Konten verwalten

Element Software

NetApp
November 12, 2025

Inhalt

Konten verwalten

Konten verwalten

In SolidFire Speichersystemen können Mandanten Konten verwenden, um Clients die Verbindung zu Volumes in einem Cluster zu ermöglichen. Wenn Sie ein Volume erstellen, wird es einem bestimmten Konto zugeordnet. Sie können auch Cluster-Administratorkonten für ein SolidFire Speichersystem verwalten.

- "Arbeiten Sie mit Konten, die CHAP verwenden."
- "Cluster-Administrator-Benutzerkonten verwalten"

Weitere Informationen

- "SolidFire und Element-Softwaredokumentation"
- "NetApp Element Plug-in für vCenter Server"

Arbeiten Sie mit Konten, die CHAP verwenden.

In SolidFire Speichersystemen können Mandanten Konten verwenden, um Clients die Verbindung zu Volumes in einem Cluster zu ermöglichen. Ein Konto enthält die Challenge-Handshake Authentication Protocol (CHAP)-Authentifizierung, die für den Zugriff auf die ihm zugewiesenen Volumes erforderlich ist. Wenn Sie ein Volume erstellen, wird es einem bestimmten Konto zugeordnet.

Einem Konto können bis zu zweitausend Volumes zugeordnet werden, aber ein Volume kann nur zu einem Konto gehören.

CHAP-Algorithmen

Ab Element 12.7 werden sichere, FIPS-konforme CHAP-Algorithmen wie SHA1, SHA-256 und SHA3-256 unterstützt. Wenn ein Host-iSCSI-Initiator eine iSCSI-Sitzung mit einem Element-iSCSI-Ziel erstellt, fordert er eine Liste der zu verwendenden CHAP-Algorithmen an. Das Element iSCSI-Ziel wählt den ersten Algorithmus aus der vom Host-iSCSI-Initiator angeforderten Liste aus, den es unterstützt. Um sicherzustellen, dass das Element iSCSI-Ziel den sichersten Algorithmus auswählt, müssen Sie den Host iSCSI-Initiator so konfigurieren, dass er eine Liste von Algorithmen sendet, die vom sichersten Algorithmus, z. B. SHA3-256, bis zum am wenigsten sicheren Algorithmus, z. B. SHA1 oder MD5, geordnet sind. Wenn vom Host-iSCSI-Initiator keine SHA-Algorithmen angefordert werden, wählt das Element-iSCSI-Ziel MD5, vorausgesetzt, die vom Host vorgeschlagene Algorithmenliste enthält MD5. Möglicherweise müssen Sie die iSCSI-Initiatorkonfiguration des Hosts aktualisieren, um die Unterstützung für die sicheren Algorithmen zu aktivieren.

Während eines Upgrades auf Element 12.7 oder höher, wenn Sie die Host-iSCSI-Initiator-Konfiguration bereits aktualisiert haben, um eine Sitzungsanforderung mit einer Liste zu senden, die SHA-Algorithmen enthält, werden beim Neustart der Speicherknoten die neuen sicheren Algorithmen aktiviert und neue oder wiederhergestellte iSCSI-Sitzungen werden mit dem sichersten Protokoll hergestellt. Alle bestehenden iSCSI-Sitzungen werden während des Upgrades von MD5 auf SHA umgestellt. Wenn Sie die Host-iSCSI-Initiator-Konfiguration nicht aktualisieren, um SHA anzufordern, verwenden die bestehenden iSCSI-Sitzungen weiterhin MD5. Zu einem späteren Zeitpunkt, nachdem Sie die CHAP-Algorithmen des Host-iSCSI-Initiators aktualisiert haben, sollten die iSCSI-Sitzungen im Laufe der Zeit schrittweise von MD5 auf SHA umgestellt werden,

basierend auf Wartungsaktivitäten, die zu iSCSI-Sitzungs-Wiederverbindungen führen.

Beispielsweise verfügt der standardmäßige Host-iSCSI-Initiator in Red Hat Enterprise Linux (RHEL) 8.3 über Folgendes: `node.session.auth.chap_algs = SHA3-256,SHA256,SHA1,MD5` Die Einstellung ist auskommentiert, was dazu führt, dass der iSCSI-Initiator nur MD5 verwendet. Durch das Auskommentieren dieser Einstellung auf dem Host und den Neustart des iSCSI-Initiators werden iSCSI-Sitzungen von diesem Host dazu veranlasst, SHA3-256 zu verwenden.

Bei Bedarf können Sie die "ListISCSISessions" API-Methode zur Anzeige der für jede Sitzung verwendeten CHAP-Algorithmen.

Ein Konto erstellen

Sie können ein Konto erstellen, um den Zugriff auf Volumes zu ermöglichen.

Jeder Kontoname im System muss eindeutig sein.

1. Wählen Sie **Verwaltung** > **Konten**.
2. Klicken Sie auf **Konto erstellen**.
3. Geben Sie einen **Benutzernamen** ein.
4. Geben Sie im Abschnitt **CHAP-Einstellungen** die folgenden Informationen ein:

   Lassen Sie die Felder für die Anmeldeinformationen leer, um ein Passwort automatisch zu generieren.

   - **Initiator-Geheimnis** für die CHAP-Knotensitzungsauthentifizierung.
   - **Zielgeheimnis** für die CHAP-Knotensitzungsauthentifizierung.
5. Klicken Sie auf **Konto erstellen**.

