



Méthodes API de sécurité

Element Software

NetApp
January 15, 2024

Sommaire

Méthodes API de sécurité	1
Trouvez plus d'informations	1
AddKeyServerToProviderKmpip	1
CreateKeyProviderKmpip	3
CreateKeyServerKmpip	4
CreatePublicPrivateKeypair	7
DeleteKeyProviderKmpip	9
DeleteKeyServerKmpip	10
DisableEncryptionAtRest	11
EnableEncryptionAtRest	12
GetClientCertificateSignRequest	15
GetKeyProviderKmpip	16
GetKeyServerKmpip	17
GetSoftwareEncryptionAtRestInfo	19
ListeKeyProvidersKmpip	21
ListKeyServersKmpip	24
ModifyKeyServerKmpip	27
RekeySoftwareEncryptionAtRestMasterKey	30
RemoveKeyServerFromProviderKmpip	33
TestKeyProviderKmpip	34
TestKeyServerKmpip	35

Méthodes API de sécurité

Vous pouvez intégrer le logiciel Element avec des services de sécurité externes, comme un serveur de gestion externe des clés. Ces méthodes de sécurité vous permettent de configurer les fonctionnalités de sécurité d'Element, telles que la gestion externe des clés pour le chiffrement des données au repos.

- [AddKeyServerToProviderKmip](#)
- [CreateKeyProviderKmip](#)
- [CreateKeyServerKmip](#)
- [CreatePublicPrivateKeypair](#)
- [DeleteKeyProviderKmip](#)
- [DeleteKeyServerKmip](#)
- [DisableEncryptionAtRest](#)
- [EnableEncryptionAtRest](#)
- [GetClientCertificateSignRequest](#)
- [GetKeyProviderKmip](#)
- [GetKeyServerKmip](#)
- [ListeKeyProvidersKmip](#)
- [ListKeyServersKmip](#)
- [ModifyKeyServerKmip](#)
- [RemoveKeyServerFromProviderKmip](#)
- [TestKeyProviderKmip](#)
- [TestKeyServerKmip](#)

Trouvez plus d'informations

- ["Documentation SolidFire et Element"](#)
- ["Documentation relative aux versions antérieures des produits NetApp SolidFire et Element"](#)

AddKeyServerToProviderKmip

Vous pouvez utiliser le `AddKeyServerToProviderKmip` Méthode permettant d'attribuer un serveur de clés KMIP (Key Management Interoperability Protocol) au fournisseur de clés spécifié. Lors de l'affectation, le serveur est contacté pour vérifier la fonctionnalité. Si le serveur de clés spécifié est déjà affecté au fournisseur de clés spécifié, aucune action n'est effectuée et aucune erreur n'est renvoyée. Vous pouvez supprimer l'affectation à l'aide du `RemoveKeyServerFromProviderKmip` méthode.

Paramètres

Cette méthode présente les paramètres d'entrée suivants :

Nom	Description	Type	Valeur par défaut	Obligatoire
KeyProviderID	ID du fournisseur de clés auquel affecter le serveur de clés.	entier	Aucune	Oui.
KeyServerID	L'ID du serveur de clés à affecter.	entier	Aucune	Oui.

Valeurs de retour

Cette méthode n'a pas de valeur de retour. L'affectation est considérée comme réussie tant qu'aucune erreur n'est renvoyée.

Exemple de demande

Les demandes pour cette méthode sont similaires à l'exemple suivant :

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

Exemple de réponse

Cette méthode renvoie une réponse similaire à l'exemple suivant :

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

Nouveau depuis la version

11.7

CreateKeyProviderKmip

Vous pouvez utiliser le `CreateKeyProviderKmip` Méthode de création d'un fournisseur de clés KMIP (Key Management Interoperability Protocol) avec le nom spécifié. Un fournisseur de clés définit un mécanisme et un emplacement pour récupérer les clés d'authentification. Lorsque vous créez un nouveau fournisseur de clés KMIP, aucun serveur de clés KMIP n'est affecté. Pour créer un serveur de clés KMIP, utilisez le `CreateKeyServerKmip` méthode. Pour l'affecter à un fournisseur, voir `AddKeyServerToProviderKmip`.

Paramètres

Cette méthode présente les paramètres d'entrée suivants :

Nom	Description	Type	Valeur par défaut	Obligatoire
KeyProviderName	Nom à associer au fournisseur de clés KMIP créé. Ce nom est utilisé uniquement à des fins d'affichage et n'a pas besoin d'être unique.	chaîne	Aucune	Oui.

