Gestire gli account

Element Software

NetApp
October 01, 2024

Sommario

Gestire gli account

Nei sistemi storage SolidFire, i tenant possono utilizzare gli account per consentire ai client di connettersi ai volumi di un cluster. Quando si crea un volume, questo viene assegnato a un account specifico. È inoltre possibile gestire gli account amministratore del cluster per un sistema storage SolidFire.

- "Utilizzare gli account con CHAP"
- "Gestire gli account utente degli amministratori del cluster"

Per ulteriori informazioni

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

Utilizzare gli account con CHAP

Nei sistemi storage SolidFire, i tenant possono utilizzare gli account per consentire ai client di connettersi ai volumi di un cluster. Un account contiene l'autenticazione CHAP (Challenge-Handshake Authentication Protocol) richiesta per accedere ai volumi assegnati. Quando si crea un volume, questo viene assegnato a un account specifico.

A un account possono essere assegnati fino a duemila volumi, ma un volume può appartenere a un solo account.

Algoritmi CHAP

A partire dall'elemento 12,7, sono supportati gli algoritmi CHAP SHA1, SHA-256 e SHA3-256 sicuri e conformi FIPS. Con l'elemento 12,7, quando un iniziatore iSCSI host crea una sessione iSCSI con una destinazione iSCSI Element, richiede un elenco di algoritmi CHAP da utilizzare. La destinazione iSCSI Element sceglie il primo algoritmo supportato dall'elenco richiesto dall'iniziatore iSCSI host. Per confermare che la destinazione iSCSI Element sceglie l'algoritmo più sicuro, è necessario configurare l'iniziatore iSCSI host in modo che invii un elenco di algoritmi ordinati da più sicuri, ad esempio, SHA3-256, a meno sicuri, ad esempio, SHA1 o MD5. Quando gli algoritmi SHA non sono richiesti dall'iniziatore iSCSI host, l'elemento iSCSI target sceglie MD5, supponendo che l'elenco di algoritmi proposto dall'host contenga MD5. Potrebbe essere necessario aggiornare la configurazione dell'iniziatore iSCSI host per abilitare il supporto per gli algoritmi protetti.

Durante un aggiornamento di Element 12,7, se la configurazione dell'iniziatore iSCSI dell'host è già stata aggiornata per inviare una richiesta di sessione con un elenco che include gli algoritmi SHA, al riavvio dei nodi storage, vengono attivati i nuovi algoritmi sicuri e vengono stabilite sessioni iSCSI nuove o riconnesse utilizzando il protocollo più sicuro. Durante l'upgrade, tutte le sessioni iSCSI esistenti passeranno da MD5 alla SHA. Se non si aggiorna la configurazione dell'iniziatore iSCSI dell'host per richiedere SHA, le sessioni iSCSI esistenti continueranno a utilizzare MD5. In un secondo momento, dopo l'aggiornamento degli algoritmi CHAP dell'iniziatore iSCSI dell'host, le sessioni iSCSI dovrebbero passare gradualmente da MD5 a SHA nel tempo, in base ad attività di manutenzione che determinano riconnesse delle sessioni iSCSI.

Ad esempio, l'iniziatore iSCSI dell'host predefinito in Red Hat Enterprise Linux (RHEL) 8,3 ha l' `node.session.auth.chap_algs = SHA3-256,SHA256,SHA1,MD5`impostazione commentata, il che fa sì che l'iniziatore iSCSI utilizzi solo MD5. Se si annulla questa impostazione sull'host e si riavvia l'iniziatore iSCSI, le sessioni iSCSI da tale host verranno avviate utilizzando SHA3-256.

Se necessario, è possibile utilizzare il "ListISCSISessions" metodo API per visualizzare gli algoritmi CHAP utilizzati per ogni sessione.

Creare un account

È possibile creare un account per consentire l'accesso ai volumi.

Ogni nome account nel sistema deve essere univoco.

1. Selezionare **Gestione** > **account**.
2. Fare clic su **Create account** (Crea account).
3. Immettere un **Nome utente**.
4. Nella sezione **Impostazioni CHAP**, immettere le seguenti informazioni:

   Lasciare vuoti i campi delle credenziali per generare automaticamente una delle due password.

   - **Initiator Secret** per l'autenticazione della sessione del nodo CHAP.
   - **Target Secret** per l'autenticazione della sessione del nodo CHAP.
5. Fare clic su **Create account** (Crea account).