Kontodetails anzeigen

Die Performanceentwicklung einzelner Konten kann in grafischer Form angezeigt werden.

Die Diagramminformationen liefern Informationen zu E/A und Durchsatz für das Konto. Die durchschnittlichen und maximalen Aktivitätswerte werden in 10-Sekunden-Intervallen angezeigt. Diese Statistiken umfassen die Aktivitäten aller dem Konto zugeordneten Volumina.

1. Wählen Sie **Verwaltung** > **Konten**.
2. Klicken Sie auf das Symbol „Aktionen“, um ein Konto aufzurufen.
3. Klicken Sie auf **Details anzeigen**.

Hier einige Details:

- **Status**: Der Status des Kontos. Mögliche Werte:
  - aktiv: Ein aktives Konto.
  - gesperrt: Ein gesperrtes Konto.
  - entfernt: Ein Konto, das gelöscht und endgültig entfernt wurde.
- **Aktive Volumes**: Die Anzahl der dem Konto zugewiesenen aktiven Volumes.

- **Komprimierung**: Der Komprimierungseffizienz-Score für die dem Konto zugewiesenen Datenmengen.
- **Deduplizierung**: Der Effizienzwert der Deduplizierung für die dem Konto zugewiesenen Datenträger.
- **Thin Provisioning**: Der Thin-Provisioning-Effizienzwert für die dem Konto zugewiesenen Volumes.
- **Gesamteffizienz**: Die Gesamteffizienzbewertung für die dem Konto zugewiesenen Volumina.

Konto bearbeiten

Sie können ein Konto bearbeiten, um den Status zu ändern, die CHAP-Geheimnisse zu ändern oder den Kontonamen zu modifizieren.

Das Ändern von CHAP-Einstellungen in einem Konto oder das Entfernen von Initiatoren oder Volumes aus einer Zugriffsgruppe kann dazu führen, dass Initiatoren unerwartet den Zugriff auf Volumes verlieren. Um sicherzustellen, dass der Zugriff auf die Volumes nicht unerwartet verloren geht, sollten Sie iSCSI-Sitzungen, die von einer Änderung des Kontos oder der Zugriffsgruppe betroffen sind, immer abmelden und überprüfen, ob die Initiatoren nach Abschluss aller Änderungen an den Initiator- und Clustereinstellungen wieder eine Verbindung zu den Volumes herstellen können.

Persistente Volumes, die mit Verwaltungsdiensten verknüpft sind, werden einem neuen Konto zugewiesen, das während der Installation oder des Upgrades erstellt wird. Wenn Sie persistente Volumes verwenden, ändern oder löschen Sie nicht das zugehörige Konto.

1. Wählen Sie **Verwaltung** > **Konten**.
2. Klicken Sie auf das Symbol „Aktionen“, um ein Konto aufzurufen.
3. Im daraufhin angezeigten Menü wählen Sie **Bearbeiten**.
4. **Optional:** Bearbeiten Sie den **Benutzernamen**.
5. **Optional:** Klicken Sie auf die Dropdown-Liste **Status** und wählen Sie einen anderen Status aus.

   Durch Ändern des Status auf **gesperrt** werden alle iSCSI-Verbindungen zum Konto beendet, und das Konto ist nicht mehr zugänglich. Die dem Konto zugeordneten Volumes werden beibehalten; allerdings sind die Volumes nicht über iSCSI auffindbar.

6. **Optional:** Unter **CHAP-Einstellungen** können Sie die Anmeldeinformationen für **Initiator Secret** und **Target Secret** bearbeiten, die für die Knotensitzungsauthentifizierung verwendet werden.

   Wenn Sie die Zugangsdaten für die **CHAP-Einstellungen** nicht ändern, bleiben diese unverändert. Wenn Sie die Felder für die Anmeldeinformationen leer lassen, generiert das System neue Passwörter.

7. Klicken Sie auf **Änderungen speichern**.

Konto löschen

Sie können ein Konto löschen, wenn es nicht mehr benötigt wird.

Löschen und bereinigen Sie alle mit dem Konto verknüpften Volumes, bevor Sie das Konto löschen.

Persistente Volumes, die mit Verwaltungsdiensten verknüpft sind, werden einem neuen Konto zugewiesen, das während der Installation oder des Upgrades erstellt wird. Wenn Sie persistente Volumes verwenden, ändern oder löschen Sie nicht das zugehörige Konto.

1. Wählen Sie **Verwaltung** > **Konten**.
2. Klicken Sie auf das Aktionssymbol für das Konto, das Sie löschen möchten.
3. Im daraufhin angezeigten Menü wählen Sie **Löschen**.
4. Bestätigen Sie die Aktion.

Weitere Informationen

- "SolidFire und Element-Softwaredokumentation"
- "NetApp Element Plug-in für vCenter Server"

Cluster-Administrator-Benutzerkonten verwalten

Sie können Cluster-Administratorkonten für ein SolidFire Speichersystem verwalten, indem Sie Cluster-Administratorkonten erstellen, löschen und bearbeiten, das Cluster-Administratorpasswort ändern und LDAP-Einstellungen konfigurieren, um den Systemzugriff für Benutzer zu verwalten.

Arten von Administratorkonten für Speichercluster

In einem Speichercluster, auf dem die NetApp Element -Software ausgeführt wird, können zwei Arten von Administratorkonten existieren: das primäre Cluster-Administratorkonto und ein Cluster-Administratorkonto.

