Sicherheits-API-Methoden

Element Software

NetApp
October 01, 2024

Inhalt

Sicherheits-API-Methoden

Sie können Element Software in externe, sicherheitsbezogene Services wie einen externen Verschlüsselungsmanagementserver integrieren. Mit diesen sicherheitsbezogenen Methoden können Sie Sicherheitsfunktionen für Komponenten wie externes Verschlüsselungsmanagement für die Verschlüsselung im Ruhezustand konfigurieren.

- AddKeyServerToProviderKmip
- CreateKeyProviderKmip
- CreateKeyServerkmip
- CreatePublicPrivateKeyPair
- DeleteKeyProviderKmip
- DeleteKeyServerkmip
- UnbeständigkeitVerverschlüsselungAttest
- EnableVerschlüsselungAtZiel
- GetClientCertificateSignRequest
- GetKeyProviderKmip
- GetKeyServerkmip
- ListKeyProvidersKmip
- ListKeyServersKmip
- ModifyKeyServerkmip
- RemoveKeyServerFromProviderKmip
- Signalschlüssel
- TestKeyProviderKmip
- TestKeyServerkmip

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

AddKeyServerToProviderKmip

Mit dieser Methode kann `AddKeyServerToProviderKmip` dem angegebenen Schlüsselanbieter ein KMIP-Schlüsselserver (Key Management Interoperability Protocol) zugewiesen werden. 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 mit der Methode entfernen `RemoveKeyServerFromProviderKmip`.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
ID von Schlüsselausweisungs-ID	Die ID des Schlüsselanbieters, dem der Schlüsselserver zugewiesen werden soll.	Ganzzahl	Keine	Ja.
KeyServer-ID	Die ID des zu zuweisenden Schlüsselservers.	Ganzzahl	Keine	Ja.

Rückgabewerte

Diese Methode hat keinen Rückgabewert. Die Zuweisung gilt als erfolgreich, solange kein Fehler zurückgegeben wurde.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

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

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

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

Neu seit Version

11,7

CreateKeyProviderKmip

Sie können die Methode verwenden `CreateKeyProviderKmip`, um einen KMIP-Schlüsselanbieter (Key Management Interoperability Protocol) mit dem angegebenen Namen zu erstellen. Ein Schlüsselanbieter definiert einen Mechanismus und einen Speicherort zum Abrufen von Authentifizierungsschlüsseln. Beim Erstellen eines neuen KMIP-Schlüsselanbieters verfügt dieser über keine KMIP-Schlüsselserver. Verwenden Sie zum Erstellen eines KMIP-Schlüsselservers die `CreateKeyServerKmip` Methode. Informationen zur Zuordnung zu einem Provider finden Sie unter `AddKeyServerToProviderKmip`.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SchlüsselProvidername	Der Name, der mit dem erstellten KMIP-Schlüsselanbieter verknüpft werden soll. Dieser Name wird nur für Anzeigezwecke verwendet und muss nicht eindeutig sein.	Zeichenfolge	Keine	Ja.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
KmSchlüsselanbieter	Ein Objekt, das Details zum neu erstellten Schlüsselanbieter enthält.	"KeyProviderKmip"

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

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

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, 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