Visualizza i dettagli dell'account

È possibile visualizzare l'attività delle performance per i singoli account in un formato grafico.

Le informazioni del grafico forniscono informazioni di i/o e throughput per l'account. I livelli di attività medi e di picco sono indicati in incrementi di periodi di reporting di 10 secondi. Queste statistiche includono l'attività per tutti i volumi assegnati all'account.

1. Selezionare **Gestione** > **account**.
2. Fare clic sull'icona azioni di un account.
3. Fare clic su **View Details** (Visualizza dettagli).

Di seguito sono riportati alcuni dettagli:

- **Status**: Lo stato dell'account. Valori possibili:
  - Attivo: Un account attivo.
  - Locked (bloccato): Un account bloccato.
  - Rimosso: Un account che è stato eliminato e rimosso.
- **Active Volumes** (volumi attivi): Il numero di volumi attivi assegnati all'account.
- **Compressione**: Il punteggio di efficienza della compressione per i volumi assegnati all'account.
- **Deduplica**: Il punteggio di efficienza della deduplica per i volumi assegnati all'account.
- **Thin Provisioning**: Il punteggio di efficienza del thin provisioning per i volumi assegnati all'account.
- **Efficienza complessiva**: Il punteggio di efficienza globale per i volumi assegnati all'account.

Modificare un account

È possibile modificare un account per modificare lo stato, i segreti CHAP o il nome dell'account.

La modifica delle impostazioni CHAP in un account o la rimozione di iniziatori o volumi da un gruppo di accesso può causare la perdita improvvisa dell'accesso ai volumi da parte degli iniziatori. Per verificare che l'accesso al volume non venga perso in modo imprevisto, disconnettersi sempre dalle sessioni iSCSI che saranno interessate dalla modifica di un account o di un gruppo di accesso e verificare che gli iniziatori possano riconnettersi ai volumi dopo aver apportato modifiche alle impostazioni dell'iniziatore e del cluster.

I volumi persistenti associati ai servizi di gestione vengono assegnati a un nuovo account creato durante l'installazione o l'aggiornamento. Se si utilizzano volumi persistenti, non modificare o eliminare l'account associato.

1. Selezionare **Gestione** > **account**.
2. Fare clic sull'icona azioni di un account.
3. Nel menu visualizzato, selezionare **Edit** (Modifica).
4. **Opzionale:** modificare il **Nome utente**.
5. **Opzionale:** fare clic sull'elenco a discesa **Stato** e selezionare un altro stato.

   Se si modifica lo stato su **Locked**, tutte le connessioni iSCSI all'account vengono terminate e l'account non è più accessibile. I volumi associati all'account vengono mantenuti; tuttavia, i volumi non sono rilevabili tramite iSCSI.

6. **Opzionale:** in **Impostazioni CHAP**, modificare le credenziali **Segreto iniziatore** e **Segreto di destinazione** utilizzate per l'autenticazione della sessione del nodo.

   Se non si modificano le credenziali **CHAP Settings**, queste rimangono invariate. Se i campi delle credenziali vengono vuoti, il sistema genera nuove password.

7. Fare clic su **Save Changes** (Salva modifiche).

Eliminare un account

È possibile eliminare un account quando non è più necessario.

Eliminare e rimuovere tutti i volumi associati all'account prima di eliminarlo.

I volumi persistenti associati ai servizi di gestione vengono assegnati a un nuovo account creato durante l'installazione o l'aggiornamento. Se si utilizzano volumi persistenti, non modificare o eliminare l'account associato.

1. Selezionare **Gestione** > **account**.
2. Fare clic sull'icona azioni dell'account che si desidera eliminare.
3. Nel menu visualizzato, selezionare **Delete** (Elimina).
4. Confermare l'azione.

Trova ulteriori informazioni

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

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.

- **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).

Trova ulteriori informazioni

- "Abilitare l'autenticazione LDAP con l'interfaccia utente Element"
- "Disattivare LDAP"
- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Manage LDAP (Gestisci SNMP)

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 l' `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" dell' `readonly`utente. In questo modo, si convaliderà la corretta configurazione del cluster per l'autenticazione LDAP e si convaliderà anche la correttezza delle credenziali e dell' `readonly`accesso. 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.

In questo esempio viene illustrato come configurare l’autenticazione LDAP su SolidFire e viene utilizzata `SearchAndBind` come tipo di autenticazione. Nell’esempio viene utilizzato un singolo Windows Server 2012 R2 Active Directory Server.