- **Primäres Cluster-Administratorkonto**

  Dieses Administratorkonto wird bei der Erstellung des Clusters angelegt. Dieses Konto ist das primäre Administratorkonto mit dem höchsten Zugriffsniveau auf den Cluster. Dieses Konto ist vergleichbar mit einem Root-Benutzer in einem Linux-System. Sie können das Passwort für dieses Administratorkonto ändern.

- **Cluster-Administratorkonto**

  Sie können einem Cluster-Administratorkonto einen begrenzten administrativen Zugriff gewähren, um bestimmte Aufgaben innerhalb eines Clusters auszuführen. Die jedem Cluster-Administratorkonto zugewiesenen Anmeldeinformationen werden zur Authentifizierung von API- und Element-UI-Anfragen innerhalb des Speichersystems verwendet.

> Um über die Benutzeroberfläche pro Knoten auf aktive Knoten in einem Cluster zuzugreifen, ist ein lokales (nicht-LDAP-)Cluster-Administratorkonto erforderlich. Für den Zugriff auf einen Knoten, der noch nicht Teil eines Clusters ist, werden keine Kontodaten benötigt.

Cluster-Administratordetails anzeigen

1. Um ein clusterweites (nicht-LDAP-)Clusteradministratorkonto zu erstellen, führen Sie die folgenden Schritte aus:
   a. Klicken Sie auf **Benutzer** > **Cluster-Administratoren**.
2. Auf der Seite „Cluster-Administratoren“ im Reiter „Benutzer“ können Sie die folgenden Informationen einsehen.

- **ID**: Laufende Nummer des Cluster-Administratorkontos.
- **Benutzername**: Der Name, der dem Cluster-Administratorkonto bei seiner Erstellung gegeben wurde.
- **Zugriff**: Die dem Benutzerkonto zugewiesenen Benutzerberechtigungen. Mögliche Werte:
  - lesen
  - Berichterstattung
  - Knoten
  - Laufwerke
  - Bände
  - Konten
  - Cluster-Administratoren
  - Administrator
  - Support-Admin

> Dem Administrator stehen alle Berechtigungen zur Verfügung.
>
> Über die API stehen Zugriffstypen zur Verfügung, die in der Element-Benutzeroberfläche nicht verfügbar sind.

+

- **Typ**: Der Typ des Cluster-Administrators. Mögliche Werte:
  - Cluster
  - Ldap
- **Attribute**: Wenn das Cluster-Administratorkonto mithilfe der Element-API erstellt wurde, zeigt diese Spalte alle Name-Wert-Paare an, die mit dieser Methode festgelegt wurden.

  Sehen"NetApp Element Software-API-Referenz" .

Erstellen Sie ein Cluster-Administratorkonto

Sie können neue Cluster-Administratorkonten mit Berechtigungen erstellen, um den Zugriff auf bestimmte Bereiche des Speichersystems zu erlauben oder einzuschränken. Wenn Sie die Berechtigungen für das Cluster-Administratorkonto festlegen, gewährt das System Leserechte für alle Berechtigungen, die Sie dem Cluster-Administrator nicht zuweisen.

Wenn Sie ein LDAP-Cluster-Administratorkonto erstellen möchten, stellen Sie sicher, dass LDAP auf dem Cluster konfiguriert ist, bevor Sie beginnen.

"Aktivieren Sie die LDAP-Authentifizierung mit der Element-Benutzeroberfläche."

Sie können die Berechtigungen des Cluster-Administratorkontos für Berichte, Knoten, Laufwerke, Volumes, Konten und den Zugriff auf Clusterebene später ändern. Wenn Sie eine Berechtigung aktivieren, weist das System Ihnen Schreibzugriff auf dieser Ebene zu. Das System gewährt dem Administrator nur Lesezugriff auf die Ebenen, die Sie nicht auswählen.

Sie können später auch jedes vom Systemadministrator erstellte Cluster-Administrator-Benutzerkonto entfernen. Das primäre Cluster-Administratorkonto, das bei der Erstellung des Clusters angelegt wurde, kann nicht entfernt werden.

1. Um ein clusterweites (nicht-LDAP-)Clusteradministratorkonto zu erstellen, führen Sie die folgenden Schritte aus:
   a. Klicken Sie auf **Benutzer** > **Cluster-Administratoren**.
   b. Klicken Sie auf **Cluster-Administrator erstellen**.
   c. Wählen Sie den Benutzertyp **Cluster** aus.
   d. Geben Sie einen Benutzernamen und ein Passwort für das Konto ein und bestätigen Sie das Passwort.
   e. Wählen Sie die Benutzerberechtigungen aus, die auf das Konto angewendet werden sollen.
   f. Aktivieren Sie das Kontrollkästchen, um der Endbenutzer-Lizenzvereinbarung zuzustimmen.
   g. Klicken Sie auf **Cluster-Administrator erstellen**.
2. Um ein Cluster-Administratorkonto im LDAP-Verzeichnis zu erstellen, führen Sie die folgenden Schritte aus:
   a. Klicken Sie auf **Cluster** > **LDAP**.
   b. Stellen Sie sicher, dass die LDAP-Authentifizierung aktiviert ist.
   c. Klicken Sie auf **Benutzerauthentifizierung testen** und kopieren Sie den angezeigten Distinguished Name des Benutzers oder einer der Gruppen, denen der Benutzer angehört, damit Sie ihn später einfügen können.
   d. Klicken Sie auf **Benutzer** > **Cluster-Administratoren**.
   e. Klicken Sie auf **Cluster-Administrator erstellen**.
   f. Wählen Sie den LDAP-Benutzertyp aus.
   g. Im Feld „Distinguished Name“ folgen Sie dem Beispiel im Textfeld, um einen vollständigen Distinguished Name für den Benutzer oder die Gruppe einzugeben. Alternativ können Sie ihn auch aus dem zuvor kopierten Namen einfügen.

