



# **LDAP-API-Methoden**

## **Element Software**

NetApp

November 12, 2025

This PDF was generated from [https://docs.netapp.com/de-de/element-software-128/api/reference\\_element\\_api\\_addldapclusteradmin.html](https://docs.netapp.com/de-de/element-software-128/api/reference_element_api_addldapclusteradmin.html) on November 12, 2025. Always check [docs.netapp.com](https://docs.netapp.com) for the latest.

# Inhalt

|   |    |
|---|----|
| LDAP-API-Methoden .....                   | 1  |
| AddLdapClusterAdmin .....                 | 1  |
| Parameter .....                           | 1  |
| Rückgabewerte .....                       | 2  |
| Anforderungsbeispiel .....                | 2  |
| Antwortbeispiel .....                     | 2  |
| Neu seit Version .....                    | 2  |
| Weitere Informationen .....               | 2  |
| LDAP-Authentifizierung aktivieren .....   | 2  |
| Parameter .....                           | 2  |
| Rückgabewerte .....                       | 6  |
| Anforderungsbeispiel .....                | 7  |
| Antwortbeispiel .....                     | 7  |
| Neu seit Version .....                    | 7  |
| LDAP-Authentifizierung deaktivieren ..... | 7  |
| Parameter .....                           | 8  |
| Rückgabewerte .....                       | 8  |
| Anforderungsbeispiel .....                | 8  |
| Antwortbeispiel .....                     | 8  |
| Neu seit Version .....                    | 8  |
| GetLdapConfiguration .....                | 8  |
| Parameter .....                           | 8  |
| Rückgabewert .....                        | 8  |
| Anforderungsbeispiel .....                | 9  |
| Antwortbeispiel .....                     | 9  |
| Neu seit Version .....                    | 10 |
| TestLdapAuthentication .....              | 10 |
| Parameter .....                           | 10 |
| Rückgabewerte .....                       | 11 |
| Anforderungsbeispiel .....                | 11 |
| Antwortbeispiel .....                     | 11 |
| Neu seit Version .....                    | 12 |

# LDAP-API-Methoden

## AddLdapClusterAdmin

Sie können die `AddLdapClusterAdmin` einen neuen LDAP-Cluster-Administratorbenutzer hinzufügen. Ein LDAP-Cluster-Administrator kann den Cluster mithilfe der API und der Verwaltungstools verwalten. LDAP-Cluster-Administratorkonten sind vollständig getrennt und stehen in keinem Zusammenhang mit Standard-Mandantenkonten.

### Parameter

Mit dieser Methode können Sie auch eine LDAP-Gruppe hinzufügen, die in Active Directory® definiert wurde. Die der Gruppe zugewiesene Zugriffsebene wird an die einzelnen Benutzer in der LDAP-Gruppe weitergegeben.

Diese Methode hat die folgenden Eingabeparameter:

| Name         | Beschreibung  | Typ                 | Standardwert | Erforderlich |
|--------------|---|---------------------|--------------|--------------|
| Zugang       | Steuert, welche Methoden dieser Cluster-Administrator verwenden kann.   | Zeichenketten-Array | Keine        | Ja           |
| acceptEula   | Akzeptieren Sie die Endbenutzer-Lizenzvereinbarung. Auf „true“ setzen, um dem System ein Cluster-Administratorkonto hinzuzufügen. Wird der Parameter weggelassen oder auf „false“ gesetzt, schlägt der Methodenaufruf fehl. | boolescher Wert     | Keine        | Ja           |
| Attribute    | Liste von Name-Wert-Paaren im JSON-Objektformat.  | JSON-Objekt         | Keine        | Nein         |
| Benutzername | Der eindeutige Benutzername für den neuen LDAP-Clusteradministrator.  | Schnur              | Keine        | Ja           |

## Rückgabewerte

Diese Methode hat keinen Rückgabewert.

## Anforderungsbeispiel

Anfragen für diese Methode ähneln dem folgenden Beispiel:

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

## Antwortbeispiel

Diese Methode liefert eine Antwort, die dem folgenden Beispiel ähnelt:

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

## Neu seit Version

9,6

## Weitere Informationen

[Zugriffskontrolle](#)

## LDAP-Authentifizierung aktivieren

Sie können die `EnableLdapAuthentication` Methode zum Konfigurieren einer LDAP-Verzeichnisverbindung für die LDAP-Authentifizierung an einem Cluster. Benutzer, die Mitglieder des LDAP-Verzeichnisses sind, können sich dann mit ihren LDAP-Zugangsdaten im Speichersystem anmelden.

