Configure los servicios de nombres

ONTAP 9

NetApp
April 24, 2024

Tabla de contenidos

Configure los servicios de nombres

Cómo funciona la configuración de switch de servicio de nombres ONTAP

ONTAP almacena información de configuración del servicio de nombres en una tabla que equivale a `/etc/nsswitch.conf` Fichero de sistemas UNIX. Debe comprender la función de la tabla y cómo la utiliza ONTAP para poder configurarla de forma adecuada para su entorno.

La tabla de conmutador de servicio de nombres ONTAP determina qué orígenes de servicio de nombres consulta ONTAP para recuperar información de un determinado tipo de información del servicio de nombres. ONTAP mantiene una tabla de switch de servicio de nombres independiente para cada SVM.

Tipos de base de datos

La tabla almacena una lista de servicios de nombres independiente para cada uno de los siguientes tipos de base de datos:

Tipo de base de datos	Define orígenes de servicio de nombres para…	Los orígenes válidos son…
hosts	Conversión de nombres de host a direcciones IP	archivos, dns
grupo	Búsqueda de información de grupo de usuarios	archivos, nis, ldap
passwd	Búsqueda de información de usuario	archivos, nis, ldap
grupo de red	Buscando información de netgroup	archivos, nis, ldap
mapa de nombres	Asignando los nombres de usuario	archivos, ldap

Tipos de origen

Los orígenes especifican el nombre de origen de servicio que se utilizará para recuperar la información adecuada.

Especificar tipo de origen…	Para buscar información en…	Administrado por las familias de comandos…

archivos	Archivos de origen local	`vserver services name-service unix-user` `vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

nis	Servidores NIS externos tal como se especifica en la configuración de dominio NIS de la SVM	`vserver services name-service nis-domain`
ldap	Servidores LDAP externos tal como se especifica en la configuración del cliente LDAP de la SVM	`vserver services name-service ldap`
dns	Servidores DNS externos como se especifica en la configuración de DNS de la SVM	`vserver services name-service dns`

Aunque tenga pensado utilizar NIS o LDAP tanto para el acceso a datos como para la autenticación de administración de SVM, debería seguir incluyéndose `files` Y configure los usuarios locales como respaldo en caso de que falle la autenticación de NIS o LDAP.

Protocolos utilizados para acceder a fuentes externas

Para acceder a los servidores de fuentes externas, ONTAP utiliza los siguientes protocolos:

Fuente externa del servicio de nombres	Protocolo utilizado para acceder
NIS	UDP
DNS	UDP
LDAP	TCP

Ejemplo

En el ejemplo siguiente se muestra el nombre de configuración del switch de servicio para la SVM svm svm_1:

