Metodi API di sicurezza

Element Software

NetApp
November 18, 2025

Sommario

Metodi API di sicurezza

AggiungiKeyServerAlProviderKmip

Puoi usare il `AddKeyServerToProviderKmip` metodo per assegnare un server di chiavi KMIP (Key Management Interoperability Protocol) al fornitore di chiavi specificato. Durante l'assegnazione, il server viene contattato per verificarne la funzionalità. Se il server delle chiavi specificato è già assegnato al fornitore delle chiavi specificato, non viene intrapresa alcuna azione e non viene restituito alcun errore. È possibile rimuovere l'assegnazione utilizzando `RemoveKeyServerFromProviderKmip` metodo.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID fornitore di chiavi	ID del fornitore delle chiavi a cui assegnare il server delle chiavi.	intero	Nessuno	SÌ
ID del server chiave	L'ID del server delle chiavi da assegnare.	intero	Nessuno	SÌ

Valori di ritorno

Questo metodo non ha valore di ritorno. L'assegnazione è considerata riuscita finché non viene restituito alcun errore.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

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

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

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

Nuovo dalla versione

11,7

CreateKeyProviderKmip

Puoi usare il `CreateKeyProviderKmip` metodo per creare un fornitore di chiavi KMIP (Key Management Interoperability Protocol) con il nome specificato. Un fornitore di chiavi definisce un meccanismo e una posizione per recuperare le chiavi di autenticazione. Quando si crea un nuovo fornitore di chiavi KMIP, non gli viene assegnato alcun server di chiavi KMIP. Per creare un server di chiavi KMIP, utilizzare `CreateKeyServerKmip` metodo. Per assegnarlo a un fornitore, vedere `AddKeyServerToProviderKmip` .

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
Nome del fornitore di chiavi	Nome da associare al fornitore di chiavi KMIP creato. Questo nome viene utilizzato solo a scopo di visualizzazione e non deve essere univoco.	corda	Nessuno	SÌ

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
kmipKeyProvider	Un oggetto contenente dettagli sul fornitore di chiavi appena creato.	"Fornitore di chiaviKmip"

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

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

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

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

Nuovo dalla versione

11,7

CreateKeyServerKmip

Puoi usare il `CreateKeyServerKmip` metodo per creare un server di chiavi KMIP (Key Management Interoperability Protocol) con gli attributi specificati. Durante la creazione, il server non viene contattato; non è necessario che esista prima di poter utilizzare questo metodo. Per le configurazioni di server chiave in cluster, è necessario fornire i nomi host o gli indirizzi IP di tutti i nodi del server nel parametro kmipKeyServerHostnames. Puoi usare il `TestKeyServerKmip` metodo per testare un server di chiavi.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
kmipCaCertificate	Il certificato della chiave pubblica della CA radice del server delle chiavi esterno. Verrà utilizzato per verificare il certificato presentato dal server delle chiavi esterno nella comunicazione TLS. Per i cluster di server chiave in cui i singoli server utilizzano CA diverse, fornire una stringa concatenata contenente i certificati radice di tutte le CA.	corda	Nessuno	SÌ
kmipClientCertificate	Un certificato PKCS#10 X.509 codificato Base64 in formato PEM utilizzato dal client Solidfire KMIP.	corda	Nessuno	SÌ
kmipKeyServerHostnames	Matrice dei nomi host o degli indirizzi IP associati a questo server di chiavi KMIP. È necessario fornire più nomi host o indirizzi IP solo se i server chiave sono in una configurazione cluster.	matrice di stringhe	Nessuno	SÌ

Nome	Descrizione	Tipo	Valore predefinito	Necessario
kmipKeyServerNam e	Il nome del server delle chiavi KMIP. Questo nome viene utilizzato solo a scopo di visualizzazione e non deve essere univoco.	corda	Nessuno	SÌ
kmipKeyServerPort	Il numero di porta associato a questo server di chiavi KMIP (in genere 5696).	intero	Nessuno	NO

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
kmipKeyServer	Un oggetto contenente dettagli sul server delle chiavi appena creato.	"KeyServerKmip"