## Parameter

Diese Methode hat die folgenden Eingabeparameter:

| Name              | Beschreibung   | Typ    | Standardwert    | Erforderlich |
|-------------------|--|--------|-----------------|--------------|
| authType          | <p>Legt fest, welche Benutzerauthentifizierungsmethode verwendet werden soll. Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• DirectBind</li> <li>• SearchAndBind</li> </ul>  | Schnur | SearchAndBind   | Nein         |
| groupSearchBaseDN | Der Basis-DN des Baums, um die Suche nach Gruppenunterbäumen zu starten.   | Schnur | Keine           | Nein         |
| Gruppensuchetyp   | <p>Steuert den standardmäßig verwendeten Gruppensuchfilter. Mögliche Werte:</p> <ul style="list-style-type: none"> <li>• NoGroups: Keine Gruppenunterstützung.</li> <li>• ActiveDirectory: Verschachtelte Mitgliedschaft aller Active Directory-Gruppen eines Benutzers.</li> <li>• MemberDN: MemberDN-Stilgruppen (einstufig).</li> </ul> | Schnur | ActiveDirectory | Nein         |

| Name             | Beschreibung  | Typ                 | Standardwert | Erforderlich |
|------------------|---|---------------------|--------------|--------------|
| Server-URIs      | Eine durch Kommas getrennte Liste von LDAP- oder LDAPS-Server-URIs. Sie können einen benutzerdefinierten Port an das Ende einer LDAP- oder LDAPS-URI anhängen, indem Sie einen Doppelpunkt gefolgt von der Portnummer verwenden. Beispielsweise verwendet die URI "ldap://1.2.3.4" den Standardport und die URI "ldaps://1.2.3.4:123" verwendet den benutzerdefinierten Port 123. | Zeichenketten-Array | Keine        | Ja           |
| userSearchBaseDN | Der Basis-DN des Baums, um die Teilbaumsuche zu starten. Dieser Parameter ist erforderlich, wenn der Authentifizierungstyp SearchAndBind verwendet wird.  | Schnur              | Keine        | Nein         |
| searchBindDN     | Ein vollständig qualifizierter DN, mit dem man sich anmelden kann, um eine LDAP-Suche für den Benutzer durchzuführen. Der DN benötigt Lesezugriff auf das LDAP-Verzeichnis. Dieser Parameter ist erforderlich, wenn der Authentifizierungstyp SearchAndBind verwendet wird.   | Schnur              | Keine        | Ja           |

| Name                | Beschreibung  | Typ    | Standardwert | Erforderlich |
|---------------------|---|--------|--------------|--------------|
| searchBindPassword  | Das Passwort für das searchBindDN-Konto, das für die Suche verwendet wird. Dieser Parameter ist erforderlich, wenn der Authentifizierungstyp SearchAndBind verwendet wird.  | Schnur | Keine        | Ja           |
| Benutzer-Suchfilter | Der LDAP-Suchfilter, der bei Abfragen des LDAP-Servers verwendet werden soll. Die Zeichenkette sollte den Platzhaltertext "%USERNAME%" enthalten, der durch den Benutzernamen des authentifizierenden Benutzers ersetzt wird. Beispielsweise verwendet (&(objectClass=person)(sAMAccountName=%USERNAME%)) das Feld sAMAccountName in Active Directory, um den beim Cluster-Login eingegebenen Benutzernamen abzugleichen. Dieser Parameter ist erforderlich, wenn der Authentifizierungstyp SearchAndBind verwendet wird. | Schnur | Keine        | Ja           |

| Name                                   | Beschreibung  | Typ    | Standardwert | Erforderlich |
|--|---|--------|--------------|--------------|
| userDNTemplate                         | Eine Zeichenkettenvorlage, die verwendet wird, um ein Muster für die Erstellung eines vollständigen Benutzernamens (Distinguished Name, DN) zu definieren. Die Zeichenkette sollte den Platzhaltertext "%USERNAME%" enthalten, der durch den Benutzernamen des authentifizierenden Benutzers ersetzt wird. Dieser Parameter ist erforderlich, wenn der Authentifizierungstyp DirectBind verwendet wird. | Schnur | Keine        | Ja           |
| GruppensucheBenutzerdefinierter Filter | Zur Verwendung mit dem Suchtyp CustomFilter: Ein LDAP-Filter, der die DNs der Gruppen eines Benutzers zurückgibt. Die Zeichenkette kann Platzhaltertexte für %USERNAME% und %USERDN% enthalten, die bei Bedarf durch den Benutzernamen bzw. den vollständigen Benutzer-DN ersetzt werden.   | Schnur | Keine        | Ja           |

## Rückgabewerte

Diese Methode hat keinen Rückgabewert.



