



Métodos de API de LDAP

Element Software

NetApp
January 15, 2024

Tabla de contenidos

- Métodos de API de LDAP 1
 - Obtenga más información 1
 - AddLdapClusterAdmin 1
 - EnableLdapAuthentication 3
 - Autenticación DisableLdapAuthentication 8
 - GetLdapConfiguration 9
 - TestLdapAuthentication 11

Métodos de API de LDAP

Puede usar el protocolo ligero de acceso a directorios (LDAP) para autenticar el acceso al almacenamiento de Element. Los métodos de API de LDAP que se describen en esta sección le permiten configurar el acceso LDAP al clúster de almacenamiento.

- [AddLdapClusterAdmin](#)
- [EnableLdapAuthentication](#)
- [Autenticación DisableLdapAuthentication](#)
- [GetLdapConfiguration](#)
- [TestLdapAuthentication](#)

Obtenga más información

- ["Documentación de SolidFire y el software Element"](#)
- ["Documentación para versiones anteriores de SolidFire de NetApp y los productos Element"](#)

AddLdapClusterAdmin

Puede utilizar el `AddLdapClusterAdmin` Para añadir un nuevo usuario administrador de clúster LDAP. Un administrador de clúster LDAP puede gestionar el clúster mediante las herramientas API y de gestión. Las cuentas de administrador de clúster LDAP están completamente separadas y no están relacionadas con las cuentas de cliente estándar.

Parámetros

También puede utilizar este método para agregar un grupo LDAP definido en Active Directory®. El nivel de acceso que se da al grupo se pasa a los usuarios individuales del grupo LDAP.

Este método tiene los siguientes parámetros de entrada:

| Nombre | Descripción | Tipo | Valor predeterminado | Obligatorio |
|--------|--|-------------------|----------------------|-------------|
| acceso | Controla qué métodos puede utilizar este administrador de clúster. | matriz de cadenas | Ninguno | Sí |

| Nombre | Descripción | Tipo | Valor predeterminado | Obligatorio |
|-------------------|---|-------------|----------------------|-------------|
| AceptEula | Acepte el contrato de licencia para usuario final. Establezca esta opción en true para añadir una cuenta de administrador de clúster al sistema. Si se omite o se establece en falso, la llamada al método falla. | booleano | Ninguno | Sí |
| atributos | La lista de pares nombre-valor en el formato de objetos JSON. | Objeto JSON | Ninguno | No |
| nombre de usuario | El nombre de usuario distintivo del nuevo administrador de clúster LDAP. | cadena | Ninguno | Sí |