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                Source
Vserver         Database        Order
--------------- ------------    ---------
svm_1           hosts           files,
                                dns
svm_1           group           files
svm_1           passwd          files
svm_1           netgroup        nis,
                                files
```

Para buscar direcciones IP para hosts, ONTAP consulta primero los archivos de origen local. Si la consulta no devuelve ningún resultado, los servidores DNS se comprueban a continuación.

Para buscar información de usuarios o grupos, ONTAP sólo consulta archivos de fuentes locales. Si la consulta no devuelve ningún resultado, la búsqueda fallará.

Para buscar información de grupos de red, ONTAP consulta primero los servidores NIS externos. Si la consulta no devuelve ningún resultado, el archivo de netgroup local se activa a continuación.

No hay entradas del servicio de nombres para la asignación de nombres en la tabla de la SVM svm svm_1. Por lo tanto, ONTAP sólo consulta archivos de origen local de forma predeterminada.

Información relacionada

"Informe técnico de NetApp 4668: Guía de prácticas recomendadas de servicios de nombres"

Utilice LDAP

Descripción general de LDAP

Un servidor LDAP (protocolo ligero de acceso a directorios) le permite mantener la información de usuario de forma centralizada. Si almacena su base de datos de usuario en un servidor LDAP del entorno, puede configurar el sistema de almacenamiento para buscar información de usuario en su base de datos LDAP existente.

- Antes de configurar LDAP para ONTAP, debe verificar que la implementación del sitio cumple las prácticas recomendadas para la configuración del cliente y el servidor LDAP. En particular, deben cumplirse las siguientes condiciones:
  - El nombre de dominio del servidor LDAP debe coincidir con la entrada del cliente LDAP.
  - Los tipos hash de contraseña de usuario LDAP compatibles con el servidor LDAP deben incluir los compatibles con ONTAP:
    - CRIPTA (todos los tipos) y SHA-1 (SHA, SSHA).
    - A partir de los valores hash de ONTAP 9.8, SHA-2 (SHA-256, SSH-384, SHA-512, SSHA-256, También se admiten SSHA-384 y SSHA-512).
  - Si el servidor LDAP requiere medidas de seguridad de la sesión, debe configurarlas en el cliente LDAP.

Están disponibles las siguientes opciones de seguridad de la sesión:

  - La firma LDAP (proporciona comprobación de la integridad de los datos) y la firma y el sellado LDAP (proporciona cifrado y comprobación de la integridad de los datos).
  - INICIE TLS
  - LDAPS (LDAP sobre TLS o SSL)
- Para habilitar consultas LDAP firmadas y selladas, se deben configurar los siguientes servicios:
  - Los servidores LDAP deben ser compatibles con el mecanismo SASL GSSAPI (Kerberos).
  - Los servidores LDAP deben tener registros DNS A/AAAA, así como registros PTR configurados en el servidor DNS.
  - Los servidores Kerberos deben tener registros SRV presentes en el servidor DNS.
- Para habilitar el INICIO de TLS o LDAPS, se deben tener en cuenta los siguientes puntos.
  - Se trata de una práctica recomendada de NetApp para usar Start TLS en lugar de LDAPS.
  - Si se usa LDAPS, el servidor LDAP debe habilitar para TLS o SSL en ONTAP 9.5 y versiones posteriores. SSL no es compatible con ONTAP 9.0-9.4.
  - Ya debe configurarse un servidor de certificados en el dominio.
- Para habilitar la búsqueda de referencias LDAP (en ONTAP 9.5 y posterior), se deben cumplir las siguientes condiciones:
  - Ambos dominios deben configurarse con una de las siguientes relaciones de confianza:
    - Bidireccional
    - Unidireccional, donde la primaria confía en el dominio de referencia
    - Padre-hijo
  - El DNS debe configurarse de modo que resuelva todos los nombres de servidor a los que se hace referencia.
  - Las contraseñas de dominio deben ser las mismas para autenticar cuándo `--bind-as-cifs-server` establezca en true.

> Las siguientes configuraciones no son compatibles con la búsqueda de referencias LDAP.
