



# **Méthodes d'API d'authentification multifactorielle**

**Element Software**

NetApp

November 12, 2025

# Sommaire

Méthodes d'API d'authentification multifactorielle .....	1
AjouterIdpClusterAdmin .....	1
Paramètres .....	1
Valeurs de retour .....	2
Exemple de demande .....	2
Exemple de réponse .....	2
Nouveautés depuis la version .....	3
Créer une configuration Idp .....	3
Paramètres .....	3
Valeurs de retour .....	3
Exemple de demande .....	4
Exemple de réponse .....	4
Nouveautés depuis la version .....	5
Supprimer la session d'authentification .....	5
Paramètres .....	5
Valeurs de retour .....	5
Exemple de demande .....	5
Exemple de réponse .....	5
Nouveautés depuis la version .....	6
Supprimer les sessions d'authentification par l'administrateur du cluster .....	6
Paramètres .....	6
Valeurs de retour .....	7
Exemple de demande .....	7
Exemple de réponse .....	7
Nouveautés depuis la version .....	8
Supprimer les sessions d'authentification par nom d'utilisateur .....	8
Paramètres .....	8
Valeurs de retour .....	9
Exemple de demande .....	10
Exemple de réponse .....	10
Nouveautés depuis la version .....	10
Supprimer la configuration Idp .....	11
Paramètres .....	11
Valeurs de retour .....	11
Exemple de demande .....	11
Exemple de réponse .....	11
Nouveautés depuis la version .....	12
Désactiver l'authentification Idp .....	12
Paramètres .....	12
Valeurs de retour .....	12
Exemple de demande .....	12
Exemple de réponse .....	12
Nouveautés depuis la version .....	13

Activer l'authentification Idp . . . . .	13
Paramètres . . . . .	13
Valeurs de retour . . . . .	13
Exemple de demande . . . . .	13
Exemple de réponse . . . . .	14
Nouveautés depuis la version . . . . .	14
Obtenir l'état d'authentification Idp . . . . .	14
Paramètres . . . . .	14
Valeurs de retour . . . . .	14
Exemple de demande . . . . .	14
Exemple de réponse . . . . .	15
Nouveautés depuis la version . . . . .	15
Lister les sessions d'authentification actives . . . . .	15
Paramètres . . . . .	15
Valeurs de retour . . . . .	15
Exemple de demande . . . . .	15
Exemple de réponse . . . . .	16
Nouveautés depuis la version . . . . .	16
ListIdpConfigurations . . . . .	16
Paramètres . . . . .	16
Valeurs de retour . . . . .	17
Exemple de demande . . . . .	17
Exemple de réponse . . . . .	17
Nouveautés depuis la version . . . . .	18
Mise à jour de la configuration Idp . . . . .	18
Paramètres . . . . .	18
Valeurs de retour . . . . .	20
Exemple de demande . . . . .	20
Exemple de réponse . . . . .	20
Nouveautés depuis la version . . . . .	21

# Méthodes d'API d'authentification multifactorielle

## AjouterIdpClusterAdmin

Vous pouvez utiliser le `AddIdpClusterAdmin` méthode pour ajouter un utilisateur administrateur de cluster authentifié par un fournisseur d'identité tiers (IdP). Les comptes d'administrateur du cluster IdP sont configurés en fonction des informations de valeur d'attribut SAML fournies dans l'assertion SAML de l'IdP associée à l'utilisateur. Si un utilisateur s'authentifie avec succès auprès du fournisseur d'identité et que les déclarations d'attributs SAML au sein de l'assertion SAML correspondent à plusieurs comptes d'administrateur de cluster IdP, l'utilisateur disposera du niveau d'accès combiné de ces comptes d'administrateur de cluster IdP correspondants.