Valeurs de retour

Cette méthode a les valeurs de retour suivantes :

Nom	Description	Type
KmipKeyProvider	Objet contenant des détails sur le fournisseur de clés nouvellement créé.	"KeyProviderKmip"

Exemple de demande

Les demandes pour cette méthode sont similaires à l'exemple suivant :

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

Exemple de réponse

Cette méthode renvoie une réponse similaire à l'exemple suivant :

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

Nouveau depuis la version

11.7

CreateKeyServerKmip

Vous pouvez utiliser le `CreateKeyServerKmip` Méthode de création d'un serveur de clés KMIP (Key Management Interoperability Protocol) avec les attributs spécifiés. Lors de la création, le serveur n'est pas contacté ; il n'a pas besoin d'exister avant d'utiliser cette méthode. Pour les configurations de serveur à clé en cluster, vous devez fournir les noms d'hôte ou les adresses IP de tous les nœuds de serveur dans le paramètre `kmipKeyServerHostnames`. Vous pouvez utiliser le `TestKeyServerKmip` méthode de test d'un serveur de clés.

Paramètres

Cette méthode présente les paramètres d'entrée suivants :

Nom	Description	Type	Valeur par défaut	Obligatoire
KmipCaCertificate	Certificat de clé publique de l'autorité de certification racine du serveur de clés externe. Cette option permet de vérifier le certificat présenté par le serveur de clés externe dans la communication TLS. Pour les grappes de serveurs de clés où des serveurs individuels utilisent des autorités de certification différentes, fournissez une chaîne concaténée contenant les certificats racine de toutes les autorités de certification.	chaîne	Aucune	Oui.
KmipClientCertificate	Certificat PKCS#10 X.509 codé au format PEM utilisé par le client SolidFire KMIP.	chaîne	Aucune	Oui.
Noms d'hôte kmipKeyServerHost Names	Tableau des noms d'hôte ou adresses IP associés à ce serveur de clés KMIP. Plusieurs noms d'hôte ou adresses IP ne doivent être fournis que si les serveurs clés sont dans une configuration en cluster.	tableau de chaînes	Aucune	Oui.

Nom	Description	Type	Valeur par défaut	Obligatoire
KmipKeyServerName	Nom du serveur de clés KMIP. Ce nom est utilisé uniquement à des fins d'affichage et n'a pas besoin d'être unique.	chaîne	Aucune	Oui.
KmipKeyServerPort	Numéro de port associé à ce serveur de clés KMIP (généralement 5696).	entier	Aucune	Non

Valeurs de retour

Cette méthode a les valeurs de retour suivantes :

Nom	Description	Type
KmipKeyServer	Objet contenant des détails sur le nouveau serveur de clés créé.	"KeyServerKmip"

Exemple de demande

Les demandes pour cette méthode sont similaires à l'exemple suivant :

```
{
  "method": "CreateKeyServerKmip",
  "params": {
    "kmipCaCertificate": "MIICPCCAaUCEDyRMcsf9tAbDpq40ES/E...",
    "kmipClientCertificate": "dKkkirWmnWXbj9T/UWZYB2oK0z5...",
    "kmipKeyServerHostnames": ["server1.hostname.com",
"server2.hostname.com"],
    "kmipKeyServerName" : "keyserverName",
    "kmipKeyServerPort" : 5696
  },
  "id": 1
}
```

Exemple de réponse

Cette méthode renvoie une réponse similaire à l'exemple suivant :


```

{
  "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
    }
  }
}

```

Nouveau depuis la version

11.7

CreatePublicPrivateKeypair

Vous pouvez utiliser le `CreatePublicPrivateKeyPair` Méthode permettant de créer des clés SSL publiques et privées. Vous pouvez utiliser ces clés pour générer des demandes de signature de certificat. Seule une paire de clés peut être utilisée pour chaque cluster de stockage. Avant d'utiliser cette méthode pour remplacer les clés existantes, assurez-vous que les clés ne sont plus utilisées par aucun fournisseur.

