Gestionar cuentas

Element Software

NetApp
April 17, 2024

Tabla de contenidos

Gestionar cuentas

En los sistemas de almacenamiento de SolidFire, los inquilinos pueden utilizar las cuentas para permitir que los clientes se conecten a volúmenes en un clúster. Cuando crea un volumen, este se asigna a una cuenta específica. También se pueden gestionar cuentas de administrador de clúster para un sistema de almacenamiento SolidFire.

- "Trabaje con cuentas que utilicen CHAP"
- "Gestione cuentas de usuario administrador del clúster"

Si quiere más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Trabaje con cuentas que utilicen CHAP

En los sistemas de almacenamiento de SolidFire, los inquilinos pueden utilizar las cuentas para permitir que los clientes se conecten a volúmenes en un clúster. Una cuenta contiene la autenticación mediante protocolo de autenticación por desafío mutuo (CHAP) que se necesita para acceder a los volúmenes que tiene asignados. Cuando crea un volumen, este se asigna a una cuenta específica.

Una cuenta puede tener hasta 2000 volúmenes asignados, pero un volumen solo puede pertenecer a una cuenta.

Algoritmos CHAP

A partir de Element 12.7, se admiten los algoritmos CHAP SHA1, SHA-256 y SHA3-256 compatibles con FIPS. Con Element 12.7, cuando un iniciador de iSCSI de host crea una sesión iSCSI con un destino iSCSI de Element, solicita una lista de algoritmos CHAP que se van a utilizar. El destino iSCSI de Element elige el primer algoritmo que admite en la lista solicitada por el iniciador iSCSI del host. Para confirmar que el destino iSCSI de Element elige el algoritmo más seguro, debe configurar el iniciador iSCSI del host para que envíe una lista de algoritmos ordenados de la más segura, por ejemplo, SHA3-256, a la menos segura, por ejemplo, SHA1 o MD5. Cuando el iniciador iSCSI del host no solicita los algoritmos SHA, el destino iSCSI de Element elige MD5, suponiendo que la lista de algoritmos propuesta del host contenga MD5. Es posible que necesite actualizar la configuración del iniciador iSCSI del host para habilitar la compatibilidad con los algoritmos seguros.

Durante una actualización de Element 12.7, si ya se actualizó la configuración del iniciador iSCSI del host para enviar una solicitud de sesión con una lista que incluye algoritmos SHA, a medida que se reinician los nodos de almacenamiento, Se activan los nuevos algoritmos seguros y se establecen sesiones iSCSI nuevas o reconectadas mediante el protocolo más seguro. Todas las sesiones iSCSI existentes pasan de MD5 a SHA durante la actualización. Si no se actualiza la configuración del iniciador iSCSI host para solicitar SHA, las sesiones iSCSI existentes seguirán utilizando MD5. Posteriormente, después de actualizar los algoritmos CHAP del iniciador iSCSI del host, las sesiones iSCSI deberían realizar una transición gradual de MD5 a SHA a lo largo del tiempo en función de las actividades de mantenimiento que den lugar a la reconexión de sesiones iSCSI.

Por ejemplo, el iniciador de iSCSI del host predeterminado en Red Hat Enterprise Linux (RHEL) 8.3 tiene el `node.session.auth.chap_algs = SHA3-256,SHA256,SHA1,MD5` Si se establecen comentarios, los resultados del iniciador iSCSI solo se obtienen con MD5. Si no se hace comentarios sobre esta configuración en el host y se reinicia el iniciador de iSCSI, se activan las sesiones iSCSI desde ese host para comenzar a utilizar SHA3-256.

Si es necesario, puede utilizar la "ListISCSISessions" Método API para ver los algoritmos CHAP que se utilizan para cada sesión.

Crear una cuenta

Es posible crear una cuenta para permitir el acceso a los volúmenes.

Cada nombre de cuenta del sistema debe ser exclusivo.

1. Seleccione **Administración** > **Cuentas**.
2. Haga clic en **Crear cuenta**.
3. Introduzca un **Nombre de usuario**.
4. En la sección **Configuración CHAP**, introduzca la siguiente información:

   > Puede dejar los campos de credenciales vacíos para que cualquier contraseña se genere automáticamente.

   - **Secreto de iniciador** para la autenticación de sesión de nodo CHAP.
   - **Secreto de destino** para la autenticación de sesión de nodo CHAP.
5. Haga clic en **Crear cuenta**.

Ver los detalles de la cuenta

La actividad de rendimiento de cada cuenta se puede ver como un gráfico.

