Metodi API di sicurezza

Element Software

NetApp
October 01, 2024

Sommario

Metodi API di sicurezza

È possibile integrare il software Element con servizi esterni correlati alla sicurezza, ad esempio un server di gestione delle chiavi esterno. Questi metodi relativi alla sicurezza consentono di configurare le funzionalità di sicurezza degli elementi, ad esempio la gestione delle chiavi esterne per la crittografia a riposo.

- AddKeyServerToProviderKmip
- CreateKeyProviderKmip
- CreateKeyServerKmip
- CreatePublicPrivateKeyPair
- DeleteKeyProviderKmip
- DeleteKeyServerKmip
- DisableEncryptionAtRest
- EnableEncryptionAtRest
- GetClientCertificateSignRequest
- GetKeyProviderKmip
- GetKeyServerKmip
- ListKeyProvidersKmip
- ListKeyServerKmip
- ModifyKeyServerKmip
- RemoveKeyServerFromProviderKmip
- SignSshKeys
- TestKeyProviderKmip
- TestKeyServerKmip

Trova ulteriori informazioni

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

AddKeyServerToProviderKmip

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

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
KeyProviderID	L'ID del provider di chiavi a cui assegnare il server di chiavi.	intero	Nessuno	Sì
KeyServerID	L'ID del server chiavi da assegnare.	intero	Nessuno	Sì

Valori restituiti

Questo metodo non ha alcun valore restituito. L'assegnazione viene considerata riuscita a condizione che non venga restituito alcun errore.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

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

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

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

Novità dalla versione

11,7

CreateKeyProviderKmip

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

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
KeyProviderName	Il nome da associare al provider di chiavi KMIP creato. Questo nome viene utilizzato solo per scopi di visualizzazione e non deve essere univoco.	stringa	Nessuno	Sì

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
KmipKeyProvider	Oggetto contenente dettagli sul provider di chiavi appena creato.	"KeyProviderKmip"

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

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

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

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

Novità dalla versione

11,7

CreateKeyServerKmip

Puoi utilizzare questo `CreateKeyServerKmip` metodo per creare un server delle 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 utilizzare questo metodo. Per le configurazioni dei server delle chiavi in cluster, è necessario fornire i nomi host o gli indirizzi IP di tutti i nodi del server nel parametro kmipKeyServerHostnames. È possibile utilizzare il `TestKeyServerKmip` metodo per testare un server delle chiavi.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
KmipCaCertificate	Il certificato a chiave pubblica della CA principale del server di chiavi esterno. Questa opzione viene utilizzata per verificare il certificato presentato dal server delle chiavi esterno nella comunicazione TLS. Per i cluster di server di chiavi in cui i singoli server utilizzano CA diverse, fornire una stringa concatenata contenente i certificati root di tutte le CA.	stringa	Nessuno	Sì
KmipClientCertificate	Un certificato PKCS 10 X.509 con codifica Base64 in formato PEM utilizzato dal client KMIP di SolidFire.	stringa	Nessuno	Sì
KmipKeyServerHostnames	Array dei nomi host o degli indirizzi IP associati al server delle chiavi KMIP. È necessario fornire più nomi host o indirizzi IP solo se i server delle chiavi sono in una configurazione in cluster.	array di stringhe	Nessuno	Sì
KmipKeyServerName	Il nome del server delle chiavi KMIP. Questo nome viene utilizzato solo per scopi di visualizzazione e non deve essere univoco.	stringa	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
KmipKeyServerPort	Il numero di porta associato al server delle chiavi KMIP (generalmente 5696).	intero	Nessuno	No

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
KmipKeyServer	Oggetto contenente dettagli sul server chiavi appena creato.	"KeyServerKmip"

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "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 all'esempio seguente:

```
{
   "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
        }
     }
}
```

