Konten verwalten

Element Software

NetApp
March 01, 2023

Inhaltsverzeichnis

Konten verwalten

In SolidFire Storage-Systemen können Mandanten Konten verwenden, um Clients eine Verbindung zu Volumes in einem Cluster zu ermöglichen. Wenn Sie ein Volume erstellen, wird es einem bestimmten Konto zugewiesen. Sie können auch Cluster-Administratorkonten für ein SolidFire Storage-System verwalten.

- "Arbeiten Sie mit Konten, die CHAP verwenden"
- "Verwalten von Benutzerkonten für Cluster-Administratoren"

Finden Sie weitere Informationen

- "Seite „SolidFire und Element Ressourcen“"
- "NetApp Element Plug-in für vCenter Server"

Arbeiten Sie mit Konten, die CHAP verwenden

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

Einem Konto können bis zu zweitausend Volumes zugewiesen sein, ein Volume kann jedoch nur zu einem Konto gehören.

CHAP-Algorithmen

Ab Element 12.7 werden sichere FIPS-kompatible CHAP-Algorithmen SHA1, SHA-256 und SHA3-256 unterstützt. Wenn in Element 12.7 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 es aus der vom Host-iSCSI-Initiator angeforderten Liste unterstützt. Um zu überprüfen, ob das Element iSCSI-Ziel den sichersten Algorithmus wählt, müssen Sie den Host-iSCSI-Initiator so konfigurieren, dass eine Liste von Algorithmen gesendet wird, die von der sichersten geordnet sind, z. B. SHA3-256, um die Sicherheit am wenigsten zu gewährleisten. SHA1 oder MD5. Wenn SHA-Algorithmen nicht vom Host-iSCSI-Initiator angefordert werden, wählt das Element iSCSI-Ziel MD5 aus, vorausgesetzt, die vorgeschlagene Algorithmusliste vom Host enthält MD5. Möglicherweise müssen Sie die Host-iSCSI-Initiator-Konfiguration aktualisieren, um die Unterstützung für die sicheren Algorithmen zu aktivieren.

Wenn Sie während eines Upgrades von Element 12.7 die Host-iSCSI-Initiator-Konfiguration aktualisiert haben, um eine Sitzungsanfrage mit einer Liste zu senden, die SHA-Algorithmen enthält, wenn die Storage-Nodes neu gestartet werden, Die neuen sicheren Algorithmen werden aktiviert und neue oder neu verbundene iSCSI-Sitzungen werden über das sicherste Protokoll eingerichtet. Alle bestehenden iSCSI-Sitzungen wechseln während des Upgrades von MD5 auf SHA. Wenn Sie die Host-iSCSI-Initiator-Konfiguration nicht aktualisieren, um SHA anzufordern, werden die vorhandenen iSCSI-Sitzungen weiterhin MD5 verwenden. Nach der Aktualisierung der CHAP-Algorithmen des Host-iSCSI-Initiators sollten die iSCSI-Sitzungen auf der Grundlage von Wartungsaktivitäten schrittweise von MD5 auf SHA umstellen, was zu einer erneuten Verbindung der iSCSI-Sitzung führt.

Der Standard-Host-iSCSI-Initiator in Red hat Enterprise Linux (RHEL) 8.3 verfügt beispielsweise über die `node.session.auth.chap_algs = SHA3-256,SHA256,SHA1,MD5` Die Einstellung hat kommentiert, was zu einem iSCSI-Initiator nur mit MD5 führt. Wenn Sie diese Einstellung auf dem Host kommentieren und den iSCSI-Initiator neu starten, werden iSCSI-Sitzungen von diesem Host ausgelöst, um SHA3-256 zu verwenden.

Bei Bedarf können Sie das verwenden "ListISSessions" API-Methode zum Anzeigen der CHAP-Algorithmen, die für jede Sitzung verwendet werden.

Erstellen Sie ein Konto

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

Jeder Kontoname im System muss eindeutig sein.

1. Wählen Sie **Management** > **Konten**.
2. Klicken Sie Auf **Konto Erstellen**.
3. Geben Sie einen **Benutzername** ein.
4. Geben Sie im Abschnitt **CHAP-Einstellungen** die folgenden Informationen ein:

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

   - **Initiatorschlüssel** für CHAP-Knoten-Session-Authentifizierung.
   - **Target Secret** für CHAP-Knoten-Session-Authentifizierung.
5. Klicken Sie Auf **Konto Erstellen**.

Kontodetails anzeigen

Sie können Leistungsaktivitäten für einzelne Konten in einem grafischen Format anzeigen.