El gráfico proporciona información de I/o y rendimiento de la cuenta. Los niveles de actividad promedio y pico se muestran en incrementos de períodos de informe de 10 segundos. Estas estadísticas incluyen la actividad de todos los volúmenes asignados a la cuenta.

1. Seleccione **Administración** > **Cuentas**.
2. Haga clic en el icono Actions de una cuenta.
3. Haga clic en **Ver detalles**.

Estos son algunos de los detalles:

- **Estado**: El estado de la cuenta. Los posibles valores son los siguientes:
  - Active: Una cuenta activa.
  - Locked: Una cuenta bloqueada.
  - Deleted: Una cuenta que se ha eliminado y purgado.
- **Volúmenes activos**: Número de volúmenes activos asignados a la cuenta.
- **Compresión**: La puntuación de eficiencia de compresión para los volúmenes asignados a la cuenta.
- **Deduplicación**: La puntuación de eficiencia de deduplicación para los volúmenes asignados a la cuenta.

- **Thin Provisioning**: La puntuación de eficiencia de thin provisioning para los volúmenes asignados a la cuenta.
- **Eficiencia general**: La puntuación de eficiencia general para los volúmenes asignados a la cuenta.

Editar una cuenta

Una cuenta se puede editar para cambiar el estado, cambiar los secretos de CHAP o modificar el nombre de la cuenta.

Si se modifica la configuración de CHAP en una cuenta o se quitan los iniciadores o los volúmenes de un grupo de acceso, se podría interrumpir el acceso de los iniciadores a los volúmenes de forma inesperada. Para asegurarse de que no se interrumpirá el acceso a los volúmenes de forma inesperada, siempre debe cerrar las sesiones iSCSI afectadas por alguno de los cambios en la cuenta o en el grupo de acceso. Asimismo, compruebe que los iniciadores pueden volver a conectarse con los volúmenes una vez que se hayan realizado los cambios en la configuración del iniciador y la configuración del clúster.

> Los volúmenes persistentes asociados con servicios de gestión se asignan a una cuenta nueva que se crea durante la instalación o la actualización. Si utiliza volúmenes persistentes, no modifique o elimine su cuenta asociada.

1. Seleccione **Administración** > **Cuentas**.
2. Haga clic en el icono Actions de una cuenta.
3. En el menú que se abre, seleccione **Editar**.
4. **Opcional:** edite el **Nombre de usuario**.
5. **Opcional:** haga clic en la lista desplegable **Estado** y seleccione un estado diferente.

   > Al cambiar el estado a **Locked** se cierran todas las conexiones iSCSI a la cuenta y ya no se puede acceder a ella. Los volúmenes asociados con la cuenta se mantienen, pero ya no se podrán detectar los volúmenes con iSCSI.

6. **Opcional:** en **Configuración CHAP**, edite las credenciales **Secreto de iniciador** y **Secreto de destino** utilizadas para la autenticación de sesión de nodo.

   > Si no cambia las credenciales **Configuración CHAP**, seguirán siendo las mismas. Si deja vacíos los campos de las credenciales, el sistema generará contraseñas nuevas.

7. Haga clic en **Guardar cambios**.

Eliminar una cuenta

Una cuenta se puede eliminar cuando ya no se necesita.

Debe eliminar y purgar los volúmenes asociados con la cuenta antes de eliminarla.

> Los volúmenes persistentes asociados con servicios de gestión se asignan a una cuenta nueva que se crea durante la instalación o la actualización. Si utiliza volúmenes persistentes, no modifique o elimine su cuenta asociada.

1. Seleccione **Administración** > **Cuentas**.

2. Haga clic en el icono Actions de la cuenta que quiera eliminar.
3. En el menú que se abre, seleccione **Eliminar**.
4. Confirme la acción.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Gestione cuentas de usuario administrador del clúster

Para gestionar las cuentas de administrador de clúster correspondientes a un sistema de almacenamiento de SolidFire, debe crear, eliminar y editar cuentas de administrador de clúster, cambiar la contraseña de administrador de clúster y configurar las opciones de LDAP para gestionar el acceso a los usuarios al sistema.

Tipos de cuenta de administrador del clúster de almacenamiento

Existen dos tipos de cuentas de administrador que pueden existir en un clúster de almacenamiento que ejecuta el software NetApp Element: La cuenta de administrador de clúster principal y una cuenta de administrador de clúster.

- **Cuenta de administrador del clúster principal**

  Esta cuenta de administrador se crea cuando se crea el clúster. Es la cuenta administrativa principal con el nivel de acceso al clúster más alto. Esta cuenta es similar a un usuario raíz en un sistema Linux. Puede cambiar la contraseña de esta cuenta de administrador.

