



Méthodes d'API LDAP

Element Software

NetApp
January 15, 2024

Sommaire

- Méthodes d'API LDAP 1
 - Trouvez plus d'informations 1
 - AddapClusterAdmin 1
 - EnableLdapAuthentication 3
 - DisableLdapAuthentication 8
 - GetLdapConfiguration 9
 - TestLdapAuthentication 10

Méthodes d'API LDAP

Vous pouvez utiliser le protocole LDAP (Lightweight Directory Access Protocol) pour authentifier l'accès au stockage Element. Les méthodes de l'API LDAP décrites dans cette section permettent de configurer l'accès LDAP au cluster de stockage.

- [AddapClusterAdmin](#)
- [EnableLdapAuthentication](#)
- [DisableLdapAuthentication](#)
- [GetLdapConfiguration](#)
- [TestLdapAuthentication](#)

Trouvez plus d'informations

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

AddapClusterAdmin

Vous pouvez utiliser le `AddLdapClusterAdmin` Pour ajouter un nouvel utilisateur administrateur de cluster LDAP. Un administrateur de cluster LDAP peut gérer le cluster à l'aide de l'API et des outils de gestion. Les comptes d'administrateur de cluster LDAP sont complètement séparés et n'ont pas de rapport avec les comptes de tenant standard.

Paramètres

Vous pouvez également utiliser cette méthode pour ajouter un groupe LDAP défini dans Active Directory®. Le niveau d'accès attribué au groupe est transmis aux utilisateurs individuels du groupe LDAP.

Cette méthode présente les paramètres d'entrée suivants :

Nom	Description	Type	Valeur par défaut	Obligatoire
l'accès	Contrôle les méthodes que cet administrateur du cluster peut utiliser.	tableau de chaînes	Aucune	Oui.

Nom	Description	Type	Valeur par défaut	Obligatoire
AcceptEula	Acceptez le contrat de licence de l'utilisateur final. Définissez sur vrai pour ajouter un compte d'administrateur de cluster au système. Si omis ou défini sur FALSE, l'appel de méthode échoue.	booléen	Aucune	Oui.
attributs	Liste des paires nom-valeur au format d'objet JSON.	Objet JSON	Aucune	Non
nom d'utilisateur	Nom d'utilisateur distinct pour le nouvel administrateur de cluster LDAP.	chaîne	Aucune	Oui.

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": "AddLdapClusterAdmin",
  "params": {"username": "cn=mike
jones,ou=ptusers,dc=prodtest,dc=solidfire,dc=net",
  "access": ["administrator", "read"
  ]
},
  "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

[Contrôle d'accès](#)

EnableLdapAuthentication

Vous pouvez utiliser le `EnableLdapAuthentication` Méthode de configuration de la connexion d'un annuaire LDAP à un cluster pour l'authentification LDAP. Les utilisateurs membres de l'annuaire LDAP peuvent ensuite se connecter au système de stockage à l'aide de leurs informations d'identification LDAP.

Paramètres

Cette méthode présente les paramètres d'entrée suivants :

Nom	Description	Type	Valeur par défaut	Obligatoire
Type d'autorisation	Identifie la méthode d'authentification utilisateur à utiliser. Valeurs possibles : <ul style="list-style-type: none">• DirectBind• SearchAndBind	chaîne	SearchAndBind	Non
GroupSearchBaseDN	Le DN de base de l'arborescence pour lancer la recherche dans la sous-arborescence du groupe.	chaîne	Aucune	Non

Nom	Description	Type	Valeur par défaut	Obligatoire
GroupSearchType	<p>Contrôle le filtre de recherche de groupe utilisé par défaut. Valeurs possibles :</p> <ul style="list-style-type: none"> • Aucun groupe : pas de prise en charge de groupe. • ActiveDirectory : appartenance imbriquée de tous les groupes Active Directory d'un utilisateur. • MemberDN : groupes de style MemberDN (niveau unique). 	chaîne	ActiveDirectory	Non
URI de serveur	<p>Liste séparée par des virgules d'URI de serveur LDAP ou LDAPS. Vous pouvez ajouter un port personnalisé à la fin d'un URI LDAP ou LDAPS en utilisant un point-virgule suivi du numéro de port. Par exemple, l'URI "ldap://1.2.3.4" utilise le port par défaut et l'URI "ldaps://1.2.3.4:123" utilise le port personnalisé 123.</p>	tableau de chaînes	Aucune	Oui.
UserSearchBaseDN	<p>Le DN de base de l'arborescence pour lancer la recherche dans la sous-arborescence. Ce paramètre est requis lors de l'utilisation d'un AuthType de SearchAndBind.</p>	chaîne	Aucune	Non

Nom	Description	Type	Valeur par défaut	Obligatoire
SearchBindDN	Un DN complet qualifié pour se connecter avec pour effectuer une recherche LDAP pour l'utilisateur. Le DN requiert un accès en lecture au répertoire LDAP. Ce paramètre est requis lors de l'utilisation d'un AuthType de SearchAndBind.	chaîne	Aucune	Oui.
SearchBindPassword	Mot de passe du compte searchBindDN utilisé pour la recherche. Ce paramètre est requis lors de l'utilisation d'un AuthType de SearchAndBind.	chaîne	Aucune	Oui.