      Wenn der Distinguished Name Teil einer Gruppe ist, dann hat jeder Benutzer, der Mitglied dieser Gruppe auf dem LDAP-Server ist, die Berechtigungen dieses Administratorkontos.

   Um LDAP-Cluster-Administratorbenutzer oder -gruppen hinzuzufügen, lautet das allgemeine Format des Benutzernamens “LDAP:<Vollständiger Distinguished Name>”.

   a. Wählen Sie die Benutzerberechtigungen aus, die auf das Konto angewendet werden sollen.
   b. Aktivieren Sie das Kontrollkästchen, um der Endbenutzer-Lizenzvereinbarung zuzustimmen.
   c. Klicken Sie auf **Cluster-Administrator erstellen**.

Cluster-Administratorberechtigungen bearbeiten

Sie können die Berechtigungen des Cluster-Administratorkontos für Berichte, Knoten, Laufwerke, Volumes, Konten und den Zugriff auf Clusterebene ändern. Wenn Sie eine Berechtigung aktivieren, weist das System Ihnen Schreibzugriff auf dieser Ebene zu. Das System gewährt dem Administrator nur Lesezugriff auf die Ebenen, die Sie nicht auswählen.

1. Klicken Sie auf **Benutzer** > **Cluster-Administratoren**.
2. Klicken Sie auf das Aktionssymbol für den Clusteradministrator, den Sie bearbeiten möchten.
3. Klicken Sie auf **Bearbeiten**.
4. Wählen Sie die Benutzerberechtigungen aus, die auf das Konto angewendet werden sollen.

5. Klicken Sie auf **Änderungen speichern**.

Passwörter für Cluster-Administratorkonten ändern

Über die Element-Benutzeroberfläche können Sie die Passwörter der Clusteradministratoren ändern.

1. Klicken Sie auf **Benutzer** > **Cluster-Administratoren**.
2. Klicken Sie auf das Aktionssymbol für den Clusteradministrator, den Sie bearbeiten möchten.
3. Klicken Sie auf **Bearbeiten**.
4. Geben Sie im Feld „Passwort ändern“ ein neues Passwort ein und bestätigen Sie es.
5. Klicken Sie auf **Änderungen speichern**.

Ähnliche Informationen

- "Erfahren Sie mehr über die für Element-APIs verfügbaren Zugriffstypen."
- "Aktivieren Sie die LDAP-Authentifizierung mit der Element-Benutzeroberfläche."
- "LDAP deaktivieren"
- "NetApp Element Plug-in für vCenter Server"

LDAP verwalten

Sie können das Lightweight Directory Access Protocol (LDAP) einrichten, um eine sichere, verzeichnisbasierte Anmeldefunktion für den SolidFire -Speicher zu ermöglichen. Sie können LDAP auf Clusterebene konfigurieren und LDAP-Benutzer und -Gruppen autorisieren.

Die Verwaltung von LDAP umfasst die Einrichtung der LDAP-Authentifizierung für einen SolidFire -Cluster unter Verwendung einer bestehenden Microsoft Active Directory-Umgebung und das Testen der Konfiguration.

Sie können sowohl IPv4- als auch IPv6-Adressen verwenden.

Die Aktivierung von LDAP umfasst die folgenden übergeordneten Schritte, die im Detail beschrieben werden:

1. **Führen Sie alle Vorkonfigurationsschritte für die LDAP-Unterstützung durch**. Vergewissern Sie sich, dass Sie alle erforderlichen Angaben zur Konfiguration der LDAP-Authentifizierung haben.
2. **LDAP-Authentifizierung aktivieren**. Verwenden Sie entweder die Element-Benutzeroberfläche oder die Element-API.
3. **LDAP-Konfiguration prüfen**. Optional können Sie überprüfen, ob der Cluster mit den richtigen Werten konfiguriert ist, indem Sie die API-Methode GetLdapConfiguration ausführen oder die LCAP-Konfiguration über die Element-Benutzeroberfläche überprüfen.
4. **Testen Sie die LDAP-Authentifizierung** (mit dem `readonly` Benutzer). Prüfen Sie, ob die LDAP-Konfiguration korrekt ist, indem Sie entweder die API-Methode TestLdapAuthentication ausführen oder die Element-Benutzeroberfläche verwenden. Verwenden Sie für diesen ersten Test den Benutzernamen “sAMAccountName” von `readonly` Benutzer. Dies dient der Überprüfung, ob Ihr Cluster korrekt für die LDAP-Authentifizierung konfiguriert ist, und bestätigt außerdem, dass `readonly` Die Anmeldedaten und der Zugriff sind korrekt. Falls dieser Schritt fehlschlägt, wiederholen Sie die Schritte 1 bis 3.
5. **Testen Sie die LDAP-Authentifizierung** (mit einem Benutzerkonto, das Sie hinzufügen möchten). Wiederholen Sie Schritt 4 mit einem Benutzerkonto, das Sie als Element-Cluster-Administrator hinzufügen

möchten. Kopiere die `distinguished` Name (DN) oder der Benutzer (oder die Gruppe). Dieser DN wird in Schritt 6 verwendet.

