Gestire gli account utente degli amministratori del cluster

Element Software

NetApp
August 18, 2025

This PDF was generated from https://docs.netapp.com/it-it/element-software/storage/concept_system_manage_manage_ldap.html on August 18, 2025. Always check docs.netapp.com for the latest.

Sommario

Gestire gli account utente degli amministratori del cluster . . . 1
- Tipi di account amministratore del cluster di storage . . . 1
- Visualizzare i dettagli dell'amministratore del cluster . . . 1
- Creare un account amministratore del cluster . . . 2
- Modificare le autorizzazioni di amministratore del cluster . . . 3
- Modificare le password per gli account amministratore del cluster . . . 3
- Gestire LDAP . . . 4
  - Completare la procedura di preconfigurazione per il supporto LDAP . . . 5
  - Abilitare l'autenticazione LDAP con l'interfaccia utente Element . . . 5
  - Abilitare l'autenticazione LDAP con l'API Element . . . 7
  - Visualizza i dettagli LDAP . . . 10
  - Verificare la configurazione LDAP . . . 10
  - Disattivare LDAP . . . 12
  - Trova ulteriori informazioni . . . 12

Gestire gli account utente degli amministratori del cluster

È possibile gestire gli account amministratore del cluster per un sistema storage SolidFire creando, eliminando e modificando gli account amministratore del cluster, modificando la password amministratore del cluster e configurando le impostazioni LDAP per gestire l'accesso al sistema per gli utenti.

Tipi di account amministratore del cluster di storage

Esistono due tipi di account amministratore in un cluster di storage che esegue il software NetApp Element: L'account primario dell'amministratore del cluster e un account dell'amministratore del cluster.

- **Account primario amministratore del cluster**

  Questo account amministratore viene creato al momento della creazione del cluster. Questo account è l'account amministrativo principale con il livello di accesso più elevato al cluster. Questo account è analogo a un utente root in un sistema Linux. È possibile modificare la password per questo account amministratore.

- **Account amministratore del cluster**

  È possibile assegnare a un account amministratore del cluster un intervallo limitato di accesso amministrativo per eseguire attività specifiche all'interno di un cluster. Le credenziali assegnate a ciascun account amministratore del cluster vengono utilizzate per autenticare le richieste API ed Element UI all'interno del sistema di storage.

Per accedere ai nodi attivi di un cluster tramite l'interfaccia utente per nodo, è necessario un account amministratore locale (non LDAP). Le credenziali dell'account non sono richieste per accedere a un nodo che non fa ancora parte di un cluster.

Visualizzare i dettagli dell'amministratore del cluster

1. Per creare un account di amministratore del cluster a livello di cluster (non LDAP), eseguire le seguenti operazioni:
   a. Fare clic su **utenti** > **amministratori cluster**.
2. Nella pagina Cluster Admins della scheda Users (utenti), è possibile visualizzare le seguenti informazioni.
   - **ID**: Numero sequenziale assegnato all'account dell'amministratore del cluster.
   - **Username**: Il nome assegnato all'account dell'amministratore del cluster al momento della creazione.
   - **Access**: Le autorizzazioni utente assegnate all'account utente. Valori possibili:
     - leggi
     - creazione di report
     - nodi
     - dischi

- volumi
- account
- ClusterAdmins
- amministratore
- SupportAdmin

> Tutte le autorizzazioni sono disponibili per il tipo di accesso amministratore.
>
> Ci sono tipi di accesso disponibili tramite l'API che non sono disponibili nell'interfaccia utente di Element.

+

- **Type**: Il tipo di amministratore del cluster. Valori possibili:
  - Cluster
  - LDAP
- **Attributes**: Se l'account amministratore del cluster è stato creato utilizzando l'API Element, questa colonna mostra tutte le coppie nome-valore impostate utilizzando tale metodo.

  Vedere "Riferimento API software NetApp Element".

Creare un account amministratore del cluster

È possibile creare nuovi account amministratore del cluster con autorizzazioni per consentire o limitare l'accesso a specifiche aree del sistema di storage. Quando si impostano le autorizzazioni dell'account amministratore del cluster, il sistema concede i diritti di sola lettura per le autorizzazioni non assegnate all'amministratore del cluster.

Se si desidera creare un account amministratore del cluster LDAP, assicurarsi che LDAP sia configurato sul cluster prima di iniziare.