Novità dalla versione

11,7

CreatePublicPrivateKeyPair

È possibile utilizzare questo `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 storage 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	Obbligatorio
Nome comune	Il campo Nome distinto X.509 **Nome comune** (CN).	stringa	Nessuno	No
paese	Il campo Nome distinto X.509 **Paese** ©.	stringa	Nessuno	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
EmailAddress	Il campo Nome distinto X.509 **Indirizzo e-mail** (E-MAIL).	stringa	Nessuno	No
località	Il campo Nome distinto X.509 **Nome località** (L).	stringa	Nessuno	No
organizzazione	Il campo Nome distinto X.509 **Nome organizzazione** (o).	stringa	Nessuno	No
OrganisationalUnit	Il campo Nome distinto X.509 **Nome unità organizzativa** (OU).	stringa	Nessuno	No
stato	Il campo Nome distinto X.509 **Stato** o **Nome provincia** (ST o SP o S).	stringa	Nessuno	No

Valori restituiti

Questo metodo non ha valori restituiti. Se non si verificano errori, la creazione della chiave viene considerata corretta.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

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

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

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

Novità dalla versione

11,7

DeleteKeyProviderKmip

Puoi utilizzare questo `DeleteKeyProviderKmip` metodo per eliminare il provider di chiavi inattivo specificato dal Key Management Interoperability Protocol (KMIP).

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
KeyProviderID	L'ID del provider di chiavi da eliminare.	intero	Nessuno	Sì

Valori restituiti

Questo metodo non ha valori restituiti. L'operazione di eliminazione viene considerata riuscita finché non si verifica alcun errore.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

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

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

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

Novità dalla versione

11,7

DeleteKeyServerKmip

Puoi utilizzare questo `DeleteKeyServerKmip` metodo per eliminare un server delle chiavi KMIP (Key Management Interoperability Protocol) esistente. È possibile eliminare un server chiavi a meno che non sia l'ultimo assegnato al proprio provider e il provider non stia fornendo chiavi attualmente in uso.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
KeyServerID	L'ID del server chiavi KMIP da eliminare.	intero	Nessuno	Sì

Valori restituiti

Questo metodo non ha valori restituiti. L'operazione di eliminazione viene considerata corretta se non si verificano errori.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

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

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

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

Novità dalla versione

11,7

DisableEncryptionAtRest

È possibile utilizzare il `DisableEncryptionAtRest` metodo per rimuovere la crittografia applicata in precedenza al cluster utilizzando il `EnableEncryptionAtRest` metodo. Questo metodo di disattivazione è asincrono e restituisce una risposta prima che la crittografia venga disattivata. È possibile utilizzare il `GetClusterInfo` metodo per eseguire il polling del sistema per verificare il completamento del processo.

Per visualizzare lo stato attuale della crittografia a riposo e/o della crittografia software a riposo nel cluster, utilizzare il "ottieni il metodo delle informazioni sul cluster". È possibile utilizzare `GetSoftwareEncryptionAtRestInfo` "metodo per ottenere informazioni utilizzate dal cluster per crittografare i dati inattivi".

Non è possibile utilizzare questo metodo per disattivare la crittografia software a riposo. Per disattivare la crittografia software a riposo, è necessario "creare un nuovo cluster"disattivare la crittografia software a riposo.

Parametri

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

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

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

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

Novità dalla versione

9,6

Trova ulteriori informazioni

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

EnableEncryptionAtRest

Puoi utilizzare questo `EnableEncryptionAtRest` metodo per abilitare la crittografia a 256 bit Advanced Encryption Standard (AES) a riposo nel cluster, in modo che il cluster possa gestire la chiave di crittografia utilizzata per i dischi di ogni nodo. Questa funzione non è attivata per impostazione predefinita.

Per visualizzare lo stato attuale della crittografia a riposo e/o della crittografia software a riposo nel cluster, utilizzare il "ottieni il metodo delle informazioni sul cluster". È possibile utilizzare `GetSoftwareEncryptionAtRestInfo` "metodo per ottenere informazioni utilizzate dal cluster per crittografare i dati inattivi".