Mit dieser Methode kann `CreateKeyServerKmip` ein KMIP-Schlüsselserver (Key Management Interoperability Protocol) mit den angegebenen Attributen erstellt werden. Während der Erstellung wird der Server nicht kontaktiert. Er muss nicht vorhanden sein, bevor Sie diese Methode verwenden. Bei Konfigurationen von geclusterten Key-Servern müssen Sie die Hostnamen oder IP-Adressen aller Serverknoten im Parameter kmipKeyServerHostnames angeben. Sie können die Methode zum Testen eines Schlüsselservers verwenden `TestKeyServerKmip`.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
KmipCaCertificate	Das öffentliche Schlüsselzertifikat der Stammzertifizierungsstelle des externen Schlüsselservers. Dies wird verwendet, um das Zertifikat, das von einem externen Schlüsselserver in der TLS-Kommunikation präsentiert wird, zu überprüfen. Stellen Sie für Schlüsselservercluster, in denen einzelne Server unterschiedliche CAS verwenden, einen verketteten String bereit, der die Stammzertifikate aller CAS enthält.	Zeichenfolge	Keine	Ja.
KmipClientZertifikat	Ein PEM-Format Base64-codiertes PKCS#10 X.509-Zertifikat, das vom SolidFire KMIP-Client verwendet wird.	Zeichenfolge	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
KmipKeyServerHostnames	Array der Hostnamen oder IP-Adressen, die mit diesem KMIP-Schlüsselserver verbunden sind. Mehrere Hostnamen oder IP-Adressen dürfen nur bereitgestellt werden, wenn sich die Schlüsselserver in einer Clusterkonfiguration befinden.	String-Array	Keine	Ja.
KmipKeyServerName	Der Name des KMIP-Schlüsselservers. Dieser Name wird nur für Anzeigezwecke verwendet und muss nicht eindeutig sein.	Zeichenfolge	Keine	Ja.
KmipKeyServerPort	Die diesem KMIP-Schlüsselserver zugeordnete Port-Nummer (in der Regel 5696).	Ganzzahl	Keine	Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
KmSchlüsselserver	Ein Objekt, das Details zum neu erstellten Schlüsselserver enthält.	"KeyServerkmip"

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende 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 gibt eine Antwort zurück, 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

CreatePublicPrivateKeyPair

Sie können die Methode verwenden `CreatePublicPrivateKeyPair`, um öffentliche und private SSL-Schlüssel zu erstellen. Mit diesen Schlüsseln können Sie Anforderungen

zum Signieren von Zertifikaten erstellen. Es kann für jedes Storage-Cluster nur ein Schlüsselpaar verwendet werden. Bevor Sie diese Methode zum Austausch vorhandener Schlüssel verwenden, stellen Sie sicher, dass die Schlüssel von keinem Provider mehr verwendet werden.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

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

Rückgabewerte

Diese Methode hat keine Rückgabewerte. Wenn kein Fehler auftritt, gilt die Schlüsselerstellung als erfolgreich.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

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

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

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

Neu seit Version

11,7

DeleteKeyProviderKmip

Sie können die Methode verwenden `DeleteKeyProviderKmip`, um den angegebenen inaktiven Schlüsselanbieter für das Key Management Interoperability Protocol (KMIP) zu löschen.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
ID von Schlüsselausweisungs-ID	Die ID des zu löschenden Schlüsselanbieters.	Ganzzahl	Keine	Ja.

Rückgabewerte

Diese Methode hat keine Rückgabewerte. Der Löschvorgang gilt als erfolgreich, solange kein Fehler vorhanden ist.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

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

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

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

Neu seit Version

11,7

DeleteKeyServerkmip

Sie können diese Methode verwenden `DeleteKeyServerKmip`, um einen vorhandenen KMIP-Schlüsselserver (Key Management Interoperability Protocol) zu löschen. Sie können einen Schlüsselserver löschen, es sei denn, er ist der letzte seinem Provider zugewiesene, und dieser Provider stellt derzeit verwendete Schlüssel zur Verfügung.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
KeyServer-ID	Die ID des zu löschenden KMIP-Schlüsselservers.	Ganzzahl	Keine	Ja.

Rückgabewerte

Diese Methode hat die Werte ohne Rückgabewert. Der Löschvorgang wird als erfolgreich betrachtet, wenn keine Fehler vorliegen.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

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

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

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

Neu seit Version

11,7

UnbeständigkeitVerverschlüsselungAttest

Sie können die Methode verwenden `DisableEncryptionAtRest`, um die Verschlüsselung zu entfernen, die zuvor auf den Cluster angewendet wurde, indem Sie die Methode verwenden `EnableEncryptionAtRest`. Diese Disable-Methode ist asynchron und gibt eine Antwort zurück, bevor die Verschlüsselung deaktiviert wird. Sie können die Methode verwenden `GetClusterInfo`, um das System abzufragen, um zu sehen, wann der Vorgang abgeschlossen ist.

Um den aktuellen Status der Verschlüsselung im Ruhezustand und/oder der Softwareverschlüsselung im Ruhezustand auf dem Cluster anzuzeigen, verwenden Sie die "Abrufen der Cluster Info-Methode". Sie können die verwenden `GetSoftwareEncryptionAtRestInfo` "Methode zum Abrufen von Informationen, die das Cluster verwendet, um Daten im Ruhezustand zu verschlüsseln".