6. **Fügen Sie den LDAP-Clusteradministrator hinzu** (kopieren Sie den DN aus dem Schritt „LDAP-Authentifizierung testen“ und fügen Sie ihn ein). Erstellen Sie mithilfe der Element-Benutzeroberfläche oder der AddLdapClusterAdmin-API-Methode einen neuen Cluster-Administratorbenutzer mit der entsprechenden Zugriffsebene. Fügen Sie für den Benutzernamen den vollständigen DN ein, den Sie in Schritt 5 kopiert haben. Dadurch wird sichergestellt, dass der DN korrekt formatiert ist.
7. **Testen Sie den Cluster-Administratorzugriff**. Melden Sie sich mit dem neu erstellten LDAP-Cluster-Administratorbenutzer am Cluster an. Wenn Sie eine LDAP-Gruppe hinzugefügt haben, können Sie sich als jeder Benutzer dieser Gruppe anmelden.

Vollständige Vorkonfigurationsschritte für die LDAP-Unterstützung

Bevor Sie die LDAP-Unterstützung in Element aktivieren, sollten Sie einen Windows Active Directory Server einrichten und weitere vorbereitende Konfigurationsaufgaben durchführen.

Schritte

1. Einen Windows Active Directory-Server einrichten.
2. **Optional:** LDAPS-Unterstützung aktivieren.
3. Benutzer und Gruppen erstellen.
4. Erstellen Sie ein schreibgeschütztes Dienstkonto (z. B. “sfreadonly”), das für die Suche im LDAP-Verzeichnis verwendet werden soll.

Aktivieren Sie die LDAP-Authentifizierung mit der Element-Benutzeroberfläche.

Sie können die Integration des Speichersystems mit einem bestehenden LDAP-Server konfigurieren. Dies ermöglicht es LDAP-Administratoren, den Zugriff von Benutzern auf das Speichersystem zentral zu verwalten.

LDAP kann entweder über die Element-Benutzeroberfläche oder über die Element-API konfiguriert werden. Dieses Verfahren beschreibt, wie LDAP mithilfe der Element-Benutzeroberfläche konfiguriert wird.

Dieses Beispiel zeigt, wie die LDAP-Authentifizierung auf SolidFire konfiguriert wird und wie sie verwendet wird. `SearchAndBind` als Authentifizierungstyp. Das Beispiel verwendet einen einzelnen Windows Server 2012 R2 Active Directory-Server.