### Paramètres

Cette méthode possède les paramètres d'entrée suivants :

Nom	Description	Type	Valeur par défaut	Obligatoire
accéder	Contrôle les méthodes que cet administrateur de cluster IdP peut utiliser.	tableau de chaînes	Aucune	Oui
accepterEula	Acceptez le contrat de licence utilisateur final. Définissez cette valeur sur « true » pour ajouter un compte d'administrateur de cluster au système. Si cette valeur est omise ou définie sur <code>false</code> , l'appel de méthode échoue.	booléen	Aucune	Oui
attributs	Liste de paires nom-valeur au format objet JSON.	objet JSON	Aucune	Non

Nom	Description	Type	Valeur par défaut	Obligatoire
nom d'utilisateur	Un mappage attribut-valeur SAML vers un administrateur de cluster IdP (par exemple, email= <a href="mailto:test@example.com">test@example.com</a> ). Cela peut être défini à l'aide d'un sujet SAML spécifique. NameID ou comme entrée dans la déclaration d'attribut SAML, par exemple : eduPersonAffiliation .	chaîne	Aucune	Oui

## Valeurs de retour

Cette méthode a la valeur de retour suivante :

Nom	Description	Type
clusterAdminID	Identifiant unique pour l'administrateur du cluster nouvellement créé.	entier

## Exemple de demande

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

```
{
  "method": "AddIdpClusterAdmin",
  "params": {
    "username": "email=test@example.com",
    "acceptEula": true,
    "access": ["administrator"]
  }
}
```

## Exemple de réponse

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

```
{
  "result": {
    "clusterAdminID": 13
  }
}
```

## Nouveautés depuis la version

12,0

## Créer une configuration Idp

Vous pouvez utiliser la `CreateIdpConfiguration` méthode pour créer une relation de confiance potentielle pour l'authentification utilisant un fournisseur d'identité tiers (IdP) pour le cluster. Un certificat de fournisseur de services SAML est requis pour la communication avec le fournisseur d'identité. Ce certificat est généré conformément aux exigences et renvoyé par cet appel API.

### Paramètres

Cette méthode possède les paramètres d'entrée suivants :

Nom	Description	Type	Valeur par défaut	Obligatoire
Métadonnées idp	Métadonnées IdP à stocker.	chaîne	Aucune	Oui
Nom idp	Nom utilisé pour identifier un fournisseur d'identité (IdP) pour l'authentification unique SAML 2.0.	chaîne	Aucune	Oui

### Valeurs de retour

Cette méthode a la valeur de retour suivante :

Nom	Description	Type
idpConfigInfo	Informations concernant la configuration du fournisseur d'identité tiers (IdP).	" <a href="#">idpConfigInfo</a> "

## Exemple de demande

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

```
{  
  "method": "CreateIdpConfiguration",  
  "params": {  
    "idpMetadata": "<?xml version=\"1.0\" encoding=\"UTF-8\"?>  
      <EntityDescriptor  
        xmlns=\"urn:oasis:names:tc:SAML:2.0:metadata\"  
        xmlns:ds=\"http://www.w3.org/2000/09/xmldsig#\"  
        xmlns:shibmd=\"urn:mace:shibboleth:metadata:1.0\"  
        xmlns:xml=\"http://www.w3.org/XML/1998/namespace\"  
        ...</Organization>  
      </EntityDescriptor>",  
    "idpName": "https://provider.name.url.com"  
  },  
}
```

## Exemple de réponse

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

```
{  
  "result": {  
    "idpConfigInfo": {  
      "enabled": false,  
      "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",  
      "idpMetadata": "<?xml version=\"1.0\" encoding=\"UTF-8\"?>\r\n        <EntityDescriptor  
          xmlns=\"urn:oasis:names:tc:SAML:2.0:metadata\"\r\n          xmlns:ds=\"http://www.w3.org/2000/09/xmldsig#\"\r\n          xmlns:shibmd=\"urn:mace:shibboleth:metadata:1.0\"\r\n          xmlns:xml=\"http://www.w3.org/XML/1998/namespace\"\r\n          ... </Organization>\r\n        </EntityDescriptor>",  
      "idpName": "https://privider.name.url.com",  
      "serviceProviderCertificate": "-----BEGIN CERTIFICATE-----\nMIID...SlBHi\n-----END CERTIFICATE-----\n",  
      "spMetadataUrl": "https://10.193.100.100/auth/ui/saml2"  
    }  
  }  
}
```

## Nouveautés depuis la version

12,0

# Supprimer la session d'authentification

Vous pouvez utiliser le `DeleteAuthSession` Méthode permettant de supprimer une session d'authentification d'un utilisateur individuel. Si l'utilisateur appelant n'appartient pas au groupe d'accès `ClusterAdmins` / `Administrator`, seule la session d'authentification de cet utilisateur peut être supprimée.