"Abilitare l'autenticazione LDAP con l'interfaccia utente Element"

In seguito, è possibile modificare i privilegi degli account amministratore del cluster per report, nodi, dischi, volumi, account, e a livello di cluster. Quando si abilita un'autorizzazione, il sistema assegna l'accesso in scrittura per quel livello. Il sistema concede all'utente amministratore l'accesso in sola lettura per i livelli non selezionati.

È inoltre possibile rimuovere in seguito qualsiasi account utente amministratore del cluster creato da un amministratore di sistema. Non è possibile rimuovere l'account amministratore del cluster primario creato al momento della creazione del cluster.

1. Per creare un account di amministratore del cluster a livello di cluster (non LDAP), eseguire le seguenti operazioni:
   a. Fare clic su **utenti** > **amministratori cluster**.
   b. Fare clic su **Create Cluster Admin** (Crea amministratore cluster).
   c. Selezionare il tipo di utente **Cluster**.
   d. Immettere un nome utente e una password per l'account e confermare la password.

e. Selezionare le autorizzazioni utente da applicare all'account.
f. Selezionare la casella di controllo per accettare il Contratto di licenza con l'utente finale.
g. Fare clic su **Create Cluster Admin** (Crea amministratore cluster).

2. Per creare un account amministratore del cluster nella directory LDAP, eseguire le seguenti operazioni:

a. Fare clic su **Cluster** > **LDAP**.
b. Assicurarsi che l'autenticazione LDAP sia attivata.
c. Fare clic su **Test User Authentication** (verifica autenticazione utente) e copiare il nome distinto visualizzato per l'utente o per uno dei gruppi di cui l'utente è membro in modo da poterlo incollare in un secondo momento.
d. Fare clic su **utenti** > **amministratori cluster**.
e. Fare clic su **Create Cluster Admin** (Crea amministratore cluster).
f. Selezionare il tipo di utente LDAP.
g. Nel campo Distinguished Name (Nome distinto), seguire l'esempio nella casella di testo per immettere un nome distinto completo per l'utente o il gruppo. In alternativa, incollarlo dal nome distinto precedentemente copiato.

   Se il nome distinto fa parte di un gruppo, tutti gli utenti che fanno parte di tale gruppo sul server LDAP disporranno delle autorizzazioni per questo account admin.

Per aggiungere utenti o gruppi amministratori cluster LDAP, il formato generale del nome utente è "LDAP:<Full Distinguished Name>".

a. Selezionare le autorizzazioni utente da applicare all'account.
b. Selezionare la casella di controllo per accettare il Contratto di licenza con l'utente finale.
c. Fare clic su **Create Cluster Admin** (Crea amministratore cluster).

Modificare le autorizzazioni di amministratore del cluster

È possibile modificare i privilegi dell'account amministratore del cluster per report, nodi, dischi, volumi, account, e a livello di cluster. Quando si abilita un'autorizzazione, il sistema assegna l'accesso in scrittura per quel livello. Il sistema concede all'utente amministratore l'accesso in sola lettura per i livelli non selezionati.

1. Fare clic su **utenti** > **amministratori cluster**.
2. Fare clic sull'icona Actions (azioni) dell'amministratore del cluster che si desidera modificare.
3. Fare clic su **Edit** (Modifica).
4. Selezionare le autorizzazioni utente da applicare all'account.
5. Fare clic su **Save Changes** (Salva modifiche).

Modificare le password per gli account amministratore del cluster

È possibile utilizzare l'interfaccia utente Element per modificare le password dell'amministratore del cluster.

1. Fare clic su **utenti** > **amministratori cluster**.

2. Fare clic sull'icona Actions (azioni) dell'amministratore del cluster che si desidera modificare.
3. Fare clic su **Edit** (Modifica).
4. Nel campo Change Password (Modifica password), immettere una nuova password e confermarla.
5. Fare clic su **Save Changes** (Salva modifiche).

Informazioni correlate

- "Informazioni sui tipi di accesso disponibili per le API Element"
- "Abilitare l'autenticazione LDAP con l'interfaccia utente Element"
- "Disattivare LDAP"
- "Plug-in NetApp Element per server vCenter"

Gestire LDAP

È possibile impostare il protocollo LDAP (Lightweight Directory Access Protocol) per abilitare la funzionalità di accesso sicura e basata su directory allo storage SolidFire. È possibile configurare LDAP a livello di cluster e autorizzare utenti e gruppi LDAP.