- **Cuenta de administrador de clúster**

  Puede conceder a una cuenta de administrador de clúster una gama limitada de accesos de administrador para realizar determinadas tareas dentro de un clúster. Las credenciales que se asignan a cada cuenta de administrador de clúster sirven para autenticar las solicitudes de la API y la interfaz de usuario de Element dentro del sistema de almacenamiento.

> Se necesita una cuenta de administrador de clúster local (que no sea LDAP) para acceder a los nodos activos en un clúster a través de la interfaz de usuario por nodo. No se necesitan credenciales de cuenta para acceder a un nodo que aún no forme parte de un clúster.

Ver los detalles de administrador del clúster

1. Si desea crear una cuenta de administrador de clúster (que no sea LDAP) para todo el clúster, realice las siguientes acciones:
   a. Haga clic en **usuarios** > **Administradores de clúster**.
2. En la página Cluster Admins de la pestaña Users, puede ver la siguiente información.
   - **ID**: Número secuencial asignado a la cuenta de administrador del clúster.
   - **Nombre de usuario**: El nombre otorgado a la cuenta de administrador del clúster cuando se creó.

- **Acceso**: Los permisos de usuario asignados a la cuenta de usuario. Los posibles valores son los siguientes:
  - lea
  - creación de informes
  - nodos
  - unidades
  - volúmenes
  - cuentas
  - Administradores de clústeres
  - administrador
  - SupportAdmin

  Todos los permisos están disponibles para el tipo de acceso del administrador.

- **Tipo**: El tipo de administrador de clúster. Los posibles valores son los siguientes:
  - Clúster
  - LDAP
- **Atributos**: Si la cuenta de administrador de clúster se creó mediante la API de elemento, esta columna muestra cualquier par nombre-valor que se haya establecido utilizando ese método.

  Consulte "Referencia de API del software NetApp Element".

Cree una cuenta de administrador de clúster

Es posible crear nuevas cuentas de administrador de clúster con permisos para conceder o restringir el acceso a determinadas áreas del sistema de almacenamiento. Cuando se configuran los permisos de la cuenta de administrador del clúster, el sistema otorga derechos de solo lectura a aquellos permisos que no se asignen al administrador del clúster.

Si desea crear una cuenta de administrador de clúster LDAP, asegúrese de que LDAP esté configurado en el clúster antes de comenzar.

"Habilite la autenticación de LDAP con la interfaz de usuario de Element"

Más adelante, los privilegios de la cuenta de administrador de clúster se pueden cambiar para crear informes, nodos, unidades, volúmenes, cuentas y acceso a nivel de clúster. Cuando habilita un permiso, el sistema asigna acceso de escritura para ese nivel. Para los niveles que no se seleccionan, el sistema concede al usuario administrador acceso de solo lectura.

También es posible quitar más adelante cualquier cuenta de usuario administrador de clúster que haya creado un administrador del sistema. Sin embargo, no es posible quitar la cuenta de administrador de clúster principal que se generó al crear el clúster.

1. Si desea crear una cuenta de administrador de clúster (que no sea LDAP) para todo el clúster, realice las siguientes acciones:
   a. Haga clic en **usuarios** > **Administradores de clúster**.
   b. Haga clic en **Crear administrador de clúster**.

c. Seleccione el tipo de usuario **Cluster**.
d. Introduzca un nombre de usuario y una contraseña para la cuenta y confirme la contraseña.
e. Seleccione los permisos de usuario que se van a aplicar a la cuenta.
f. Active la casilla con la que se acepta el contrato de licencia para usuario final de.
g. Haga clic en **Crear administrador de clúster**.

2. Para crear una cuenta de administrador de clúster en el directorio LDAP, realice las siguientes acciones:

   a. Haga clic en **Cluster** > **LDAP**.
   b. Asegúrese de que la autenticación LDAP está habilitada.
   c. Haga clic en **probar autenticación de usuario** y copie el nombre completo que aparece para el usuario o uno de los grupos de los que el usuario es miembro para poder pegarlo más tarde.
   d. Haga clic en **usuarios** > **Administradores de clúster**.
   e. Haga clic en **Crear administrador de clúster**.
   f. Seleccione el tipo de usuario LDAP.
   g. En el campo Nombre distintivo, siga el ejemplo del cuadro de texto para introducir un nombre completo distintivo para el usuario o grupo. Como alternativa, péguela desde el nombre distintivo que copió anteriormente.