## Paramètres

Cette méthode possède le paramètre d'entrée suivant :

Nom	Description	Type	Valeur par défaut	Obligatoire
sessionID	Identifiant unique de la session d'authentification à supprimer.	UUID	Aucune	Oui

## Valeurs de retour

Cette méthode a la valeur de retour suivante :

Nom	Description	Type
session	Informations de session pour la suppression de la session d'authentification.	"authSessionInfo"

## Exemple de demande

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

```
{  
  "method": "DeleteAuthSession",  
  "params": {  
    "sessionID": "a862a8bb-2c5b-4774-a592-2148e2304713"  
  },  
  "id": 1  
}
```

## Exemple de réponse

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

```

{
  "id": 1,
  "result": {
    "session": {
      "accessGroupList": [
        "administrator"
      ],
      "authMethod": "Cluster",
      "clusterAdminIDs": [
        1
      ],
      "finalTimeout": "2020-04-09T17:51:30Z",
      "idpConfigVersion": 0,
      "lastAccessTimeout": "2020-04-06T18:21:33Z",
      "sessionCreationTime": "2020-04-06T17:51:30Z",
      "sessionID": "a862a8bb-2c5b-4774-a592-2148e2304713",
      "username": "admin"
    }
  }
}

```

## Nouveautés depuis la version

12,0

## Supprimer les sessions d'authentification par l'administrateur du cluster

Vous pouvez utiliser la `DeleteAuthSessionsByClusterAdmin` méthode permettant de supprimer toutes les sessions d'authentification associées à l'élément spécifié `ClusterAdminID`. Si l'identifiant `ClusterAdminID` spécifié correspond à un groupe d'utilisateurs, toutes les sessions d'authentification de tous les membres de ce groupe seront supprimées. Pour afficher la liste des sessions susceptibles d'être supprimées, utilisez la méthode `ListAuthSessionsByClusterAdmin` avec le `ClusterAdminID` paramètre.

### Paramètres

Cette méthode possède le paramètre d'entrée suivant :

Nom	Description	Type	Valeur par défaut	Obligatoire
<code>clusterAdminID</code>	Identifiant unique de l'administrateur du cluster.	entier	Aucune	Oui

## Valeurs de retour

Cette méthode a la valeur de retour suivante :

Nom	Description	Type
séances	Informations de session pour les sessions d'authentification supprimées.	"authSessionInfo"

## Exemple de demande

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

```
{  
  "method": "DeleteAuthSessionsByClusterAdmin",  
  "params": {  
    "clusterAdminID": 1  
  }  
}
```

## Exemple de réponse

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

```
{  
  "sessions": [  
    {  
      "accessGroupList": [  
        "administrator"  
      ],  
      "authMethod": "Cluster",  
      "clusterAdminIDs": [  
        1  
      ],  
      "finalTimeout": "2020-03-14T19:21:24Z",  
      "idpConfigVersion": 0,  
      "lastAccessTimeout": "2020-03-11T19:51:24Z",  
      "sessionCreationTime": "2020-03-11T19:21:24Z",  
      "sessionId": "b12bfc64-f233-44df-8b9f-6fb6c011abf7",  
      "username": "admin"  
    }  
  ]  
}
```

## Nouveautés depuis la version

12,0

## Supprimer les sessions d'authentification par nom d'utilisateur

Vous pouvez utiliser le `DeleteAuthSessionsByUsername` méthode permettant de supprimer toutes les sessions d'authentification pour un ou plusieurs utilisateurs donnés. Un appelant n'appartenant pas au groupe d'accès `ClusterAdmins/Administrateur` ne peut supprimer que ses propres sessions. Un appelant disposant des privilèges `ClusterAdmins/Administrateur` peut supprimer les sessions appartenant à n'importe quel utilisateur. Pour consulter la liste des sessions pouvant être supprimées, utilisez `ListAuthSessionsByUsername` avec les mêmes paramètres. Pour consulter la liste des sessions susceptibles d'être supprimées, utilisez le `ListAuthSessionsByUsername` méthode avec le même paramètre.