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

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

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
   "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
        }
     }
}
```


Nuovo dalla versione

11,7

Crea coppia di chiavi pubbliche e private

Puoi usare il `CreatePublicPrivateKeyPair` metodo per creare chiavi SSL pubbliche e private. È possibile utilizzare queste chiavi per generare richieste di firma del certificato. Per ogni cluster di archiviazione può essere utilizzata una sola coppia di chiavi. Prima di utilizzare questo metodo per sostituire le chiavi esistenti, assicurarsi che le chiavi non siano più utilizzate da alcun provider.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
Nome comune	Il campo **Nome comune** del nome distinto X.509 (CN).	corda	Nessuno	NO
Paese	Il campo **Paese** del nome distinto X.509 ©.	corda	Nessuno	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
indirizzo e-mail	Il campo **Indirizzo e-mail** del nome distinto X.509 (MAIL).	corda	Nessuno	NO
località	Il campo **Nome località** del nome distinto X.509 (L).	corda	Nessuno	NO
organizzazione	Il campo **Nome organizzazione** del nome distinto X.509 (O).	corda	Nessuno	NO
unità organizzativa	Il campo **Nome unità organizzativa** (OU) del nome distinto X.509.	corda	Nessuno	NO
stato	Il campo **Stato** o **Nome della provincia** del nome distinto X.509 (ST o SP o S).	corda	Nessuno	NO

Valori di ritorno

Questo metodo non ha valori di ritorno. Se non si verificano errori, la creazione della chiave è considerata riuscita.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

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

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

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

Nuovo dalla versione

11,7

DeleteKeyProviderKmip

Puoi usare il `DeleteKeyProviderKmip` metodo per eliminare il fornitore di chiavi KMIP (Key Management Interoperability Protocol) inattivo specificato.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID fornitore di chiavi	L'ID del fornitore della chiave da eliminare.	intero	Nessuno	SÌ

Valori di ritorno

Questo metodo non ha valori di ritorno. L'operazione di eliminazione è considerata riuscita finché non si verificano errori.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

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

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

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

Nuovo dalla versione

11,7

DeleteKeyServerKmip

Puoi usare il `DeleteKeyServerKmip` metodo per eliminare un server di chiavi KMIP (Key Management Interoperability Protocol) esistente. È possibile eliminare un server di chiavi a meno che non sia l'ultimo assegnato al suo provider e che il provider fornisca chiavi attualmente in uso.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID del server chiave	ID del server delle chiavi KMIP da eliminare.	intero	Nessuno	SÌ

Valori di ritorno

Questo metodo non ha valori di ritorno. L'operazione di eliminazione è considerata riuscita se non si verificano errori.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

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

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

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

Nuovo dalla versione

11,7

Disabilita la crittografia a riposo

Puoi usare il `DisableEncryptionAtRest` metodo per rimuovere la crittografia precedentemente applicata al cluster utilizzando `EnableEncryptionAtRest` metodo. Questo metodo di disattivazione è asincrono e restituisce una risposta prima che la crittografia venga disabilitata. Puoi usare il `GetClusterInfo` metodo per interrogare il sistema per vedere quando il processo è stato completato.

- Non è possibile utilizzare questo metodo per disattivare la crittografia software a riposo. Per disabilitare la crittografia software a riposo, è necessario"creare un nuovo cluster" con la crittografia software a riposo disabilitata.
- Per visualizzare lo stato corrente della crittografia a riposo, della crittografia software a riposo o di entrambe sul cluster, utilizzare "metodo per ottenere informazioni sul cluster". Puoi usare il `GetSoftwareEncryptionAtRestInfo` "metodo per ottenere informazioni che il cluster utilizza per crittografare i dati a riposo".

Parametri

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

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

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

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

Nuovo dalla versione

9,6

Trova maggiori informazioni

- "Ottieni informazioni sul cluster"
- "Documentazione del software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"

Abilita crittografia a riposo

Puoi usare il `EnableEncryptionAtRest` metodo per abilitare la crittografia Advanced Encryption Standard (AES) a 256 bit a riposo sul cluster, in modo che il cluster possa gestire la chiave di crittografia utilizzata per le unità su ciascun nodo. Questa funzione non è abilitata per impostazione predefinita.

- Per visualizzare lo stato corrente della crittografia a riposo e/o della crittografia software a riposo sul cluster, utilizzare"metodo per ottenere informazioni sul cluster" . Puoi usare il `GetSoftwareEncryptionAtRestInfo` "metodo per ottenere informazioni che il cluster utilizza per crittografare i dati a riposo".
- Questo metodo non abilita la crittografia software a riposo. Questo può essere fatto solo utilizzando il"metodo di creazione del cluster" con `enableSoftwareEncryptionAtRest` impostato su `true` .

Quando si abilita la crittografia a riposo, il cluster gestisce automaticamente le chiavi di crittografia internamente per le unità su ciascun nodo del cluster.

Se viene specificato un keyProviderID, la password viene generata e recuperata in base al tipo di fornitore di chiavi. In genere, questa operazione viene eseguita utilizzando un server di chiavi KMIP (Key Management Interoperability Protocol) nel caso di un fornitore di chiavi KMIP. Dopo questa operazione, il provider specificato viene considerato attivo e non può essere eliminato finché la crittografia a riposo non viene disabilitata utilizzando `DisableEncryptionAtRest` metodo.

Se si dispone di un tipo di nodo con un numero di modello che termina con "-NE", il `EnableEncryptionAtRest` la chiamata al metodo fallirà con una risposta del tipo "Crittografia non consentita". Il cluster ha rilevato un nodo non crittografabile".

È opportuno abilitare o disabilitare la crittografia solo quando il cluster è in esecuzione e in buono stato. Puoi abilitare o disabilitare la crittografia a tua discrezione e tutte le volte che ne hai bisogno.

Questo processo è asincrono e restituisce una risposta prima che la crittografia venga abilitata. Puoi usare il `GetClusterInfo` metodo per interrogare il sistema per vedere quando il processo è stato completato.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID fornitore di chiavi	L'ID di un fornitore di chiavi KMIP da utilizzare.	intero	Nessuno	NO

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

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

Esempi di risposta

Questo metodo restituisce una risposta simile al seguente esempio dal metodo EnableEncryptionAtRest. Non ci sono risultati da segnalare.

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

Quando la crittografia a riposo è abilitata su un cluster, GetClusterInfo restituisce un risultato che descrive lo stato della crittografia a riposo ("encryptionAtRestState") come "abilitato". Dopo che la crittografia a riposo è completamente abilitata, lo stato restituito cambia in "abilitato".

