Schlüsselwert wird nur dann zurückgegeben, wenn die API einen vollständigen Schlüsselbund für den Endbenutzer generiert.  Der Wert ist Base64-kodiert; Sie müssen den Wert dekodieren, wenn er in eine Datei geschrieben wird, um sicherzustellen, dass er als gültiger privater Schlüssel gelesen wird.	Schnur

Name	Beschreibung	Typ
öffentlicher Schlüssel	Ein öffentlicher SSH-Schlüsselwert wird nur dann zurückgegeben, wenn die API einen vollständigen Schlüsselbund für den Endbenutzer generiert. Wenn Sie einen public_key-Parameter an die API-Methode übergeben, wird nur der `signed_public_key` Der Wert wird in der Antwort zurückgegeben.	Schnur
signierter öffentlicher Schlüssel	Der SSH-öffentliche Schlüssel, der durch Signieren des öffentlichen Schlüssels entsteht, unabhängig davon, ob dieser vom Benutzer bereitgestellt oder von der API generiert wurde.	Schnur

Anforderungsbeispiel

Anfragen für diese Methode ähneln dem folgenden Beispiel:

```
{
    "method": "SignSshKeys",
    "params": {
        "duration": 2,
        "publicKey":<string>
    },
    "id": 1
}
```

Antwortbeispiel

Diese Methode liefert eine Antwort, die dem folgenden Beispiel ähnelt:

```
{
  "id": null,
  "result": {
    "signedKeys": {
      "keygen_status": <keygen_status>,
      "signed_public_key": <signed_public_key>
    }
  }
}
```

In diesem Beispiel wird ein öffentlicher Schlüssel signiert und zurückgegeben, der für die Dauer (1-24 Stunden) gültig ist.

Neu seit Version

12,5

TestKeyProviderKmip

Sie können die `TestKeyProviderKmip` Methode zum Testen, ob der angegebene KMIP-Schlüsselanbieter (Key Management Interoperability Protocol) erreichbar ist und normal funktioniert.

Parameter

Diese Methode hat die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
keyProviderID	Die ID des zu testenden Schlüsselanbieters.	ganze Zahl	Keine	Ja

Rückgabewerte

Diese Methode hat keinen Rückgabewert. Der Test gilt als erfolgreich, solange kein Fehler zurückgegeben wird.

Anforderungsbeispiel

Anfragen für diese Methode ähneln dem folgenden Beispiel:

```
{
  "method": "TestKeyProviderKmip",
  "params": {
    "keyProviderID": 15
  },
"id": 1
}
```

Antwortbeispiel

Diese Methode liefert eine Antwort, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result":
      {}
    }
}
```

Neu seit Version

11,7

TestKeyServerKmip

Sie können die `TestKeyServerKmip` Methode zum Testen, ob der angegebene KMIP-Schlüsselserver (Key Management Interoperability Protocol) erreichbar ist und normal funktioniert.

Parameter

Diese Methode hat die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SchlüsselServerID	Die ID des zu testenden KMIP-Schlüsselservers.	ganze Zahl	Keine	Ja

Rückgabewerte

Diese Methode hat keinen Rückgabewert. Der Test gilt als erfolgreich, wenn keine Fehler zurückgegeben werden.

Anforderungsbeispiel

Anfragen für diese Methode ähneln dem folgenden Beispiel:

```
{
  "method": "TestKeyServerKmip",
  "params": {
    "keyServerID": 15
  },
"id": 1
}
```

Antwortbeispiel

Diese Methode liefert eine Antwort, die dem folgenden Beispiel ähnelt:

```
{
   "id": 1,
   "result":
      {}
    }
```

Neu seit Version

11,7