Questo metodo non attiva la crittografia software a riposo. Questa operazione può essere eseguita solo utilizzando il "creare il metodo del cluster" con `enableSoftwareEncryptionAtRest` impostato su `true`.

Quando si attiva la crittografia a riposo, il cluster gestisce automaticamente le chiavi di crittografia interne per i dischi su ciascun nodo del cluster.

Se viene specificato keyProviderID, la password viene generata e recuperata in base al tipo di provider di

chiavi. In genere, questa operazione viene eseguita utilizzando un server di chiavi KMIP (Key Management Interoperability Protocol) nel caso di un provider di chiavi KMIP. Al termine di questa operazione, il provider specificato viene considerato attivo e non può essere eliminato finché non viene disattivata la crittografia a riposo mediante il `DisableEncryptionAtRest` metodo.

Se si dispone di un tipo di nodo con un numero di modello che termina con "-NE", la `EnableEncryptionAtRest` chiamata al metodo non riesce e viene visualizzato il messaggio "crittografia non consentita. Il cluster ha rilevato un nodo non crittografabile".

Attivare o disattivare la crittografia solo quando il cluster è in esecuzione e in stato di integrità. È possibile attivare o disattivare la crittografia a propria discrezione e con la frequenza richiesta.

Questo processo è asincrono e restituisce una risposta prima dell'attivazione della crittografia. È possibile utilizzare il `GetClusterInfo` metodo per eseguire il polling del sistema per verificare il completamento del processo.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
KeyProviderID	L'ID di un provider di chiavi KMIP da utilizzare.	intero	Nessuno	No

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

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

Esempi di risposte

Questo metodo restituisce una risposta simile all'esempio seguente dal metodo EnableEncryptionAtRest. Nessun risultato da segnalare.

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

Durante l'attivazione della crittografia a riposo su un cluster, GetClusterInfo restituisce un risultato che descrive lo stato di crittografia a riposo ("EncryptionAtRestState") come "abilitazione". Una volta attivata la crittografia a riposo, lo stato restituito diventa "Enabled" (attivato).

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

Novità dalla versione

9,6

Trova ulteriori informazioni

- "SecureEraseDrive"
- "GetClusterInfo"
- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

GetClientCertificateSignRequest

È possibile utilizzare questo `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 trust per l'interazione con i servizi esterni.

Parametri

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
ClientCertificateSignRequest	Una richiesta di firma del certificato client X.509 con codifica PKCS n. 10 in formato PEM Base64.	stringa

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

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

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

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

Novità dalla versione

11,7

GetKeyProviderKmip

Puoi utilizzare questo `GetKeyProviderKmip` metodo per recuperare le informazioni relative al provider di chiavi KMIP (Key Management Interoperability Protocol) specificato.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
KeyProviderID	L'ID dell'oggetto provider della chiave KMIP da restituire.	intero	Nessuno	Sì

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
KmipKeyProvider	Oggetto contenente dettagli sul provider di chiavi richiesto.	"KeyProviderKmip"

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

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

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

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

Novità dalla versione

11,7

GetKeyServerKmip

È possibile utilizzare questo `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	Obbligatorio
KeyServerID	L'ID del server chiavi KMIP su cui restituire le informazioni.	intero	Nessuno	Sì

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
KmipKeyServer	Oggetto contenente dettagli sul server delle chiavi richiesto.	"KeyServerKmip"