```
{
   "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"
      }
   }
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

- "SecureEraseDrives"
- "Ottieni informazioni sul cluster"
- "Documentazione del software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"

Ottieni richiesta di firma del certificato del client

Puoi usare il `GetClientCertificateSignRequest` metodo per generare una richiesta di firma del certificato che può essere firmata da un'autorità di certificazione per generare un certificato client per il cluster. I certificati firmati sono necessari per stabilire una relazione di fiducia per l'interazione con servizi esterni.

Parametri

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
clientCertificateSignRequest	Una richiesta di firma del certificato client PKCS#10 X.509 codificato in formato PEM Base64.	corda

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

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

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

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

Nuovo dalla versione

11,7

GetKeyProviderKmip

Puoi usare il `GetKeyProviderKmip` metodo per recuperare informazioni sul fornitore di chiavi KMIP (Key Management Interoperability Protocol) specificato.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID fornitore di chiavi	ID dell'oggetto fornitore di chiavi KMIP da restituire.	intero	Nessuno	SÌ

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
kmipKeyProvider	Un oggetto contenente dettagli sul fornitore della chiave richiesto.	"Fornitore di chiaviKmip"

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

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

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

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

Nuovo dalla versione

11,7

GetKeyServerKmip

Puoi usare il `GetKeyServerKmip` metodo per restituire informazioni sul server delle chiavi KMIP (Key Management Interoperability Protocol) specificato.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID del server chiave	ID del server delle chiavi KMIP su cui restituire informazioni.	intero	Nessuno	SÌ

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
kmipKeyServer	Un oggetto contenente dettagli sul server delle chiavi richiesto.	"KeyServerKmip"