>
> - Para todas las versiones de ONTAP:
> - Clientes LDAP en una SVM de administrador
> - Para ONTAP 9.8 y versiones anteriores (se admiten en la versión 9.9.1 y posteriores):
> - Firma y sellado LDAP (la `-session-security` opción)
> - Conexiones TLS cifradas (la `-use-start-tls` opción)
> - Comunicaciones por puerto LDAPS 636 (el `-use-ldaps-for-ad-ldap` opción)

- A partir de ONTAP 9.11.1, se puede utilizar "Enlace rápido LDAP para la autenticación nsswitch."
- Debe introducir un esquema de LDAP al configurar el cliente LDAP en la SVM.

  En la mayoría de los casos, uno de los esquemas ONTAP predeterminados será apropiado. Sin embargo, si el esquema LDAP del entorno difiere de éste, debe crear un nuevo esquema de cliente LDAP para ONTAP antes de crear el cliente LDAP. Consulte a su administrador LDAP sobre los requisitos de su entorno.

- No se admite el uso de LDAP para la resolución de nombres de host.

Para obtener más información, consulte "Informe técnico de NetApp 4835: Cómo configurar LDAP en ONTAP".

Conceptos de firma y sellado LDAP

A partir de ONTAP 9, puede configurar la firma y el sellado para habilitar la seguridad de la sesión LDAP en consultas a un servidor de Active Directory (AD). Debe configurar los ajustes de seguridad del servidor NFS en la máquina virtual de almacenamiento (SVM) para corresponder a los del servidor LDAP.

La firma comprueba la integridad de la carga de datos LDAP mediante una tecnología de clave secreta. El sellado cifra la carga de datos LDAP para impedir la transmisión de información confidencial en texto sin cifrar. Una opción *LDAP Security Level* indica si es necesario firmar, firmar y sellar el tráfico LDAP o no. El valor predeterminado es `none`. prueba

La firma LDAP y el sellado en el tráfico SMB se habilitan en la SVM con el `-session-security-for-ad-ldap` de la `vserver cifs security modify` comando.

Conceptos LDAPS

Debe comprender ciertos términos y conceptos sobre cómo ONTAP protege la comunicación LDAP. ONTAP puede usar START TLS o LDAPS para configurar sesiones autenticadas entre servidores LDAP integrados de Active Directory o servidores LDAP basados en UNIX.

Terminología

Existen ciertos términos que se deben entender de qué manera ONTAP utiliza LDAPS para proteger la comunicación de LDAP.

- **LDAP**

  (Protocolo ligero de acceso a directorios) Protocolo para acceder y administrar directorios de información. LDAP se utiliza como directorio de información para almacenar objetos como usuarios, grupos y netgroups. LDAP también proporciona servicios de directorio que administran estos objetos y satisfacen las solicitudes LDAP de los clientes LDAP.

- **SSL**

  (Capa de sockets seguros) Protocolo desarrollado para enviar información de forma segura a través de Internet. SSL es compatible con ONTAP 9 y posterior, pero ha sido anticuado a favor de TLS.

- **TLS**

  (Transport Layer Security) Protocolo de seguimiento de estándares IETF basado en las especificaciones anteriores de SSL. Es el sucesor de SSL. TLS es compatible con ONTAP 9,5 y versiones posteriores.

- **LDAPS (LDAP sobre SSL o TLS)**

  Protocolo que utiliza TLS o SSL para proteger la comunicación entre clientes LDAP y servidores LDAP.

Los términos *ldap sobre SSL* y *ldap sobre TLS* a veces se utilizan indistintamente. ONTAP 9,5 y versiones posteriores es compatible con LDAPS.

- En ONTAP 9.5-9.8, LDAPS solo puede habilitar LDAPS en el puerto 636. Para ello, utilice `-use -ldaps-for-ad-ldap` con el `vserver cifs security modify` comando.
- A partir de ONTAP 9.9.1, LDAPS puede habilitar LDAPS en cualquier puerto, aunque el puerto 636 sigue siendo el predeterminado. Para ello, ajuste la `-ldaps-enabled` parámetro a. `true` y especifique lo que desee `-port` parámetro. Para obtener más información, consulte `vserver services name-service ldap client create` página de manual

Se trata de una práctica recomendada de NetApp para usar Start TLS en lugar de LDAPS.

- **Iniciar TLS**