## Paramètres

Cette méthode possède les paramètres d'entrée suivants :

Nom	Description	Type	Valeur par défaut	Obligatoire
méthode d'authentification	<p>Méthode d'authentification des sessions utilisateur à supprimer. Seul un appelant appartenant au groupe d'accès ClusterAdmins/Administrator peut fournir ce paramètre. Les valeurs possibles sont :</p> <ul style="list-style-type: none"> <li>• <b>authMethod=Cluster</b> spécifie le nom d'utilisateur ClusterAdmin.</li> <li>• <b>authMethod=LDAP</b> spécifie le DN LDAP de l'utilisateur.</li> <li>• <b>authMethod=Id</b> spécifie soit l'UUID ou le NameID du fournisseur d'identité de l'utilisateur. Si le fournisseur d'identité n'est pas configuré pour renvoyer l'une ou l'autre option, ceci spécifie un UUID aléatoire émis lors de la création de la session.</li> </ul>	méthode d'authentification	Aucune	Non
nom d'utilisateur	Identifiant unique de l'utilisateur.	chaîne	Aucune	Non

## Valeurs de retour

Cette méthode a la valeur de retour suivante :

Nom	Description	Type
-----	-------------	------

séances	Informations de session pour les sessions d'authentification supprimées.	"authSessionInfo"
---------	--	-------------------

## Exemple de demande

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

```
{
  "method": "DeleteAuthSessionsByUsername",
  "params": {
    "authMethod": "Cluster",
    "username": "admin"
  }
}
```

## Exemple de réponse

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

```
{
  "sessions": [
    {
      "accessGroupList": [
        "administrator"
      ],
      "authMethod": "Cluster",
      "clusterAdminIDs": [
        1
      ],
      "finalTimeout": "2020-03-14T19:21:24Z",
      "idpConfigVersion": 0,
      "lastAccessTimeout": "2020-03-11T19:51:24Z",
      "sessionCreationTime": "2020-03-11T19:21:24Z",
      "sessionID": "b12bfc64-f233-44df-8b9f-6fb6c011abf7",
      "username": "admin"
    }
  ]
}
```

## Nouveautés depuis la version

12,0

# Supprimer la configuration Idp

Vous pouvez utiliser la `DeleteIdpConfiguration` méthode pour supprimer une configuration existante d'un fournisseur d'identité tiers pour le cluster. La suppression de la dernière configuration IdP supprime le certificat du fournisseur de services SAML du cluster.

## Paramètres

Cette méthode possède les paramètres d'entrée suivants :

Nom	Description	Type	Valeur par défaut	Obligatoire
ID de configuration idp	UUID pour la configuration du fournisseur d'identité tiers.	UUID	Aucune	Non
Nom idp	Nom utilisé pour identifier et récupérer un fournisseur d'identité (IdP) pour l'authentification unique SAML 2.0.	chaîne	Aucune	Non

## Valeurs de retour

Cette méthode ne renvoie aucune valeur.

## Exemple de demande

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

```
{
  "method": "DeleteIdpConfiguration",
  "params": {
    "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
    "idpName": "https://provider.name.url.com"
  }
}
```

## Exemple de réponse

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

```
{  
  "result": {}  
}
```

## Nouveautés depuis la version

12,0

## Désactiver l'authentification Idp

Vous pouvez utiliser le `DisableIdpAuthentication` Méthode permettant de désactiver la prise en charge de l'authentification via des fournisseurs d'identité tiers pour le cluster. Une fois désactivée, l'authentification des utilisateurs par des fournisseurs d'identité tiers les empêche d'accéder au cluster et toutes les sessions authentifiées actives sont invalidées/déconnectées. Les administrateurs LDAP et de cluster peuvent accéder au cluster via les interfaces utilisateur prises en charge.

### Paramètres

Cette méthode ne requiert aucun paramètre d'entrée.

### Valeurs de retour

Cette méthode ne renvoie aucune valeur.

### Exemple de demande

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

```
{  
  "method": "DisableIdpAuthentication",  
  "params": {}  
}
```

### Exemple de réponse

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

```
{  
  "result": {}  
}
```

## Nouveautés depuis la version

12,0

## Activer l'authentification Idp

Vous pouvez utiliser le `EnableIdpAuthentication` méthode permettant de prendre en charge l'authentification à l'aide de fournisseurs d'identité tiers pour le cluster. Une fois l'authentification IdP activée, les administrateurs LDAP et de cluster ne peuvent plus accéder au cluster via les interfaces utilisateur prises en charge et toutes les sessions authentifiées actives sont invalidées/déconnectées. Seuls les utilisateurs authentifiés par des fournisseurs d'identité tiers peuvent accéder au cluster via les interfaces utilisateur prises en charge.