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

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

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
   "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
        }
     }
}
```


Nuovo dalla versione

11,7

Ottieni informazioni sulla crittografia software a riposo

Puoi usare il `GetSoftwareEncryptionAtRestInfo` Metodo per ottenere informazioni sulla crittografia software a riposo che il cluster utilizza per crittografare i dati a riposo.

Parametri

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Parametro	Descrizione	Tipo	Opzionale
masterKeyInfo	Informazioni sulla chiave master di crittografia a riposo del software corrente.	EncryptionKeyInfo	VERO

Parametro	Descrizione	Tipo	Opzionale
rekeyMasterKeyAsyncResultID	ID del risultato asincrono dell'operazione di reimpostazione delle chiavi corrente o più recente (se presente), se non è stata ancora eliminata. `GetAsyncResult` l'output includerà un `newKey` campo che contiene informazioni sulla nuova chiave principale e un `keyToDecommission` campo che contiene informazioni sulla vecchia chiave.	intero	VERO
stato	Stato attuale della crittografia software a riposo. I valori possibili sono `disabled` O `enabled` .	corda	Falso
versione	Numero di versione che viene incrementato ogni volta che viene abilitata la crittografia software a riposo.	intero	Falso

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

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

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

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

Nuovo dalla versione

12,3

Trova maggiori informazioni

- "Documentazione del software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"

ListKeyProvidersKmip

Puoi usare il `ListKeyProvidersKmip` metodo per recuperare un elenco di tutti i fornitori di chiavi KMIP (Key Management Interoperability Protocol) esistenti. È possibile filtrare l'elenco specificando parametri aggiuntivi.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
keyProviderIsActive	I filtri hanno restituito oggetti server chiave KMIP in base al loro stato attivo. Valori possibili: • true: restituisce solo i provider di chiavi KMIP attivi (che forniscono chiavi attualmente in uso). • false: restituisce solo i provider di chiavi KMIP inattivi (che non forniscono chiavi e possono essere eliminati). Se omesso, i provider di chiavi KMIP restituiti non vengono filtrati in base al fatto che siano attivi.	booleano	Nessuno	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
kmipKeyProviderHasServerAssigned	I filtri hanno restituito i provider di chiavi KMIP in base al fatto che abbiano o meno un server di chiavi KMIP assegnato. Valori possibili: • true: restituisce solo i provider di chiavi KMIP a cui è assegnato un server di chiavi KMIP. • false: restituisce solo i provider di chiavi KMIP a cui non è assegnato un server di chiavi KMIP. Se omesso, i provider di chiavi KMIP restituiti non vengono filtrati in base all'assegnazione o meno di un server di chiavi KMIP.	booleano	Nessuno	NO

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
kmipKeyProviders	Un elenco dei fornitori di chiavi KMIP che sono stati creati.	"Fornitore di chiaviKmip"vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

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

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

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

Nuovo dalla versione

11,7

ListKeyServersKmip

Puoi usare il `ListKeyServersKmip` metodo per elencare tutti i server chiave KMIP (Key Management Interoperability Protocol) creati. È possibile filtrare i risultati specificando parametri aggiuntivi.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID fornitore di chiavi	Se specificato, il metodo restituisce solo i server delle chiavi KMIP assegnati al provider delle chiavi KMIP specificato. Se omesso, i server delle chiavi KMIP restituiti non verranno filtrati in base al fatto che siano assegnati o meno al fornitore di chiavi KMIP specificato.	intero	Nessuno	NO
kmipAssignedProviderIsActive	I filtri hanno restituito oggetti server chiave KMIP in base al loro stato attivo. Valori possibili: • true: restituisce solo i server delle chiavi KMIP attivi (che forniscono le chiavi attualmente in uso). • false: restituisce solo i server delle chiavi KMIP inattivi (che non forniscono chiavi e possono essere eliminati). Se omesso, i server delle chiavi KMIP restituiti non vengono filtrati in base al fatto che siano attivi o meno.	booleano	Nessuno	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
kmipHasProviderAssigned	I filtri hanno restituito i server delle chiavi KMIP in base all'assegnazione o meno di un fornitore di chiavi KMIP. Valori possibili: • true: restituisce solo i server di chiavi KMIP a cui è assegnato un provider di chiavi KMIP. • false: restituisce solo i server di chiavi KMIP a cui non è assegnato un provider di chiavi KMIP. Se omesso, i server delle chiavi KMIP restituiti non vengono filtrati in base all'assegnazione o meno di un provider di chiavi KMIP.	booleano	Nessuno	NO

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
kmipKeyServers	L'elenco completo dei server chiave KMIP che sono stati creati.	"KeyServerKmip"vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

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

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

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

Nuovo dalla versione

11,7

ModifyKeyServerKmip

Puoi usare il `ModifyKeyServerKmip` metodo per modificare un server di chiavi KMIP (Key Management Interoperability Protocol) esistente con gli attributi specificati. Sebbene l'unico parametro obbligatorio sia keyServerID, una richiesta contenente solo keyServerID non eseguirà alcuna azione e non restituirà alcun errore. Tutti gli altri parametri specificati sostituiranno i valori esistenti per il server delle chiavi con il keyServerID specificato. Durante l'operazione viene contattato il server delle chiavi per verificarne il funzionamento. È possibile specificare più nomi host o indirizzi IP con il parametro kmipKeyServerHostnames, ma solo se i server chiave sono in una configurazione in cluster.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID del server chiave	ID del server chiavi KMIP da modificare.	intero	Nessuno	SÌ
kmipCaCertificate	Il certificato della chiave pubblica della CA radice del server delle chiavi esterno. Verrà utilizzato per verificare il certificato presentato dal server delle chiavi esterno nella comunicazione TLS. Per i cluster di server chiave in cui i singoli server utilizzano CA diverse, fornire una stringa concatenata contenente i certificati radice di tutte le CA.	corda	Nessuno	NO
kmipClientCertificate	Un certificato PKCS#10 X.509 codificato Base64 in formato PEM utilizzato dal client Solidfire KMIP.	corda	Nessuno	NO
kmipKeyServerHostnames	Matrice dei nomi host o degli indirizzi IP associati a questo server di chiavi KMIP. È necessario fornire più nomi host o indirizzi IP solo se i server chiave sono in una configurazione cluster.	matrice di stringhe	Nessuno	NO

kmipKeyServerNam e	Il nome del server delle chiavi KMIP. Questo nome viene utilizzato solo a scopo di visualizzazione e non deve essere univoco.	corda	Nessuno	NO
kmipKeyServerPort	Il numero di porta associato a questo server di chiavi KMIP (in genere 5696).	intero	Nessuno	NO

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
kmipKeyServer	Un oggetto contenente dettagli sul server delle chiavi appena modificato.	"KeyServerKmip"

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

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

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
   "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
        }
     }
}
```