## Anforderungsbeispiel

Anfragen für diese Methode ähneln dem folgenden Beispiel:

```
{
  "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
}
```

## Antwortbeispiel

Diese Methode liefert eine Antwort, die dem folgenden Beispiel ähnelt:

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

## Neu seit Version

9,6

## LDAP-Authentifizierung deaktivieren

Sie können die `DisableLdapAuthentication` Methode zum Deaktivieren der LDAP-Authentifizierung und zum Entfernen aller LDAP-Konfigurationseinstellungen. Bei dieser Methode werden keine konfigurierten Cluster-Administratorkonten für Benutzer oder Gruppen entfernt. Nach der Deaktivierung der LDAP-Authentifizierung können Cluster-

Administratoren, die für die Verwendung der LDAP-Authentifizierung konfiguriert sind, nicht mehr auf den Cluster zugreifen.

### Parameter

Diese Methode hat keine Eingabeparameter.

### Rückgabewerte

Diese Methode hat keinen Rückgabewert.

### Anforderungsbeispiel

Anfragen für diese Methode ähneln dem folgenden Beispiel:

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

### Antwortbeispiel

Diese Methode liefert eine Antwort, die dem folgenden Beispiel ähnelt:

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

### Neu seit Version

9,6

## GetLdapConfiguration

Sie können die `GetLdapConfiguration` Methode zum Abrufen der aktuell aktiven LDAP-Konfiguration im Cluster.

### Parameter

Diese Methode hat keine Eingabeparameter.

### Rückgabewert

Diese Methode hat den folgenden Rückgabewert.

| Name               | Beschreibung  | Typ                                |
|--------------------|---|------------------------------------|
| LDAP-Konfiguration | <p>Liste der aktuellen LDAP-Konfigurationseinstellungen. Dieser API-Aufruf gibt nicht den Klartext des Suchkontopassworts zurück.</p> <p><b>Hinweis:</b> Wenn die LDAP-Authentifizierung derzeit deaktiviert ist, sind alle zurückgegebenen Einstellungen leer, mit Ausnahme von "authType" und "groupSearchType", die auf "SearchAndBind" bzw. "ActiveDirectory" gesetzt sind.</p> | <a href="#">LDAP-Konfiguration</a> |

## Anforderungsbeispiel

Anfragen für diese Methode ähneln dem folgenden Beispiel:

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

## Antwortbeispiel

Diese Methode liefert eine Antwort, die dem folgenden Beispiel ähnelt:

```

{
  "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%))"
    }
  }
}

```

## Neu seit Version

9,6

## TestLdapAuthentication

Sie können die `TestLdapAuthentication` Methode zur Überprüfung der aktuell aktivierten LDAP-Authentifizierungseinstellungen. Wenn die Konfiguration korrekt ist, gibt der API-Aufruf die Gruppenzugehörigkeit des getesteten Benutzers zurück.

## Parameter

Diese Methode hat die folgenden Eingabeparameter:

| Name         | Beschreibung                                     | Typ    | Standardwert | Erforderlich |
|--------------|--|--------|--------------|--------------|
| Benutzername | Der zu testende Benutzername.                    | Schnur | Keine        | Ja           |
| Passwort     | Das Passwort für den zu testenden Benutzernamen. | Schnur | Keine        | Ja           |

| Name               | Beschreibung   | Typ                                | Standardwert | Erforderlich |
|--------------------|--|------------------------------------|--------------|--------------|
| LDAP-Konfiguration | Ein zu testendes IdapConfiguration-Objekt. Wenn Sie diesen Parameter angeben, testet das System die angegebene Konfiguration auch dann, wenn die LDAP-Authentifizierung derzeit deaktiviert ist. | <a href="#">LDAP-Konfiguration</a> | Keine        | Nein         |

## Rückgabewerte

Diese Methode hat die folgenden Rückgabewerte:

| Name       | Beschreibung  | Typ    |
|------------|---|--------|
| Gruppen    | Liste der LDAP-Gruppen, die den getesteten Benutzer als Mitglied enthalten. | Array  |
| BenutzerDN | Der vollständige LDAP-Distinguished Name des getesteten Benutzers.          | Schnur |

## Anforderungsbeispiel

Anfragen für diese Methode ähneln dem folgenden Beispiel:

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

## Antwortbeispiel

Diese Methode liefert eine Antwort, die dem folgenden Beispiel ähnelt:

```
{
  "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"
  }
}
```

## Neu seit Version

9,6

## Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

## Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.