  (También conocido como *start_tls*, *STARTTLS* y *StartTLS*) un mecanismo para proporcionar una comunicación segura mediante el uso de los protocolos TLS.

  ONTAP utiliza STARTTLS para garantizar la comunicación LDAP y utiliza el puerto LDAP predeterminado (389) para comunicarse con el servidor LDAP. El servidor LDAP debe configurarse para permitir conexiones a través del puerto LDAP 389; de lo contrario, se producirá un error en las conexiones LDAP TLS desde la SVM al servidor LDAP.

Cómo utiliza ONTAP LDAPS

ONTAP admite la autenticación del servidor TLS, lo que permite que el cliente LDAP de SVM confirme la identidad del servidor LDAP durante la operación de enlace. Los clientes LDAP habilitados para TLS pueden utilizar técnicas estándar de criptografía de clave pública para comprobar que el certificado y el ID público de un servidor son válidos y que han sido emitidos por una entidad emisora de certificados (CA) que aparece en la lista de entidades emisoras de certificados de confianza del cliente.

LDAP admite STARTTLS para cifrar las comunicaciones mediante TLS. STARTTLS comienza como una conexión de texto sin formato a través del puerto LDAP estándar (389), y esa conexión se actualiza a TLS.

ONTAP admite lo siguiente:

- LDAPS para tráfico relacionado con SMB entre los servidores LDAP integrados de Active Directory y la SVM
- LDAPS para el tráfico LDAP para la asignación de nombres y otra información de UNIX

  Los servidores LDAP integrados en Active Directory o los servidores LDAP basados en UNIX se pueden utilizar para almacenar información para la asignación de nombres LDAP y otra información UNIX, como usuarios, grupos y netgroups.

- Certificados de CA raíz autofirmados

  Cuando se utiliza un LDAP integrado de Active Directory, el certificado raíz autofirmado se genera cuando el servicio de certificados de Windows Server está instalado en el dominio. Cuando se utiliza un servidor LDAP basado en UNIX para asignar nombres LDAP, se genera el certificado raíz autofirmado y se guarda mediante medios adecuados para esa aplicación LDAP.

De manera predeterminada, LDAPS.

Active la compatibilidad con LDAP RFC2307bis

Si desea utilizar LDAP y necesita la capacidad adicional para utilizar pertenencias a grupos anidados, puede configurar ONTAP para habilitar la compatibilidad con RFC2307bis LDAP.

Lo que necesitará

Debe haber creado una copia de uno de los esquemas de cliente LDAP predeterminados que desea utilizar.

Acerca de esta tarea

En los esquemas de cliente LDAP, los objetos de grupo utilizan el atributo memberUid. Este atributo puede contener varios valores y enumera los nombres de los usuarios que pertenecen a ese grupo. En los esquemas de cliente LDAP habilitados para RFC2307bis, los objetos de grupo utilizan el atributo uniqueMember. Este atributo puede contener el nombre completo (DN) de otro objeto del directorio LDAP. Esto le permite utilizar grupos anidados porque los grupos pueden tener otros grupos como miembros.

El usuario no debe ser miembro de más de 256 grupos, incluidos los grupos anidados. ONTAP ignora los grupos por encima del límite de 256 grupos.

De forma predeterminada, la compatibilidad con RFC2307bis está desactivada.

> La compatibilidad con RFC2307bis se habilita automáticamente en ONTAP cuando se crea un cliente LDAP con el esquema MS-AD-BIS.

Para obtener más información, consulte "Informe técnico de NetApp 4835: Cómo configurar LDAP en ONTAP".

Pasos

1. Configure el nivel de privilegio en Advanced:

   ```
   set -privilege advanced
   ```

2. Modifique el esquema de cliente LDAP RFC2307 copiado para habilitar la compatibilidad con RFC2307bis:

   ```
   vserver services name-service ldap client schema modify -vserver vserver_name
   -schema schema-name -enable-rfc2307bis true
   ```

3. Modifique el esquema para que coincida con la clase de objeto admitida en el servidor LDAP:

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -group-of-unique-names-object-class object_class
   ```