Paramètres

Cette méthode présente les paramètres d'entrée suivants :

Nom	Description	Type	Valeur par défaut	Obligatoire
Nom CommonName	Le champ Nom distinctif X.509 Nom commun (CN).	chaîne	Aucune	Non
pays	Le champ Nom distinctif X.509 pays ©.	chaîne	Aucune	Non

Nom	Description	Type	Valeur par défaut	Obligatoire
Adresse électronique	Le champ Nom distinctif X.509 adresse électronique (MAIL).	chaîne	Aucune	Non
localité	Le champ L (Nom distinctif) de X.509 Nom de localité .	chaîne	Aucune	Non
entreprise	Le champ Nom distinctif X.509 Nom de l'organisation (O).	chaîne	Aucune	Non
Unité organisationnelle	Le champ Nom distinctif X.509 Nom de l'unité organisationnelle (ou).	chaîne	Aucune	Non
état	Le champ Nom distinctif X.509 État ou Nom de province (ST ou SP ou S).	chaîne	Aucune	Non

Valeurs de retour

Cette méthode n'a pas de valeurs de retour. En l'absence d'erreur, la création de clé est considérée comme réussie.

Exemple de demande

Les demandes pour cette méthode sont similaires à l'exemple suivant :

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

Exemple de réponse

Cette méthode renvoie une réponse similaire à l'exemple suivant :

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

Nouveau depuis la version

11.7

DeleteKeyProviderKmip

Vous pouvez utiliser le `DeleteKeyProviderKmip` Méthode de suppression du fournisseur de clés KMIP (Key Management Interoperability Protocol) inactif spécifié.

Paramètres

Cette méthode présente les paramètres d'entrée suivants :

Nom	Description	Type	Valeur par défaut	Obligatoire
KeyProviderID	ID du fournisseur de clés à supprimer.	entier	Aucune	Oui.

Valeurs de retour

Cette méthode n'a pas de valeurs de retour. L'opération de suppression est considérée comme réussie car il n'y a pas d'erreur.

Exemple de demande

Les demandes pour cette méthode sont similaires à l'exemple suivant :

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

Exemple de réponse

Cette méthode renvoie une réponse similaire à l'exemple suivant :

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

Nouveau depuis la version

11.7

DeleteKeyServerKmip

Vous pouvez utiliser le `DeleteKeyServerKmip` Méthode de suppression d'un serveur de clés KMIP (Key Management Interoperability Protocol) existant. Vous pouvez supprimer un serveur de clés à moins qu'il ne soit le dernier affecté à son fournisseur et que ce fournisseur fournit des clés actuellement utilisées.

Paramètres

Cette méthode présente les paramètres d'entrée suivants :

Nom	Description	Type	Valeur par défaut	Obligatoire
KeyServerID	ID du serveur de clés KMIP à supprimer.	entier	Aucune	Oui.

Valeurs de retour

Cette méthode a les valeurs no return. L'opération de suppression est considérée comme réussie en l'absence d'erreur.

Exemple de demande

Les demandes pour cette méthode sont similaires à l'exemple suivant :

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

Exemple de réponse

Cette méthode renvoie une réponse similaire à l'exemple suivant :

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

Nouveau depuis la version

11.7

DisableEncryptionAtRest

Vous pouvez utiliser le `DisableEncryptionAtRest` méthode de suppression du chiffrement précédemment appliqué au cluster à l'aide du `EnableEncryptionAtRest` méthode. Cette méthode de désactivation est asynchrone et renvoie une réponse avant que le cryptage ne soit désactivé. Vous pouvez utiliser le `GetClusterInfo` méthode d'interrogation du système pour voir quand le processus est terminé.



Pour voir l'état actuel du chiffrement au repos et/ou logiciel au repos sur le cluster, utilisez le ["obtenir la méthode d'information sur le cluster"](#). Vous pouvez utiliser le `GetSoftwareEncryptionAtRestInfo` ["méthode d'obtention des informations que le cluster utilise pour chiffrer les données au repos"](#).



Vous ne pouvez pas utiliser cette méthode pour désactiver le chiffrement logiciel au repos. Pour désactiver le chiffrement logiciel au repos, vous devez ["créer un nouveau cluster"](#) le chiffrement logiciel des données au repos est désactivé.

Paramètres

Cette méthode n'a pas de paramètres d'entrée.

Valeurs de retour

Cette méthode n'a pas de valeurs de retour.