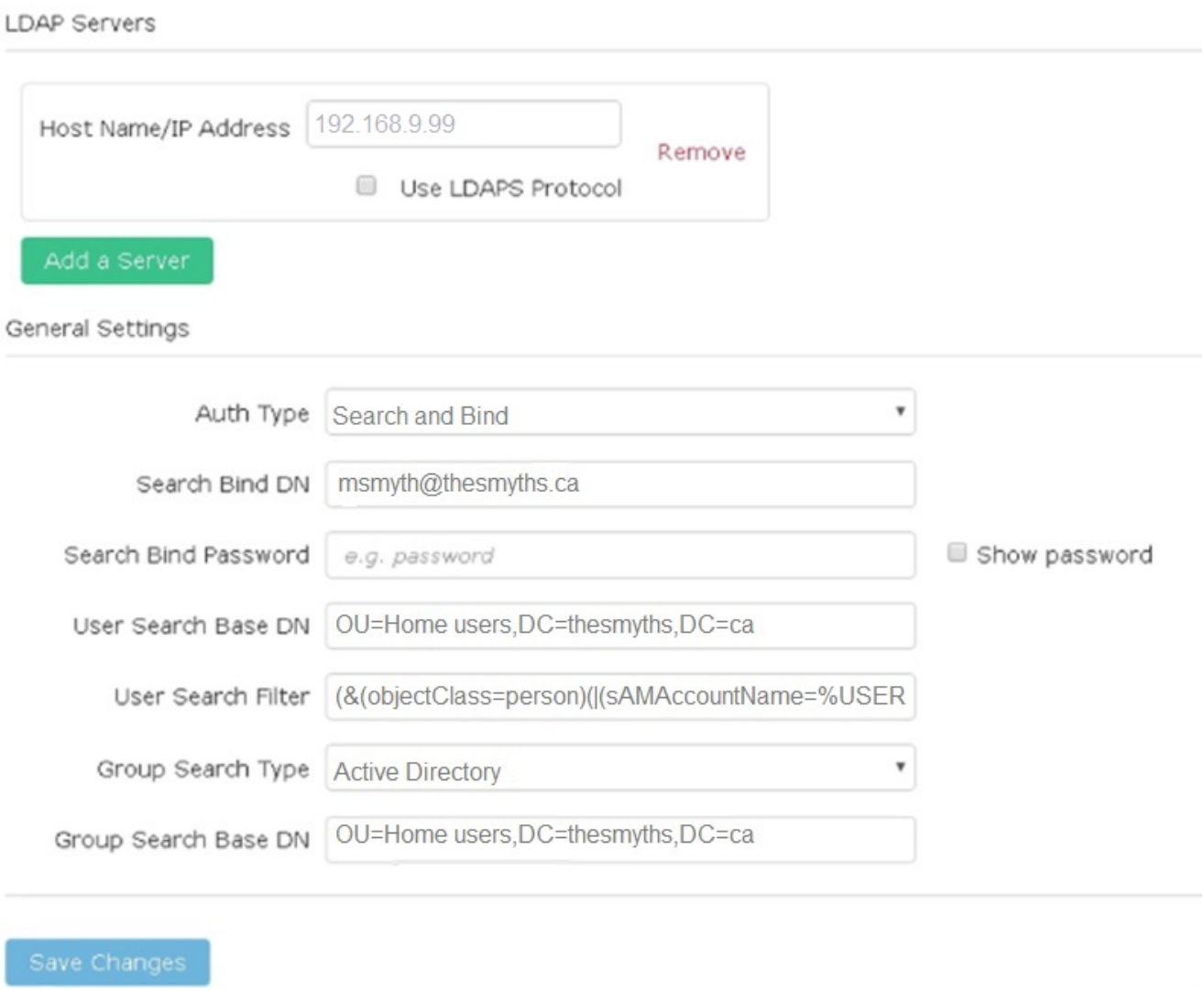
Schritte

1. Klicken Sie auf **Cluster** > **LDAP**.
2. Klicken Sie auf **Ja**, um die LDAP-Authentifizierung zu aktivieren.
3. Klicken Sie auf **Server hinzufügen**.
4. Geben Sie den **Hostnamen/die IP-Adresse** ein.

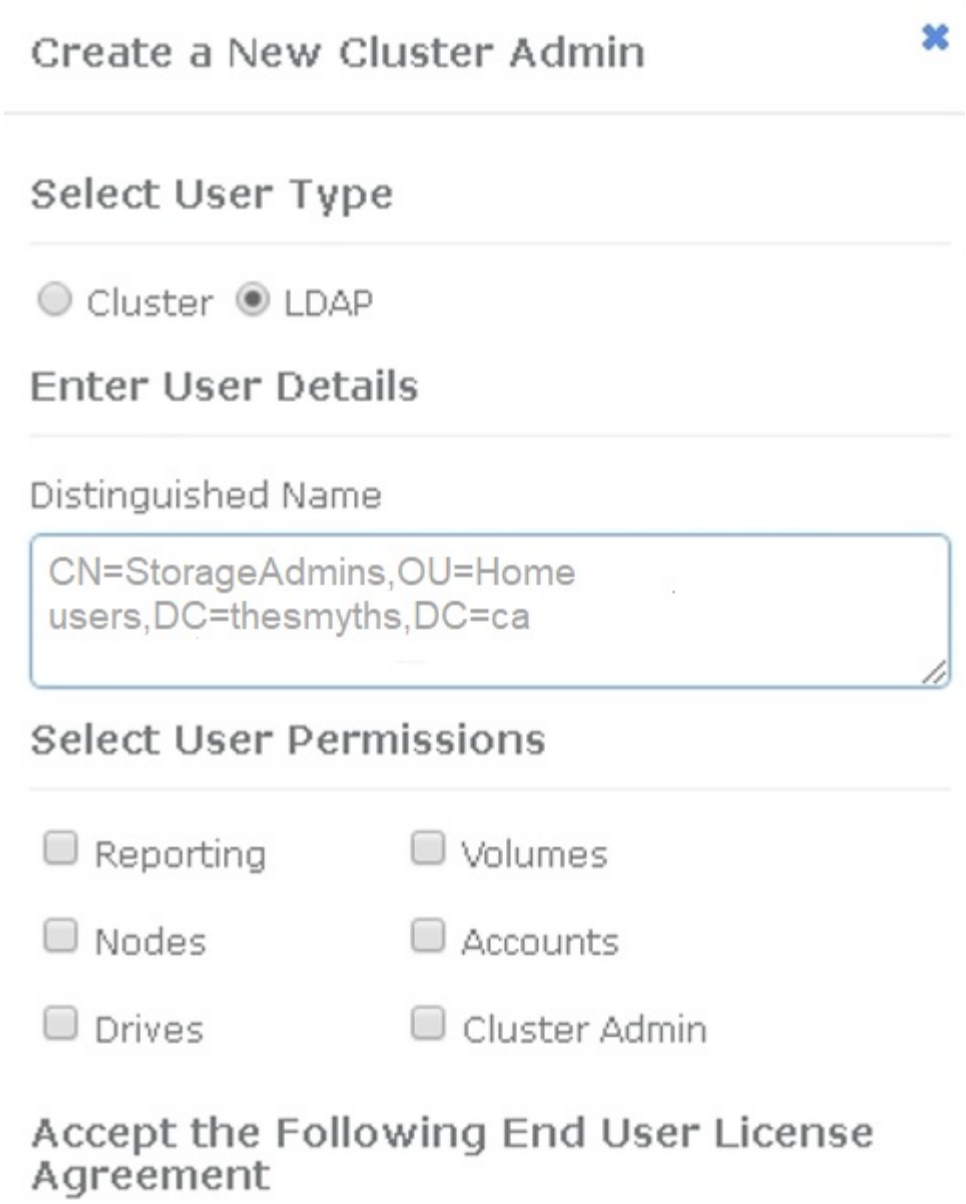
   Es kann auch eine optionale benutzerdefinierte Portnummer eingegeben werden.

   Um beispielsweise eine benutzerdefinierte Portnummer hinzuzufügen, geben Sie <Hostname oder IP-Adresse>:<Portnummer> ein.

5. **Optional:** Wählen Sie **LDAPS-Protokoll verwenden**.
6. Geben Sie die erforderlichen Informationen unter **Allgemeine Einstellungen** ein.



