



Metodi API LDAP

Element Software

NetApp

November 12, 2025

This PDF was generated from https://docs.netapp.com/it-it/element-software-128/api/reference_element_api_addldapclusteradmin.html on November 12, 2025. Always check docs.netapp.com for the latest.

Sommario

- Metodi API LDAP 1
 - AggiungiLdapClusterAdmin 1
 - Parametri 1
 - Valori di ritorno 2
 - Richiedi esempio 2
 - Esempio di risposta 2
 - Nuovo dalla versione 2
 - Trova maggiori informazioni 2
 - Abilita autenticazione LDAP 2
 - Parametri 2
 - Valori di ritorno 6
 - Richiedi esempio 6
 - Esempio di risposta 7
 - Nuovo dalla versione 7
 - Disabilita l'autenticazione LDAP 7
 - Parametri 8
 - Valori di ritorno 8
 - Richiedi esempio 8
 - Esempio di risposta 8
 - Nuovo dalla versione 8
 - OttieniLdapConfiguration 8
 - Parametri 8
 - Valore di ritorno 8
 - Richiedi esempio 9
 - Esempio di risposta 9
 - Nuovo dalla versione 10
 - TestLdapAuthentication 10
 - Parametri 10
 - Valori di ritorno 11
 - Richiedi esempio 11
 - Esempio di risposta 11
 - Nuovo dalla versione 12

Metodi API LDAP

AggiungiLdapClusterAdmin

Puoi usare il `AddLdapClusterAdmin` per aggiungere un nuovo utente amministratore del cluster LDAP. Un amministratore del cluster LDAP può gestire il cluster utilizzando l'API e gli strumenti di gestione. Gli account di amministrazione del cluster LDAP sono completamente separati e non correlati agli account tenant standard.

Parametri

È possibile utilizzare questo metodo anche per aggiungere un gruppo LDAP definito in Active Directory®. Il livello di accesso concesso al gruppo viene trasmesso ai singoli utenti del gruppo LDAP.

Questo metodo ha i seguenti parametri di input:

| Nome | Descrizione | Tipo | Valore predefinito | Necessario |
|---------------|---|---------------------|--------------------|------------|
| accesso | Controlla quali metodi può utilizzare questo amministratore del cluster. | matrice di stringhe | Nessuno | Sì |
| accettareEula | Accettare il Contratto di licenza con l'utente finale. Impostare su true per aggiungere un account amministratore del cluster al sistema. Se omesso o impostato su false, la chiamata al metodo fallisce. | booleano | Nessuno | Sì |
| attributi | Elenco di coppie nome-valore nel formato oggetto JSON. | Oggetto JSON | Nessuno | NO |
| nome utente | Nome utente distinto per il nuovo amministratore del cluster LDAP. | corda | Nessuno | Sì |

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "AddLdapClusterAdmin",
  "params": {"username": "cn=mike
jones,ou=ptusers,dc=prodtest,dc=solidfire,dc=net",
    "access": ["administrator", "read"]
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

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

Nuovo dalla versione

9,6

Trova maggiori informazioni

[Controllo degli accessi](#)

Abilita autenticazione LDAP

Puoi usare il `EnableLdapAuthentication` metodo per configurare una connessione alla directory LDAP per l'autenticazione LDAP a un cluster. Gli utenti che sono membri della directory LDAP possono quindi accedere al sistema di archiviazione utilizzando le proprie credenziali LDAP.

Parametri

Questo metodo ha i seguenti parametri di input:

| Nome | Descrizione | Tipo | Valore predefinito | Necessario |
|------------------------|---|-------|--------------------|------------|
| tipo di autorizzazione | <p>Identifica quale metodo di autenticazione utente utilizzare. Valori possibili:</p> <ul style="list-style-type: none"> • DirectBind • SearchAndBind | corda | Cerca e associa | NO |
| groupSearchBaseDN | Il DN di base dell'albero da cui iniziare la ricerca del sottoalbero del gruppo. | corda | Nessuno | NO |
| groupSearchType | <p>Controlla il filtro di ricerca del gruppo predefinito utilizzato. Valori possibili:</p> <ul style="list-style-type: none"> • NoGroups: nessun supporto di gruppo. • ActiveDirectory: appartenenza annidata a tutti i gruppi di Active Directory di un utente. • MemberDN: gruppi di stile MemberDN (livello singolo). | corda | Directory attiva | NO |

| Nome | Descrizione | Tipo | Valore predefinito | Necessario |
|------------------|--|---------------------|--------------------|------------|
| serverURLs | Un elenco separato da virgole di URI del server LDAP o LDAPS. È possibile aggiungere una porta personalizzata alla fine di un URI LDAP o LDAPS utilizzando due punti seguiti dal numero di porta. Ad esempio, l'URI "ldap://1.2.3.4" utilizza la porta predefinita e l'URI "ldaps://1.2.3.4:123" utilizza la porta personalizzata 123. | matrice di stringhe | Nessuno | Sì |
| userSearchBaseDN | Il DN di base dell'albero da cui iniziare la ricerca del sottoalbero. Questo parametro è obbligatorio quando si utilizza un authType di SearchAndBind. | corda | Nessuno | NO |
| searchBindDN | Un DN completamente qualificato con cui effettuare l'accesso per eseguire una ricerca LDAP per l'utente. Il DN richiede l'accesso in lettura alla directory LDAP. Questo parametro è obbligatorio quando si utilizza un authType di SearchAndBind. | corda | Nessuno | Sì |