Nuovo dalla versione

11,7

RekeySoftwareEncryptionAtRestMasterKey

Puoi usare il `RekeySoftwareEncryptionAtRestMasterKey` Metodo per ricodificare la chiave master di crittografia software a riposo utilizzata per crittografare le DEK (chiavi di crittografia dei dati). Durante la creazione del cluster, la crittografia software a riposo viene configurata per utilizzare Internal Key Management (IKM). Questo metodo di reimpostazione delle chiavi può essere utilizzato dopo la creazione del cluster per utilizzare IKM o External Key Management (EKM).

Parametri

Questo metodo ha i seguenti parametri di input. Se il `keyManagementType` Se il parametro non è specificato, l'operazione di reimpostazione delle chiavi viene eseguita utilizzando la configurazione di gestione delle chiavi esistente. Se il `keyManagementType` è specificato e il fornitore della chiave è esterno, il `keyProviderID` deve essere utilizzato anche il parametro.

Parametro	Descrizione	Tipo	Opzionale
Tipo di gestione delle chiavi	Tipo di gestione delle chiavi utilizzato per gestire la chiave principale. I valori possibili sono: `Internal` : Reimpostare la chiave utilizzando la gestione delle chiavi interne. `External` : Reimpostare la chiave utilizzando la gestione delle chiavi esterne. Se questo parametro non viene specificato, l'operazione di reimpostazione delle chiavi viene eseguita utilizzando la configurazione di gestione delle chiavi esistente.	corda	VERO
ID fornitore di chiavi	L'ID del fornitore della chiave da utilizzare. Questo è un valore univoco restituito come parte di uno dei `CreateKeyProvider` metodi. L'ID è richiesto solo quando `keyManagementType` È `External` e non è altrimenti valido.	intero	VERO

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Parametro	Descrizione	Tipo	Opzionale
asyncHandle	Determinare lo stato dell'operazione di reimpostazione delle chiavi utilizzando questo `asyncHandle` valore con `GetAsyncResult`. `GetAsyncResult` l'output includerà un `newKey` campo che contiene informazioni sulla nuova chiave principale e un `keyToDecommission` campo che contiene informazioni sulla vecchia chiave.	intero	Falso

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

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

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

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

Nuovo dalla versione

12,3

Trova maggiori informazioni

- "Documentazione del software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"

RemoveKeyServerFromProviderKmip

Puoi usare il `RemoveKeyServerFromProviderKmip` metodo per annullare l'assegnazione del server delle chiavi KMIP (Key Management Interoperability Protocol) specificato al provider a cui era assegnato. È possibile annullare l'assegnazione di un server di chiavi al suo provider, a meno che non sia l'ultimo e il suo provider sia attivo (che fornisce chiavi attualmente in uso). Se il server delle chiavi specificato non è assegnato a un provider, non viene intrapresa alcuna azione e non viene restituito alcun errore.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID del server chiave	ID del server delle chiavi KMIP da annullare l'assegnazione.	intero	Nessuno	SÌ