La gestione di LDAP implica la configurazione dell'autenticazione LDAP su un cluster SolidFire utilizzando un ambiente Microsoft Active Directory esistente e il test della configurazione.

È possibile utilizzare indirizzi IPv4 e IPv6.

L'abilitazione di LDAP prevede le seguenti procedure di alto livello, descritte in dettaglio:

1. **Completare la procedura di preconfigurazione per il supporto LDAP**. Verificare di disporre di tutti i dettagli necessari per configurare l'autenticazione LDAP.
2. **Attiva autenticazione LDAP**. Utilizzare l'interfaccia utente Element o l'API Element.
3. **Convalidare la configurazione LDAP**. Facoltativamente, verificare che il cluster sia configurato con i valori corretti eseguendo il metodo GetLdapConfiguration API o controllando la configurazione LCAP utilizzando l'interfaccia utente Element.
4. **Verificare l'autenticazione LDAP** (con il `readonly` utente). Verificare che la configurazione LDAP sia corretta eseguendo il metodo TestLdapAuthentication API o utilizzando l'interfaccia utente Element. Per questo test iniziale, utilizzare il nome utente "sAMAccountName" di `readonly` utente. In questo modo, il cluster viene convalidato per verificare che sia configurato correttamente per l'autenticazione LDAP `readonly` le credenziali e l'accesso sono corretti. Se questo passaggio non riesce, ripetere i passi da 1 a 3.
5. **Verificare l'autenticazione LDAP** (con un account utente che si desidera aggiungere). Ripetere il setp 4 con un account utente che si desidera aggiungere come amministratore del cluster di elementi. Copiare il `distinguished` Nome (DN) o l'utente (o il gruppo). Questo DN verrà utilizzato nella fase 6.
6. **Aggiungere l'amministratore del cluster LDAP** (copiare e incollare il DN dalla fase di autenticazione LDAP di prova). Utilizzando l'interfaccia utente Element o il metodo API AddLdapClusterAdmin, creare un nuovo utente amministratore del cluster con il livello di accesso appropriato. Per il nome utente, incollare il DN completo copiato al punto 5. In questo modo si garantisce che il DN sia formattato correttamente.
7. **Verificare l'accesso dell'amministratore del cluster**. Accedere al cluster utilizzando l'utente amministratore del cluster LDAP appena creato. Se è stato aggiunto un gruppo LDAP, è possibile effettuare l'accesso come qualsiasi utente del gruppo.

Completare la procedura di preconfigurazione per il supporto LDAP

Prima di attivare il supporto LDAP in Element, è necessario configurare un server Windows Active Directory ed eseguire altre attività di preconfigurazione.

Fasi

1. Configurare un server Windows Active Directory.
2. **Opzionale:** attiva il supporto LDAPS.
3. Creare utenti e gruppi.
4. Creare un account di servizio di sola lettura (ad esempio “sfreadonly”) da utilizzare per la ricerca nella directory LDAP.

Abilitare l’autenticazione LDAP con l’interfaccia utente Element

È possibile configurare l’integrazione del sistema di storage con un server LDAP esistente. Ciò consente agli amministratori LDAP di gestire centralmente l’accesso al sistema storage per gli utenti.

È possibile configurare LDAP con l’interfaccia utente Element o l’API Element. Questa procedura descrive come configurare LDAP utilizzando l’interfaccia utente Element.

Questo esempio mostra come configurare l’autenticazione LDAP su SolidFire e in uso `SearchAndBind` come tipo di autenticazione. Nell’esempio viene utilizzato un singolo Windows Server 2012 R2 Active Directory Server.