| Nome | Descrizione | Tipo | Valore predefinito | Necessario |
|---------------------|--|-------|--------------------|------------|
| cercaBindPassword | Password per l'account searchBindDN utilizzato per la ricerca. Questo parametro è obbligatorio quando si utilizza un authType di SearchAndBind. | corda | Nessuno | Sì |
| filtroricercautente | Filtro di ricerca LDAP da utilizzare quando si interroga il server LDAP. La stringa dovrebbe contenere il testo segnaposto "%USERNAME%" che viene sostituito con il nome utente dell'utente che esegue l'autenticazione. Ad esempio, (&(objectClass=person)(sAMAccountName=%USERNAME%)) utilizzerà il campo sAMAccountName in Active Directory per far corrispondere il nome utente immesso durante l'accesso al cluster. Questo parametro è obbligatorio quando si utilizza un authType di SearchAndBind. | corda | Nessuno | Sì |

| Nome | Descrizione | Tipo | Valore predefinito | Necessario |
|--------------------------|---|-------|--------------------|------------|
| ModelloDNutente | Un modello di stringa utilizzato per definire un modello per la costruzione di un nome distinto (DN) utente completo. La stringa dovrebbe contenere il testo segnaposto "%USERNAME%" che viene sostituito con il nome utente dell'utente che esegue l'autenticazione. Questo parametro è obbligatorio quando si utilizza un authType di DirectBind. | corda | Nessuno | Sì |
| groupSearchCustom Filter | Da utilizzare con il tipo di ricerca CustomFilter, un filtro LDAP da utilizzare per restituire i DN dei gruppi di un utente. La stringa può contenere il testo segnaposto %USERNAME% e %USERDN% da sostituire con il nome utente e il nome utente completo, se necessario. | corda | Nessuno | Sì |

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:


```
{
  "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
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

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

Nuovo dalla versione

9,6

Disabilita l'autenticazione LDAP

Puoi usare il `DisableLdapAuthentication` metodo per disabilitare l'autenticazione LDAP e rimuovere tutte le impostazioni di configurazione LDAP. Questo metodo non rimuove alcun account amministratore del cluster configurato per utenti o gruppi. Dopo aver disabilitato l'autenticazione LDAP, gli amministratori del cluster configurati per utilizzare l'autenticazione LDAP non potranno più accedere al cluster.

Parametri

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

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

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

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

Nuovo dalla versione

9,6

OttieniLdapConfiguration

Puoi usare il `GetLdapConfiguration` metodo per ottenere la configurazione LDAP attualmente attiva sul cluster.

Parametri

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno.

| Nome | Descrizione | Tipo |
|---------------------|---|-------------------------------------|
| Configurazione ldap | <p>Elenco delle impostazioni di configurazione LDAP correnti. Questa chiamata API non restituisce il testo normale della password dell'account di ricerca.</p> <p>Nota: se l'autenticazione LDAP è attualmente disabilitata, tutte le impostazioni restituite sono vuote, ad eccezione di "authType" e "groupSearchType", che sono impostate rispettivamente su "SearchAndBind" e "ActiveDirectory".</p> | Configurazione ldap |

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

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

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```

{
  "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%))"
    }
  }
}

```

Nuovo dalla versione

9,6

TestLdapAuthentication

Puoi usare il `TestLdapAuthentication` metodo per convalidare le impostazioni di autenticazione LDAP attualmente abilitate. Se la configurazione è corretta, la chiamata API restituisce l'appartenenza al gruppo dell'utente testato.

Parametri

Questo metodo ha i seguenti parametri di input:

| Nome | Descrizione | Tipo | Valore predefinito | Necessario |
|-------------|--|-------|--------------------|------------|
| nome utente | Il nome utente da testare. | corda | Nessuno | Sì |
| password | La password per il nome utente da testare. | corda | Nessuno | Sì |

| Nome | Descrizione | Tipo | Valore predefinito | Necessario |
|---------------------|--|-------------------------------------|--------------------|------------|
| Configurazione ldap | Un oggetto ldapConfiguration da testare. Se si fornisce questo parametro, il sistema verifica la configurazione fornita anche se l'autenticazione LDAP è attualmente disabilitata. | Configurazione ldap | Nessuno | NO |

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

| Nome | Descrizione | Tipo |
|------------|--|---------|
| gruppi | Elenco dei gruppi LDAP che includono l'utente testato come membro. | vettore |
| nomeutente | Nome distinto LDAP completo dell'utente testato. | corda |

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

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

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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"
  }
}
```

Nuovo dalla versione

9,6

Informazioni sul copyright

Copyright © 2025 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.