Exemple de demande

Les demandes pour cette méthode sont similaires à l'exemple suivant :

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

Exemple de réponse

Cette méthode renvoie une réponse similaire à l'exemple suivant :

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

Nouveau depuis la version

9.6

Trouvez plus d'informations

- ["GetClusterInfo"](#)
- ["Documentation SolidFire et Element"](#)
- ["Documentation relative aux versions antérieures des produits NetApp SolidFire et Element"](#)

EnableEncryptionAtRest

Vous pouvez utiliser le `EnableEncryptionAtRest` Méthode permettant d'activer le chiffrement AES 256 bits au repos sur le cluster. Le cluster peut ainsi gérer la clé de chiffrement utilisée pour les disques sur chaque nœud. Cette fonctionnalité n'est pas activée par défaut.



Pour voir l'état actuel du chiffrement au repos et/ou logiciel au repos sur le cluster, utilisez le ["obtenir la méthode d'information sur le cluster"](#). Vous pouvez utiliser le `GetSoftwareEncryptionAtRestInfo` ["méthode d'obtention des informations que le cluster utilise pour chiffrer les données au repos"](#).



Cette méthode n'active pas le chiffrement logiciel au repos. Ceci peut uniquement être effectué à l'aide du "créer une méthode de cluster" avec `enableSoftwareEncryptionAtRest` réglé sur `true`.

Lorsque vous activez le chiffrement au repos, le cluster gère automatiquement les clés de chiffrement en interne pour les disques de chaque nœud du cluster.

Si un `keyProviderID` est spécifié, le mot de passe est généré et récupéré selon le type de fournisseur de clés. Cette opération est généralement effectuée à l'aide d'un serveur de clés KMIP (Key Management Interoperability Protocol) dans le cas d'un fournisseur de clés KMIP. Après cette opération, le fournisseur spécifié est considéré comme actif et ne peut pas être supprimé tant que le chiffrement au repos n'est pas désactivé à l'aide du `DisableEncryptionAtRest` méthode.



Si vous avez un type de nœud avec un numéro de modèle se terminant par « -ne », le `EnableEncryptionAtRest` L'appel de méthode échouera avec une réponse de « cryptage non autorisé. Cluster détecté noeud non encryptable ».



Vous devez activer ou désactiver le chiffrement uniquement lorsque le cluster est en cours d'exécution et qu'il est en état de santé. Vous pouvez activer ou désactiver le cryptage à votre discrétion et aussi souvent que vous le souhaitez.



Ce processus est asynchrone et renvoie une réponse avant l'activation du chiffrement. Vous pouvez utiliser le `GetClusterInfo` méthode d'interrogation du système pour voir quand le processus est terminé.

Paramètres

Cette méthode présente les paramètres d'entrée suivants :

Nom	Description	Type	Valeur par défaut	Obligatoire
<code>KeyProviderID</code>	ID d'un fournisseur de clés KMIP à utiliser.	entier	Aucune	Non

Valeurs de retour

Cette méthode n'a pas de valeurs de retour.

Exemple de demande

Les demandes pour cette méthode sont similaires à l'exemple suivant :

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

Exemples de réponse

Cette méthode renvoie une réponse similaire à l'exemple suivant de la méthode `EnableEncryptionAtRest`. Aucun résultat à signaler.

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

Bien que le chiffrement au repos soit activé sur un cluster, `GetClusterInfo` renvoie un résultat décrivant l'état du chiffrement au repos (« `EncryptionAtRestState` ») comme « activation ». Une fois le chiffrement au repos entièrement activé, l'état renvoyé est « activé ».

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

Nouveau depuis la version

9.6

Trouvez plus d'informations

- ["SecureEraseDrives"](#)
- ["GetClusterInfo"](#)
- ["Documentation SolidFire et Element"](#)

- ["Documentation relative aux versions antérieures des produits NetApp SolidFire et Element"](#)

GetClientCertificateSignRequest

Vous pouvez utiliser le `GetClientCertificateSignRequest` méthode permettant de générer une demande de signature de certificat qui peut être signée par une autorité de certification afin de générer un certificat client pour le cluster. Les certificats signés sont nécessaires pour établir une relation de confiance pour interagir avec les services externes.

Paramètres

Cette méthode n'a pas de paramètres d'entrée.

Valeurs de retour

Cette méthode a les valeurs de retour suivantes :

Nom	Description	Type
CertificataclientSignRequest	Demande de signature de certificat de client PKCS#10 X.509 codée au format PEM Base64.	chaîne

Exemple de demande

Les demandes pour cette méthode sont similaires à l'exemple suivant :

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

Exemple de réponse

Cette méthode renvoie une réponse similaire à l'exemple suivant :

```

{
  "id": 1,
  "result":
  {
    "clientCertificateSignRequest":
    "MIIBYjCCATMCAQAwwYkxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybm..."
  }
}

```

Nouveau depuis la version

11.7

GetKeyProviderKmip

Vous pouvez utiliser le `GetKeyProviderKmip` Méthode d'extraction d'informations relatives au fournisseur de clés KMIP (Key Management Interoperability Protocol) spécifié.