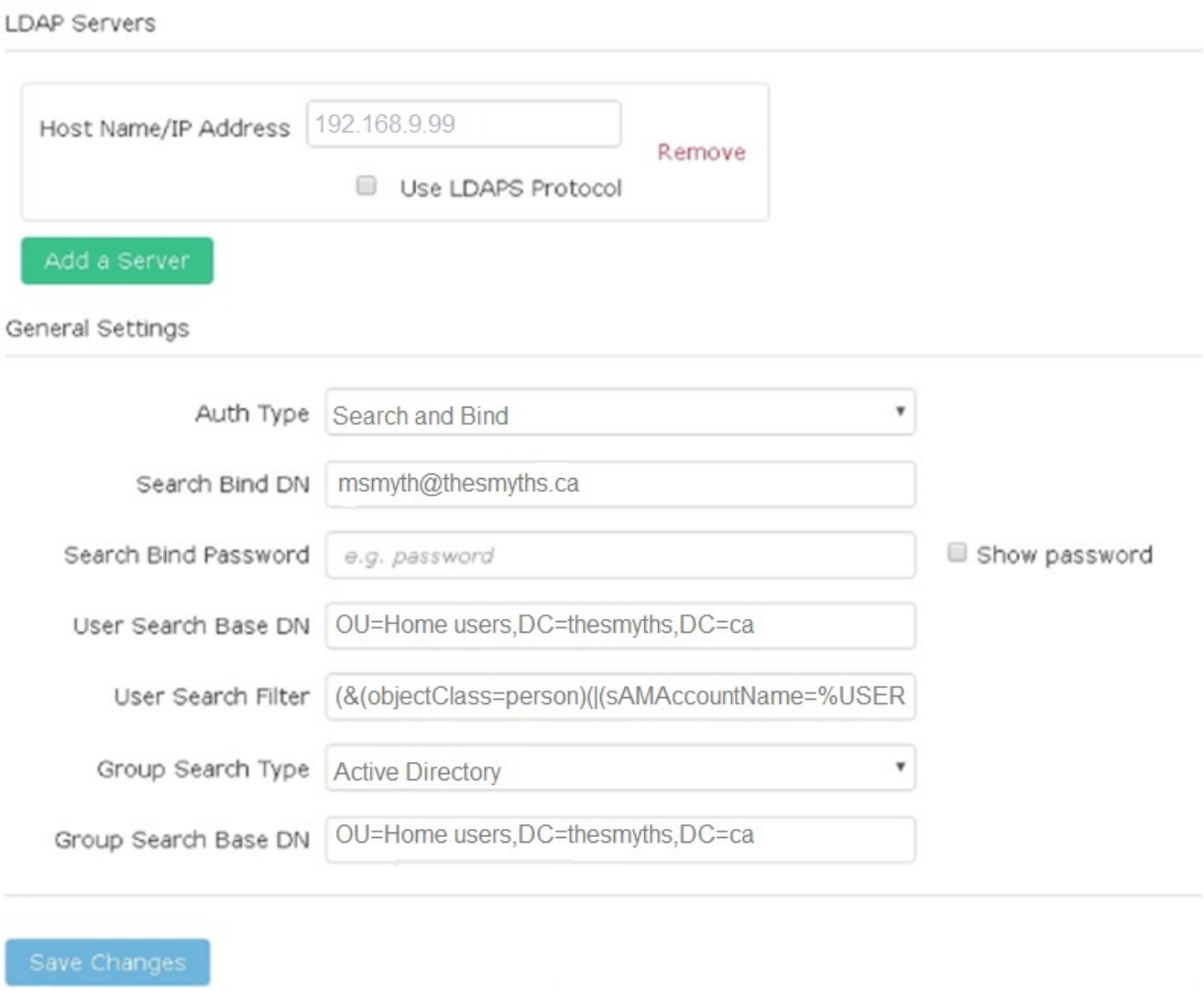
Fasi

1. Fare clic su **Cluster** > **LDAP**.
2. Fare clic su **Sì** per attivare l’autenticazione LDAP.
3. Fare clic su **Aggiungi un server**.
4. Inserire il campo **host Name/IP Address** (Nome host/Indirizzo IP).