Sie können diese Methode nicht verwenden, um die Softwareverschlüsselung im Ruhezustand zu deaktivieren. Um die Softwareverschlüsselung im Ruhezustand zu deaktivieren, muss die "Erstellen Sie einen neuen Cluster"Softwareverschlüsselung im Ruhezustand deaktiviert sein.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

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

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

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

Neu seit Version

9,6

Weitere Informationen

- "GetClusterInfo"
- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

EnableVerschlüsselungAtZiel

Mit dieser Methode kann `EnableEncryptionAtRest` die 256-Bit-Verschlüsselung des Advanced Encryption Standard (AES) im Ruhezustand auf dem Cluster aktiviert werden, sodass das Cluster den für die Laufwerke auf jedem Node verwendeten Verschlüsselungsschlüssel verwalten kann. Diese Funktion ist standardmäßig nicht aktiviert.

Um den aktuellen Status der Verschlüsselung im Ruhezustand und/oder der Softwareverschlüsselung im Ruhezustand auf dem Cluster anzuzeigen, verwenden Sie die "Abrufen der Cluster Info-Methode". Sie können die verwenden `GetSoftwareEncryptionAtRestInfo` "Methode zum Abrufen von Informationen, die das Cluster verwendet, um Daten im Ruhezustand zu verschlüsseln".

Bei dieser Methode wird die Softwareverschlüsselung im Ruhezustand nicht aktiviert. Dies kann nur mit der Option mit `enableSoftwareEncryptionAtRest` gesetzt auf `true` erfolgen"Cluster-Methode erstellen".

Wenn Sie die Verschlüsselung im Ruhezustand aktivieren, managt der Cluster automatisch die Schlüssel intern für die Laufwerke auf jedem Node im Cluster.

Wenn eine keyProviderID angegeben wird, wird das Passwort entsprechend dem Typ des Schlüsselanbieters generiert und abgerufen. Dies erfolgt in der Regel mit einem KMIP-Schlüsselserver (Key Management Interoperability Protocol) im Fall eines KMIP-Schlüsselanbieters. Nach diesem Vorgang gilt der angegebene Anbieter als aktiv und kann erst gelöscht werden, wenn die Verschlüsselung im Ruhezustand mithilfe der Methode deaktiviert wurde `DisableEncryptionAtRest`.

Wenn Sie einen Node-Typ mit einer Modellnummer haben, die auf „-NE“ endet, schlägt der `EnableEncryptionAtRest` Methodenaufruf mit der Antwort „Verschlüsselung nicht zulässig“ fehl. Nicht verschlüsselbarer Node durch das Cluster erkannt“.

Sie sollten die Verschlüsselung nur aktivieren oder deaktivieren, wenn das Cluster ausgeführt wird und sich in einem ordnungsgemäßen Zustand befindet. Sie können die Verschlüsselung nach Ihrem Ermessen und so oft wie nötig aktivieren oder deaktivieren.

Dieser Prozess ist asynchron und gibt vor Aktivierung der Verschlüsselung eine Antwort zurück. Sie können die Methode verwenden `GetClusterInfo`, um das System abzufragen, um zu sehen, wann der Vorgang abgeschlossen ist.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
ID von Schlüsselausweisungs-ID	Die ID eines KMIP-Schlüsselanbieters zu verwenden.	Ganzzahl	Keine	Nein

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

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

Antwortbeispiele

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel aus der EnableVerschlüsselungAtRest-Methode ähnelt. Es gibt kein Ergebnis zu berichten.

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

Während die Verschlüsselung im Ruhezustand auf einem Cluster aktiviert wird, gibt GetClusterInfo ein Ergebnis zurück, das den Status von Verschlüsselung im Ruhezustand („Encryption AttRestState“) als „Enabled“ beschreibt. Nachdem die Verschlüsselung im Ruhezustand 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"
- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

GetClientCertificateSignRequest

Sie können die Methode verwenden `GetClientCertificateSignRequest`, um eine Zertifikatsignierungsanforderung zu generieren, die von einer Zertifizierungsstelle signiert werden kann, um ein Clientzertifikat für das 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 verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
ClientCertificateSignRequest	Eine PEM-Format Base64-codierte PKCS#10 X.509-Client-Zertifikatanforderung.	Zeichenfolge