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

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

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "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
        }
    }
}
```

Novità dalla versione

11,7

GetSoftwareEncryptionAtRestInfo

Puoi utilizzare `GetSoftwareEncryptionAtRestInfo` il metodo per ottenere informazioni di crittografia software a riposo che il cluster utilizza per crittografare i dati a riposo.

Parametri

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Parametro	Descrizione	Tipo	Opzionale
MasterKeyInfo	Informazioni sulla chiave master di crittografia a riposo software corrente.	EncryptionKeyInfo	Vero
RekeyMasterKeyAsyncResultID	L'ID risultato asincrono dell'operazione di rekey 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 master e un `keyToDecommission` campo che contiene informazioni sulla vecchia chiave.	intero	Vero
stato	Lo stato corrente di crittografia software a riposo. I valori possibili sono `disabled` o `enabled`.	stringa	Falso
versione	Numero di versione incrementato ogni volta che viene attivata la crittografia software a riposo.	intero	Falso

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

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

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

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


Novità dalla versione

12,3

Trova ulteriori informazioni

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

ListKeyProvidersKmip

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

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
KeyProviderIsActive	I filtri hanno restituito oggetti KMIP Key Server in base all'attivazione o meno. Valori possibili: • Vero: Restituisce solo i provider di chiavi KMIP attivi (fornendo le chiavi attualmente in uso). • Falso: Restituisce solo i provider di chiavi KMIP inattivi (non fornendo alcuna chiave e che possono essere cancellati). Se omessi, i provider di chiavi KMIP restituiti non vengono filtrati in base alla loro attivazione o meno.	booleano	Nessuno	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
KmipKeyProviderHasServerAssigned	I filtri hanno restituito i provider di chiavi KMIP in base all'assegnazione o meno di un server di chiavi KMIP. Valori possibili: • Vero: Restituisce solo i provider di chiavi KMIP a cui è stato assegnato un server di chiavi KMIP. • Falso: Restituisce solo i provider di chiavi KMIP che non hanno un server di chiavi KMIP assegnato. Se omessi, 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 restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
KmipKeyProviders	Elenco dei provider di chiavi KMIP creati.	"KeyProviderKmip" array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

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

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

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

Novità dalla versione

11,7

ListKeyServerKmip

Puoi utilizzare questo `ListKeyServersKmip` metodo per elencare tutti i server chiave KMIP (Key Management Interoperability Protocol) che sono stati creati. È possibile filtrare i risultati specificando parametri aggiuntivi.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
KeyProviderID	Quando specificato, il metodo restituisce solo i server delle chiavi KMIP assegnati al provider di chiavi KMIP specificato. Se omessi, i server delle chiavi KMIP restituiti non verranno filtrati in base all'assegnazione o meno al provider di chiavi KMIP specificato.	intero	Nessuno	No
KmipAssignedProviderIsActive	I filtri hanno restituito oggetti KMIP Key Server in base all'attivazione o meno. Valori possibili: • Vero: Restituisce solo i server delle chiavi KMIP attivi (fornendo le chiavi attualmente in uso). • Falso: Restituisce solo i server delle chiavi KMIP inattivi (non fornendo alcuna chiave e che possono essere cancellati). Se omessi, i server delle chiavi KMIP restituiti non vengono filtrati in base alla loro attivazione o meno.	booleano	Nessuno	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
KmipHasProviderAssigned	I filtri hanno restituito i server delle chiavi KMIP in base all'assegnazione o meno di un provider di chiavi KMIP. Valori possibili: • Vero: Restituisce solo i server delle chiavi KMIP a cui è stato assegnato un provider di chiavi KMIP. • Falso: Restituisce solo i server di chiavi KMIP che non hanno un provider di chiavi KMIP assegnato. Se omessi, 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 restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
KmipKeyServers	L'elenco completo dei server delle chiavi KMIP creati.	"KeyServerKmip" array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

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

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

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

Novità dalla versione

11,7

ModifyKeyServerKmip

È possibile utilizzare questo `ModifyKeyServerKmip` metodo per modificare un server chiave KMIP (Key Management Interoperability Protocol) esistente in base agli attributi specificati. Sebbene l'unico parametro richiesto sia keyServerID, una richiesta contenente solo keyServerID non eseguirà alcuna azione e non restituirà alcun errore. Qualsiasi altro parametro specificato sostituirà i valori esistenti per il server chiavi con il keyServerID specificato. Il server delle chiavi viene contattato durante l'operazione per assicurarne il funzionamento. È possibile fornire più nomi host o indirizzi IP con il parametro kmipKeyServerHostnames, ma solo se i server delle chiavi sono in una configurazione in cluster.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
KeyServerID	L'ID del KMIP Key Server da modificare.	intero	Nessuno	Sì
KmipCaCertificate	Il certificato a chiave pubblica della CA principale del server di chiavi esterno. Questa opzione viene utilizzata per verificare il certificato presentato dal server delle chiavi esterno nella comunicazione TLS. Per i cluster di server di chiavi in cui i singoli server utilizzano CA diverse, fornire una stringa concatenata contenente i certificati root di tutte le CA.	stringa	Nessuno	No
KmipClientCertificate	Un certificato PKCS 10 X.509 con codifica Base64 in formato PEM utilizzato dal client KMIP di SolidFire.	stringa	Nessuno	No
KmipKeyServerHostnames	Array dei nomi host o degli indirizzi IP associati al server delle chiavi KMIP. È necessario fornire più nomi host o indirizzi IP solo se i server delle chiavi sono in una configurazione in cluster.	array di stringhe	Nessuno	No

KmipKeyServerNam e	Il nome del server delle chiavi KMIP. Questo nome viene utilizzato solo per scopi di visualizzazione e non deve essere univoco.	stringa	Nessuno	No
KmipKeyServerPort	Il numero di porta associato al server delle chiavi KMIP (generalmente 5696).	intero	Nessuno	No

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
KmipKeyServer	Oggetto contenente dettagli sul server delle chiavi appena modificato.	"KeyServerKmip"

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "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 all'esempio seguente:

```
{
   "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
        }
     }
}
```

Novità dalla versione

11,7

RekeySoftwareEncryptionAtRestMasterKey

È possibile utilizzare il `RekeySoftwareEncryptionAtRestMasterKey` metodo per riassegnare la chiave master di crittografia del software a riposo utilizzata per crittografare le chiavi DEK (Data Encryption Keys). Durante la creazione del cluster, la crittografia software a riposo viene configurata per l'utilizzo di IKM (Internal Key Management). Questo metodo di rekey 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` parametro non è specificato, l'operazione di rekey viene eseguita utilizzando la configurazione di gestione delle chiavi esistente. Se `keyManagementType` viene specificato e il provider della chiave è esterno, `keyProviderID` è necessario utilizzare anche il parametro.

Parametro	Descrizione	Tipo	Opzionale
KeyManagementType	Il tipo di gestione delle chiavi utilizzato per gestire la chiave master. I valori possibili sono: `Internal`: Eseguire la reimpostazione della chiave utilizzando la gestione interna della chiave. `External`: Eseguire nuovamente la chiave utilizzando la gestione esterna della chiave. Se questo parametro non viene specificato, l'operazione di rekey viene eseguita utilizzando la configurazione di gestione delle chiavi esistente.	stringa	Vero
KeyProviderID	L'ID del provider di chiavi da utilizzare. Si tratta di un valore univoco restituito come parte di uno dei `CreateKeyProvider` metodi. L'ID è richiesto solo quando `keyManagementType` è `External` e altrimenti non è valido.	intero	Vero

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

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

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

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

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

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

Novità dalla versione

12,3

Trova ulteriori informazioni

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

RemoveKeyServerFromProviderKmip

Puoi utilizzare questo `RemoveKeyServerFromProviderKmip` metodo per annullare l'assegnazione del server chiave KMIP (Key Management Interoperability Protocol) specificato dal provider a cui è stato assegnato. È possibile annullare l'assegnazione di un server chiavi dal proprio provider, a meno che non sia l'ultimo e il relativo provider sia attivo (fornendo le chiavi attualmente in uso). Se il server chiavi specificato non è assegnato a un provider, non viene eseguita alcuna azione e non viene restituito alcun errore.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
KeyServerID	L'ID del server chiavi KMIP da annullare l'assegnazione.	intero	Nessuno	Sì

Valori restituiti

Questo metodo non ha valori restituiti. La rimozione viene considerata riuscita a condizione che non venga restituito alcun errore.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

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

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

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

Novità dalla versione

11,7

SignSshKeys

Dopo che SSH è stato abilitato sul cluster utilizzando il "Metodo EnableSSH", è possibile utilizzare il `SignSshKeys` metodo per ottenere l'accesso ad una shell su un nodo.

A partire da Element 12,5, `sfreadonly` è un nuovo account di sistema che consente il troubleshooting di base di un nodo. Questa API abilita l'accesso SSH utilizzando l' `sfreadonly`account di sistema in tutti i nodi del cluster.

Se non richiesto dall'assistenza NetApp, eventuali modifiche al sistema non sono supportate, annullano il contratto di assistenza e potrebbero causare instabilità o inaccessibilità dei dati.

Dopo aver utilizzato il metodo, è necessario copiare il portachiavi dalla risposta, salvarlo nel 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 a chiave pubblica e `node_ip` rappresenta l'indirizzo
IP del nodo. Per ulteriori informazioni su `identity_file`, vedere la
pagina man SSH.
```