Paramètres

Cette méthode présente les paramètres d'entrée suivants :

Nom	Description	Type	Valeur par défaut	Obligatoire
KeyProviderID	ID de l'objet du fournisseur de clés KMIP à renvoyer.	entier	Aucune	Oui.

Valeurs de retour

Cette méthode a les valeurs de retour suivantes :

Nom	Description	Type
KmipKeyProvider	Objet contenant des détails sur le fournisseur de clés demandé.	"KeyProviderKmip"

Exemple de demande

Les demandes pour cette méthode sont similaires à l'exemple suivant :

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

Exemple de réponse

Cette méthode renvoie une réponse similaire à l'exemple suivant :

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

Nouveau depuis la version

11.7

GetKeyServerKmip

Vous pouvez utiliser le `GetKeyServerKmip` Méthode de retour des informations sur le serveur de clés KMIP (Key Management Interoperability Protocol) spécifié.

Paramètres

Cette méthode présente les paramètres d'entrée suivants :

Nom	Description	Type	Valeur par défaut	Obligatoire
KeyServerID	ID du serveur de clés KMIP pour renvoyer des informations sur.	entier	Aucune	Oui.

Valeurs de retour

Cette méthode a les valeurs de retour suivantes :

Nom	Description	Type
KmipKeyServer	Objet contenant des détails sur le serveur de clés demandé.	"KeyServerKmip"

Exemple de demande

Les demandes pour cette méthode sont similaires à l'exemple suivant :

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

Exemple de réponse

Cette méthode renvoie une réponse similaire à l'exemple suivant :

```

{
  "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
    }
  }
}

```

Nouveau depuis la version

11.7

GetSoftwareEncryptionAtRestInfo

Vous pouvez utiliser le `GetSoftwareEncryptionAtRestInfo` méthode d'obtention des informations de chiffrement logiciel au repos que le cluster utilise pour chiffrer les données au repos.

Paramètres

Cette méthode n'a pas de paramètres d'entrée.

Valeurs de retour

Cette méthode a les valeurs de retour suivantes :

Paramètre	Description	Type	Facultatif
Master KeyInfo	Informations sur la clé principale de chiffrement logiciel au repos actuelle.	Crypter_KeyInfo	Vrai

Paramètre	Description	Type	Facultatif
RekeyMasterKeyAsyncResultID	ID du résultat asynchrone de l'opération de renouvellement de clé actuelle ou la plus récente (le cas échéant), s'il n'a pas encore été supprimé. <code>GetAsyncResult</code> la sortie inclura un <code>newKey</code> champ qui contient des informations sur la nouvelle clé principale et un <code>keyToDecommission</code> champ contenant des informations sur l'ancienne clé.	entier	Vrai
état	État actuel du logiciel de chiffrement des données au repos. Les valeurs possibles sont <code>disabled</code> ou <code>enabled</code> .	chaîne	Faux
version	Un numéro de version incrémenté à chaque fois que le chiffrement logiciel au repos est activé.	entier	Faux

Exemple de demande

Les demandes pour cette méthode sont similaires à l'exemple suivant :

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

Exemple de réponse

Cette méthode renvoie une réponse similaire à l'exemple suivant :

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

Nouveau depuis la version

12.3

Trouvez plus d'informations

- ["Documentation SolidFire et Element"](#)
- ["Documentation relative aux versions antérieures des produits NetApp SolidFire et Element"](#)

ListeKeyProvidersKmip

Vous pouvez utiliser le `ListKeyProvidersKmip` Méthode d'extraction de la liste de tous les fournisseurs de clés KMIP (Key Management Interoperability Protocol) existants. Vous pouvez filtrer la liste en spécifiant des paramètres supplémentaires.

