



## **Metodi API di sicurezza**

### **Element Software**

NetApp  
April 17, 2024

This PDF was generated from [https://docs.netapp.com/it-it/element-software/api/reference\\_element\\_api\\_addkeyservertoproviderkmip.html](https://docs.netapp.com/it-it/element-software/api/reference_element_api_addkeyservertoproviderkmip.html) on April 17, 2024. Always check docs.netapp.com for the latest.

# Sommario

Metodi API di sicurezza .....	1
Trova ulteriori informazioni .....	1
AddKeyServerToProviderKmp .....	1
CreateKeyProviderKmp .....	3
CreateKeyServerKmp .....	4
CreatePublicPrivateKeyPair .....	7
DeleteKeyProviderKmp .....	9
DeleteKeyServerKmp .....	10
DisableEncryptionAtRest .....	11
EnableEncryptionAtRest .....	12
GetClientCertificateSignRequest .....	15
GetKeyProviderKmp .....	16
GetKeyServerKmp .....	17
GetSoftwareEncryptionAtRestInfo .....	18
ListKeyProvidersKmp .....	20
ListKeyServerKmp .....	23
ModifyKeyServerKmp .....	26
RekeySoftwareEncryptionAtRestMasterKey .....	29
RemoveKeyServerFromProviderKmp .....	32
SignSshKeys .....	33
TestKeyProviderKmp .....	37
TestKeyServerKmp .....	38

# 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.

- [AddKeyServerToProviderKmp](#)
- [CreateKeyProviderKmp](#)
- [CreateKeyServerKmp](#)
- [CreatePublicPrivateKeyPair](#)
- [DeleteKeyProviderKmp](#)
- [DeleteKeyServerKmp](#)
- [DisableEncryptionAtRest](#)
- [EnableEncryptionAtRest](#)
- [GetClientCertificateSignRequest](#)
- [GetKeyProviderKmp](#)
- [GetKeyServerKmp](#)
- [ListKeyProvidersKmp](#)
- [ListKeyServerKmp](#)
- [ModifyKeyServerKmp](#)
- [RemoveKeyServerFromProviderKmp](#)
- [SignSshKeys](#)
- [TestKeyProviderKmp](#)
- [TestKeyServerKmp](#)

## Trova ulteriori informazioni

- ["Documentazione software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"](#)

## AddKeyServerToProviderKmp

È possibile utilizzare `AddKeyServerToProviderKmp` Metodo per assegnare un server di 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 `RemoveKeyServerFromProviderKmp` 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": "AddKeyServerToProviderKnip",
  "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

# CreateKeyProviderK mip

È possibile utilizzare `CreateKeyProviderK mip` 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 chiavi KMIP, utilizzare `CreateKeyServerK mip` metodo. Per assegnarlo a un provider, vedere `AddKeyServerToProviderK mip`.

## 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
K mipKeyProvider	Oggetto contenente dettagli sul provider di chiavi appena creato.	<a href="#">"KeyProviderK mip"</a>