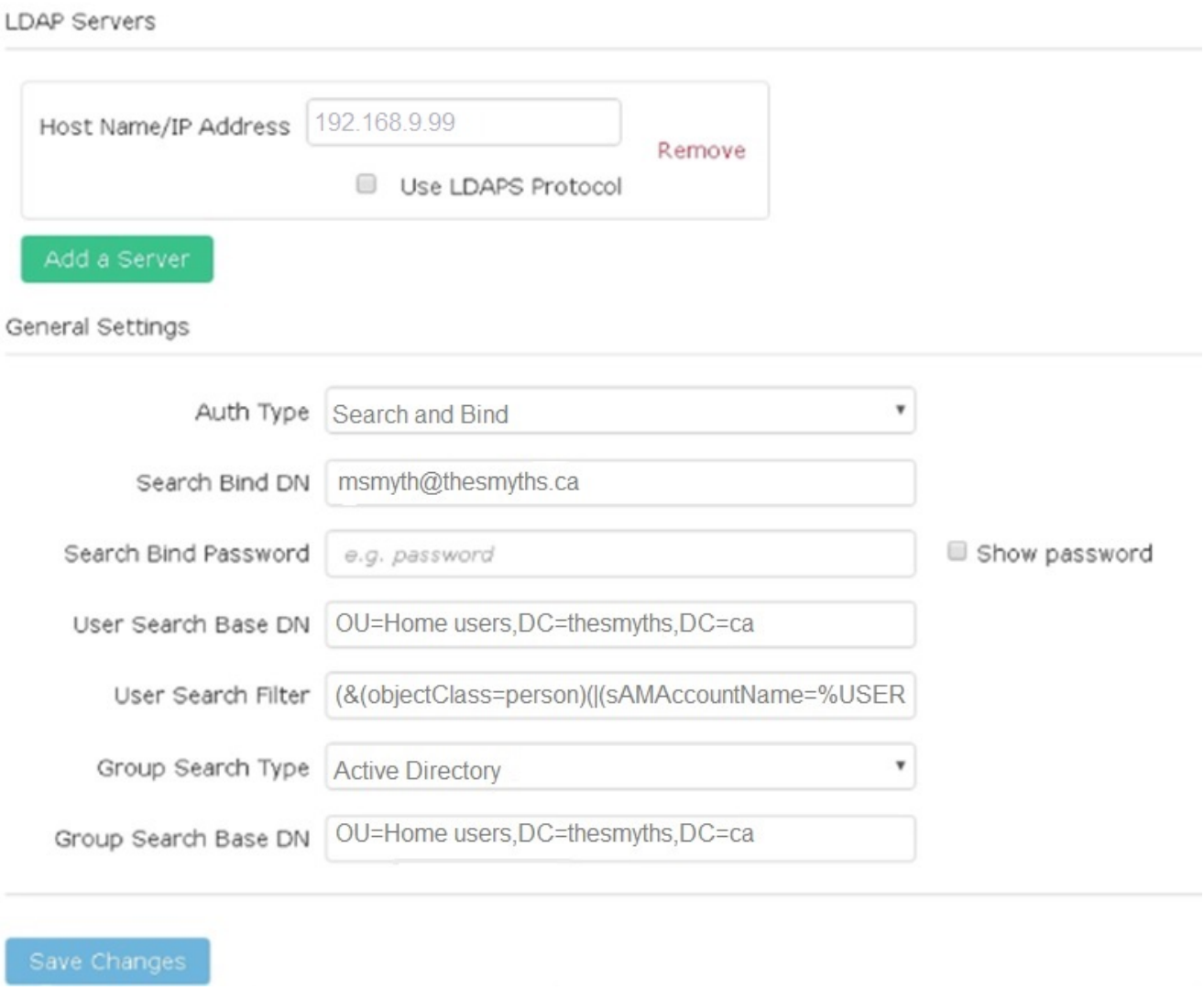
Fasi

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).