Die Diagramminformationen liefern I/O- und Durchsatzinformationen für das Konto. Die Aktivitätslevel der durchschnittlichen und Spitzenwerte werden in Schritten von 10 Sekunden angezeigt. Diese Statistiken enthalten Aktivitäten für alle Volumes, die dem Konto zugewiesen sind.

1. Wählen Sie **Management** > **Konten**.
2. Klicken Sie auf das Symbol Aktionen für ein Konto.
3. Klicken Sie Auf **Details Anzeigen**.

Hier sind einige Details:

- **Status**: Der Status des Kontos. Mögliche Werte:
  - Aktiv: Ein aktives Konto.
  - Gesperrt: Ein gesperrtes Konto.
  - Entfernt: Ein Konto, das gelöscht und gelöscht wurde.
- **Aktive Volumes**: Die Anzahl der aktiven Volumes, die dem Konto zugewiesen sind.
- **Komprimierung**: Die Komprimierungs-Effizienzbewertung für die dem Konto zugewiesenen Volumes.
- **Deduplizierung**: Die Deduplizierungs-Effizienzbewertung für die Volumes, die dem Account zugewiesen

sind.

- **Thin Provisioning**: Die Thin Provisioning-Effizienzbewertung für die dem Konto zugewiesenen Volumes.
- **Gesamteffizienz**: Die Gesamteffizienz-Punktzahl für die dem Account zugewiesenen Volumes.

Bearbeiten Sie ein Konto

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

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 zu überprüfen, ob der Volume-Zugriff nicht unerwartet verloren geht, loggen Sie sich immer iSCSI-Sitzungen aus, die von einer Konto- oder Zugriffsgruppenänderung betroffen sind, und überprüfen Sie, ob die Initiatoren nach Abschluss der Änderungen an den Initiatoreinstellungen und den Cluster-Einstellungen eine Verbindung zu Volumes herstellen können.

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

1. Wählen Sie **Management** > **Konten**.
2. Klicken Sie auf das Symbol Aktionen für ein Konto.
3. Wählen Sie im Menü Ergebnis die Option **Bearbeiten**.
4. **Optional:** Bearbeiten Sie den **Benutzername**.
5. **Optional:** Klicken Sie auf die Dropdown-Liste **Status** und wählen Sie einen anderen Status aus.

   Wenn Sie den Status auf **gesperrt** ändern, werden alle iSCSI-Verbindungen zum Konto beendet, und das Konto kann nicht mehr aufgerufen werden. Volumes, die mit dem Konto verbunden sind, werden gepflegt. Die Volumes können jedoch nicht über iSCSI erkannt werden.

6. **Optional:** Bearbeiten Sie unter **CHAP-Einstellungen** die Anmeldeinformationen **Initiator Secret** und **Target Secret** für die Knotensitzauthentifizierung.

   Wenn Sie die **CHAP-Einstellungen**-Anmeldeinformationen 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**.

Löschen Sie ein Konto

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

Löschen und löschen Sie alle Volumes, die mit dem Konto verknüpft sind, bevor Sie das Konto löschen.

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

1. Wählen Sie **Management** > **Konten**.
2. Klicken Sie auf das Aktionen-Symbol für das Konto, das Sie löschen möchten.
3. Wählen Sie im Menü Ergebnis die Option **Löschen** aus.
4. Bestätigen Sie die Aktion.

Weitere Informationen

- "Seite „SolidFire und Element Ressourcen“"
- "NetApp Element Plug-in für vCenter Server"

Verwalten von Benutzerkonten für Cluster-Administratoren

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

Kontotypen für Storage-Cluster-Administratoren

In einem Storage-Cluster mit NetApp Element Software können zwei Arten von Administratorkonten vorhanden sein: Das primäre Cluster-Administratorkonto und ein Cluster-Administratorkonto.

- **Primary Cluster Administrator Account**

  Dieses Administratorkonto wird erstellt, wenn das Cluster erstellt wird. Dieses Konto ist das primäre administrative Konto mit der höchsten Zugriffsebene auf das Cluster. Dieses Konto ist analog zu einem Root-Benutzer in einem Linux-System. Sie können das Kennwort für dieses Administratorkonto ändern.

- **Cluster-Administratorkonto**

  Sie können einem Cluster-Administratorkonto einen begrenzten administrativen Zugriff gewähren, um bestimmte Aufgaben in einem Cluster auszuführen. Die jedem Cluster-Administratorkonto zugewiesenen Zugangsdaten werden zur Authentifizierung von API- und Element-UI-Anforderungen innerhalb des Storage-Systems verwendet.