### Paramètres

Cette méthode possède le paramètre d'entrée suivant :

Nom	Description	Type	Valeur par défaut	Obligatoire
ID de configuration idp	UUID pour la configuration du fournisseur d'identité tiers. S'il n'existe qu'une seule configuration IdP, c'est cette configuration qui sera activée par défaut. Si vous n'avez qu'une seule configuration <code>IdpConfiguration</code> , vous n'avez pas besoin de fournir le paramètre <code>idpConfigurationID</code> .	UUID	Aucune	Non

### Valeurs de retour

Cette méthode ne renvoie aucune valeur.

### Exemple de demande

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

```
{  
  "method": "EnableIdpAuthentication",  
  "params": {  
    "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",  
  }  
}
```

## Exemple de réponse

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

```
{  
  "result": {}  
}
```

## Nouveautés depuis la version

12,0

## Obtenir l'état d'authentification Idp

Vous pouvez utiliser le `GetIdpAuthenticationState` Méthode permettant de renvoyer des informations concernant l'état de l'authentification à l'aide de fournisseurs d'identité tiers.

### Paramètres

Cette méthode ne requiert aucun paramètre d'entrée.

### Valeurs de retour

Cette méthode a la valeur de retour suivante :

Nom	Description	Type
activé	Indique si l'authentification IdP tierce est activée.	booléen

## Exemple de demande

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

```
{  
  "method": "GetIdpAuthenticationState"  
}
```

## Exemple de réponse

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

```
{  
  "result": {"enabled": true}  
}
```

## Nouveautés depuis la version

12,0

## Lister les sessions d'authentification actives

Vous pouvez utiliser le `ListActiveAuthSessions` Méthode permettant de lister toutes les sessions authentifiées actives. Seuls les utilisateurs disposant de droits d'accès administratif peuvent appeler cette méthode.

### Paramètres

Cette méthode ne requiert aucun paramètre d'entrée.

### Valeurs de retour

Cette méthode a la valeur de retour suivante :

Nom	Description	Type
séances	Informations de session pour les sessions d'authentification.	"authSessionInfo"

## Exemple de demande

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

```
{  
  "method": "ListActiveAuthSessions"  
}
```

## Exemple de réponse

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

```
{  
  "sessions": [  
    {  
      "accessGroupList": [  
        "administrator"  
      ],  
      "authMethod": "Cluster",  
      "clusterAdminIDs": [  
        1  
      ],  
      "finalTimeout": "2020-03-14T19:21:24Z",  
      "idpConfigVersion": 0,  
      "lastAccessTimeout": "2020-03-11T19:51:24Z",  
      "sessionCreationTime": "2020-03-11T19:21:24Z",  
      "sessionId": "b12bfc64-f233-44df-8b9f-6fb6c011abf7",  
      "username": "admin"  
    }  
  ]  
}
```

## Nouveautés depuis la version

12,0

## ListIdpConfigurations

Vous pouvez utiliser le `ListIdpConfigurations` Méthode permettant de lister les configurations des fournisseurs d'identité tiers. Vous pouvez également fournir, si vous le souhaitez : `enabledOnly` Utilisez un indicateur pour récupérer la configuration IdP actuellement activée ou un UUID de métadonnées IdP ou un nom IdP pour interroger des informations sur une configuration IdP spécifique.

## Paramètres

Cette méthode possède les paramètres d'entrée suivants :

Nom	Description	Type	Valeur par défaut	Obligatoire
activé uniquement	Filtre le résultat pour renvoyer la configuration IdP actuellement activée.	booléen	Aucune	Non
ID de configuration idp	UUID pour la configuration du fournisseur d'identité tiers.	UUID	Aucune	Non
Nom idp	Récupère les informations de configuration IdP pour un nom IdP spécifique.	chaîne	Aucune	Non

## Valeurs de retour

Cette méthode a la valeur de retour suivante :