7. Klicken Sie auf **LDAP aktivieren**.
8. Klicken Sie auf **Benutzerauthentifizierung testen**, wenn Sie den Serverzugriff eines Benutzers testen möchten.
9. Kopieren Sie den angezeigten Distinguished Name und die Benutzergruppeninformationen, um sie später beim Erstellen von Clusteradministratoren zu verwenden.
10. Klicken Sie auf **Änderungen speichern**, um die neuen Einstellungen zu speichern.
11. Um einen Benutzer in dieser Gruppe anzulegen, sodass sich jeder anmelden kann, führen Sie die folgenden Schritte aus:
    a. Klicken Sie auf **Benutzer** > **Ansicht**.



b. Klicken Sie für den neuen Benutzer auf **LDAP** als Benutzertyp und fügen Sie die kopierte Gruppe in das Feld „Distinguished Name“ ein.
c. Wählen Sie die Berechtigungen aus, in der Regel alle Berechtigungen.
d. Scrollen Sie nach unten zum Endbenutzer-Lizenzvertrag und klicken Sie auf **Ich akzeptiere**.
e. Klicken Sie auf **Cluster-Administrator erstellen**.

   Sie haben nun einen Benutzer mit dem Wert einer Active Directory-Gruppe.

Um dies zu testen, melden Sie sich von der Element-Benutzeroberfläche ab und melden Sie sich anschließend als Benutzer dieser Gruppe wieder an.

Aktivieren Sie die LDAP-Authentifizierung mit der Element-API.

Sie können die Integration des Speichersystems mit einem bestehenden LDAP-Server konfigurieren. Dies ermöglicht es LDAP-Administratoren, den Zugriff von Benutzern auf das Speichersystem zentral zu verwalten.

LDAP kann entweder über die Element-Benutzeroberfläche oder über die Element-API konfiguriert werden. Dieses Verfahren beschreibt, wie LDAP mithilfe der Element-API konfiguriert wird.

Um die LDAP-Authentifizierung auf einem SolidFire -Cluster zu nutzen, aktivieren Sie die LDAP-Authentifizierung zunächst auf dem Cluster mithilfe von `EnableLdapAuthentication` API-Methode.

