LDAP-API-Methoden

Element Software

NetApp
January 15, 2024

Inhalt

LDAP-API-Methoden

Sie können das Lightweight Directory Access Protocol (LDAP) verwenden, um den Zugriff auf Element Storage zu authentifizieren. Mit den in diesem Abschnitt beschriebenen LDAP-API-Methoden können Sie den LDAP-Zugriff auf das Storage-Cluster konfigurieren.

- AddLdapClusterAdmin
- EnableLdapAuthentifizierung
- DisableLdapAuthentifizierung
- GetLdapConfiguration
- TestLdapAuthentifizierung

Weitere Informationen

- "Dokumentation von SolidFire und Element Software"
- "Dokumentation für frühere Versionen von NetApp SolidFire und Element Produkten"

AddLdapClusterAdmin

Sie können das verwenden `AddLdapClusterAdmin` So fügen Sie einen neuen LDAP-Cluster-Administratorbenutzer hinzu: Ein LDAP-Clusteradministrator kann den Cluster mithilfe der API und Managementtools verwalten. LDAP-Cluster-Administratorkonten sind vollständig getrennt und stehen in keinem Zusammenhang mit standardmäßigen Mandantenkonten.

Parameter

Mit dieser Methode können Sie auch eine in Active Directory® definierte LDAP-Gruppe hinzufügen. Die Zugriffsebene, die der Gruppe zugewiesen wird, wird an die einzelnen Benutzer in der LDAP-Gruppe übergeben.

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Datenzugriff	Steuert, welche Methoden dieser Cluster-Administrator verwenden kann.	String-Array	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
Akzepteula	Akzeptieren Sie die Endnutzer-Lizenzvereinbarung. Setzen Sie auf „true“, um dem System ein Cluster-Administratorkonto hinzuzufügen. Wenn keine Angabe erfolgt oder auf FALSE gesetzt wird, schlägt der Methodenaufruf fehl.	boolesch	Keine	Ja.
Merkmale	Liste von Name-Wert-Paaren im JSON-Objektformat.	JSON-Objekt	Keine	Nein
Benutzername	Der Distinguished Benutzername für den neuen LDAP-Cluster Admin.	Zeichenfolge	Keine	Ja.

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

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

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

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

Neu seit Version

9.6

Weitere Informationen

Zugriffssteuerung

EnableLdapAuthentifizierung

Sie können das verwenden `EnableLdapAuthentication` Methode zum Konfigurieren einer LDAP-Verzeichnisverbindung für die LDAP-Authentifizierung in einem Cluster. Benutzer, die Mitglieder des LDAP-Verzeichnisses sind, können sich dann mithilfe ihrer LDAP-Anmeldedaten am Speichersystem anmelden.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
AuthType	Gibt an, welche Benutzerauthentifizierungsmethode verwendet werden soll. Mögliche Werte: • `DirectBind` • `SearchAndBind`	Zeichenfolge	SucheAndBind	Nein
GroupSearchBaseDN	Der Basis-DN des Baums, um die Unterstruktursuche zu starten.	Zeichenfolge	Keine	Nein

Name	Beschreibung	Typ	Standardwert	Erforderlich
GroupSearchType	Steuert den verwendeten Standardfilter für die Gruppensuche. Mögliche Werte: • NoGroups: Keine Gruppenunterstützung. • ActiveDirectory: Verschachtelte Mitgliedschaft aller Active Directory-Gruppen eines Benutzers. • MemberDN: MemberDN-Stilgruppen (einzelne Ebene).	Zeichenfolge	ActiveDirectory	Nein
Server-URIs	Eine kommagetrennte Liste von LDAP- oder LDAPS-Server-URIs. Sie können einen benutzerdefinierten Port am Ende eines LDAP- oder LDAPS-URI hinzufügen, indem Sie einen Doppelpunkt gefolgt von der Portnummer verwenden. Der URI „ldap://1.2.3.4“ verwendet beispielsweise den Standardport und der URI „ldaps://1.2.3.4:123“ verwendet den benutzerdefinierten Port 123.	String-Array	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
BenutzerSuchbaseDN	Der Basis-DN des Baums, um die Unterbaumsuche zu starten. Dieser Parameter ist erforderlich, wenn Sie einen AuthType von SearchAndBind verwenden.	Zeichenfolge	Keine	Nein
SuchhinBindDN	Ein vollständig qualifizierter DN zur Anmeldung bei, um eine LDAP-Suche für den Benutzer durchzuführen. Der DN benötigt Lesezugriff auf das LDAP-Verzeichnis. Dieser Parameter ist erforderlich, wenn Sie einen AuthType von SearchAndBind verwenden.	Zeichenfolge	Keine	Ja.
SucheBindPasswort	Das Kennwort für das SuchBindDN-Konto, das für die Suche verwendet wurde. Dieser Parameter ist erforderlich, wenn Sie einen AuthType von SearchAndBind verwenden.	Zeichenfolge	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
BenutzerSuchfilter	Der LDAP-Suchfilter, der beim Abfragen des LDAP-Servers verwendet werden soll. Die Zeichenfolge sollte den Platzhaltertext „%USERNAME%“ haben, der durch den Benutzernamen des authentifizierenden Benutzers ersetzt wird. Zum Beispiel verwendet (&(objectClass=Person)(sAMAccountName=%USERNAME%) das Feld sAMAccountName in Active Directory, um mit dem bei der Cluster-Anmeldung eingegebenen Benutzernamen überein. Dieser Parameter ist erforderlich, wenn Sie einen AuthType von SearchAndBind verwenden.	Zeichenfolge	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
BenutzerDNTemplate	Eine Zeichenkettenvorlage, mit der ein Muster zum Erstellen eines vollständigen, vom Benutzer bestimmten Namens (DN) definiert wird. Die Zeichenfolge sollte den Platzhaltertext „%USERNAME%“ haben, der durch den Benutzernamen des authentifizierenden Benutzers ersetzt wird. Dieser Parameter ist erforderlich, wenn Sie einen AuthType von DirectBind verwenden.	Zeichenfolge	Keine	Ja.
GroupSearchCustomFilter	Für die Verwendung mit dem CustomFilter-Suchtyp, ein LDAP-Filter, mit dem der DNS von Benutzergruppen zurückgegeben werden kann. Der Platzhalter-Text von %USERNAME% und %USDN% kann bei Bedarf durch ihren Benutzernamen und vollständigen Benutzer-DN ersetzt werden.	Zeichenfolge	Keine	Ja.