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "AddLdapClusterAdmin",
  "params": {"username": "cn=mike
jones,ou=ptusers,dc=prodtest,dc=solidfire,dc=net",
  "access": ["administrator", "read"
  ]
},
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {}
}
```

Nuevo desde la versión

9.6

Obtenga más información

[Control de acceso](#)

EnableLdapAuthentication

Puede utilizar el `EnableLdapAuthentication` Método para configurar una conexión de directorio LDAP para la autenticación LDAP de un clúster de. Los usuarios que son miembros del directorio LDAP pueden iniciar sesión en el sistema de almacenamiento con sus credenciales de LDAP.

Parámetros

Este método tiene los siguientes parámetros de entrada:

| Nombre | Descripción | Tipo | Valor predeterminado | Obligatorio |
|--------------------------------|---|--------|----------------------------|-------------|
| Tipo de autorización | Identifica el método de autenticación de usuarios que se va a utilizar. Los posibles valores son los siguientes: <ul style="list-style-type: none">• <code>DirectBind</code>• <code>SearchAndBind</code> | cadena | <code>SearchAndBind</code> | No |
| <code>GroupSearchBaseDN</code> | El DN base del árbol para iniciar la búsqueda del subárbol del grupo. | cadena | Ninguno | No |

| Nombre | Descripción | Tipo | Valor predeterminado | Obligatorio |
|------------------|--|-------------------|----------------------|-------------|
| GroupSearchType | <p>Controla el filtro de búsqueda de grupos predeterminado que se utiliza. Los posibles valores son los siguientes:</p> <ul style="list-style-type: none"> • NoGroups: Ningún soporte de grupo. • ActiveDirectory: Pertenencia anidada de todos los grupos de directorios activos de un usuario. • MemberDN: Grupos del estilo MemberDN (un nivel). | cadena | ActiveDirectory | No |
| URIs de servidor | <p>Lista separada por comas de URI de servidor LDAP o LDAPS. Puede agregar un puerto personalizado al final de un URI LDAP o LDAPS usando un punto y dos puntos seguidos por el número de puerto. Por ejemplo, el URI "ldap://1.2.3.4" utiliza el puerto predeterminado y el URI "ldaps://1.2.3.4:123" utiliza el puerto personalizado 123.</p> | matriz de cadenas | Ninguno | Sí |

| Nombre | Descripción | Tipo | Valor predeterminado | Obligatorio |
|--------------------|---|--------|----------------------|-------------|
| UserSearchBaseDN | El DN base del árbol para iniciar la búsqueda del subárbol. Este parámetro es obligatorio cuando se utiliza AuthType de SearchAndBind. | cadena | Ninguno | No |
| SearchBindDN | Un DN completo con el que se inicia sesión para realizar una búsqueda LDAP del usuario. El DN requiere acceso de lectura al directorio LDAP. Este parámetro es obligatorio cuando se utiliza AuthType de SearchAndBind. | cadena | Ninguno | Sí |
| SearchBindPassword | La contraseña de la cuenta searchBindDN utilizada para realizar la búsqueda. Este parámetro es obligatorio cuando se utiliza AuthType de SearchAndBind. | cadena | Ninguno | Sí |

| Nombre | Descripción | Tipo | Valor predeterminado | Obligatorio |
|------------------|--|--------|----------------------|-------------|
| UserSearchFilter | <p>Filtro de búsqueda LDAP que se va a utilizar al consultar el servidor LDAP. La cadena debe tener el texto de marcador de posición "%USERNAME%" que se sustituye por el nombre de usuario del usuario que se va a autenticar. Por ejemplo, (&(objectClass=person)(sAMAccountName=%USERNAME%)) utilizará el campo sAMAccountName de Active Directory para que coincida con el nombre de usuario introducido al iniciar sesión en el clúster. Este parámetro es obligatorio cuando se utiliza AuthType de SearchAndBind.</p> | cadena | Ninguno | Sí |
| UserDNTemplate | <p>Plantilla de cadena utilizada para definir un patrón para construir un nombre completo (DN) de usuario. La cadena debe tener el texto de marcador de posición "%USERNAME%" que se sustituye por el nombre de usuario del usuario que se va a autenticar. Este parámetro es necesario cuando se utiliza AuthType de DirectBind.</p> | cadena | Ninguno | Sí |

| Nombre | Descripción | Tipo | Valor predeterminado | Obligatorio |
|-------------------------|---|--------|----------------------|-------------|
| GroupSearchCustomFilter | Para utilizarlo con el tipo de búsqueda CustomFilter, un filtro LDAP que se utilizará para devolver el DNS de los grupos de un usuario. La cadena puede tener texto de marcador de posición de %USERNAME% y %USERDN% para ser reemplazado por su nombre de usuario y su DN de usuario completo según sea necesario. | cadena | Ninguno | Sí |

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```

{
  "method": "EnableLdapAuthentication",
  "params": {
    "authType": "SearchAndBind",
    "groupSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
    "groupSearchType": "ActiveDirectory",
    "searchBindDN": "SFReadOnly@prodtest.solidfire.net",
    "searchBindPassword": "zsw@#edcASD12",
    "sslCert": "",
    "userSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
    "userSearchFilter":
    "(&(objectClass=person)(sAMAccountName=%USERNAME%))",
    "serverURIs": [
      "ldaps://111.22.333.444",
      "ldap://555.66.777.888"
    ]
  },
  "id": 1
}