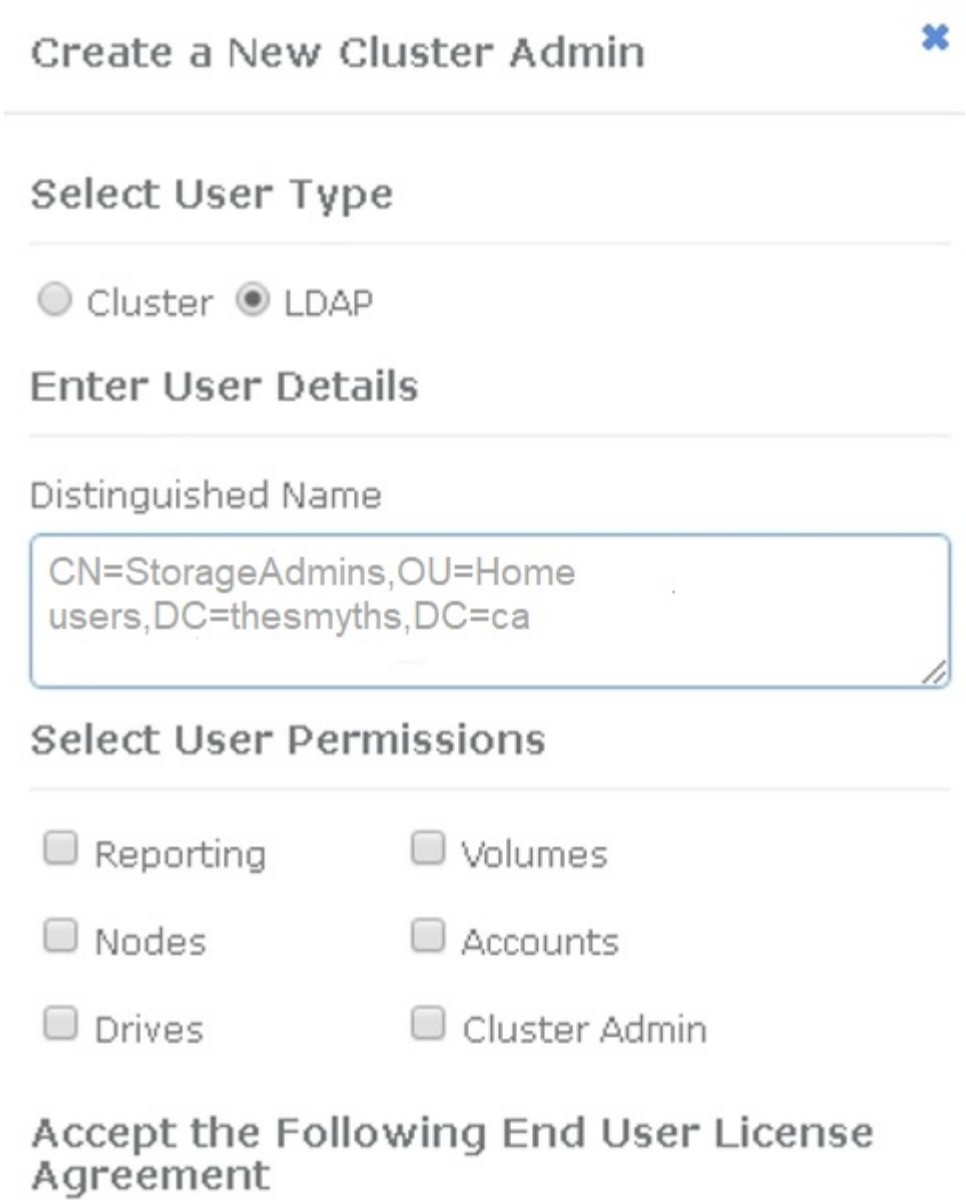
   È inoltre possibile inserire un numero di porta personalizzato opzionale.

   Ad esempio, per aggiungere un numero di porta personalizzato, immettere <host name or ip address>:<port number>

5. **Opzionale:** selezionare **Usa protocollo LDAPS**.
6. Inserire le informazioni richieste in **Impostazioni generali**.



7. Fare clic su **Enable LDAP** (attiva LDAP).
8. Fare clic su **Test User Authentication** (verifica autenticazione utente) per verificare l'accesso al server per un utente.
9. Copiare il nome distinto e le informazioni del gruppo di utenti che verranno visualizzate in seguito per la creazione degli amministratori del cluster.
10. Fare clic su **Save Changes** (Salva modifiche) per salvare le nuove impostazioni.
11. Per creare un utente in questo gruppo in modo che chiunque possa effettuare l'accesso, attenersi alla seguente procedura:
    a. Fare clic su **utente** > **Visualizza**.



b. Per il nuovo utente, fare clic su **LDAP** per tipo utente e incollare il gruppo copiato nel campo Nome distinto.
c. Selezionare le autorizzazioni, in genere tutte le autorizzazioni.
d. Scorrere verso il basso fino al Contratto di licenza con l'utente finale e fare clic su **Accetto**.
e. Fare clic su **Create Cluster Admin** (Crea amministratore cluster).

   Ora si dispone di un utente con il valore di un gruppo Active Directory.

Per verificare questo, disconnettersi dall'interfaccia utente di Element e accedere nuovamente come utente di quel gruppo.