Nom	Description	Type
idpConfigInfos	Informations sur la ou les configurations du fournisseur d'identité tiers.	"idpConfigInfo"tableau

## Exemple de demande

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

```
{
  "method": "ListIdpConfigurations",
  "params": {}
}
```

## Exemple de réponse

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

```

{
  "result": {
    "idpConfigInfo": {
      "enabled": true,
      "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
      "idpMetadata": "<?xml version=\"1.0\" encoding=\"UTF-8\"?>\r\n<EntityDescriptor
xmlns=\"urn:oasis:names:tc:SAML:2.0:metadata\"\r\n  xmlns:ds=\"http://www.w3.org/2000/09/xmldsig#\"\r\n  xmlns:shibmd=\"urn:mace:shibboleth:metadata:1.0\"\r\n  xmlns:xml=\"http://www.w3.org/XML/1998/namespace\"\r\n...</Organization>\r\n</EntityDescriptor>",
      "idpName": "https://privider.name.url.com",
      "serviceProviderCertificate": "-----BEGIN CERTIFICATE-----\nMI...BHi\r\n-----END CERTIFICATE-----\n",
      "spMetadataUrl": "https://10.193.100.100/auth/ui/saml2"
    }
  }
}

```

## Nouveautés depuis la version

12,0

## Mise à jour de la configuration Idp

Vous pouvez utiliser la `UpdateIdpConfiguration` méthode permettant de mettre à jour une configuration existante avec un fournisseur d'identité tiers pour le cluster.

### Paramètres

Cette méthode possède les paramètres d'entrée suivants :

Nom	Description	Type	Valeur par défaut	Obligatoire
générer un nouveau certificat	Si cette option est définie sur true, une nouvelle clé et un nouveau certificat SAML sont générés et remplacent la paire existante. Remarque : Le remplacement du certificat existant interrompra la relation de confiance établie entre le cluster et le fournisseur d'identité jusqu'à ce que les métadonnées du fournisseur de services du cluster soient rechargées auprès du fournisseur d'identité. Si cette option n'est pas fournie ou si sa valeur est définie sur false, le certificat et la clé SAML restent inchangés.	booléen	Aucune	Non
ID de configuration idp	UUID pour la configuration du fournisseur d'identité tiers.	UUID	Aucune	Non
Métadonnées idp	Métadonnées IdP pour les détails de configuration et d'intégration de l'authentification unique SAML 2.0.	chaîne	Aucune	Non
Nom idp	Nom utilisé pour identifier et récupérer un fournisseur d'identité (IdP) pour l'authentification unique SAML 2.0.	chaîne	Aucune	Non

Nom	Description	Type	Valeur par défaut	Obligatoire
nouveauNomIdp	Si spécifié, ce nom remplace l'ancien nom du fournisseur d'identité.	chaîne	Aucune	Non

## Valeurs de retour

Cette méthode a la valeur de retour suivante :

Nom	Description	Type
idpConfigInfo	Informations relatives à la configuration du fournisseur d'identité tiers.	"idpConfigInfo"

## Exemple de demande

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

```
{
  "method": "UpdateIdpConfiguration",
  "params": {
    "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
    "generateNewCertificate": true
  }
}
```

## Exemple de réponse

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

```

{
  "result": {
    "idpConfigInfo": {
      "enabled": true,
      "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
      "idpMetadata": "<?xml version=\"1.0\" encoding=\"UTF-8\"?>\r\n<EntityDescriptor
xmlns=\"urn:oasis:names:tc:SAML:2.0:metadata\"\r\n  xmlns:ds=\"http://www.w3.org/2000/09/xmldsig#\"\r\n  xmlns:shibmd=\"urn:mace:shibboleth:metadata:1.0\"\r\n  xmlns:xml=\"http://www.w3.org/XML/1998/namespace\"\r\n...</Organization>\r\n</EntityDescriptor>",
      "idpName": "https://privider.name.url.com",
      "serviceProviderCertificate": "-----BEGIN CERTIFICATE-----\nMI...BHi\r\n-----END CERTIFICATE-----\n",
      "spMetadataUrl": "https://10.193.100.100/auth/ui/saml2"
    }
  }
}

```

## Nouveautés depuis la version

12,0

## Informations sur le copyright

Copyright © 2025 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 JOUSSANCE, 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 DÉLICTUELLE (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.