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
durata	Intero da 1 a 24 che riflette il numero di ore per la chiave firmata valida. Se la durata non è specificata, viene utilizzato il valore predefinito.	intero	1	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
Chiave pubblica	Se fornito, questo parametro restituirà solo la chiave_pubblica_firmata invece di creare un portachiavi completo all'utente.  Le chiavi pubbliche inviate utilizzando la barra URL in un browser con + sono interpretate come firma distanziata e interrotta.	stringa	Nullo	No
sfadmin	Consente l'accesso all'account shell sfadmin quando si effettua la chiamata API con l'accesso al cluster supportAdmin o quando il nodo non si trova in un cluster.	booleano	Falso	No

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
keygen_status	Contiene l'identità nella chiave firmata, le entità consentite e le date di inizio e di fine valide per la chiave.	stringa
private_key	Un valore chiave SSH privata viene restituito solo se l'API genera un portachiavi completo per l'utente finale. Il valore è codificato Base64; è necessario decodificare il valore quando viene scritto in un file per assicurarsi che venga letto come chiave privata valida.	stringa
chiave_pubblica	Un valore chiave SSH pubblico viene restituito solo se l'API genera un portachiavi completo per l'utente finale. Quando si passa un parametro public_key al metodo API, nella risposta viene restituito solo il `signed_public_key` valore.	stringa
chiave_pubblica_firmata	La chiave pubblica SSH risultante dalla firma della chiave pubblica, fornita dall'utente o generata dall'API.	stringa

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

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

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "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).

Novità dalla versione

12,5

TestKeyProviderKmip

Puoi utilizzare questo `TestKeyProviderKmip` metodo per verificare se il provider 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	Obbligatorio
KeyProviderID	L'ID del provider di chiavi da testare.	intero	Nessuno	Sì

Valori restituiti

Questo metodo non ha valori restituiti. Il test viene considerato riuscito finché non viene restituito alcun errore.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

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

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

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

Novità dalla versione

11,7

TestKeyServerKmip

Puoi utilizzare questo `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	Obbligatorio
KeyServerID	L'ID del server chiavi KMIP da testare.	intero	Nessuno	Sì

Valori restituiti

Questo metodo non ha valori restituiti. Se non vengono restituiti errori, il test viene considerato di successo.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

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

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

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

Novità dalla versione

11,7

Informazioni sul copyright

Informazioni sul marchio commerciale