## Esempio di richiesta

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

```
{
  "method": "CreateKeyProviderK mip",
  "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

È possibile utilizzare `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 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 `TestKeyServerKmip` metodo per testare un server di 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.	<a href="#">"KeyServerKmip"</a>

## 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 `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 <b>Nome comune</b> (CN).	stringa	Nessuno	No
paese	Il campo Nome distinto X.509 <b>Paese</b> ©.	stringa	Nessuno	No

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

## DeleteKeyProviderK mip

È possibile utilizzare DeleteKeyProviderK mip Metodo per eliminare il provider di chiavi KMIP (Key Management Interoperability Protocol) inattivo specificato.

### 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": "DeleteKeyProviderK mip",
  "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

È possibile utilizzare DeleteKeyServerKmip Metodo per eliminare un server di 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 `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 disattivata. È possibile utilizzare `GetClusterInfo` metodo per eseguire il polling del sistema per verificare il completamento del processo.



Per visualizzare lo stato corrente della crittografia a riposo e/o della crittografia software a riposo nel cluster, utilizzare ["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"](#) con crittografia software a riposo disattivata.

## 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

È possibile utilizzare `EnableEncryptionAtRest` Metodo per attivare la crittografia AES (Advanced Encryption Standard) a 256 bit sul cluster in modo che il cluster possa gestire la chiave di crittografia utilizzata per i dischi su ciascun nodo. Questa funzione non è attivata per impostazione predefinita.



Per visualizzare lo stato corrente della crittografia a riposo e/o della crittografia software a riposo nel cluster, utilizzare ["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 ["creare il metodo del cluster"](#) con `enableSoftwareEncryptionAtRest` impostare 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. Dopo questa operazione, il provider specificato viene considerato attivo e non può essere eliminato fino a quando la crittografia a riposo non viene disattivata tramite `DisableEncryptionAtRest` metodo.



Se si dispone di un tipo di nodo con un numero di modello che termina con "-NE", la `EnableEncryptionAtRest` La 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 `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 `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":
    "MIIBYjCCATMCAQAwwYkxCzAJBgNVBAYTA1VTMRMwEQYDVQQIEwpDYWxpZm9ybm..."
  }
}
```

## Novità dalla versione

11,7

# GetKeyProviderKmip

È possibile utilizzare `GetKeyProviderKmip` Metodo per recuperare informazioni sul 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.	<a href="#">"KeyProviderKmip"</a>

## 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

## GetKeyServerKmp

È possibile utilizzare `GetKeyServerKmp` Metodo per restituire informazioni sul server di 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.	"KeyServerKmp"