Paramètres

Cette méthode présente les paramètres d'entrée suivants :

Nom	Description	Type	Valeur par défaut	Obligatoire
KeyProviderIsActive	<p>Les filtres ont renvoyé des objets de serveur de clés KMIP en fonction de leur état d'activité. Valeurs possibles :</p> <ul style="list-style-type: none"> • Vrai : seuls les fournisseurs de clés KMIP actifs (avec des clés en cours d'utilisation) sont renvoyées. • Faux : renvoie uniquement les fournisseurs de clés KMIP qui sont inactifs (aucune clé ne peut être supprimée). <p>Si vous ne l'omettez pas, les fournisseurs de clés KMIP renvoyés ne sont pas filtrés en fonction de la condition qu'ils soient actifs.</p>	booléen	Aucune	Non

Nom	Description	Type	Valeur par défaut	Obligatoire
KmipKeyProviderHasServerAssigned	<p>Les filtres ont renvoyé les fournisseurs de clés KMIP en fonction du serveur de clés KMIP qui est attribué ou non. Valeurs possibles :</p> <ul style="list-style-type: none"> • Vrai : ne renvoie que les fournisseurs de clés KMIP qui disposent d'un serveur de clés KMIP attribué. • FALSE : renvoie uniquement les fournisseurs de clés KMIP qui ne disposent pas d'un serveur de clés KMIP attribué. <p>En cas d'omission, les fournisseurs de clés KMIP renvoyés ne sont pas filtrés selon que le serveur de clés KMIP est attribué ou non.</p>	booléen	Aucune	Non

Valeurs de retour

Cette méthode a les valeurs de retour suivantes :

Nom	Description	Type
KmipKeyProviders	Liste de fournisseurs de clés KMIP créés.	"KeyProviderKmip" baie

Exemple de demande

Les demandes pour cette méthode sont similaires à l'exemple suivant :

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

Exemple de réponse

Cette méthode renvoie une réponse similaire à l'exemple suivant :

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

Nouveau depuis la version

11.7

ListKeyServoersKmip

Vous pouvez utiliser le `ListKeyServersKmip` Méthode qui répertorie tous les serveurs de clés KMIP (Key Management Interoperability Protocol) créés. Vous pouvez filtrer les résultats en spécifiant des paramètres supplémentaires.

Paramètres

Cette méthode présente les paramètres d'entrée suivants :

Nom	Description	Type	Valeur par défaut	Obligatoire
KeyProviderID	Lorsqu'elle est spécifiée, cette méthode renvoie uniquement les serveurs de clés KMIP qui sont affectés au fournisseur de clés KMIP spécifié. Si vous omettez le paramètre, les serveurs de clés KMIP renvoyés ne sont pas filtrés selon que ils sont attribués au fournisseur de clés KMIP spécifié ou non.	entier	Aucune	Non
KmipAssignedProvidersActive	<p>Les filtres ont renvoyé des objets de serveur de clés KMIP en fonction de leur état d'activité. Valeurs possibles :</p> <ul style="list-style-type: none"> • Vrai : seuls les serveurs de clés KMIP qui sont actifs (avec des clés en cours d'utilisation) sont renvoyées. • Faux : renvoie uniquement les serveurs de clés KMIP qui sont inactifs (ne fournissant aucune clé et ne pouvant être supprimés). <p>Si vous omettez le paramètre, les serveurs de clés KMIP renvoyés ne sont pas filtrés en fonction de la condition qu'ils soient actifs.</p>	booléen	Aucune	Non

Nom	Description	Type	Valeur par défaut	Obligatoire
KmipHasProviderAs signed	<p>Les filtres ont renvoyé des serveurs de clés KMIP en fonction du fournisseur de clés KMIP qui leur est attribué ou non. Valeurs possibles :</p> <ul style="list-style-type: none"> • Vrai : seuls les serveurs de clés KMIP qui sont affectés par un fournisseur de clés KMIP. • FALSE : renvoie uniquement les serveurs de clés KMIP qui ne disposent pas d'un fournisseur de clés KMIP attribué. <p>En cas d'omission, les serveurs de clés KMIP renvoyés ne sont pas filtrés selon que le fournisseur de clés KMIP est attribué ou non.</p>	booléen	Aucune	Non

Valeurs de retour

Cette méthode a les valeurs de retour suivantes :

Nom	Description	Type
KmipKeyServers	La liste complète des serveurs de clés KMIP qui ont été créés.	"KeyServerKmip" baie

Exemple de demande

Les demandes pour cette méthode sont similaires à l'exemple suivant :

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

Exemple de réponse

Cette méthode renvoie une réponse similaire à l'exemple suivant :