Ein lokales (nicht-LDAP)-Cluster-Administratorkonto ist erforderlich, um über die UI pro Node auf aktive Knoten in einem Cluster zuzugreifen. Kontoanmeldeinformationen sind für den Zugriff auf einen Node, der noch nicht Teil eines Clusters ist, nicht erforderlich.

Zeigen Sie Details zum Cluster-Administrator an

1. So erstellen Sie ein Cluster-weites (nicht-LDAP)-Cluster-Administratorkonto:
   a. Klicken Sie Auf **Benutzer** > **Cluster Admins**.
2. Auf der Seite Cluster-Administratoren auf der Registerkarte Benutzer können Sie die folgenden Informationen anzeigen:
   - **ID**: Dem Cluster Administrator Konto zugewiesene sequentielle Nummer.
   - **Benutzername**: Der Name, der dem Cluster Administrator-Konto bei der Erstellung gegeben wurde.

- **Zugriff**: Die dem Benutzerkonto zugewiesenen Benutzerberechtigungen. Mögliche Werte:
  - Lesen
  - Berichterstellung
  - Knoten
  - Laufwerke
  - Volumes
  - Konten
  - Clusteradministratoren
  - Verwalter
  - SupportAdmin

  Alle Berechtigungen sind für den Zugriffstyp des Administrators verfügbar.
- **Typ**: Der Typ des Clusteradministrators. Mögliche Werte:
  - Cluster
  - Ldap
- **Attributes**: Wenn das Cluster-Administratorkonto mit der Element API erstellt wurde, zeigt diese Spalte alle Name-Wert-Paare an, die mit dieser Methode festgelegt wurden.

  Siehe "NetApp Element Software-API-Referenz".

Erstellen eines Cluster-Administratorkontos

Sie können neue Cluster-Administratorkonten mit Berechtigungen erstellen, um den Zugriff auf bestimmte Bereiche des Storage-Systems zu ermöglichen oder einzuschränken. Wenn Sie Berechtigungen für ein Cluster-Administratorkonto festlegen, gewährt das System schreibgeschützte Rechte 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 über die Benutzeroberfläche von Element"

Sie können später Berechtigungen für Cluster-Administratorkonten für Berichterstellung, Nodes, Laufwerke, Volumes, Konten, Und Cluster-Level-Zugriff. Wenn Sie eine Berechtigung aktivieren, weist das System Schreibzugriff für diese Ebene zu. Das System gewährt dem Administrator-Benutzer schreibgeschützten Zugriff für die Ebenen, die Sie nicht auswählen.

Sie können auch ein vom Systemadministrator erstelltes Cluster-Administratorkonto später entfernen. Sie können das primäre Cluster-Administratorkonto, das beim Erstellen des Clusters erstellt wurde, nicht entfernen.

1. So erstellen Sie ein Cluster-weites (nicht-LDAP)-Cluster-Administratorkonto:
   a. Klicken Sie Auf **Benutzer** > **Cluster Admins**.
   b. Klicken Sie Auf **Cluster-Admin Erstellen**.
   c. Wählen Sie den Benutzertyp **Cluster** aus.

d. Geben Sie einen Benutzernamen und ein Kennwort für das Konto ein und bestätigen Sie das Passwort.
e. Wählen Sie Benutzerberechtigungen aus, die auf das Konto angewendet werden sollen.
f. Aktivieren Sie das Kontrollkästchen, um der Endnutzer-Lizenzvereinbarung zuzustimmen.
g. Klicken Sie Auf **Cluster-Admin Erstellen**.

2. So erstellen Sie ein Cluster-Administratorkonto im LDAP-Verzeichnis:

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 Distinguished Name, der für den Benutzer oder eine der Gruppen angezeigt wird, deren Mitglied der Benutzer ist, damit Sie ihn später einfügen können.
d. Klicken Sie Auf **Benutzer** > **Cluster Admins**.
e. Klicken Sie Auf **Cluster-Admin Erstellen**.
f. Wählen Sie den LDAP-Benutzertyp aus.
g. Befolgen Sie im Feld Distinguished Name das Beispiel im Textfeld, um einen vollständigen Distinguished Name für den Benutzer oder die Gruppe einzugeben. Alternativ können Sie ihn aus dem Distinguished Name einfügen, den Sie früher kopiert haben.

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

Um LDAP Cluster Admin-Benutzer oder -Gruppen hinzuzufügen, lautet das allgemeine Format des Benutzernamens „`LDAP:<Full Distinguished Name>`“.

a. Wählen Sie Benutzerberechtigungen aus, die auf das Konto angewendet werden sollen.
b. Aktivieren Sie das Kontrollkästchen, um der Endnutzer-Lizenzvereinbarung zuzustimmen.
c. Klicken Sie Auf **Cluster-Admin Erstellen**.