Abilitare l'autenticazione LDAP con l'API Element

È possibile configurare l'integrazione del sistema di storage con un server LDAP esistente. Ciò consente agli amministratori LDAP di gestire centralmente l'accesso al sistema storage per gli utenti.

È possibile configurare LDAP con l'interfaccia utente Element o l'API Element. Questa procedura descrive come configurare LDAP utilizzando l'API Element.

Per sfruttare l'autenticazione LDAP su un cluster SolidFire, attivare prima l'autenticazione LDAP sul cluster utilizzando `EnableLdapAuthentication` Metodo API.

Fasi

1. Attivare prima l'autenticazione LDAP sul cluster utilizzando `EnableLdapAuthentication` Metodo API.
2. Inserire le informazioni richieste.

```
{
     "method":"EnableLdapAuthentication",
     "params":{
          "authType": "SearchAndBind",
          "groupSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
          "groupSearchType": "ActiveDirectory",
          "searchBindDN": "SFReadOnly@prodtest.solidfire.net",
          "searchBindPassword": "ReadOnlyPW",
          "userSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net ",
          "userSearchFilter":
"(&(objectClass=person)(sAMAccountName=%USERNAME%))"
          "serverURIs": [
               "ldap://172.27.1.189",
          [
     },
  "id":"1"
}
```

3. Modificare i valori dei seguenti parametri:

Parametri utilizzati	Descrizione
AuthType: SearchAndBind	Indica che il cluster utilizzerà l'account di servizio di sola lettura per cercare prima l'utente autenticato e successivamente associare tale utente, se trovato e autenticato.
GroupSearchBaseDN: dc=prodtest,DC=solidfire,DC=net	Specifica la posizione nella struttura LDAP per avviare la ricerca dei gruppi. Per questo esempio, abbiamo utilizzato la radice del nostro albero. Se la struttura LDAP è molto grande, potrebbe essere necessario impostarla su un sottostruttura più granulare per ridurre i tempi di ricerca.

Parametri utilizzati	Descrizione
UserSearchBaseDN: dc=prodtest,DC=solidfire,DC=net	Specifica la posizione nella struttura LDAP per avviare la ricerca degli utenti. Per questo esempio, abbiamo utilizzato la radice del nostro albero. Se la struttura LDAP è molto grande, potrebbe essere necessario impostarla su un sottostruttura più granulare per ridurre i tempi di ricerca.
GroupSearchType: ActiveDirectory	Utilizza il server Windows Active Directory come server LDAP.

`userSearchFilter: "(&(objectClass=person)(sAMAccountName=%USERNAME%))"`
 	
Per utilizzare userPrincipalName (indirizzo e-mail per l'accesso), è possibile modificare userSearchFilter in:
 	
`"(&(objectClass=person)(userPrincipalName=%USERNAME%))"`
 	
In alternativa, per eseguire ricerche in userPrincipalName e sAMAccountName, è possibile utilizzare il seguente userSearchFilter:
 	
`"(&(objectClass=person)(`
	(SAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%))" ----

Utilizza sAMAccountName come nome utente per accedere al cluster SolidFire. Queste impostazioni indicano a LDAP di cercare il nome utente specificato durante l'accesso nell'attributo sAMAccountName e di limitare la ricerca alle voci che hanno "Person" come valore nell'attributo objectClass.	SearchBindDN
Si tratta del nome distinto dell'utente di sola lettura che verrà utilizzato per cercare nella directory LDAP. Per Active directory è generalmente più semplice utilizzare userPrincipalName (formato indirizzo email) per l'utente.	SearchBindPassword

Per verificare questo, disconnettersi dall'interfaccia utente di Element e accedere nuovamente come utente di quel gruppo.

Visualizza i dettagli LDAP

Visualizzare le informazioni LDAP nella pagina LDAP della scheda Cluster.

Per visualizzare queste impostazioni di configurazione LDAP, è necessario attivare LDAP.