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

Nouveau depuis la version

11.7

ModifyKeyServerKmip

Vous pouvez utiliser le `ModifyKeyServerKmip` Méthode de modification d'un serveur de clés KMIP (Key Management Interoperability Protocol) existant aux attributs spécifiés. Bien que le seul paramètre requis soit le `keyServerID`, une requête contenant uniquement le `keyServerID` ne prend aucune action et ne renvoie aucune erreur. Tous les autres paramètres que vous spécifiez remplaceront les valeurs existantes pour le serveur de clés par l'ID `keyServerID` spécifié. Le serveur principal est contacté au cours de l'opération pour s'assurer qu'il est fonctionnel. Vous pouvez fournir plusieurs noms d'hôte ou adresses IP avec le paramètre `kmipKeyServerHostnames`, mais uniquement si les serveurs de clés sont dans une configuration en cluster.

Paramètres

Cette méthode présente les paramètres d'entrée suivants :

Nom	Description	Type	Valeur par défaut	Obligatoire
KeyServerID	ID du serveur de clés KMIP à modifier.	entier	Aucune	Oui.
KmipCaCertificate	Certificat de clé publique de l'autorité de certification racine du serveur de clés externe. Cette option permet de vérifier le certificat présenté par le serveur de clés externe dans la communication TLS. Pour les grappes de serveurs de clés où des serveurs individuels utilisent des autorités de certification différentes, fournissez une chaîne concaténée contenant les certificats racine de toutes les autorités de certification.	chaîne	Aucune	Non
KmipClientCertificate	Certificat PKCS#10 X.509 codé au format PEM utilisé par le client SolidFire KMIP.	chaîne	Aucune	Non

Noms d'hôte kmpKeyServerHost Names	Tableau des noms d'hôte ou adresses IP associés à ce serveur de clés KMIP. Plusieurs noms d'hôte ou adresses IP ne doivent être fournis que si les serveurs clés sont dans une configuration en cluster.	tableau de chaînes	Aucune	Non
KmpKeyServerName	Nom du serveur de clés KMIP. Ce nom est utilisé uniquement à des fins d'affichage et n'a pas besoin d'être unique.	chaîne	Aucune	Non
KmpKeyServerPort	Numéro de port associé à ce serveur de clés KMIP (généralement 5696).	entier	Aucune	Non

Valeurs de retour

Cette méthode a les valeurs de retour suivantes :

Nom	Description	Type
KmpKeyServer	Objet contenant des détails sur le serveur de clés nouvellement modifié.	"KeyServerKmp"

Exemple de demande

Les demandes pour cette méthode sont similaires à l'exemple suivant :

```

{
  "method": "ModifyKeyServerKmip",
  "params": {
    "keyServerID": 15
    "kmipCaCertificate": "CPDCCAAUCEDyRMcsf9tAbDpq40ES/E...",
    "kmipClientCertificate": "kirWmnWXbj9T/UWZYB2oK0z5...",
    "kmipKeyServerHostnames" : ["server1.hostname.com",
"server2.hostname.com"],
    "kmipKeyServerName" : "keyserverName",
    "kmipKeyServerPort" : 5696
  },
  "id": 1
}

```

Exemple de réponse

Cette méthode renvoie une réponse similaire à l'exemple suivant :

```

{
  "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
    }
  }
}

```

Nouveau depuis la version

11.7

RekeySoftwareEncryptionAtRestMasterKey

Vous pouvez utiliser le `RekeySoftwareEncryptionAtRestMasterKey` Méthode

permettant de reKey la clé principale de chiffrement logiciel au repos utilisée pour chiffrer les clés de chiffrement des données (clés de chiffrement des données). Lors de la création du cluster, le chiffrement logiciel au repos est configuré pour utiliser la gestion interne des clés (IKM). Cette méthode de renouvellement peut être utilisée après la création du cluster pour utiliser IKM ou External Key Management (EKM).

Paramètres

Cette méthode dispose des paramètres d'entrée suivants. Si le `keyManagementType` le paramètre n'est pas spécifié, l'opération de renouvellement de clés est effectuée à l'aide de la configuration existante de gestion des clés. Si le `keyManagementType` est spécifié et le fournisseur clé est externe, le `keyProviderID` le paramètre doit également être utilisé.