Berechtigungen für Cluster-Administratoren bearbeiten

Sie können die Berechtigungen für Cluster-Administratorkonten für Berichterstellung, Nodes, Laufwerke, Volumes, Konten, Und Cluster-Level-Zugriff. Wenn Sie eine Berechtigung aktivieren, weist das System Schreibzugriff für diese Ebene zu. Das System gewährt dem Administrator-Benutzer schreibgeschützten Zugriff für die Ebenen, die Sie nicht auswählen.

1. Klicken Sie Auf **Benutzer** > **Cluster Admins**.
2. Klicken Sie auf das Symbol Aktionen für den Cluster-Administrator, den Sie bearbeiten möchten.
3. Klicken Sie Auf **Bearbeiten**.
4. Wählen Sie Benutzerberechtigungen aus, die auf das Konto angewendet werden sollen.
5. Klicken Sie Auf **Änderungen Speichern**.

Ändern Sie Passwörter für Cluster-Administratorkonten

Mithilfe der Element-UI können Sie die Kennwörter für den Cluster-Administrator ändern.

1. Klicken Sie Auf **Benutzer** > **Cluster Admins**.

2. Klicken Sie auf das Symbol Aktionen für den Cluster-Administrator, 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**.

Weitere Informationen

- "Aktivieren Sie die LDAP-Authentifizierung über die Benutzeroberfläche von Element"
- "Deaktivieren Sie LDAP"
- "Seite „SolidFire und Element Ressourcen“"
- "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.

Zum Verwalten von LDAP wird die LDAP-Authentifizierung auf einem SolidFire-Cluster unter Verwendung einer vorhandenen Microsoft Active Directory-Umgebung eingerichtet und die Konfiguration getestet.

Sie können IPv4- und IPv6-Adressen verwenden.

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

1. * Vorkonfigurationsschritte für LDAP-Unterstützung durchführen*. Stellen Sie sicher, dass Sie über alle erforderlichen Details zur Konfiguration der LDAP-Authentifizierung verfügen.
2. **LDAP-Authentifizierung aktivieren**. Verwenden Sie entweder die Element-UI oder die Element-API.
3. **Validierung der LDAP-Konfiguration**. Überprüfen Sie optional, ob der Cluster mit den richtigen Werten konfiguriert ist, indem Sie die GetLdapConfiguration API-Methode ausführen oder die LCAP-Konfiguration über die Element-UI prüfen.
4. **Testen Sie die LDAP-Authentifizierung** (mit dem `readonly` Benutzer). Überprüfen Sie, ob die LDAP-Konfiguration korrekt ist, indem Sie die TestLdapAuthentication API-Methode oder die Element-UI ausführen. Verwenden Sie für diesen ersten Test den Benutzernamen “sAMAccountName” des `readonly` Benutzer: Dadurch wird überprüft, ob Ihr Cluster für die LDAP-Authentifizierung richtig konfiguriert ist, und es wird auch überprüft, dass die `readonly` Anmeldedaten und Zugriff sind korrekt. Wenn 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 setp 4 mit einem Benutzerkonto, das Sie als Element Cluster-Administrator hinzufügen möchten. Kopieren Sie die `distinguished` Name (DN) oder der Benutzer (oder die Gruppe). Dieser DN wird in Schritt 6 verwendet.
6. **Fügen Sie den LDAP-Cluster-Admin** hinzu (kopieren Sie den DN aus dem Test-LDAP-Authentifizierungsschritt und fügen Sie ihn ein). Erstellen Sie mit der Element UI oder der AddLdapClusterAdmin API-Methode einen neuen Cluster-Admin-Benutzer 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**. Loggen Sie sich mit dem neu erstellten LDAP-Cluster-Admin-Benutzer beim Cluster ein. Wenn Sie eine LDAP-Gruppe hinzugefügt haben, können Sie sich als jeder Benutzer dieser Gruppe anmelden.

Führen Sie die Schritte zur Vorkonfiguration für die LDAP-Unterstützung durch

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

Schritte

1. Richten Sie einen Windows Active Directory-Server ein.
2. **Optional:** LDAPS-Support aktivieren.
3. Erstellen von Benutzern und Gruppen
4. Erstellen Sie ein schreibgeschütztes Dienstkonto (z. B. „`sfReadonly`“), das für das Durchsuchen des LDAP-Verzeichnisses verwendet werden soll.