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

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

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

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

Neu seit Version

11,7

GetKeyProviderKmip

Sie können diese Methode verwenden `GetKeyProviderKmip`, um Informationen über den angegebenen KMIP-Schlüsselanbieter (Key Management Interoperability Protocol) abzurufen.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
ID von Schlüsselausweisungs-ID	Die ID des KMIP-Schlüssels, das zurückgegeben werden soll.	Ganzzahl	Keine	Ja.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

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

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

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

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, 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 Methode verwenden `GetKeyServerKmip`, um Informationen über den angegebenen KMIP-Schlüsselserver (Key Management Interoperability Protocol) zurückzugeben.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

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

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
KmSchlüsselserver	Ein Objekt, das Details zum angeforderten Schlüsselserver enthält.	"KeyServerkmip"

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

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

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, 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

GetSoftwareVerschlüsselungAtRestInfo

Sie können diese Methode verwenden `GetSoftwareEncryptionAtRestInfo`, um Softwareverschlüsselung im Ruhezustand zu erhalten, die das Cluster zum Verschlüsseln von Daten im Ruhezustand verwendet.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Parameter	Beschreibung	Typ	Optional
MasterKeyInfo	Informationen zum aktuellen Master-Schlüssel für Softwareverschlüsselung im Ruhezustand	VerschlüsselungKeyInfo	Richtig
RekeyMasterKeyAsyncResultID	Die asynchrone Ergebnis-ID der aktuellen oder letzten Rekey-Operation (falls vorhanden), sofern sie noch nicht gelöscht wurde. `GetAsyncResult` Die Ausgabe enthält ein `newKey` Feld, das Informationen über den neuen Hauptschlüssel und ein `keyToDecommission` Feld enthält, das Informationen über den alten Schlüssel enthält.	Ganzzahl	Richtig
Bundesland	Der aktuelle Status der Softwareverschlüsselung im Ruhezustand. Mögliche Werte sind `disabled` oder `enabled`.	Zeichenfolge	Falsch
Version	Eine Versionsnummer, die bei jeder Aktivierung der Softwareverschlüsselung erhöht wird.	Ganzzahl	Falsch

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

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

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, 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

- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

ListKeyProvidersKmip

Mit dieser Methode können `ListKeyProvidersKmip` Sie eine Liste aller vorhandenen KMIP-Schlüsselanbieter (Key Management Interoperability Protocol) abrufen. Sie können die Liste filtern, indem Sie zusätzliche Parameter angeben.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
SchlüsselProviderIActive	Filter haben KMIP-Schlüsselserver-Objekte zurückgegeben, basierend darauf, ob sie aktiv sind. Mögliche Werte: • Richtig: Nur KMIP-Schlüsselanbieter (die aktiv sind und Schlüssel angeben, die derzeit verwendet werden) • Falsch: Gibt nur KMIP-Schlüsselanbieter zurück, die inaktiv sind (keine Schlüssel angeben und gelöscht werden können). Wenn keine Daten angegeben, werden die zurückgegebenen KMIP-Schlüsselanbieter nicht gefiltert, weil sie aktiv sind.	boolesch	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
KmipKeyProviderHasServerAssign	Die Filter haben KMIP-Schlüsselanbieter zurückgegeben, basierend darauf, ob einem KMIP-Schlüsselserver zugewiesen ist. Mögliche Werte: • Richtig: Nur KMIP-Schlüsselanbieter, die über einen KMIP-Schlüsselserver verfügen • Falsch: Gibt nur KMIP-Schlüsselanbieter zurück, denen kein KMIP-Schlüsselserver zugewiesen ist. Wenn keine Angabe durchgeführt wird, werden die zurückgegebenen KMIP-Schlüsselanbieter nicht gefiltert, weil sie einen KMIP-Schlüsselserver zugewiesen haben.	boolesch	Keine	Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

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

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

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

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, 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