Valori di ritorno

Questo metodo non ha valori di ritorno. La rimozione è considerata riuscita finché non viene restituito alcun errore.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

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

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

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

Nuovo dalla versione

11,7

SignSshKeys

Dopo che SSH è abilitato sul cluster utilizzando"Metodo EnableSSH" , puoi usare il `SignSshKeys` metodo per ottenere l'accesso a una shell su un nodo.

A partire dall'elemento 12.5, `sfreadonly` è un nuovo account di sistema che consente la risoluzione dei problemi di base su un nodo. Questa API consente l'accesso SSH utilizzando `sfreadonly` account di sistema su tutti i nodi del cluster.

> Salvo diversa indicazione da parte del supporto NetApp , qualsiasi modifica al sistema non è supportata, invalidando il contratto di supporto e potendo causare instabilità o inaccessibilità dei dati.

Dopo aver utilizzato il metodo, è necessario copiare il portachiavi dalla risposta, salvarlo sul sistema che avvierà la connessione SSH, quindi eseguire il seguente comando:

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

```
`identity_file`è un file da cui viene letta l'identità (chiave privata)
per l'autenticazione con chiave pubblica e `node_ip` è l'indirizzo IP del
nodo.  Per maggiori informazioni su `identity_file` , vedere la pagina man
di SSH.
```

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
durata	Numero intero da 1 a 24 che indica il numero di ore per cui la chiave firmata è valida. Se la durata non è specificata, viene utilizzato il valore predefinito.	intero	1	NO
chiave pubblica	Se specificato, questo parametro restituirà solo signed_public_key anziché creare un portachiavi completo per l'utente.  Chiavi pubbliche inviate tramite la barra degli URL in un browser con + vengono interpretati come segni spaziati e di interruzione.	corda	Nullo	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
sfadmin	Consente l'accesso all'account shell sfadmin quando si effettua la chiamata API con accesso al cluster supportAdmin o quando il nodo non si trova in un cluster.	booleano	Falso	NO

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
stato_keygen	Contiene l'identità nella chiave firmata, i principali consentiti e le date di inizio e fine valide per la chiave.	corda
chiave privata	Un valore di chiave SSH privata viene restituito solo se l'API sta generando un portachiavi completo per l'utente finale. Il valore è codificato in Base64; è necessario decodificare il valore quando viene scritto in un file per garantire che venga letto come una chiave privata valida.	corda

Nome	Descrizione	Tipo
chiave pubblica	Un valore di chiave SSH pubblica viene restituito solo se l'API sta generando un portachiavi completo per l'utente finale. Quando si passa un parametro public_key al metodo API, solo il `signed_public_key` il valore viene restituito nella risposta.	corda
chiave pubblica firmata	La chiave pubblica SSH risultante dalla firma della chiave pubblica, indipendentemente dal fatto che sia stata fornita dall'utente o generata tramite API.	corda

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

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

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

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

In questo esempio, viene firmata e restituita una chiave pubblica valida per la durata (1-24 ore).

Nuovo dalla versione

12,5

TestKeyProviderKmip

Puoi usare il `TestKeyProviderKmip` metodo per verificare se il fornitore di chiavi KMIP (Key Management Interoperability Protocol) specificato è raggiungibile e funziona normalmente.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID fornitore di chiavi	L'ID del fornitore della chiave da testare.	intero	Nessuno	SÌ

Valori di ritorno

Questo metodo non ha valori di ritorno. Il test è considerato riuscito finché non viene restituito alcun errore.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

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

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

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

Nuovo dalla versione

11,7

TestKeyServerKmip

Puoi usare il `TestKeyServerKmip` metodo per verificare se il server delle chiavi KMIP (Key Management Interoperability Protocol) specificato è raggiungibile e funziona normalmente.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID del server chiave	ID del server delle chiavi KMIP da testare.	intero	Nessuno	SÌ

Valori di ritorno

Questo metodo non ha valori di ritorno. Il test è considerato riuscito se non vengono restituiti errori.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

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

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

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

Nuovo dalla versione

11,7

Informazioni sul copyright

Informazioni sul marchio commerciale