Nom	Description	Type	Valeur par défaut	Obligatoire
UserSearchFilter	<p>Le filtre de recherche LDAP à utiliser lors de l'interrogation du serveur LDAP. La chaîne doit comporter le texte de l'espace réservé « %USERNAME% » qui est remplacé par le nom d'utilisateur de l'utilisateur d'authentification. Par exemple, (&(objectClass=personne)(sAMAccountName=%USERNAME%)) utilisera le champ sAMAccountName dans Active Directory pour qu'il corresponde au nom d'utilisateur entré lors de la connexion au cluster. Ce paramètre est requis lors de l'utilisation d'un AuthType de SearchAndBind.</p>	chaîne	Aucune	Oui.
UserDNTemplate	<p>Modèle de chaîne utilisé pour définir un motif pour la construction d'un nom unique (DN) utilisateur complet. La chaîne doit comporter le texte de l'espace réservé « %USERNAME% » qui est remplacé par le nom d'utilisateur de l'utilisateur d'authentification. Ce paramètre est requis lors de l'utilisation d'un AuthType de DirectBind.</p>	chaîne	Aucune	Oui.

Nom	Description	Type	Valeur par défaut	Obligatoire
GroupSearchCustomFilter	À utiliser avec le type de recherche CustomFilter, un filtre LDAP à utiliser pour renvoyer le DNS des groupes d'un utilisateur. La chaîne peut avoir un texte de marque de réservation de %USERNAME% et %USERDN% à remplacer par son nom d'utilisateur et son nom d'utilisateur complet si nécessaire.	chaîne	Aucune	Oui.

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": "EnableLdapAuthentication",
  "params": {
    "authType": "SearchAndBind",
    "groupSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
    "groupSearchType": "ActiveDirectory",
    "searchBindDN": "SFReadOnly@prodtest.solidfire.net",
    "searchBindPassword": "zsw@#edcASD12",
    "sslCert": "",
    "userSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
    "userSearchFilter":
    "(&(objectClass=person)(sAMAccountName=%USERNAME%))",
    "serverURIs": [
      "ldaps://111.22.333.444",
      "ldap://555.66.777.888"
    ]
  },
  "id": 1
}
```

Exemple de réponse

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

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

Nouveau depuis la version

9.6

DisableLdapAuthentication

Vous pouvez utiliser le `DisableLdapAuthentication` Méthode permettant de désactiver l'authentification LDAP et de supprimer tous les paramètres de configuration LDAP. Cette méthode ne supprime aucun compte d'administrateur de cluster configuré pour les utilisateurs ou les groupes. Une fois l'authentification LDAP désactivée, les administrateurs du cluster configurés pour utiliser l'authentification LDAP ne peuvent plus accéder au cluster.

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": "DisableLdapAuthentication",
  "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

GetLdapConfiguration

Vous pouvez utiliser le `GetLdapConfiguration` Méthode d'obtention de la configuration LDAP actuellement active sur le cluster.

Paramètres

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

Retour de valeur

Cette méthode a la valeur de retour suivante.

Nom	Description	Type
LdapConfiguration	Liste des paramètres de configuration LDAP actuels. Cet appel d'API ne renvoie pas le texte brut du mot de passe du compte de recherche. Remarque : si l'authentification LDAP est actuellement désactivée, tous les paramètres renvoyés sont vides à l'exception de "AuthType", et "groupSearchType", qui sont respectivement définis sur "SearchAndBind" et "ActiveDirectory".	LdapConfiguration

Exemple de demande

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

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

Exemple de réponse

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

```
{
  "id": 1,
  "result": {
    "ldapConfiguration": {
      "authType": "SearchAndBind",
      "enabled": true,
      "groupSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
      "groupSearchCustomFilter": "",
      "groupSearchType": "ActiveDirectory",
      "searchBindDN": "SFReadOnly@prodtest.solidfire.net",
      "serverURIs": [
        "ldaps://111.22.333.444",
        "ldap://555.66.777.888"
      ],
      "userDNTemplate": "",
      "userSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
      "userSearchFilter":
        "(&(objectClass=person)(sAMAccountName=%USERNAME%))"
    }
  }
}
```

Nouveau depuis la version

9.6

TestLdapAuthentication

Vous pouvez utiliser le `TestLdapAuthentication` Méthode de validation des paramètres d'authentification LDAP actuellement activés. Si la configuration est correcte, l'appel API renvoie l'appartenance au groupe de l'utilisateur testé.

Paramètres

Cette méthode présente les paramètres d'entrée suivants :

Nom	Description	Type	Valeur par défaut	Obligatoire
nom d'utilisateur	Nom d'utilisateur à tester.	chaîne	Aucune	Oui.
mot de passe	Mot de passe du nom d'utilisateur à tester.	chaîne	Aucune	Oui.
LdapConfiguration	Un objet LdapConfiguration à tester. Si vous fournissez ce paramètre, le système teste la configuration fournie, même si l'authentification LDAP est actuellement désactivée.	LdapConfiguration	Aucune	Non

Valeurs de retour

Cette méthode a les valeurs de retour suivantes :

Nom	Description	Type
groupes	Liste des groupes LDAP incluant l'utilisateur testé en tant que membre.	baie
DN utilisateur	Nom complet du LDAP de l'utilisateur testé.	chaîne

Exemple de demande

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

```
{
  "method": "TestLdapAuthentication",
  "params": {"username": "admin1",
            "password": "admin1PASS"}
},
  "id": 1
}
```

Exemple de réponse

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

```
{
  "id": 1,
  "result": {
    "groups": [
      "CN=StorageMgmt,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
    ],
    "userDN": "CN=Admin1
Jones,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
  }
}
```

Nouveau depuis la version

9.6

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.