Paramètre	Description	Type	Facultatif
Type de gestion de clés	Type de gestion des clés utilisé pour gérer la clé principale. Les valeurs possibles sont : Internal: Rekey utilisation de la gestion interne des clés. External: Rekey utilisation de la gestion externe des clés. Si ce paramètre n'est pas spécifié, l'opération de renouvellement de clés est effectuée à l'aide de la configuration existante de gestion des clés.	chaîne	Vrai
KeyProviderID	ID du fournisseur de clés à utiliser. Il s'agit d'une valeur unique renvoyée dans le cadre de l'un des <code>CreateKeyProvider</code> méthodes. L'ID n'est requis que lorsque <code>keyManagementType</code> est <code>External</code> et n'est pas valide.	entier	Vrai

Valeurs de retour

Cette méthode a les valeurs de retour suivantes :

Paramètre	Description	Type	Facultatif
Asynchrone	Déterminer l'état de l'opération de renouvellement de clé à l'aide de ce bouton <code>asyncHandle</code> valeur avec <code>GetAsyncResult</code> . <code>GetAsyncResult</code> la sortie inclura un <code>newKey</code> champ qui contient des informations sur la nouvelle clé principale et un <code>keyToDecommission</code> champ contenant des informations sur l'ancienne clé.	entier	Faux

Exemple de demande

Les demandes pour cette méthode sont similaires à l'exemple suivant :

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

Exemple de réponse

Cette méthode renvoie une réponse similaire à l'exemple suivant :

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

Nouveau depuis la version

12.3

Trouvez plus d'informations

- ["Documentation SolidFire et Element"](#)
- ["Documentation relative aux versions antérieures des produits NetApp SolidFire et Element"](#)

RemoveKeyServerFromProviderKmip

Vous pouvez utiliser le `RemoveKeyServerFromProviderKmip` Méthode permettant de désaffecter le serveur de clés KMIP (Key Management Interoperability Protocol) spécifié du fournisseur auquel il a été affecté. Vous pouvez annuler l'affectation d'un serveur de clés de son fournisseur, sauf s'il s'agit du dernier serveur et de son fournisseur actif (fournissant les clés actuellement utilisées). Si le serveur de clés spécifié n'est pas affecté à un fournisseur, aucune action n'est effectuée et aucune erreur n'est renvoyée.

Paramètres

Cette méthode présente les paramètres d'entrée suivants :

Nom	Description	Type	Valeur par défaut	Obligatoire
KeyServerID	ID du serveur de clés KMIP à désaffecter.	entier	Aucune	Oui.

Valeurs de retour

Cette méthode n'a pas de valeurs de retour. La suppression est considérée comme réussie tant qu'aucune erreur n'est renvoyée.

Exemple de demande

Les demandes pour cette méthode sont similaires à l'exemple suivant :

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

Exemple de réponse

Cette méthode renvoie une réponse similaire à l'exemple suivant :

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

Nouveau depuis la version

11.7

TestKeyProviderKmip

Vous pouvez utiliser le `TestKeyProviderKmip` Méthode de test permettant de vérifier si le fournisseur de clés KMIP (Key Management Interoperability Protocol) spécifié est accessible et fonctionne normalement.

Paramètres

Cette méthode présente les paramètres d'entrée suivants :

Nom	Description	Type	Valeur par défaut	Obligatoire
KeyProviderID	ID du fournisseur de clé à tester.	entier	Aucune	Oui.

Valeurs de retour

Cette méthode n'a pas de valeurs de retour. Le test est considéré comme réussi tant qu'aucune erreur n'est renvoyée.

Exemple de demande

Les demandes pour cette méthode sont similaires à l'exemple suivant :

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

Exemple de réponse

Cette méthode renvoie une réponse similaire à l'exemple suivant :

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

Nouveau depuis la version

11.7

TestKeyServerKmip

Vous pouvez utiliser le `TestKeyServerKmip` Méthode de test permettant de vérifier si le serveur de clés KMIP (Key Management Interoperability Protocol) spécifié est accessible et fonctionne normalement.

Paramètres

Cette méthode présente les paramètres d'entrée suivants :

Nom	Description	Type	Valeur par défaut	Obligatoire
KeyServerID	L'ID du serveur de clés KMIP à tester.	entier	Aucune	Oui.

Valeurs de retour

Cette méthode n'a pas de valeurs de retour. Le test est considéré comme réussi s'il n'y a pas d'erreur renvoyée.

Exemple de demande

Les demandes pour cette méthode sont similaires à l'exemple suivant :

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

Exemple de réponse

Cette méthode renvoie une réponse similaire à l'exemple suivant :

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

Nouveau depuis la version

11.7

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.