1. Per visualizzare i dettagli LDAP con l'interfaccia utente Element, fare clic su **Cluster** > **LDAP**.
   - **Host Name/IP Address** (Nome host/Indirizzo IP): Indirizzo di un server di directory LDAP o LDAPS.
   - **Auth Type**: Il metodo di autenticazione dell'utente. Valori possibili:
     - Binding diretto
     - Ricerca e binding
   - **Search Bind DN**: DN completo con cui effettuare l'accesso per eseguire una ricerca LDAP dell'utente (richiede l'accesso a livello di bind alla directory LDAP).
   - **Search Bind Password**: Password utilizzata per autenticare l'accesso al server LDAP.
   - **User Search base DN** (DN base ricerca utente): Il DN di base della struttura utilizzata per avviare la ricerca dell'utente. Il sistema esegue la ricerca nella sottostruttura dalla posizione specificata.
   - **User Search Filter** (filtro di ricerca utente): Immettere quanto segue utilizzando il nome di dominio:

     ```
     (&(objectClass=person)(|(sAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%)))
     ```

   - **Group Search Type** (tipo ricerca gruppo): Tipo di ricerca che controlla il filtro di ricerca gruppo predefinito utilizzato. Valori possibili:
     - Active Directory: Appartenenza nidificata a tutti i gruppi LDAP di un utente.
     - No Groups (Nessun gruppo): Nessun supporto di gruppo.
     - DN membro: Gruppi di membri in stile DN (livello singolo).
   - **Group Search base DN**: Il DN di base della struttura utilizzata per avviare la ricerca di gruppo. Il sistema esegue la ricerca nella sottostruttura dalla posizione specificata.
   - **Test User Authentication** (verifica autenticazione utente): Una volta configurato LDAP, utilizzare questa opzione per verificare l'autenticazione del nome utente e della password per il server LDAP. Immettere un account già esistente per eseguire il test. Vengono visualizzate le informazioni distinte relative al nome e al gruppo di utenti, che è possibile copiare per l'utilizzo successivo durante la creazione degli amministratori del cluster.

Verificare la configurazione LDAP

Dopo aver configurato LDAP, è necessario testarlo utilizzando l'interfaccia utente Element o l'API Element `TestLdapAuthentication` metodo.

Fasi

1. Per verificare la configurazione LDAP con l'interfaccia utente Element, procedere come segue:
   a. Fare clic su **Cluster** > **LDAP**.
   b. Fare clic su **Test autenticazione LDAP**.
   c. Risolvere eventuali problemi utilizzando le informazioni riportate nella tabella seguente:

Messaggio di errore	Descrizione
`xLDAPUserNotFound`	• L'utente sottoposto a test non è stato trovato nella configurazione `userSearchBaseDN` sottostruttura. • Il `userSearchFilter` non è configurato correttamente.
`xLDAPBindFailed (Error: Invalid credentials)`	• Il nome utente sottoposto a test è un utente LDAP valido, ma la password fornita non è corretta. • Il nome utente sottoposto a test è un utente LDAP valido, ma l'account è attualmente disattivato.
`xLDAPSearchBindFailed (Error: Can't contact LDAP server)`	L'URI del server LDAP non è corretto.
`xLDAPSearchBindFailed (Error: Invalid credentials)`	Il nome utente o la password di sola lettura non sono configurati correttamente.
`xLDAPSearchFailed (Error: No such object)`	Il `userSearchBaseDN` Non è una posizione valida all'interno della struttura LDAP.
`xLDAPSearchFailed (Error: Referral)`	• Il `userSearchBaseDN` Non è una posizione valida all'interno della struttura LDAP. • Il `userSearchBaseDN` e. `groupSearchBaseDN` Si trovano in un'unità organizzativa nidificata. Ciò può causare problemi di autorizzazione. La soluzione è includere l'unità organizzativa nelle voci DN di base dell'utente e del gruppo, ad esempio: `ou=storage, cn=company, cn=com`)

2. Per verificare la configurazione LDAP con l'API Element, procedere come indicato di seguito:
   a. Chiamare il metodo TestLdapAuthentication.

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

b. Esaminare i risultati. Se la chiamata API ha esito positivo, i risultati includono il nome distinto dell'utente specificato e un elenco di gruppi a cui l'utente è membro.

```
{
"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"
     }
}
```

Disattivare LDAP

È possibile disattivare l'integrazione LDAP utilizzando l'interfaccia utente Element.

Prima di iniziare, prendere nota di tutte le impostazioni di configurazione, poiché la disattivazione di LDAP cancella tutte le impostazioni.

Fasi

1. Fare clic su **Cluster** > **LDAP**.
2. Fare clic su **No**.
3. Fare clic su **Disable LDAP** (Disattiva LDAP).

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

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 COMMERCIABILITÀ 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 CONSEQUENZIALE (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.