      Si el nombre distintivo forma parte de un grupo, cualquier usuario que sea miembro de dicho grupo en el servidor LDAP tendrá permisos de esta cuenta de administrador.

   Para agregar usuarios o grupos de administración de clúster LDAP, el formato general del nombre de usuario es "'LDAP:<Full Distinguished Name>'".

   a. Seleccione los permisos de usuario que se van a aplicar a la cuenta.
   b. Active la casilla con la que se acepta el contrato de licencia para usuario final de.
   c. Haga clic en **Crear administrador de clúster**.

Edite los permisos de administrador del clúster

Los privilegios de la cuenta de administrador de clúster se pueden cambiar para crear informes, nodos, unidades, volúmenes y cuentas. y acceso a nivel de clúster. Cuando habilita un permiso, el sistema asigna acceso de escritura para ese nivel. Para los niveles que no se seleccionan, el sistema concede al usuario administrador acceso de solo lectura.

1. Haga clic en **usuarios** > **Administradores de clúster**.
2. Haga clic en el icono Actions del administrador de clúster que quiera editar.
3. Haga clic en **Editar**.
4. Seleccione los permisos de usuario que se van a aplicar a la cuenta.
5. Haga clic en **Guardar cambios**.

Cambiar contraseñas de las cuentas de administrador del clúster

Es posible usar la interfaz de usuario de Element para cambiar las contraseñas de administrador de clúster.

1. Haga clic en **usuarios** > **Administradores de clúster**.

2. Haga clic en el icono Actions del administrador de clúster que quiera editar.
3. Haga clic en **Editar**.
4. En el campo Change Password, introduzca una contraseña nueva y confírmela.
5. Haga clic en **Guardar cambios**.

Obtenga más información

- "Habilite la autenticación de LDAP con la interfaz de usuario de Element"
- "Deshabilite LDAP"
- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"

Gestione LDAP

Puede configurar el protocolo ligero de acceso a directorios (LDAP) para habilitar la funcionalidad de inicio de sesión seguro basado en directorios en el almacenamiento de SolidFire. Se puede configurar LDAP en el nivel del clúster y autorizar grupos y usuarios de LDAP.

La gestión de LDAP implica configurar la autenticación LDAP en un clúster de SolidFire mediante un entorno de Microsoft Active Directory existente y probar la configuración.

Es posible usar tanto direcciones IPv4 como IPv6.

Habilitar LDAP implica los siguientes pasos de alto nivel, descritos con detalle:

1. **Completar los pasos de preconfiguración para compatibilidad con LDAP**. Valide tener todos los detalles necesarios para configurar la autenticación LDAP.
2. **Activar autenticación LDAP**. Use la interfaz de usuario de Element o la API de Element.
3. **Validar la configuración LDAP**. De manera opcional, compruebe que el clúster se haya configurado con los valores correctos ejecutando el método API GetLdapConfiguration o comprobando la configuración LCAP mediante la interfaz de usuario de Element.
4. **Pruebe la autenticación LDAP** (con la `readonly` usuario). Compruebe que la configuración de LDAP sea correcta mediante la ejecución del método API TestLdapAuthentication o mediante la interfaz de usuario de Element. Para esta prueba inicial, utilice el nombre de usuario «sAMAccountName» del `readonly` usuario. Esto validará que su clúster esté configurado correctamente para la autenticación LDAP y también validará que el `readonly` las credenciales y el acceso son correctos. Si este paso falla, repita los pasos del 1 al 3.
5. **Pruebe la autenticación LDAP** (con una cuenta de usuario que desea agregar). Repita setp 4 con una cuenta de usuario que desee agregar como administrador de clúster de Element. Copie el `distinguished` Nombre (DN) o usuario (o grupo). Este DN se utilizará en el paso 6.
6. **Agregue el administrador del clúster LDAP** (copie y pegue el DN del paso probar autenticación LDAP). Mediante la interfaz de usuario de Element o el método API AddLdapClusterAdmin, cree un nuevo usuario administrador de clúster con el nivel de acceso adecuado. Para el nombre de usuario, pegue el DN completo que ha copiado en el paso 5. Esto asegura que el DN está formateado correctamente.
7. **Pruebe el acceso de administrador del clúster**. Inicie sesión en el clúster con el usuario administrador del clúster LDAP recién creado. Si agregó un grupo LDAP, puede iniciar sesión como cualquier usuario de

ese grupo.

Complete los pasos previos de configuración para ser compatible con LDAP

Antes de habilitar la compatibilidad con LDAP en Element, debe configurar un servidor de Windows Active Directory y realizar otras tareas previas a la configuración.