Mit dieser Methode können `ListKeyServersKmip` alle erstellten Key Management Interoperability Protocol (KMIP)-Schlüsselserver aufgelistet werden. Sie können die Ergebnisse filtern, indem Sie zusätzliche Parameter angeben.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
ID von Schlüsselausweisungs-ID	Bei Angabe der Methode werden nur KMIP-Schlüsselserver zurückgegeben, die dem angegebenen KMIP-Schlüsselanbieter zugewiesen sind. Wenn keine Angabe ausgeführt wird, werden KMIP-Schlüsselserver in zurückgegebenen Fällen nicht gefiltert, weil sie dem angegebenen KMIP-Schlüsselanbieter zugewiesen sind.	Ganzzahl	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
KmipAssigneedProviderIActive	Filter haben KMIP-Schlüsselserver-Objekte zurückgegeben, basierend darauf, ob sie aktiv sind. Mögliche Werte: • True: Gibt nur aktive KMIP-Schlüsselserver zurück (Angabe von Schlüsseln, die derzeit verwendet werden). • False: Gibt nur KMIP-Schlüsselserver zurück, die inaktiv sind (keine Schlüssel angeben und gelöscht werden können). Wenn keine Angabe angezeigt wird, werden die zurückgegebenen KMIP-Schlüsselserver nicht gefiltert, weil sie aktiv sind.	boolesch	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
KmipHasProviderAssign	Die Filter gaben KMIP-Schlüsselserver zurück, basierend darauf, ob ihnen ein KMIP-Schlüsselanbieter zugewiesen wurde. Mögliche Werte: • Richtig: Nur KMIP-Schlüsselserver mit einem KMIP-Schlüsselanbieter werden zurückgegeben. • Falsch: Gibt nur KMIP-Schlüsselserver zurück, denen kein KMIP-Schlüsselanbieter zugewiesen ist. Wenn keine Angabe erfolgt, werden zurückgegebene KMIP-Schlüsselserver nicht gefiltert, weil sie den KMIP-Schlüsselanbieter zugewiesen haben.	boolesch	Keine	Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
KmSchlüsselserver	Vollständige Liste der erstellten KMIP-Schlüsselserver	"KeyServerkmip" Array

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

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

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, 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

Mit dieser Methode kann `ModifyKeyServerKmip` ein vorhandener KMIP-Schlüsselserver (Key Management Interoperability Protocol) auf die angegebenen Attribute geändert werden. Obwohl der einzige erforderliche Parameter die keyServerID ist, wird eine Anforderung, die nur die keyServerID enthält, keine Aktion ausgeführt und gibt keinen Fehler zurück. Alle anderen Parameter, die Sie angeben, ersetzen die vorhandenen Werte für den Schlüsselserver durch die angegebene keyServerID. Der Schlüsselserver wird während des Betriebs kontaktiert, um sicherzustellen, dass er funktionsfähig ist. Sie können mehrere Hostnamen oder IP-Adressen mit dem Parameter kmipKeyServerHostnames bereitstellen, jedoch nur, wenn die Schlüsselserver in einer geclusterten Konfiguration sind.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
KeyServer-ID	Die ID des zu ändernden KMIP-Schlüsselservers.	Ganzzahl	Keine	Ja.
KmipCaCertificate	Das öffentliche Schlüsselzertifikat der Stammzertifizierungsstelle des externen Schlüsselservers. Dies wird verwendet, um das Zertifikat, das von einem externen Schlüsselserver in der TLS-Kommunikation präsentiert wird, zu überprüfen. Stellen Sie für Schlüsselservercluster, in denen einzelne Server unterschiedliche CAS verwenden, einen verketteten String bereit, der die Stammzertifikate aller CAS enthält.	Zeichenfolge	Keine	Nein
KmipClientZertifikat	Ein PEM-Format Base64-codiertes PKCS#10 X.509-Zertifikat, das vom SolidFire KMIP-Client verwendet wird.	Zeichenfolge	Keine	Nein

KmipKeyServerHostnames	Array der Hostnamen oder IP-Adressen, die mit diesem KMIP-Schlüsselserver verbunden sind. Mehrere Hostnamen oder IP-Adressen dürfen nur bereitgestellt werden, wenn sich die Schlüsselserver in einer Clusterkonfiguration befinden.	String-Array	Keine	Nein
KmipKeyServerName	Der Name des KMIP-Schlüsselservers. Dieser Name wird nur für Anzeigezwecke verwendet und muss nicht eindeutig sein.	Zeichenfolge	Keine	Nein
KmipKeyServerPort	Die diesem KMIP-Schlüsselserver zugeordnete Port-Nummer (in der Regel 5696).	Ganzzahl	Keine	Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
KmSchlüsselserver	Ein Objekt, das Details zum neu geänderten Schlüsselserver enthält.	"KeyServerkmip"