## Esempio di richiesta

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

```
{
  "method": "GetKeyServerKnip",
  "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

È possibile utilizzare `GetSoftwareEncryptionAtRestInfo` metodo per ottenere informazioni sulla crittografia software a riposo utilizzate dal cluster 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 ancora eliminata. <code>GetAsyncResult</code> l'output includerà un <code>newKey</code> campo contenente informazioni sulla nuova chiave master e su <code>keyToDecommission</code> campo che contiene informazioni sulla vecchia chiave.	intero	Vero
stato	Lo stato corrente di crittografia software a riposo. I valori possibili sono <code>disabled</code> oppure <code>enabled</code> .	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

È possibile utilizzare `ListKeyProvidersKmip` Metodo per recuperare un elenco di tutti i provider 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	Obbligatorio
KeyProviderIsActive	<p>I filtri hanno restituito oggetti KMIP Key Server in base all'attivazione o meno. Valori possibili:</p> <ul style="list-style-type: none"> <li>• Vero: Restituisce solo i provider di chiavi KMIP attivi (fornendo le chiavi attualmente in uso).</li> <li>• Falso: Restituisce solo i provider di chiavi KMIP inattivi (non fornendo alcuna chiave e che possono essere cancellati).</li> </ul> <p>Se omessi, i provider di chiavi KMIP restituiti non vengono filtrati in base alla loro attivazione o meno.</p>	booleano	Nessuno	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
KmipKeyProviderHasServerAssigned	<p>I filtri hanno restituito i provider di chiavi KMIP in base all'assegnazione o meno di un server di chiavi KMIP. Valori possibili:</p> <ul style="list-style-type: none"> <li>• Vero: Restituisce solo i provider di chiavi KMIP a cui è stato assegnato un server di chiavi KMIP.</li> <li>• Falso: Restituisce solo i provider di chiavi KMIP che non hanno un server di chiavi KMIP assegnato.</li> </ul> <p>Se omessi, i provider di chiavi KMIP restituiti non vengono filtrati in base all'assegnazione o meno di un server di chiavi KMIP.</p>	booleano	Nessuno	No

## Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
KmipKeyProviders	Elenco dei provider di chiavi KMIP creati.	" <a href="#">KeyProviderKmip</a> " 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

È possibile utilizzare `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	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
KmipAssignedProvidersActive	<p>I filtri hanno restituito oggetti KMIP Key Server in base all'attivazione o meno. Valori possibili:</p> <ul style="list-style-type: none"> <li>• Vero: Restituisce solo i server delle chiavi KMIP attivi (fornendo le chiavi attualmente in uso).</li> <li>• Falso: Restituisce solo i server delle chiavi KMIP inattivi (non fornendo alcuna chiave e che possono essere cancellati).</li> </ul> <p>Se omessi, i server delle chiavi KMIP restituiti non vengono filtrati in base alla loro attivazione o meno.</p>	booleano	Nessuno	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
KmipHasProviderAs signed	<p>I filtri hanno restituito i server delle chiavi KMIP in base all'assegnazione o meno di un provider di chiavi KMIP. Valori possibili:</p> <ul style="list-style-type: none"> <li>• Vero: Restituisce solo i server delle chiavi KMIP a cui è stato assegnato un provider di chiavi KMIP.</li> <li>• Falso: Restituisce solo i server di chiavi KMIP che non hanno un provider di chiavi KMIP assegnato.</li> </ul> <p>Se omessi, i server delle chiavi KMIP restituiti non vengono filtrati in base all'assegnazione o meno di un provider di chiavi KMIP.</p>	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.	" <a href="#">KeyServerKmip</a> " 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 `ModifyKeyServerKmip` Metodo per modificare un server chiavi KMIP (Key Management Interoperability Protocol) esistente con gli 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

KmipKeyServerName	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.	<a href="#">"KeyServerKmip"</a>

## 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 `RekeySoftwareEncryptionAtRestMasterKey` Metodo per reimmettere la chiave master di crittografia a riposo del software utilizzata per crittografare le chiavi di crittografia dei dati (DEK). 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 specificato, l'operazione di rekey viene eseguita utilizzando la configurazione di gestione delle chiavi esistente. Se il `keyManagementType` è specificato e il provider di chiavi è esterno, il `keyProviderID` deve essere utilizzato anche il parametro.

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

## Valori restituiti

Questo metodo ha i seguenti valori restituiti:



Parametro	Descrizione	Tipo	Opzionale
AsyncHandle	Determinare lo stato dell'operazione di rekey utilizzando questo comando <code>asyncHandle</code> valore con <code>GetAsyncResult</code> . <code>GetAsyncResult</code> l'output includerà un <code>newKey</code> campo contenente informazioni sulla nuova chiave master e su <code>keyToDecommission</code> 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

È possibile utilizzare `RemoveKeyServerFromProviderKmip` Metodo per annullare l'assegnazione del server delle chiavi 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 l'attivazione di SSH sul cluster utilizzando "[Metodo EnableSSH](#)", è possibile utilizzare `SignSshKeys` metodo per ottenere l'accesso a una shell su un nodo.

Iniziando dall'elemento 12,5, `sfreadonly` è un nuovo account di sistema che consente il troubleshooting di base su un nodo. Questa API abilita l'accesso SSH utilizzando `sfreadonly` account di sistema in tutti i nodi nel 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 ``node_ip`` È 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
Chiave pubblica	<p>Se fornito, questo parametro restituirà solo la chiave_pubblica_firmata invece di creare un portachiavi completo all'utente.</p> <div>  <p>Le chiavi pubbliche inviate utilizzando la barra URL in un browser con + sono interpretate come firma distanziata e di interruzione.</p> </div>	stringa	Nulla	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
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	<p>Un valore chiave SSH privata viene restituito solo se l'API genera un portachiavi completo per l'utente finale.</p> <div>  <p>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.</p> </div>	stringa

Nome	Descrizione	Tipo
chiave_pubblica	<p>Un valore chiave SSH pubblico viene restituito solo se l'API genera un portachiavi completo per l'utente finale.</p> <div>  <p>Quando si passa un parametro <code>public_key</code> al metodo API, solo l'<code>signed_public_key</code> il valore viene restituito nella risposta.</p> </div>	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

È possibile utilizzare `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": "TestKeyProviderKnip",
  "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

## TestKeyServerKnip

È possibile utilizzare `TestKeyServerKnip` 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": "TestKeyServerKnip",
  "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

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

## Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.