Pasos

1. Configure un servidor de Active Directory de Windows.
2. **Opcional:** Activar soporte LDAPS.
3. Crear usuarios y grupos.
4. Cree una cuenta de servicio de sólo lectura (como «sfreadonly») que se utilizará para buscar en el directorio LDAP.

Habilite la autenticación de LDAP con la interfaz de usuario de Element

Puede configurar la integración del sistema de almacenamiento con un servidor LDAP existente. De este modo, los administradores de LDAP pueden gestionar de forma centralizada el acceso al sistema de almacenamiento para los usuarios.

Es posible configurar LDAP con la interfaz de usuario de Element o la API de Element. Este procedimiento describe cómo configurar LDAP mediante la interfaz de usuario de Element.

Este ejemplo muestra cómo configurar la autenticación LDAP en SolidFire y utiliza `SearchAndBind` como tipo de autenticación. En el ejemplo se utiliza un solo servidor de Active Directory de Windows Server 2012 R2.

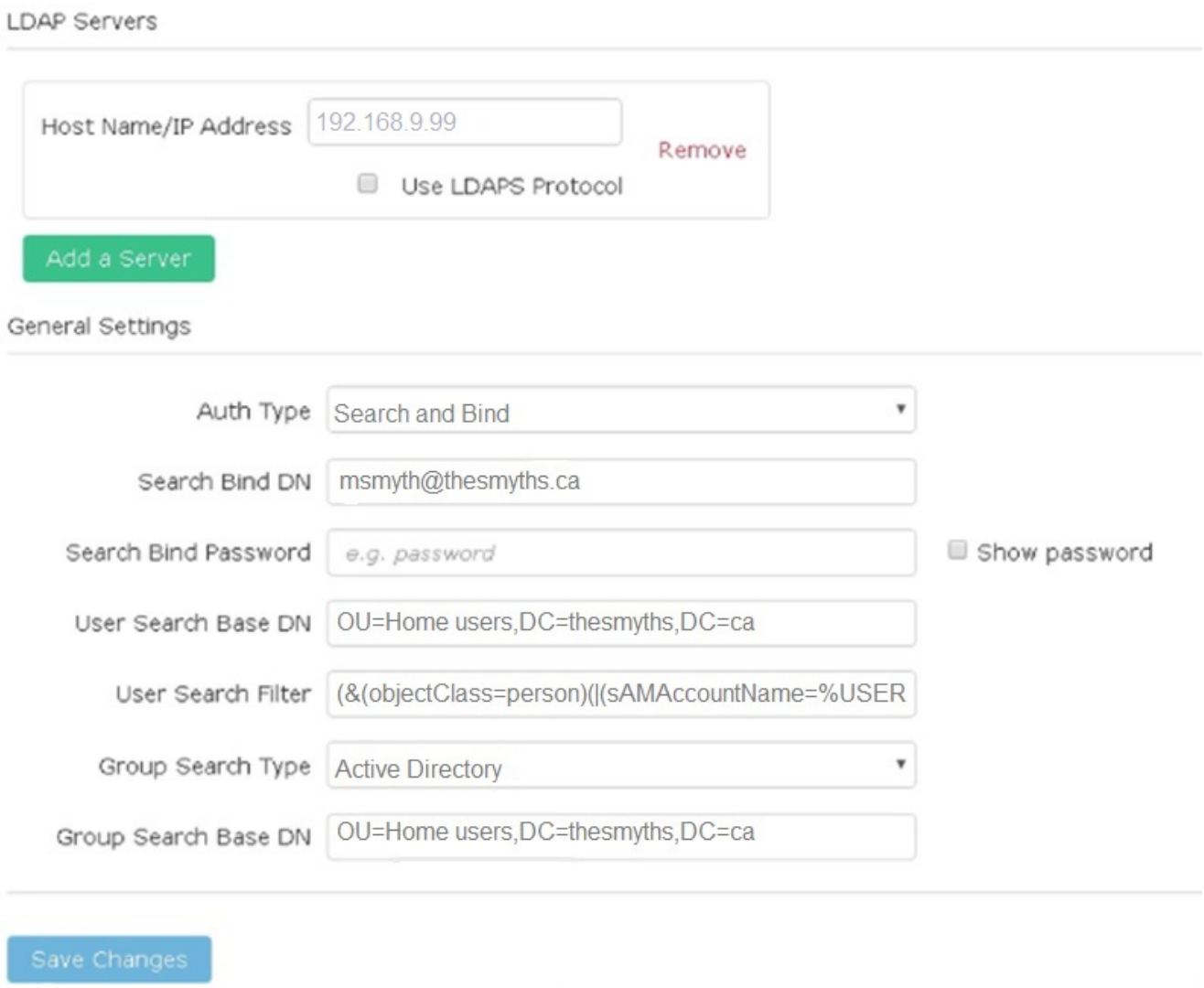
Pasos

1. Haga clic en **Cluster** > **LDAP**.
2. Haga clic en **Sí** para activar la autenticación LDAP.
3. Haga clic en **Agregar un servidor**.
4. Introduzca **Nombre de host/dirección IP**.