Aktivieren Sie die LDAP-Authentifizierung über die Benutzeroberfläche von Element

Sie können die Integration des Speichersystems mit einem vorhandenen LDAP-Server konfigurieren. Dies ermöglicht LDAP-Administratoren ein zentrales Management des Speichersystemzugriffs für Benutzer.

Sie können LDAP entweder mit der Element-Benutzeroberfläche oder der Element-API konfigurieren. In diesem Verfahren wird beschrieben, wie LDAP über die Element-UI konfiguriert wird.

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

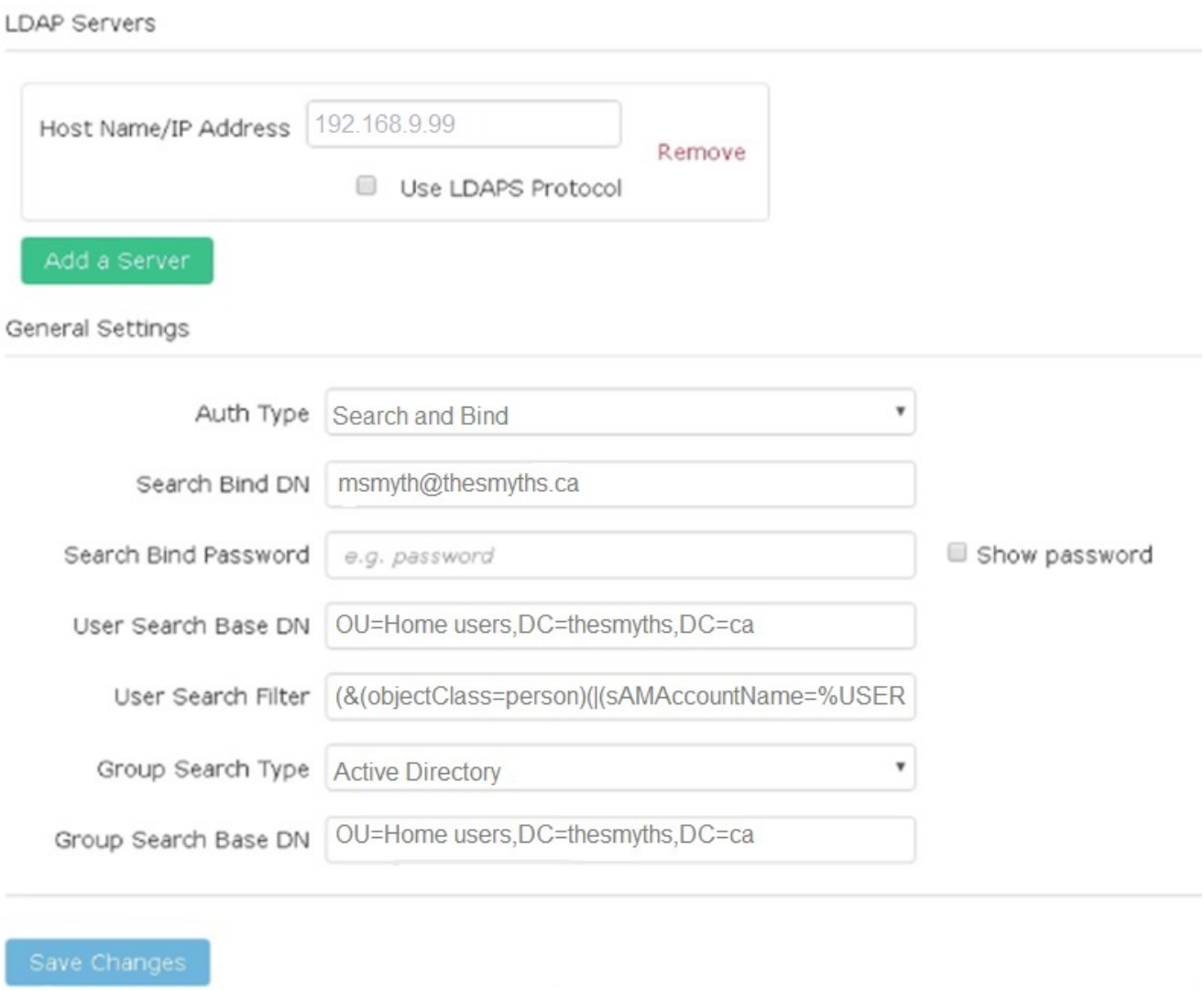
Schritte

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 die * Hostname/IP-Adresse* ein.