```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```

{
  "id": 1,
  "result": {
  }
}

```

Nuevo desde la versión

9.6

Autenticación DisableLdapAuthentication

Puede utilizar el `DisableLdapAuthentication` Método para deshabilitar la autenticación LDAP y quitar todas las opciones de configuración de LDAP. Este método no quita ninguna cuenta de administrador de clúster configurada para los usuarios o los grupos. Una vez deshabilitada la autenticación LDAP, los administradores de clúster que se configuran para usar la autenticación LDAP ya no pueden acceder al clúster.

Parámetros

Este método no tiene parámetros de entrada.

Valores devueltos

Este método no tiene valores devueltos.

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "DisableLdapAuthentication",
  "params": {},
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "id": 1,
  "result": {}
}
```

Nuevo desde la versión

9.6

GetLdapConfiguration

Puede utilizar el `GetLdapConfiguration` Método para obtener la configuración de LDAP activa actualmente en el clúster.

Parámetros

Este método no tiene parámetros de entrada.

Valor de retorno

Este método tiene el siguiente valor devuelto.

| Nombre | Descripción | Tipo |
|-------------------|--|-----------------------------------|
| LdapConfiguration | Lista de las opciones de configuración de LDAP actuales. Esta llamada API no devuelve el texto sin formato de la contraseña de la cuenta de búsqueda. Nota: Si la autenticación LDAP está deshabilitada actualmente, todas las configuraciones devueltas están vacías con la excepción de "AuthType" y "groupSearchType", que se establecen en "SearchAndBind" y "ActiveDirectory" respectivamente. | LdapConfiguration |

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

```
{
  "method": "GetLdapConfiguration",
  "params": {},
  "id": 1
}
```

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```

{
  "id": 1,
  "result": {
    "ldapConfiguration": {
      "authType": "SearchAndBind",
      "enabled": true,
      "groupSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
      "groupSearchCustomFilter": "",
      "groupSearchType": "ActiveDirectory",
      "searchBindDN": "SFReadOnly@prodtest.solidfire.net",
      "serverURIs": [
        "ldaps://111.22.333.444",
        "ldap://555.66.777.888"
      ],
      "userDNTemplate": "",
      "userSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
      "userSearchFilter":
"(&(objectClass=person)(sAMAccountName=%USERNAME%))"
    }
  }
}

```

Nuevo desde la versión

9.6

TestLdapAuthentication

Puede utilizar el `TestLdapAuthentication` Método para validar la configuración de autenticación LDAP habilitada actualmente. Si la configuración es correcta, la llamada API devuelve la pertenencia al grupo del usuario probado.

Parámetros

Este método tiene los siguientes parámetros de entrada:

| Nombre | Descripción | Tipo | Valor predeterminado | Obligatorio |
|-------------------|---|--------|----------------------|-------------|
| nombre de usuario | Nombre de usuario que se va a probar. | cadena | Ninguno | Sí |
| contraseña | La contraseña para probar el nombre de usuario. | cadena | Ninguno | Sí |

| Nombre | Descripción | Tipo | Valor predeterminado | Obligatorio |
|-------------------|---|-------------------|----------------------|-------------|
| LdapConfiguration | Objeto LdapConfiguration que se va a probar. Si se proporciona este parámetro, el sistema prueba la configuración proporcionada aunque la autenticación de LDAP esté deshabilitada actualmente. | LdapConfiguration | Ninguno | No |

Valores devueltos

Este método tiene los siguientes valores devueltos:

| Nombre | Descripción | Tipo |
|---------------|--|--------|
| grupos | Lista de grupos LDAP que incluyen al usuario probado como miembro. | cabina |
| DN de usuario | Nombre completo LDAP del usuario probado. | cadena |

Ejemplo de solicitud

Las solicitudes de este método son similares al ejemplo siguiente:

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

Ejemplo de respuesta

Este método devuelve una respuesta similar al siguiente ejemplo:

```
{
  "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"
  }
}
```

Nuevo desde la versión

9.6

Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPTIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.