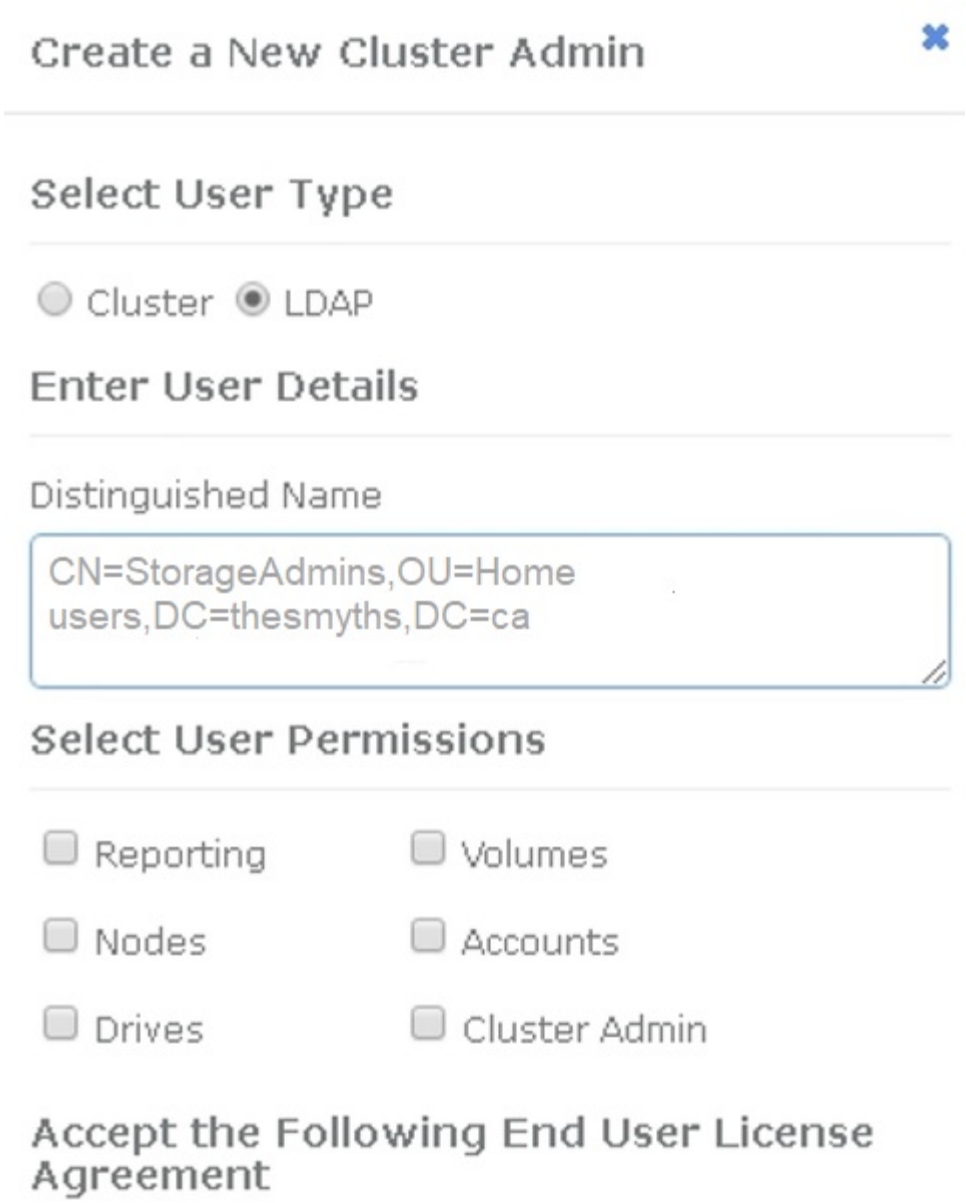
   ⓘ También puede introducir un número de puerto personalizado opcional.

   Por ejemplo, para añadir un número de puerto personalizado, introduzca <host name or ip address>:<port number>

5. **Opcional:** Seleccione **Use LDAPS Protocol**.
6. Introduzca la información necesaria en **Ajustes generales**.