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende 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 gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

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

Neu seit Version

9.6

DisableLdapAuthentifizierung

Sie können das verwenden `DisableLdapAuthentication` Methode zum Deaktivieren der LDAP-Authentifizierung und Entfernen aller LDAP-Konfigurationseinstellungen. Bei dieser Methode werden keine konfigurierten Cluster-Administratorkonten für Benutzer oder Gruppen entfernt. Nachdem die LDAP-Authentifizierung deaktiviert wurde, können Clusteradministratoren, die für die LDAP-Authentifizierung konfiguriert sind, nicht mehr auf das Cluster zugreifen.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewerte

Diese Methode hat keine Rückgabewerte.

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

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

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, die dem folgenden Beispiel ähnelt:

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

Neu seit Version

9.6

GetLdapConfiguration

Sie können das verwenden `GetLdapConfiguration` Methode zum Abrufen der derzeit aktiven LDAP-Konfiguration auf dem Cluster.

Parameter

Diese Methode hat keine Eingabeparameter.

Rückgabewert

Diese Methode hat den folgenden Rückgabewert.

Name	Beschreibung	Typ
LdapKonfiguration	Liste der aktuellen LDAP-Konfigurationseinstellungen. Dieser API-Aufruf gibt nicht den Klartext des Suchkontenpassworts zurück. **Hinweis:** Wenn die LDAP-Authentifizierung derzeit deaktiviert ist, sind alle zurückgegebenen Einstellungen mit Ausnahme von "AuthType" und "groupSearchType" leer, die auf "SearchAndBind" bzw. "ActiveDirectory" gesetzt sind.	LdapKonfiguration

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

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

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, 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

TestLdapAuthentifizierung

Sie können das verwenden `TestLdapAuthentication` Methode zum Validieren der derzeit aktivierten LDAP-Authentifizierungseinstellungen. Wenn die Konfiguration korrekt ist, gibt der API-Aufruf die Gruppenmitgliedschaft des getesteten Benutzers zurück.

Parameter

Diese Methode verfügt über die folgenden Eingabeparameter:

Name	Beschreibung	Typ	Standardwert	Erforderlich
Benutzername	Der zu testenden Benutzername.	Zeichenfolge	Keine	Ja.
Passwort	Das Kennwort für den zu testenden Benutzernamen.	Zeichenfolge	Keine	Ja.

Name	Beschreibung	Typ	Standardwert	Erforderlich
LdapKonfiguration	Ein ldapConfiguration Objekt, das getestet werden soll. Wenn Sie diesen Parameter angeben, testet das System die angegebene Konfiguration, auch wenn die LDAP-Authentifizierung derzeit deaktiviert ist.	LdapKonfiguration	Keine	Nein

Rückgabewerte

Diese Methode verfügt über die folgenden Rückgabewerte:

Name	Beschreibung	Typ
Gruppen	Liste der LDAP-Gruppen, die den getesteten Benutzer als Mitglied enthalten.	Array erledigen
Benutzer-DN	Der vollständige LDAP Distinguished Name des geprüften Benutzers.	Zeichenfolge

Anforderungsbeispiel

Anforderungen für diese Methode sind ähnlich wie das folgende Beispiel:

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

Antwortbeispiel

Diese Methode gibt eine Antwort zurück, 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