4. Modifique el esquema para que coincida con el nombre de atributo admitido en el servidor LDAP:

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -unique-member-attribute attribute_name
   ```

5. Vuelva al nivel de privilegio de administrador:

   ```
   set -privilege admin
   ```

Opciones de configuración para las búsquedas de directorios LDAP

Puede optimizar las búsquedas de directorios LDAP, incluida la información de usuario, grupo y grupo de red, configurando el cliente LDAP de ONTAP para que se conecte a servidores LDAP de la forma más adecuada para su entorno. Es necesario entender cuándo son suficientes los valores predeterminados de la base LDAP y de la búsqueda de ámbito y qué parámetros especificar cuando los valores personalizados son más apropiados.

Las opciones de búsqueda de clientes LDAP para información de usuarios, grupos y netgroup pueden ayudar a evitar consultas LDAP que han fallado y, por lo tanto, permitir que el cliente acceda a los sistemas de almacenamiento con errores. También ayudan a garantizar que las búsquedas sean lo más eficientes posible para evitar problemas de rendimiento de los clientes.

Valores de búsqueda base y ámbito predeterminados

La base LDAP es el DN base predeterminado que utiliza el cliente LDAP para realizar consultas LDAP. Todas las búsquedas, incluidas las búsquedas de usuario, grupo y netgroup, se realizan utilizando el DN base. Esta opción es apropiada cuando el directorio LDAP es relativamente pequeño y todas las entradas relevantes se encuentran en el mismo DN.

Si no especifica un DN base personalizado, el valor predeterminado es `root`. Esto significa que cada consulta busca en todo el directorio. A pesar de que esto maximiza las posibilidades de éxito de la consulta LDAP, puede resultar ineficiente y producir una reducción significativa del rendimiento con grandes directorios LDAP.

El ámbito de base LDAP es el ámbito de búsqueda predeterminado que utiliza el cliente LDAP para realizar consultas LDAP. Todas las búsquedas, incluidas las de usuario, grupo y netgroup, se realizan utilizando el ámbito base. Determina si la consulta LDAP busca sólo la entrada con nombre, las entradas de un nivel por debajo del DN o el subárbol entero por debajo del DN.

Si no especifica un ámbito base personalizado, el valor predeterminado es `subtree`. Esto significa que cada consulta busca todo el subárbol que se encuentra debajo del DN. A pesar de que esto maximiza las posibilidades de éxito de la consulta LDAP, puede resultar ineficiente y producir una reducción significativa del rendimiento con grandes directorios LDAP.

Valores de búsqueda de base y ámbito personalizados

Opcionalmente, puede especificar valores de base y ámbito independientes para búsquedas de usuarios, grupos y grupos de red. Limitar la base de búsqueda y el ámbito de las consultas de esta manera puede mejorar significativamente el rendimiento porque limita la búsqueda a una subsección más pequeña del directorio LDAP.

Si se especifican valores de base y ámbito personalizados, se reemplazan la base de búsqueda y el ámbito predeterminados generales para las búsquedas de usuarios, grupos y grupos de red. Los parámetros para especificar valores de base y ámbito personalizados están disponibles en el nivel de privilegio avanzado.

Parámetro de cliente LDAP…	Especifica el valor personalizado…
`-base-dn`	DN base de todas las búsquedas de LDAP se pueden introducir varios valores si es necesario (por ejemplo, si la búsqueda de referencias de LDAP está habilitada en ONTAP 9.5 y versiones posteriores).

`-base-scope`	Ámbito base para todas las búsquedas LDAP
`-user-dn`	DNS base para todas las búsquedas de usuarios LDAP.este parámetro también se aplica a las búsquedas de asignación de nombres de usuario.
`-user-scope`	Ámbito base para todas las búsquedas de usuarios LDAP este parámetro también se aplica a las búsquedas de asignación de nombres de usuario.
`-group-dn`	DNS base para todas las búsquedas de grupos LDAP
`-group-scope`	Ámbito base para todas las búsquedas de grupos LDAP
`-netgroup-dn`	DNS base para todas las búsquedas de grupos de red LDAP
`-netgroup-scope`	Alcance base para todas las búsquedas de grupos de red LDAP

Varios valores DN base personalizados

Si su estructura de directorios LDAP es más compleja, puede ser necesario especificar varios DNS base para buscar varias partes del directorio LDAP para cierta información. Puede especificar varios DNS para los parámetros de DN de usuario, grupo y grupo de red separándolos con punto y coma (;) y encerrando toda la lista de búsqueda de DN con comillas dobles ("). Si un DN contiene un punto y coma, debe agregar un carácter de escape (\) inmediatamente antes del punto y coma en el DN.

Tenga en cuenta que el ámbito se aplica a toda la lista de DNS especificada para el parámetro correspondiente. Por ejemplo, si especifica una lista de tres DNS de usuario y subárbol diferentes para el ámbito de usuario, el usuario LDAP buscará en todo el subárbol para cada uno de los tres DNS especificados.