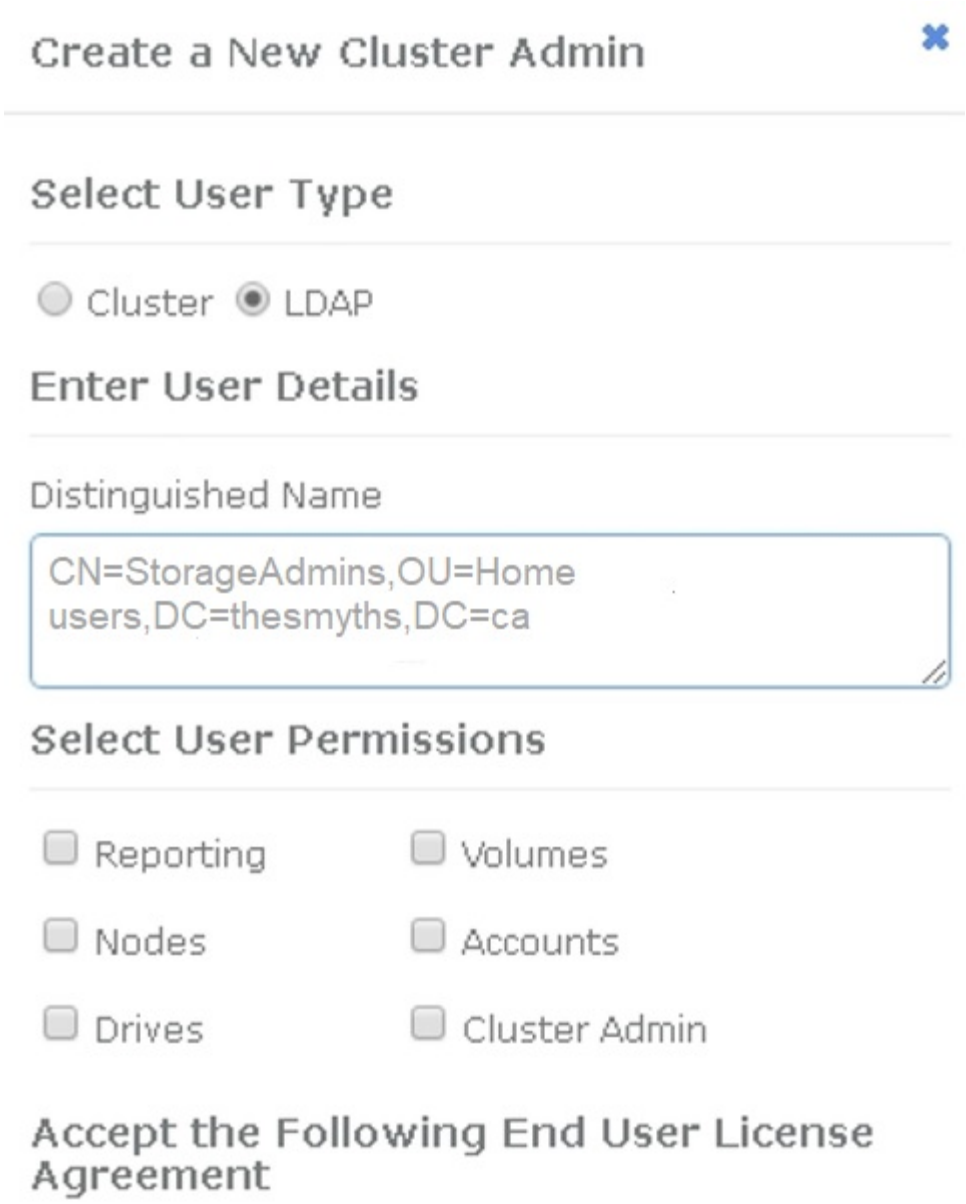
   Es kann auch eine optionale benutzerdefinierte Portnummer eingegeben werden.

   Wenn Sie beispielsweise eine benutzerdefinierte Portnummer hinzufügen möchten, geben Sie <Host Name oder ip-Adresse>:<Port number> 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 für einen Benutzer testen möchten.
9. Kopieren Sie den Distinguished Name und Benutzergruppeninformationen, die später beim Erstellen von Cluster-Administratoren angezeigt werden.
10. Klicken Sie auf **Änderungen speichern**, um neue Einstellungen zu speichern.
11. Um einen Benutzer in dieser Gruppe zu erstellen, damit sich jeder anmelden kann, führen Sie Folgendes aus:
    a. Klicken Sie Auf **Benutzer** > **Ansicht**.



b. Klicken Sie für den neuen Benutzer auf **LDAP** für den Benutzertyp, und fügen Sie die Gruppe ein, die Sie in das Feld Distinguished Name kopiert haben.
c. Wählen Sie die Berechtigungen aus, normalerweise alle Berechtigungen.
d. Scrollen Sie nach unten zur Endbenutzer-Lizenzvereinbarung und klicken Sie auf **Ich akzeptiere**.
e. Klicken Sie Auf **Cluster-Admin Erstellen**.