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende 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 gibt eine Antwort zurück, 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

RekeySoftwareVerschlüsselungAtRestMasterKey

Sie können die Methode verwenden `RekeySoftwareEncryptionAtRestMasterKey`,

um den für die Verschlüsselung von DEKs (Data Encryption Keys) verwendeten Master-Schlüssel für die Softwareverschlüsselung im Ruhezustand neu zu verschlüsseln. Während der Cluster-Erstellung wird die Softwareverschlüsselung im Ruhezustand für die Verwendung des internen Key Managements (IKM) konfiguriert. Diese Rekeymethode kann nach der Cluster-Erstellung entweder zur Verwendung von IKM oder External Key Management (EKM) verwendet werden.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter. Wenn der `keyManagementType` Parameter nicht angegeben wird, erfolgt die Rekey-Operation unter Verwendung der vorhandenen Key-Management-Konfiguration. Wenn der `keyManagementType` angegeben wird und der Key Provider extern ist, muss der `keyProviderID` Parameter ebenfalls verwendet werden.

Parameter	Beschreibung	Typ	Optional
SchlüsselManagementtyp	Die Art der Schlüsselverwaltung, die zum Verwalten des Hauptschlüssels verwendet wird. Mögliche Werte sind: `Internal`: Rekey mit internem Schlüsselmanagement. `External`: Rekey mit externer Schlüsselverwaltung. Wenn dieser Parameter nicht angegeben wird, wird der Rekeyvorgang mithilfe der bestehenden Key Management-Konfiguration durchgeführt.	Zeichenfolge	Richtig
ID von Schlüsselausweisungs-ID	Die ID des zu verwendenden Schlüsselanbieters. Dies ist ein eindeutiger Wert, der als Teil einer der Methoden zurückgegeben `CreateKeyProvider` wird. Die ID ist nur erforderlich, wenn `keyManagementType` ist und ansonsten ungültig ist `External`.	Ganzzahl	Richtig

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Parameter	Beschreibung	Typ	Optional
Asynchron	Bestimmen Sie den Status der Rekey-Operation mit diesem `asyncHandle` Wert mit `GetAsyncResult`. `GetAsyncResult` Die Ausgabe enthält ein `newKey` Feld, das Informationen über den neuen Hauptschlüssel und ein `keyToDecommission` Feld enthält, das Informationen über den alten Schlüssel enthält.	Ganzzahl	Falsch

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

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

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

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

Neu seit Version

12,3

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

RemoveKeyServerFromProviderKmip

Sie können die Methode verwenden `RemoveKeyServerFromProviderKmip`, um die Zuweisung des angegebenen KMIP-Schlüsselservers (Key Management Interoperability Protocol) vom Anbieter, dem er zugewiesen wurde, aufzuheben. Sie können die Zuweisung eines Schlüsselservers vom Provider aufheben, es sei denn, er ist der letzte und sein Provider aktiv (die Schlüssel, die derzeit verwendet werden). Wenn der angegebene Schlüsselserver einem Provider nicht zugewiesen ist, wird keine Aktion ausgeführt und es wird kein Fehler zurückgegeben.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
KeyServer-ID	Die ID des KMIP-Schlüsselservers, der die Zuweisung aufheben soll.	Ganzzahl	Keine	Ja.

Rückgabewerte

Diese Methode hat keine Rückgabewerte. Die Entfernung gilt als erfolgreich, solange kein Fehler zurückgegeben wird.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

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

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

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

Neu seit Version

11,7

Signalschlüssel

Nachdem SSH auf dem Cluster mithilfe von aktiviert "EnableSSH-Methode"wurde, können Sie die Methode verwenden `SignSshKeys`, um Zugriff auf eine Shell auf einem Node zu erhalten.

Ab Element 12.5 `sfreadonly` ist ein neues Systemkonto, das grundlegende Fehlerbehebungsmaßnahmen an einem Knoten ermöglicht. Diese API ermöglicht den SSH-Zugriff über das `sfreadonly` Systemkonto hinweg über alle Nodes im Cluster hinweg.