A partir de ONTAP 9.5, también puede especificar LDAP *referenciación persiguiendo*, lo que permite al cliente LDAP de ONTAP remitir solicitudes de búsqueda a otros servidores LDAP si el servidor LDAP principal no devuelve una respuesta de referencia LDAP. El cliente utiliza esos datos de referencia para recuperar el objeto de destino del servidor descrito en los datos de referencia. Para buscar objetos presentes en los servidores LDAP a los que se hace referencia, se puede agregar la base-dn de los objetos a los que se hace referencia a base-dn como parte de la configuración del cliente LDAP. Sin embargo, los objetos a los que se hace referencia sólo se buscan cuando se activa la búsqueda de referencias (mediante la `-referral-enabled true` Opción) durante la creación o modificación de un cliente LDAP.

Mejorar el rendimiento de las búsquedas de red de directorio LDAP-por-host

Si el entorno LDAP está configurado para permitir búsquedas de netgroup-by-host, puede configurar ONTAP para aprovechar esta característica y realizar búsquedas de netgroup-by-host. Esto puede acelerar significativamente las búsquedas de netgroup y reducir posibles problemas de acceso de clientes NFS debido a la latencia durante las búsquedas de netgroup.

Lo que necesitará

Su directorio LDAP debe contener un `netgroup.byhost` mapa.

Los servidores DNS deben contener registros de búsqueda de reenvío (A) e inverso (PTR) para clientes NFS.

Al especificar direcciones IPv6 en grupos de red, siempre debe acortar y comprimir cada dirección como se especifica en RFC 5952.

Acerca de esta tarea

Los servidores NIS almacenan información sobre el grupo de red en tres mapas independientes denominados `netgroup`, `netgroup.byuser`, y. `netgroup.byhost`. El propósito de la `netgroup.byuser` y.. `netgroup.byhost` mapas es acelerar las búsquedas de netgroup. ONTAP puede realizar búsquedas de netgroup-by-host en servidores NIS para mejorar los tiempos de respuesta de montaje.

De forma predeterminada, los directorios LDAP no tienen tal `netgroup.byhost` Asignar como servidores NIS. Sin embargo, con la ayuda de herramientas de terceros es posible importar un NIS `netgroup.byhost` Asignar a directorios LDAP para permitir búsquedas rápidas de netgroup-by-host. Si ha configurado el entorno LDAP para permitir búsquedas de netgroup-by-host, puede configurar el cliente LDAP de ONTAP con el `netgroup.byhost` Asignar el nombre, el DN y el alcance de búsqueda para realizar búsquedas más rápidas de netgroup-by-host.

Al recibir los resultados de las búsquedas de netgroup-by-host con mayor rapidez, ONTAP procesa las reglas de exportación con mayor rapidez cuando los clientes NFS solicitan acceso a las exportaciones. Esto reduce la posibilidad de retrasos en el acceso debido a problemas de latencia de búsqueda en netgroup.

Pasos

1. Obtenga el nombre completo exacto del NIS `netgroup.byhost` Asignar importado a su directorio LDAP.

   El DN de mapa puede variar en función de la herramienta de terceros que haya utilizado para la importación. Para obtener el mejor rendimiento, debe especificar el DN exacto del mapa.

2. Configure el nivel de privilegio en Advanced: `set -privilege advanced`
3. Habilite las búsquedas de netgroup-by-host en la configuración de cliente LDAP de la máquina virtual de almacenamiento (SVM): `vserver services name-service ldap client modify -vserver vserver_name -client-config config_name -is-netgroup-byhost-enabled true -netgroup-byhost-dn netgroup-by-host_map_distinguished_name -netgroup-byhost -scope netgroup-by-host_search_scope`

   `-is-netgroup-byhost-enabled` {`true` `false`} Activa o desactiva la búsqueda netgroup-by-host para directorios LDAP. El valor predeterminado es `false`.

   `-netgroup-byhost-dn` `netgroup-by-host_map_distinguished_name` especifica el nombre distintivo de `netgroup.byhost` Asignar en el directorio LDAP. Reemplaza el DN base para las búsquedas de netgroup-by-host. Si no se especifica este parámetro, ONTAP utiliza el DN base.

   `-netgroup-byhost-scope` {`base`|`onelevel` `subtree`} especifica el ámbito de búsqueda para las búsquedas de netgroup-by-host. Si no se especifica este parámetro, el valor predeterminado es `subtree`.

   Si todavía no existe la configuración de cliente LDAP, puede habilitar las búsquedas de netgroup-by-host especificando estos parámetros al crear una nueva configuración de cliente LDAP mediante la `vserver services name-service ldap client create` comando.

> A partir de ONTAP 9.2, el campo `-ldap-servers` reemplaza el campo `-servers`. Este nuevo campo puede tomar un nombre de host o una dirección IP para el servidor LDAP.

4. Vuelva al nivel de privilegio de administrador: `set -privilege admin`

Ejemplo

El siguiente comando modifica la configuración de cliente LDAP existente denominada "'ldap_corp'" para permitir búsquedas de netgroup-by-host mediante el `netgroup.byhost` Mapa denominado "'nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com'" y el ámbito de búsqueda predeterminado `subtree`:

```
cluster1::*> vserver services name-service ldap client modify -vserver vs1
-client-config ldap_corp -is-netgroup-byhost-enabled true -netgroup-byhost
-dn nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

Después de terminar

La `netgroup.byhost` y.. `netgroup` los mapas del directorio deben mantenerse sincronizados en todo momento para evitar problemas de acceso de los clientes.

Información relacionada

"RFC de IETF 5952: Recomendación para la representación de texto de direcciones IPv6"

Utilice el enlace rápido LDAP para la autenticación nsswitch

A partir de ONTAP 9.11.1, puede aprovechar la funcionalidad LDAP *fast bind* (también conocida como *concurrente bind*) para obtener solicitudes de autenticación de clientes más rápidas y sencillas. Para utilizar esta funcionalidad, el servidor LDAP debe admitir la funcionalidad de enlace rápido.

Acerca de esta tarea

Sin enlace rápido, ONTAP utiliza la vinculación simple de LDAP para autenticar usuarios administradores con el servidor LDAP. Con este método de autenticación, ONTAP envía un nombre de usuario o de grupo al servidor LDAP, recibe la contraseña hash almacenada y compara el código hash del servidor con la contraseña hash generada localmente desde la contraseña de usuario. Si son idénticas, ONTAP otorga permiso de inicio de sesión.

Con la funcionalidad de enlace rápido, ONTAP sólo envía credenciales de usuario (nombre de usuario y contraseña) al servidor LDAP a través de una conexión segura. A continuación, el servidor LDAP valida estas credenciales y le indica a ONTAP que conceda permisos de inicio de sesión.

Una ventaja de enlace rápido es que no es necesario que ONTAP admita todos los nuevos algoritmos de hash compatibles con los servidores LDAP, ya que el servidor LDAP realiza hash de contraseñas.

"Aprenda sobre el uso de FAST BIND."

Puede utilizar las configuraciones de cliente LDAP existentes para enlace rápido LDAP. Sin embargo, se recomienda encarecidamente que el cliente LDAP esté configurado para TLS o LDAPS; de lo contrario, la contraseña se envía por el cable en texto sin formato.

Para habilitar el enlace rápido de LDAP en un entorno ONTAP, debe cumplir con estos requisitos:

- Los usuarios del administrador de ONTAP deben estar configurados en un servidor LDAP que admita el enlace rápido.
- La SVM de ONTAP debe configurarse para LDAP en la base de datos de switches de servicios de nombres (nsswitch).
- Las cuentas de usuario y de grupo admin de ONTAP deben configurarse para la autenticación nsswitch mediante fast bind.

Pasos

1. Confirme con el administrador LDAP que el enlace rápido LDAP es compatible con el servidor LDAP.
2. Asegúrese de que las credenciales de usuario administrador de ONTAP estén configuradas en el servidor LDAP.
3. Confirmar que el administrador o la SVM de datos están configurados correctamente para el enlace LDAP rápido.

   a. Para confirmar que el servidor de enlace rápido LDAP aparece en la configuración de cliente LDAP, introduzca:

   ```
   vserver services name-service ldap client show
   ```

   "Obtenga información acerca de la configuración del cliente LDAP."

   b. Para confirmarlo `ldap` es una de las fuentes configuradas para nsswitch `passwd` database, introduzca:

   ```
   vserver services name-service ns-switch show
   ```

   "Más información sobre la configuración de nsswitch."

4. Asegúrese de que los usuarios de administrador se autenticen con nsswitch y de que la autenticación de enlace rápido LDAP esté habilitada en sus cuentas.

   - Para los usuarios existentes, introduzca `security login modify` y verifique los siguientes ajustes de parámetros:

   ```
   -authentication-method nsswitch
   ```

   ```
   -is-ldap-fastbind true
   ```

   - Para los nuevos usuarios administradores, consulte "Habilite el acceso a cuenta de LDAP o NIS."

Mostrar estadísticas de LDAP

A partir de ONTAP 9.2, puede mostrar estadísticas de LDAP de las máquinas virtuales de almacenamiento (SVM) en un sistema de almacenamiento para supervisar el rendimiento y diagnosticar problemas.

Lo que necesitará

- Debe haber configurado un cliente LDAP en la SVM.
- Debe haber identificado los objetos LDAP desde los cuales se pueden ver datos.

Paso

1. Vea los datos de rendimiento para los objetos de contador:

   ```
   statistics show
   ```

Ejemplos

El siguiente ejemplo muestra los datos de rendimiento de un objeto `secd_external_service_op`:

```
cluster::*> statistics show -vserver vserverName -object
secd_external_service_op -instance "vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1"

Object: secd_external_service_op
Instance: vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1
Start-time: 4/13/2016 22:15:38
End-time: 4/13/2016 22:15:38
Scope: vserverName
Counter                             Value
-------------------------------- --------------------------------
instance_name                       vserverName:LDAP (NIS & Name
                                    Mapping):GetUserInfoFromName:
                                    1.1.1.1
last_modified_time                  1460610787
node_name                           nodeName
num_not_found_responses             1
num_request_failures                1
num_requests_sent                   1
num_responses_received              1
num_successful_responses            0
num_timeouts                        0
operation                           GetUserInfoFromName
process_name                        secd
request_latency                     52131us
```