7. Haga clic en **Activar LDAP**.
8. Haga clic en **probar autenticación de usuario** si desea probar el acceso al servidor para un usuario.
9. Copie la información del nombre distintivo y del grupo de usuarios que aparece para usarla más adelante cuando se crean administradores de clúster.
10. Haga clic en **Guardar cambios** para guardar cualquier configuración nueva.
11. Para crear un usuario en este grupo de modo que cualquiera pueda iniciar sesión, realice lo siguiente:
    a. Haga clic en **Usuario** > **Ver**.



b. Para el nuevo usuario, haga clic en **LDAP** para el tipo de usuario y pegue el grupo que copió en el campo Nombre distintivo.
c. Seleccione los permisos, normalmente todos los permisos.
d. Desplácese hasta el Contrato de licencia para el usuario final y haga clic en **Acepto**.
e. Haga clic en **Crear administrador de clúster**.

   Ahora tiene un usuario con el valor de un grupo de Active Directory.

Para probarlo, cierre sesión en la interfaz de usuario del elemento y vuelva a iniciarla como usuario en ese grupo.

Habilite la autenticación de LDAP con la API de Element

Puede configurar la integración del sistema de almacenamiento con un servidor LDAP existente. De este modo, los administradores de LDAP pueden gestionar de forma centralizada el acceso al sistema de almacenamiento para los usuarios.

Es posible configurar LDAP con la interfaz de usuario de Element o la API de Element. Este procedimiento describe cómo configurar LDAP mediante la API de Element.

Para aprovechar la autenticación LDAP en un clúster de SolidFire, primero debe habilitar la autenticación LDAP en el clúster mediante el `EnableLdapAuthentication` Método API.