> Sofern vom NetApp Support nicht empfohlen, werden Änderungen am System nicht unterstützt, sodass Sie Ihren Support-Vertrag aufgeben und möglicherweise die Daten instabil oder unzugänglich machen können.

Nachdem Sie die Methode verwendet haben, müssen Sie die Schlüsselkette aus der Antwort kopieren, sie in das System speichern, das die SSH-Verbindung initiiert, und führen Sie dann den folgenden Befehl aus:

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

```
`identity_file` Ist eine Datei, aus der die Identität (privater Schlüssel)
für die Authentifizierung mit öffentlichem Schlüssel gelesen wird und
`node_ip` die IP-Adresse des Knotens ist. Weitere Informationen zu
`identity_file` finden Sie auf der SSH man-Seite.
```

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Dauer	Ganzzahl zwischen 1 und 24, die die Anzahl der Stunden für die signierte Taste angibt, gültig zu sein. Wenn keine Dauer angegeben wird, wird der Standardwert verwendet.	Ganzzahl	1	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
Publizieren	Wenn angegeben, gibt dieser Parameter nur den signierten_Public_Key zurück, anstatt eine vollständige Schlüsselkette für den Benutzer zu erstellen. Öffentliche Schlüssel, die über die URL-Leiste in einem Browser mit über mittelt + werden, werden als Abstände interpretiert und die Signatur unterbrochen.	Zeichenfolge	Null	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
Sfadmin	Ermöglicht den Zugriff auf das sfadmin-Shell-Konto, wenn Sie den API-Aufruf mit supportAdmin-Cluster-Zugriff tätigen oder wenn sich der Node nicht in einem Cluster befindet.	boolesch	Falsch	Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
keygen_Status	Enthält die Identität im signierten Schlüssel, die zulässigen Prinzipale und die gültigen Start- und Enddaten für den Schlüssel.	Zeichenfolge
Privater_Schlüssel	Ein privater SSH-Schlüsselwert wird nur zurückgegeben, wenn die API eine vollständige Schlüsselkette für den Endbenutzer generiert. Der Wert ist Base64-codiert; Sie müssen den Wert decodieren, wenn er in eine Datei geschrieben wird, um sicherzustellen, dass er als gültiger privater Schlüssel gelesen wird.	Zeichenfolge

Name	Beschreibung	Typ
Öffentlicher_Schlüssel	Ein öffentlicher SSH-Schlüsselwert wird nur zurückgegeben, wenn die API eine vollständige Schlüsselkette für den Endbenutzer generiert. Wenn Sie einen Parameter public_key an die API-Methode übergeben, wird nur der `signed_public_key` Wert in der Antwort zurückgegeben.	Zeichenfolge
Signiert_Public_Key	Der öffentliche SSH-Schlüssel, der sich aus dem Signieren des öffentlichen Schlüssels ergibt, unabhängig davon, ob dieser von der API bereitgestellt oder generiert wurde.	Zeichenfolge

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

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

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, 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 gültig ist (1-24 Stunden).

Neu seit Version

12,5

TestKeyProviderKmip

Sie können die Methode verwenden `TestKeyProviderKmip`, um zu testen, ob der angegebene KMIP-Schlüsselanbieter (Key Management Interoperability Protocol) erreichbar ist und ordnungsgemäß funktioniert.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
ID von Schlüsselausweisungs-ID	Die ID des zu testenden Schlüsselanbieters.	Ganzzahl	Keine	Ja.

Rückgabewerte

Diese Methode hat keine Rückgabewerte. Der Test gilt als erfolgreich, solange kein Fehler zurückgegeben wird.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

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

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

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

Neu seit Version

11,7

TestKeyServerkmip

Sie können die Methode verwenden `TestKeyServerKmip`, um zu testen, ob der angegebene KMIP-Schlüsselserver (Key Management Interoperability Protocol) erreichbar ist und ordnungsgemäß funktioniert.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
KeyServer-ID	Die ID des zu testenden KMIP-Schlüsselservers.	Ganzzahl	Keine	Ja.

Rückgabewerte

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

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

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

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

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

Neu seit Version

11,7