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

Um dies zu testen, melden Sie sich von der Element UI ab und melden Sie sich als Benutzer in dieser Gruppe an.

Aktivieren Sie die LDAP-Authentifizierung mit der Element API

Sie können die Integration des Speichersystems mit einem vorhandenen LDAP-Server konfigurieren. Dies ermöglicht LDAP-Administratoren ein zentrales Management des Speichersystemzugriffs für Benutzer.

Sie können LDAP entweder mit der Element-Benutzeroberfläche oder der Element-API konfigurieren. In

diesem Verfahren wird beschrieben, wie LDAP mithilfe der Element-API konfiguriert wird.

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

Schritte

1. Aktivieren Sie die LDAP-Authentifizierung zuerst auf dem Cluster mithilfe des `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
AuthType: SearchAndBind	Gibt an, dass der Cluster das Readonly-Dienstkonto verwendet, um zuerst nach dem authentifizierten Benutzer zu suchen und diesen Benutzer anschließend zu binden, wenn er gefunden und authentifiziert wurde.
GroupSearchBaseDN: dc=prodtest,dc=solidfire,dc=net	Gibt den Speicherort in der LDAP-Struktur an, der mit der Suche nach Gruppen beginnt. In diesem Beispiel haben wir die Wurzel unseres Baumes verwendet. Wenn Ihr LDAP-Baum sehr groß ist, sollten Sie diesen auf eine granularere Unterstruktur setzen, um die Suchzeiten zu verkürzen.

Verwendete Parameter	Beschreibung
UserSearchBaseDN: dc=prodtest,dc=solidfire,dc=net	Gibt den Speicherort in der LDAP-Struktur an, der mit der Suche nach Benutzern beginnt. In diesem Beispiel haben wir die Wurzel unseres Baumes verwendet. Wenn Ihr LDAP-Baum sehr groß ist, sollten Sie diesen auf eine granularere Unterstruktur setzen, um die Suchzeiten zu verkürzen.
GroupSearchType: ActiveDirectory	Verwendet den Windows Active Directory-Server als LDAP-Server.

`userSearchFilter: "(&(objectClass=person)(sAMAccountName=%USERNAME%))"`
 	
Um den userPrincipalName (E-Mail-Adresse für die Anmeldung) zu verwenden, können Sie den Suchfilter folgendermaßen ändern:
 	
`"(&(objectClass=person)(userPrincipalName=%USERNAME%))"`
 	
Oder, um sowohl userPrincipalName als auch sAMAccountName zu suchen, können Sie den folgenden BenutzerSearchFilter verwenden:
 	
`"(&(objectClass=person)(`
	(SAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%)))“ ----

Nutzt den sAMAccountName als unseren Benutzernamen für die Anmeldung beim SolidFire-Cluster. Diese Einstellungen weisen LDAP darauf hin, nach dem bei der Anmeldung im sAMAccountName angegebenen Benutzernamen zu suchen und die Suche auch auf Einträge zu beschränken, die “Person” als Wert im objectClass-Attribut haben.	SuchhinBindDN
Dies ist der Distinguished Name of Readonly user, der für die Suche nach dem LDAP-Verzeichnis verwendet wird. Für Active Directory ist es in der Regel am einfachsten, den userPrincipalName (E-Mail-Adressformat) für den Benutzer zu verwenden.	SucheBindPasswort

Um dies zu testen, melden Sie sich von der Element UI ab und melden Sie sich als Benutzer in dieser Gruppe an.

LDAP-Details anzeigen

Zeigen Sie LDAP-Informationen auf der LDAP-Seite auf der Registerkarte Cluster an.