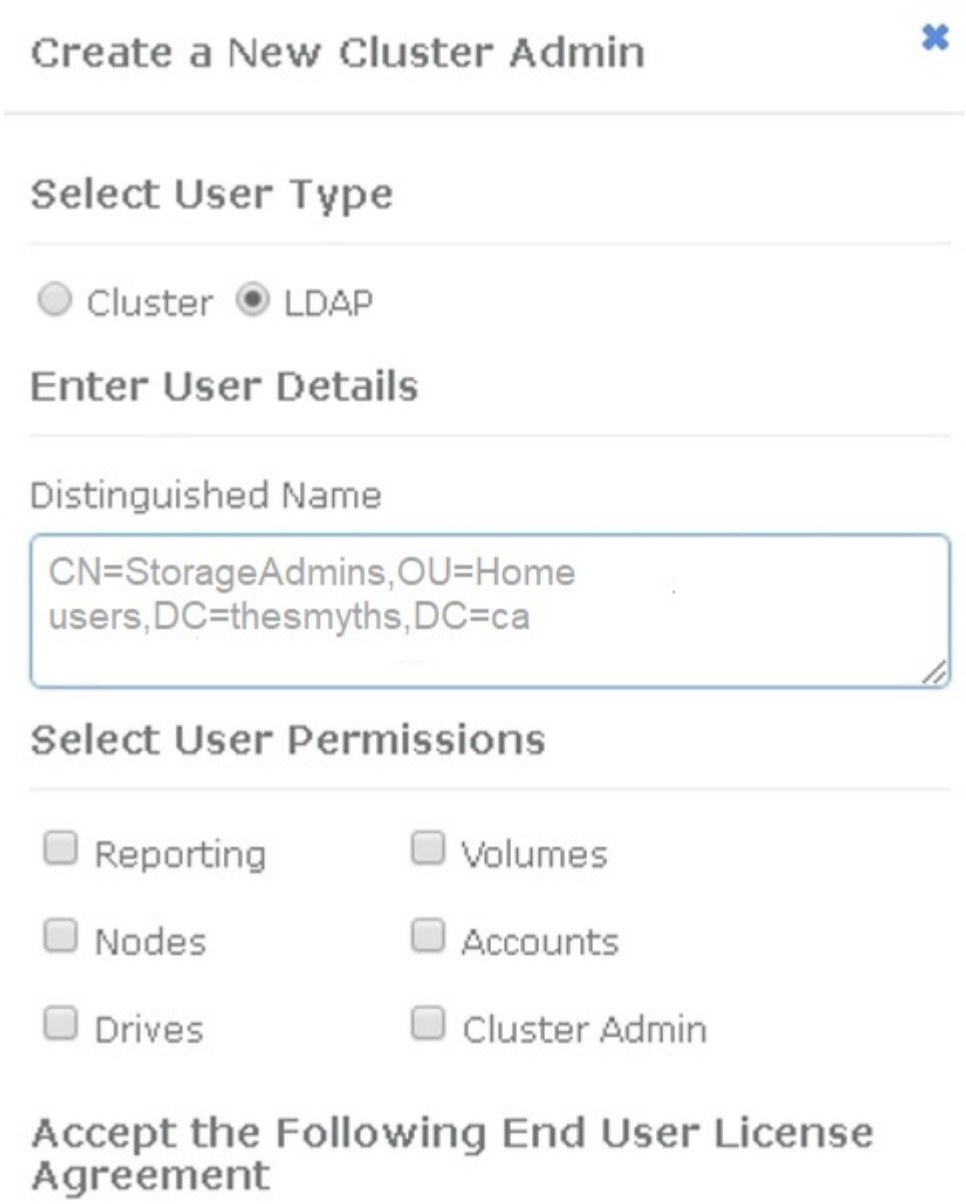
   È inoltre possibile inserire un numero di porta personalizzato opzionale.

   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 FC).
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, è necessario abilitare prima l'autenticazione LDAP sul cluster utilizzando il `EnableLdapAuthentication` metodo API.

Fasi

1. Abilitare prima l'autenticazione LDAP sul cluster utilizzando il `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=%NOME UTENTE%)(userPrincipalName=%NOME UTENTE%))" ----

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 di 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 il metodo API Element `TestLdapAuthentication`.

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 sottostruttura configurata `userSearchBaseDN`. • La `userSearchFilter` non è configurata 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)`	La `userSearchBaseDN` non è una posizione valida all'interno della struttura LDAP.
`xLDAPSearchFailed (Error: Referral)`	• La `userSearchBaseDN` non è una posizione valida all'interno della struttura LDAP. • `userSearchBaseDN`E `groupSearchBaseDN` si trovano in un'unità organizzativa annidata. Ciò può causare problemi di autorizzazione. La soluzione è includere l'unità organizzativa nelle voci DN base utenti e gruppi (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"