Pasos

1. Habilite la autenticación LDAP primero en el clúster de mediante el `EnableLdapAuthentication` Método API.
2. Especifique la información obligatoria.

```
{
     "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. Cambie los valores de los siguientes parámetros:

Parámetros utilizados	Descripción
AuthType: SearchAndBind	Dicta que el clúster utilizará la cuenta de servicio readonly para buscar primero el usuario que se va a autenticar y, a continuación, enlazar ese usuario si se encuentra y se autentica.
GroupSearchBaseDN: dc=prodtest,dc=solidfire,dc=net	Especifica la ubicación en el árbol LDAP para comenzar a buscar grupos. Para este ejemplo, hemos utilizado la raíz de nuestro árbol. Si su árbol LDAP es muy grande, quizás desee establecer este árbol en un subárbol más granular para reducir los tiempos de búsqueda.

Parámetros utilizados	Descripción
UserSearchBaseDN: dc=prodtest,dc=solidfire,dc=net	Especifica la ubicación en el árbol LDAP para comenzar a buscar usuarios. Para este ejemplo, hemos utilizado la raíz de nuestro árbol. Si su árbol LDAP es muy grande, quizás desee establecer este árbol en un subárbol más granular para reducir los tiempos de búsqueda.
GroupSearchType: ActiveDirectory	Utiliza el servidor de Windows Active Directory como servidor LDAP.

`userSearchFilter: "(&(objectClass=person)(sAMAccountName=%USERNAME%))"`
 	
Para utilizar userPrincipalName (dirección de correo electrónico para el inicio de sesión), puede cambiar userSearchFilter a:
 	
`"(&(objectClass=person)(userPrincipalName=%USERNAME%))"`
 	
O bien, para buscar userPrincipalName y sAMAccountName, puede usar el siguiente usuarioSearchFilter:
 	
`"(&(objectClass=person)(`
	(SAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%))" ----

Utiliza sAMAccountName como nombre de usuario para iniciar sesión en el clúster de SolidFire. Esta configuración indica a LDAP que busque el nombre de usuario especificado durante el inicio de sesión en el atributo sAMAccountName y que también limite la búsqueda a entradas que tengan "'Person'" como valor en el atributo objectClass.	SearchBindDN
Es el nombre completo del usuario readonly que se utilizará para buscar en el directorio LDAP. Para un directorio activo suele ser más fácil utilizar userPrincipalName (formato de dirección de correo electrónico) para el usuario.	SearchBindPassword

Para probarlo, cierre sesión en la interfaz de usuario del elemento y vuelva a iniciarla como usuario en ese grupo.

Ver los detalles de LDAP

Consulte la información de LDAP en la página LDAP de la pestaña Cluster.

> Debe habilitar LDAP para ver estas opciones de configuración de LDAP.

1. Para ver los detalles de LDAP con la interfaz de usuario de Element, haga clic en **Cluster** > **LDAP**.
   - **Nombre de host/Dirección IP**: Dirección de un servidor de directorio LDAP o LDAPS.
   - **Tipo de autenticación**: El método de autenticación de usuario. Los posibles valores son los siguientes:
     - Enlace directo
     - Búsqueda y vinculación
   - **Buscar Bind DN**: Un DN completo con el que conectarse para realizar una búsqueda LDAP del usuario (necesita acceso de nivel de enlace al directorio LDAP).
   - **Buscar Contraseña de enlace**: Contraseña utilizada para autenticar el acceso al servidor LDAP.
   - **User Search base DN**: El DN base del árbol utilizado para iniciar la búsqueda del usuario. El sistema busca el subárbol de la ubicación especificada.
   - **Filtro de búsqueda de usuario**: Introduzca lo siguiente utilizando su nombre de dominio:

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

   - **Tipo de búsqueda de grupo**: Tipo de búsqueda que controla el filtro de búsqueda de grupo predeterminado utilizado. Los posibles valores son los siguientes:
     - Active Directory: Pertenencia anidada de todos los grupos LDAP de un usuario.
     - No hay grupos: Ningún soporte de grupo.
     - DN de miembro: Grupos de tipo DN de miembro (un nivel).
   - **DN base de búsqueda de grupo**: El DN base del árbol utilizado para iniciar la búsqueda de grupo. El sistema busca el subárbol de la ubicación especificada.
   - **Probar autenticación de usuario**: Después de configurar LDAP, utilice esta opción para probar la autenticación de nombre de usuario y contraseña para el servidor LDAP. Introduzca una cuenta que ya existe para probarlo. Se muestra la información relacionada con el nombre distintivo y el grupo de usuarios, que se puede copiar para usarlo más adelante al crear administradores de clúster.

Pruebe la configuración de LDAP

Después de configurar LDAP, debe probarla mediante la interfaz de usuario de Element o la API de Element `TestLdapAuthentication` método.

Pasos

1. Para probar la configuración de LDAP con la interfaz de usuario de Element, haga lo siguiente:
   a. Haga clic en **Cluster** > **LDAP**.
   b. Haga clic en **probar autenticación LDAP**.
   c. Resuelva cualquier problema utilizando la información de la siguiente tabla:

Mensaje de error	Descripción
`xLDAPUserNotFound`	• El usuario que se está probando no se encontró en el configurado `userSearchBaseDN` subárbol. • La `userSearchFilter` está configurado incorrectamente.
`xLDAPBindFailed (Error: Invalid credentials)`	• El nombre de usuario que se está probando es un usuario LDAP válido, pero la contraseña proporcionada es incorrecta. • El nombre de usuario que se está probando es un usuario LDAP válido, pero la cuenta está deshabilitada actualmente.
`xLDAPSearchBindFailed (Error: Can't contact LDAP server)`	El URI del servidor LDAP es incorrecto.
`xLDAPSearchBindFailed (Error: Invalid credentials)`	El nombre de usuario o la contraseña de solo lectura están configurados incorrectamente.
`xLDAPSearchFailed (Error: No such object)`	La `userSearchBaseDN` No es una ubicación válida dentro del árbol LDAP.
`xLDAPSearchFailed (Error: Referral)`	• La `userSearchBaseDN` No es una ubicación válida dentro del árbol LDAP. • La `userSearchBaseDN` y.. `groupSearchBaseDN` Están en una unidad organizativa anidada. Esto puede provocar problemas de permisos. La solución alternativa es incluir la unidad organizativa en las entradas DN base de usuario y grupo (por ejemplo: `ou=storage, cn=company, cn=com`)

2. Para probar la configuración de LDAP con la API de Element, haga lo siguiente:
   a. Llame al método TestLdapAuthentication.

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

b. Revise los resultados. Si la llamada API es correcta, los resultados incluyen el nombre completo del usuario especificado y una lista de grupos en los que el usuario es miembro.

```
{
"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"
     }
}
```

Deshabilite LDAP

Es posible deshabilitar la integración de LDAP con la interfaz de usuario de Element.

Antes de comenzar, debe tener en cuenta todas las opciones de configuración, ya que al deshabilitar LDAP se borran todas las opciones.

Pasos

1. Haga clic en **Cluster** > **LDAP**.
2. Haga clic en **no**.
3. Haga clic en **Desactivar LDAP**.

Obtenga más información

- "Documentación de SolidFire y el software Element"
- "Plugin de NetApp Element para vCenter Server"