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

1. Um LDAP-Details mit der Element UI anzuzeigen, klicken Sie auf **Cluster** > **LDAP**.
   - **Hostname/IP-Adresse**: Adresse eines LDAP- oder LDAPS-Verzeichnisservers.
   - **Auth Typ**: Die Benutzerauthentifizierungsmethode. Mögliche Werte:
     - Direct Bind
     - Suche Und Bindung
   - **Suche Bind DN**: Ein vollständig qualifizierter DN zur Anmeldung bei, um eine LDAP-Suche für den Benutzer durchzuführen (benötigt Bindeebene-Zugriff auf das LDAP-Verzeichnis).
   - **Suche Bind Password**: Passwort zur Authentifizierung des Zugriffs auf den LDAP-Server.
   - **Basis-DN der Benutzersuche**: Der Basis-DN des Baums, der zum Starten der Benutzersuche verwendet wird. Das System sucht die Unterstruktur vom angegebenen Speicherort aus.
   - **User Search Filter**: Geben Sie unter Verwendung Ihres Domainnamens Folgendes ein:

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

   - **Gruppenkuchsart**: Suchart, die den verwendeten Standardfilter für die Gruppensuche steuert. Mögliche Werte:
     - Active Directory: Verschachtelte Mitgliedschaft aller LDAP-Gruppen eines Benutzers.
     - Keine Gruppen: Keine Gruppenunterstützung.
     - Mitglied-DN: Gruppen im Mitgliedsstil (Einzelebene).
   - **Gruppensuche Basis-DN**: Der Basis-DN des Baumes, der zum Starten der Gruppensuche verwendet wird. Das System sucht die Unterstruktur vom angegebenen Speicherort aus.
   - **Benutzerauthentifizierung testen**: Nachdem LDAP konfiguriert ist, testen Sie den Benutzernamen und die Passwort-Authentifizierung für den LDAP-Server. Geben Sie ein Konto ein, das bereits vorhanden ist, um dies zu testen. Der Distinguished Name und Benutzergruppeninformationen werden angezeigt, die Sie beim Erstellen von Cluster-Administratoren kopieren können.

Testen Sie die LDAP-Konfiguration

Nach der Konfiguration von LDAP sollten Sie es entweder mit der Element-UI oder der Element-API testen `TestLdapAuthentication` Methode.

Schritte

1. So testen Sie die LDAP-Konfiguration mit der Element UI:
   a. Klicken Sie auf **Cluster** > **LDAP**.
   b. Klicken Sie auf **LDAP-Authentifizierung testen**.
   c. Lösen Sie Probleme, indem Sie die Informationen in der folgenden Tabelle verwenden:

Fehlermeldung	Beschreibung
`xLDAPUserNotFound`	• Der zu testenden Benutzer wurde im konfigurierten nicht gefunden `userSearchBaseDN` Unterbaum. • Der `userSearchFilter` Ist falsch konfiguriert.
`xLDAPBindFailed (Error: Invalid credentials)`	• Der getestete Benutzername ist ein gültiger LDAP-Benutzer, aber das angegebene Passwort ist falsch. • Der getestete Benutzername ist ein gültiger LDAP-Benutzer, das Konto ist jedoch derzeit deaktiviert.
`xLDAPSearchBindFailed (Error: Can't contact LDAP server)`	Der LDAP-Server-URI ist falsch.
`xLDAPSearchBindFailed (Error: Invalid credentials)`	Der schreibgeschützte Benutzername oder das Kennwort ist falsch konfiguriert.
`xLDAPSearchFailed (Error: No such object)`	Der `userSearchBaseDN` Ist kein gültiger Speicherort innerhalb der LDAP-Struktur.
`xLDAPSearchFailed (Error: Referral)`	• Der `userSearchBaseDN` Ist kein gültiger Speicherort innerhalb der LDAP-Struktur. • Der `userSearchBaseDN` Und `groupSearchBaseDN` Befinden sich in einer geschachtelten Organisationseinheit. Dies kann zu Berechtigungsproblemen führen. Die Problemumgehung besteht darin, die Organisationseinheit in die Benutzer- und Gruppenbasis-DN-Einträge einzubeziehen (z. B.: `ou=storage, cn=company, cn=com`)

2. So testen Sie die LDAP-Konfiguration mit der Element API:
   a. Rufen Sie die TestLdapAuthentication-Methode auf.

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

b. Überprüfen Sie die Ergebnisse. Wenn der API-Aufruf erfolgreich ist, enthalten die Ergebnisse den Distinguished Name des angegebenen Benutzers sowie eine Liste der Gruppen, in denen der Benutzer Mitglied ist.

```
{
"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"
     }
}
```

Deaktivieren Sie LDAP

Sie können die LDAP-Integration über die Element-UI deaktivieren.

Bevor Sie beginnen, sollten Sie alle Konfigurationseinstellungen beachten, da die Deaktivierung von LDAP alle Einstellungen löscht.

Schritte

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

Weitere Informationen

- "Seite „SolidFire und Element Ressourcen“"
- "NetApp Element Plug-in für vCenter Server"