Schritte

1. Aktivieren Sie zuerst die LDAP-Authentifizierung auf dem Cluster mithilfe von `EnableLdapAuthentication` API-Methode.
2. Geben Sie die erforderlichen Informationen ein.

```
{
     "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. Ändern Sie die Werte der folgenden Parameter:

Verwendete Parameter	Beschreibung
Authentifizierungstyp: SearchAndBind	Legt fest, dass der Cluster das schreibgeschützte Dienstkonto verwendet, um zunächst nach dem zu authentifizierenden Benutzer zu suchen und diesen anschließend zu binden, falls er gefunden und authentifiziert wurde.
groupSearchBaseDN: dc=prodtest,dc=solidfire,dc=net	Gibt den Startpunkt der Gruppensuche im LDAP-Baum an. Für dieses Beispiel haben wir die Wurzel unseres Baums verwendet. Wenn Ihr LDAP-Baum sehr groß ist, sollten Sie dies möglicherweise auf einen feineren Unterbaum einstellen, um die Suchzeiten zu verkürzen.

Verwendete Parameter	Beschreibung
userSearchBaseDN: dc=prodtest,dc=solidfire,dc=net	Gibt den Startpunkt der Benutzersuche im LDAP-Baum an. Für dieses Beispiel haben wir die Wurzel unseres Baums verwendet. Wenn Ihr LDAP-Baum sehr groß ist, sollten Sie dies möglicherweise auf einen feineren Unterbaum einstellen, um die Suchzeiten zu verkürzen.
Gruppensuchtyp: ActiveDirectory	Verwendet den Windows Active Directory-Server als LDAP-Server.

`userSearchFilter: "(&(objectClass=person)(sAMAccountName=%USERNAME%))"`
 	
Um den Benutzerprinzipalnamen (E-Mail-Adresse für die Anmeldung) zu verwenden, können Sie den Benutzersuchfilter wie folgt ändern:
 	
`"(&(objectClass=person)(userPrincipalName=%USERNAME%))"`
 	
Alternativ können Sie den folgenden Benutzersuchfilter verwenden, um sowohl nach userPrincipalName als auch nach sAMAccountName zu suchen:
 	
`"(&(objectClass=person)(`
	(sAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%)))" ----

Verwendet den sAMAccountName als Benutzernamen für die Anmeldung am SolidFire -Cluster. Diese Einstellungen weisen LDAP an, im Attribut sAMAccountName nach dem beim Login angegebenen Benutzernamen zu suchen und die Suche auf Einträge zu beschränken, die im Attribut objectClass den Wert “person” haben.	searchBindDN
Dies ist der eindeutige Name des schreibgeschützten Benutzers, der zur Suche im LDAP-Verzeichnis verwendet wird. Für Active Directory ist es in der Regel am einfachsten, den Benutzerprinzipalnamen (E-Mail-Adressformat) für den Benutzer zu verwenden.	searchBindPassword

Um dies zu testen, melden Sie sich von der Element-Benutzeroberfläche ab und melden Sie sich anschließend

als Benutzer dieser Gruppe wieder an.

LDAP-Details anzeigen

LDAP-Informationen können Sie auf der LDAP-Seite auf der Registerkarte „Cluster“ einsehen.

Sie müssen LDAP aktivieren, um diese LDAP-Konfigurationseinstellungen anzuzeigen.

1. Um LDAP-Details mit der Element-Benutzeroberfläche anzuzeigen, klicken Sie auf **Cluster** > **LDAP**.
   - **Hostname/IP-Adresse**: Adresse eines LDAP- oder LDAPS-Verzeichnisservers.
   - **Authentifizierungstyp**: Die Benutzerauthentifizierungsmethode. Mögliche Werte:
     - Direktbindung
     - Suchen und Binden
   - **Search Bind DN**: Ein vollständig qualifizierter DN, mit dem man sich anmelden kann, um eine LDAP-Suche für den Benutzer durchzuführen (erfordert Zugriff auf Bind-Ebene auf das LDAP-Verzeichnis).
   - **Suchkennwort**: Kennwort zur Authentifizierung des Zugriffs auf den LDAP-Server.
   - **Benutzer-Suchbasis-DN**: Der Basis-DN des Baums, der zum Starten der Benutzersuche verwendet wird. Das System durchsucht den Teilbaum vom angegebenen Speicherort aus.
   - **Benutzer-Suchfilter**: Geben Sie Folgendes mit Ihrem Domainnamen ein:

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

   - **Gruppensuchtyp**: Suchtyp, der den standardmäßig verwendeten Gruppensuchfilter steuert. Mögliche Werte:
     - Active Directory: Verschachtelte Mitgliedschaft aller LDAP-Gruppen eines Benutzers.
     - Keine Gruppen: Keine Gruppenunterstützung.
     - Mitglied DN: Gruppen im Stil von Mitglied DN (einstufig).
   - **Basis-DN der Gruppensuche**: Der Basis-DN des Baums, der zum Starten der Gruppensuche verwendet wird. Das System durchsucht den Teilbaum vom angegebenen Speicherort aus.
   - **Benutzerauthentifizierung testen**: Nachdem LDAP konfiguriert wurde, verwenden Sie diese Funktion, um die Authentifizierung von Benutzername und Passwort für den LDAP-Server zu testen. Geben Sie ein bereits existierendes Konto ein, um dies zu testen. Der Distinguished Name und die Benutzergruppeninformationen werden angezeigt. Diese können Sie kopieren, um sie später beim Erstellen von Clusteradministratoren zu verwenden.

Testen Sie die LDAP-Konfiguration

Nach der LDAP-Konfiguration sollten Sie diese entweder über die Element-Benutzeroberfläche oder die Element-API testen. `TestLdapAuthentication` Verfahren.

Schritte

1. Um die LDAP-Konfiguration mit der Element-Benutzeroberfläche zu testen, gehen Sie wie folgt vor:
   a. Klicken Sie auf **Cluster** > **LDAP**.
   b. Klicken Sie auf **LDAP-Authentifizierung testen**.
   c. Beheben Sie alle Probleme mithilfe der Informationen in der folgenden Tabelle:

Fehlermeldung	Beschreibung
`xLDAPUserNotFound`	• Der zu testende Benutzer wurde in der Konfiguration nicht gefunden. `userSearchBaseDN` Teilbaum. • Der `userSearchFilter` ist falsch konfiguriert.
`xLDAPBindFailed (Error: Invalid credentials)`	• Der zu testende Benutzername ist ein gültiger LDAP-Benutzer, das angegebene Passwort ist jedoch falsch. • Der zu testende Benutzername ist ein gültiger LDAP-Benutzer, das Konto ist jedoch derzeit deaktiviert.
`xLDAPSearchBindFailed (Error: Can't contact LDAP server)`	Die LDAP-Server-URI ist falsch.
`xLDAPSearchBindFailed (Error: Invalid credentials)`	Der Benutzername oder das Passwort für den Lesezugriff ist falsch konfiguriert.
`xLDAPSearchFailed (Error: No such object)`	Der `userSearchBaseDN` ist kein gültiger Speicherort innerhalb des LDAP-Baums.
`xLDAPSearchFailed (Error: Referral)`	• Der `userSearchBaseDN` ist kein gültiger Speicherort innerhalb des LDAP-Baums. • Der `userSearchBaseDN` Und `groupSearchBaseDN` befinden sich in einer verschachtelten Organisationseinheit. Dies kann zu Berechtigungsproblemen führen. Die Umgehungslösung besteht darin, die Organisationseinheit (OU) in die Basis-DN-Einträge für Benutzer und Gruppen aufzunehmen (zum Beispiel: `ou=storage, cn=company, cn=com`)

2. Um die LDAP-Konfiguration mit der Element-API zu testen, gehen Sie wie folgt vor:
   a. Rufen Sie die TestLdapAuthentication-Methode auf.

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

b. Ergebnisse prüfen. Bei erfolgreichem API-Aufruf enthalten die Ergebnisse den Distinguished Name des angegebenen Benutzers und eine Liste der Gruppen, denen der Benutzer angehört.

```
{
"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"
     }
}
```

LDAP deaktivieren

Die LDAP-Integration kann über die Element-Benutzeroberfläche deaktiviert werden.

Bevor Sie beginnen, sollten Sie sich alle Konfigurationseinstellungen notieren, da durch die Deaktivierung von LDAP alle Einstellungen gelöscht werden.

Schritte

1. Klicken Sie auf **Cluster** > **LDAP**.
2. Klicken Sie auf **Nein**.
3. Klicken Sie auf **LDAP deaktivieren**.

Weitere Informationen

- "SolidFire und Element-Softwaredokumentation"
- "NetApp Element Plug-in für vCenter Server"